SpammiltaSuojautuminen - Ei-toivottu viestintä Internetissä

Etusivu

Spämmiltä suojautuminen

Sisällys

Perinteiseltä ei-sähköiseltä puhelin- ja postisuoramarkkinoinnilta suojautumisesta kerrotaan dokumentissa EiMainoksiaKiitos.

Hyvän spämmisuodattimen ominaisuudet

Erilaiset spämmisuodattimet ovat yksi keino helpottaa spämmiongelmaa. **Hyvän spämmisuodattimen ainoa suunnittelukriteeri ei voi olla mahdollisimman vähäinen läpi päässeen spämmin määrä.** Mitä ominaisuuksia hyvältä spämmisuodattimelta voi vaatia:

- Suodatin ei estä muiden kuin spämmiviestien vastaanottamista (ei "vääriä positiivisia", ilman tätä ominaisuutta verkkojohdon irrottaminen olisi helpoin ratkaisu)
- Suodatin estää spämmiviestien vastaanottamisen (ei "vääriä negatiivisia")
- Suodatin vaikeuttaa mahdollisimman vähän tavallista viestintää (viestintä voi esimerkiksi vaikeutua kohtuuttoman paljon, jos vastaanottajalla käytössä on vahvistuspyyntöviestejä lähettävä suodatin)
- Suodatin ei aiheuta haittaa kolmansille osapuolille (Esimerkiksi monet sähköpostivirusten suodatusohjelmat lähettävät virusvaroituksen viestin lähettäjälle, vaikka suodatusohjelman tekijät tietävät, että kyseinen haittaohjelma väärentää lähettäjän sähköpostiosoitteen. Parempi vaihtoehto olisi esimerkiksi tallettaa viesti (haittaohjelma poistettuna) viestin vastaanottajan spämmikansioon.)
- Suodatin toimii luotettavasti (tästä syystä ostettu suodatuspalvelu voi olla parempi kuin itse rakennettu, jos ei halua käyttää aikaa spämmisuodattimen ylläpitoon)

- Suodatin ei vaaranna sähköpostiviestinnän luotettavuutta (luotettavuus tarkoittaa sitä, että sähköpostin lähettäjä voi olla varma siitä, että vastaanottaja *joko* saa viestin *tai* lähettäjä saa virheilmoituksen, jossa kerrotaan, että viestiä ei voitu toimittaa perille)
- Suodatin ei vaaranna viestinnän luottamuksellisuutta (suodatin ei saa esimerkiksi lähettää suodattimen ylläpitäjälle kopiota jokaisesta sähköpostiviestistä suodatussääntöjen kehittämistä varten)
- Suodattimen käyttö ei kasvata viestinnän kustannuksia (muuten kannattaisi palkata sihteeri käymään sähköpostiviestit läpi)

Täydellistä suodatinta, joka toteuttaisi kaikki edellä luetellut ehdot, ei ole olemassa. Vaikka täydellistä ratkaisua spämmin suodattamiseen ei olekaan olemassa, on spämmin suodattamiseen kuitenkin saatavana tehokkaita ja varsin hyviä vaihtoehtoja, jotka suurimmaksi osaksi täyttävät edellä luetellut ehdot.

Nyyssispämmin suodatus

Spämmiksi luokiteltuja nyyssiartikkeleja cancelloidaan automaattisesti. Jos omalla nyyssipalvelimella näkyy paljon spämmiviestejä johtuu tämä yleensä siitä, että palvelimen ylläpitäjä ei kunnioita cancelviestejä. Tällöin helpoin ratkaisu voi olla vaihtaa palveluntarjoajaa tai ottaa käyttöön toinen nyyssipalvelin (esimerkiksi News.Individual.NET).

Jotkut uutistenlukuohjelmat tukevat myös NoCeM-viestejä. Useimmissa uutistenlukuohjelmissa on mahdollista käyttää niin sanottuja kill- tai score-tiedostoja, joiden avulla voi suodattaa esimerkiksi tietyn kirjoittajan artikkeleja.

Sähköpostispämmin suodatus

Suodatuspalvelut

Nykyään useimmat Internet-palveluntarjoajat tarjoavat erilaisia spämmisuodatuspalveluja joko lisäpalveluna tai liittymän ominaisuutena, mikä on usein helppo tapa ottaa spämmisuodatus käyttöön.

Sähköisen viestinnän tietosuojalain 29 § mukaan Internet-palveluntarjoaja voi sähköpostin vastaanottajan luvalla estää ei-toivottujen sähköpostimainosten vastaanottamisen. Viestin vastaanottaja voi antaa tämän luvan esimerkiksi hyväksymällä palvelun käyttöehdot, joissa kerrotaan spämmisuodatuksesta. Palveluntarjoajan tulee kertoa asiakkailleen luvan hankkimisen yhteydessä (esim. palvelun käyttöehdoissa) miten suodatus toimii. Käyttöehtojenkin hyväksymisen jälkeenkin palveluntarjoajan tulee pitää asiakkaansa ajan tasalla niistä periaatteista, joilla roskapostia suodatetaan.

Spämmisuodatuspalvelun voi ostaa myös kolmannelta osapuolelta. Yhtenä esimerkkinä spämminsuodatuspalvelusta SpamCop tarjoaa estolistoja, spämmisuodatettuja sähköpostisoitteita ja forwardointipalvelua. SpamCopin suodatuspalvelut maksavat yhtä käyttäjää kohden 30 dollaria (noin 30 euroa) vuodessa, mikä antaa jonkinlaista kuvaa spämmisuodatuksen kustannuksista.

Estolistat

Kustannustehokas tapa meilispämmin suodattamiseen on pyytää omaa Internet-palveluntarjoajaa ottamaan käyttöön jokin RBL-tyyppinen (DNSBL) estolista. Estolistaa voi käyttää sisältöpohjaisen suodatuksen apuna, tai sitten palveluntarjoajan postipalvelin voi kieltäytyä vastaanottamaan mitään postia estolistalla olevilta postipalvelimilta. Jälkimmäisen kaltainen suodatus on yleensä halvinta toteuttaa, koska spämmiksi luokiteltuja viestejä ei tarvitse lainkaan ottaa vastaan tai tallettaa järjestelmään (esimerkiksi käyttäjien spämmikansioihin). Resursseja ei myöskään kulu viestien sisältöanalyysiin - viestien sisältöjä ei edes voisi analysoida, koska viestejä ei oteta vastaan.

Spamhausin sivuilla kuvataan tyypillinen estolistoja käyttävä monitasoinen spämmisuodatusjärjestelmä.

Estolistoja on monia ja erilaisia. Estolistoilla listataan erilaisia asioita, joillakin listoilla on esimerkiksi avoimia releitä, toisilla spämmimyönteisiä Internet-palveluntarjoajia. Estolistojan suodatusperiaatteet kerrotaan yleensä listan kotisivulla. Estolistoja löytyy kootusti Google Directorystä. Jeff Makey on vertaillut eri estolistoja.

Edustava kokoelma käyttökelpoisia estolistoja aakkosjärjestyksessä:

- Distributed Server Boycott List (DSBL)
- Open Relay Database (ORDB)
- RFC-Ignorant
- Spam and Open-Relay Blocking System (SORBS)
- SpamCop Blocking List (SCBL)
- The Spamhaus Block List (SBL)
- The Spamhaus Exploits Block List (XBL)
- Spam Prevention Early Warning System (SPEWS)

Näiden estolistojen käyttöönoton pitäisi olla teknisesti varsin yksinkertainen ja kivuton toimitus. Moderneissa postinvälitysohjelmistoissa estolistojen käyttöönotto vaatii vain pari riviä konfiguraatiotiedostoon. Myös esimerkiksi SpamAssassin voi käyttää muun muassa edellä lueteltuja estolistoja.

Ennen estolistan käyttöönottoa on hyvä miettiä seuraavia asioita:

- Millä perusteilla ja kuinka agressiivisesti haluat suodattaa spämmiä? (Kannattaa aina tutustua periaatteisiin, joiden mukaan estolista toimii ennen kyseisen listan käyttöönottoa - nämä periaatteet vaihtelevat listoittain.)
- Luotatko estolistan ylläpitäjiin?
- Haluatko suodattaa vain omaa postiasi vai ylläpidätkö muidenkin käyttämää palvelinta?
- Haluatko estää spämmiksi luokitellun postin vastaanottamisen kokonaan vai vain merkitä sen spämmiksi ja ehkä tallettaa spämmiksi luokitellut viestit erilliseen spämmikansioon?

Suodatinohjelmat

Yksi mielenkiintoinen luokka spämmisuodattimia ovat Bayesilaiset suodattimet. Nämä suodattimet toimivat siten, että aluksi käyttäjä kertoo, mitkä sähköpostiviesteistä ovat spämmiä. Suodatin oppii pian tekemään tämän erottelun itse hyvin tehokkaasti. SpamAssassin sisältää tällaisen oppivan suodattimen. Myös esimerkiksi avoimeen lähdekoodiin perustuvan Mozillan sähköpostiohjelma sisältää tehokkaan Bayesilaisen spämmisuodattimen. Mozillan sähköpostiohjelma, Thunderbird, on myös saatavana erillisenä ohjelmana. Ehkä helpoin tapa ottaa Bayesilainen spämmisuodatus käyttöön on ladata Thunderbird.

Spämmiä voi myös suodattaa itse asennettavan suodatinohjelman avulla. Google Web Directoryssä on lueteltu suodatuspalveluja ja -ohjelmistoja.

Joitakin poimintoja:

- Procmail on tehokas apuväline sähköpostin lajitteluun (suomenkielistä Procmail-materiaalia Googlesta). Esimerkiksi SpamAssassinia voi käyttää Procmailin avulla.
- SpamAssassin on kehuja kerännyt Perl-pohjainen spämmifiltteri
- Mail::Audit on Perlille kirjoitettu paketti postisuodattimien tekoon

- CRM114 - tekijänsä mukaan ihmistäkin tarkempi Bayesilainen suodatin
- Suodattimia Windowsille:
  - SAproxy - SpamAssassiniin pohjautuva spämmisuodatin Windowsille
  - POPFile - perustuu avoimeen lähdekoodiin
  - Spamihilator
  - MailWasher
  - K9

Edellä mainittujen lisäksi netistä on saatavan myös niin sanottuja haaste-vastaus-suodattimia ("challenge-response", C/R), jotka siirtävät spämmin suodattamisesta aiheutuvan vaivan viestin lähettäjän - tai sen jonka spämmeri on väärentänyt lähettäjäksi - harteille. Nämä suodattimet toimivat sillä periaatteella, että tuntemattomalta lähettäjältä tulevaa sähköpostiviestiä ei päästetä suodattimen läpi, ennen kuin viestin lähettäjä on vastannut suodattimen lähettämään vahvistuspyyntöviestiin. Tällaisten suodattimien ajatuksena on, että spämmerit eivät tällaisiin vahvistuspyyntöviesteihin viitsisi vastata, toisin kuin viestien oikeat lähettäjät. Haaste-vastaus-suodattimista voi kuitenkin olla enemmän haittaa kuin hyötyä, eikä niiden käyttöä voi suositella.

Ennen oman meilifiltterin käyttöönottoa kannattaa muistaa, että ongelmaan ei ole olemassa helppoa ja takuuvarmaa ratkaisua. Suodatin tekee aina joskus virheitä ja vaatii ylläpitoa. Myöskään pyörää ei kannata keksiä uudestaan: omakin spämmifiltteri kannattaa melkein aina rakentaa jonkun toimivan ratkaisun, kuten SpamAssassinin pohjalle.

Hyviä yhteenvetoja spämmisuodatuksesta:

- Jyväskylän yliopiston roskapostisivut
- Ei-toivotun postin torjunta Tietojenkäsittelytieteen laitoksella
- Spam-torjunta HY:ssä

Osoitteen jakaminen ja sotkeminen

Luovuta sähköpostiosoitettasi harkiten, äläkä anna sitä turhaan esimerkiksi erilaisiin webbilomakkeisiin.

Muista kuitenkin, että sähköpostiosoite on olemassa yhteydenpitoa varten. Käytä oikeaa sähköpostiosoitettasi, kun siihen on aihetta. Jos sähköpostiosoitetta käyttää, niin joutuu se valitettavasti ennen pitkää spämmereiden listoille. Osoitteen piilottelu tai sotkeminen voi toki hidastaa sen leviämistä spämmilistoille, vaikka se ei sitä estäkään; ks. "Miten voin estää sähköpostiosoitteeni joutumisen spämmerien listoille? Miten spämmerit keräävät sähköpostiosoitteita?" ryhmän sfnet.viestinta.roskapostit VUKKista.

Pitkällä tähtäimellä osoitteen piilottamisesta tai sotkemisesta voi siis olla enemmän haittaa viestinnän vaikeutumisen muodossa:

- Yksi tapa yrittää piilottaa osoite on ilmoittaa se webbisivulla kuvatiedostona, jota automaattiset lukijat eivät osaa helposti lukea. Tästä kuitenkin seuraa vaikeuksia heikkonäköisille ihmisille. Useimmat selaimet osaavat esittää tekstimuotoisen, mutta ei kuvana esitetyn, sähköpostiosoitteen suurennettuna. Kuvana ilmoitettua osoitetta ei myöskään voi klikata tai maalata, leikata ja liimata suoraan sähköpostiohjelman osoitekenttään.
- Useiden yritysten ja yhteisöjen sivuilla sanotaan, että sähköpostiosoitteet ovat muotoa `etunimi.sukunimi@yritys.example`. Tämäkin voi vaikeuttaa viestintää, jos yrityksessä on töissä useampia saman nimisiä henkilöitä (mahdollista vähänkin isommassa yrityksessä). Ongelmia tulee myös, jos ihmisten nimissä on skandinaavisia merkkejä (ääö): Kai.Puolam**a**ki@iki.fi on toimiva osoite, Kai.Puolam**ä**ki@iki.fi ei ole. Entä onko Maija-Liisa Meikäläisen osoite Maija.Meikalainen@yritys.example vai Maija-Liisa.Meikalainen@yritys.example?

- Ongelmatonta ei ole myöskään osoitteen sotkeminen erilaisilla nospam-lisäyksillä.
- Ongelmattomin ja standardien mukainen tapasotkea osoite webbisivuilla on käyttää HTML-entiteettejä. Toisin sanoen, sen sijaan että, osoite kirjoitettaisiin WWW-sivulle muotoon

  ```
  <a href="mailto:Kai.Puolamaki@iki.fi»Kai.Puolamaki@iki.fi</a>
  ```

  korvataan ainakin `@`-merkki entiteetillä `&#64;`:

  ```
  <a href="mailto:Kai.Puolamaki&#64;iki.fi»Kai.Puolamaki&#64;iki.fi</a>
  ```

  Tämä ilmeisesti hämää nykyään useita osoitteenkerääjiä, vaikka tietenkään ei ole mitään takuuta siitä, että tämä tai mikään muukaan osoitteiden sotkemistapa olisi tulevaisuudessakin tehokas. Tällä tavalla "sotkettujen" mailto-linkkien pitäisi kuitenkin toimia normaalisti standardeja noudattavissa selaimissa, eikä sivujen käyttäjän pitäisi huomata mitään erikoista.

Lisätietoja

- OikeaoppinenOsoitteenSotkeminen
- SpammereilleEiKannataVastata

[PDF, TXT]
http://kaip.iki.fi/spam/SpammiltaSuojautuminen.html
Puolusta sähköisiä oikeuksiasi. Liity EFFIn jäseneksi.
Kai Puolamäki, Kai.Puolamaki@iki.fi