TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

Sähköpostin suodatusohje

Turun ammattikorkeakoulu 13.9.2015

Sisältö

Sähköpostin suodatusohje

Johdanto

Sähköpostin käsittelysäännöissä määritellään periaatteet, joilla sähköpostia välitetään. Tässä ohjeessa täsmennetään, miten sähköpostiviestejä ammattikorkeakoulussa suodatetaan. Suodatuksen tulee aina tapahtua ohjelmallisesti eikä toimenpiteellä saa rajoittaa sananvapautta tai luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä. Tämä ohje on julkinen ja sen tulee olla julkisesti saatavilla.

Koska haittaohjelmat ja roskapostit vaarantavat tietoturvallisuutta ja voivat jopa estää viestinnän, suodatetut viestit voidaan tapauskohtaisesti jättää välittämättä, tuhota tai poistaa liite, eristää erilliselle karanteenialueelle määräajaksi, jonka jälkeen ne tuhotaan, tai välittää vastaanottajalle roskapostiksi merkittynä. Haittaohjelmat tulee aina pyrkiä poistamaan välitettävistä viesteistä. Suodatetuista viesteistä lähettäjälle tai lähettävälle postipalvelimelle ja/tai vastaanottajalle lähetettävien virheilmoitusten tulee olla RFC 2821 -standardin mukaisia. Virheilmoitukseen voidaan myös liittää käyttäjäystävällinen kuvaus virheestä silloin, kun se on mahdollista.

Suodatusmenetelmät

1 Third party open relay -esto, eli releointihyökkäysten esto ammattikorkeakoulu koneiden kautta

Ammattikorkeakoulu ei välitä ulospäin sellaisia viestejä, jotka eivät ole lähtöisin ammattikorkeakoulun osoiteavaruudesta ja joiden vastaanottajan osoite ei ole ammattikorkeakoulun sähköpostiosoite. Lisäksi ammattikorkeakoulu estää palomuurikonfiguraatiossaan SMTP-yhteydet muihin kuin pääasiallisiin postipalvelimiinsa Internetistä käsin.

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: ”550 Relaying denied”

2 Postin välitys tuntemattomista toimialueista tai koneista

Ammattikorkeakoulun postipalvelin tekee nimipalvelutarkastuksen lähettäjätoimialueen tai -koneen olemassaolon varmistamiseksi. Mikäli lähettävä toimialue tai kone ei selviä nimipalvelukyselystä, postitus estetään tilapäisesti, kunnes lähettävän koneen tai toimialueen nimipalvelutietueet ovat kunnossa.

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: ”451 Sender domain must resolve”

3 Mustat listat (Black Lists)

Ammattikorkeakoulu ei välitä postia sellaisista postikoneista, joita voidaan käyttää releointihyökkäyksiin (ks. kohta 1). Ammattikorkeakoulu saa käyttää tarkastuksessa apunaan kansainvälisiä, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja.

Käytössä olevat mustalistapalvelut:

- ORDB (Open Relay DataBase)
- Blitzed Open Proxy Monitor List
- DSBL (Distributed Server Boycott List)
- SPAMHAUS (The Spamhaus Project)
- CBL (Composite Blocking List)
- SORBS (Spam and Open-Relay Blocking System)

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: ”550 Mail from <lähettäjä> rejected as spam; see http://www.käytettävä_musta_lista.domain”

Kohdissa 3 ja 4 ammattikorkeakoulu saa käyttää tarkastuksessa apunaan kansainvälisiä, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja. Tietokantoja käytettäessä tulee varmistua niiden asianmukaisuudesta mm. tarkastamalla periaatteet, joilla osoitteita kantaan

lisätään. Tietokantoja ylläpitävän palveluntarjoajan on tarjottava helppokäyttöinen mekanismi, jolla osoitteita voi pyytää poistettavaksi kannasta. Poistopyynnöt on käsiteltävä kohtuullisen ajan kuluessa niiden tekemisestä. Tietokantoja käytettäessä tarkastus voi olla reaaliaikainen tai ammattikorkeakoulu voi ylläpitää omaa kopiotaan tietokannoista, jota kuitenkin tulee päivittää kohtuullisin väliajoin.

4 Palvelinkohtainen pääsylista

Ammattikorkeakoulu käyttää tarvittaessa haittapostin torjumiseen itse ylläpitämiään palvelinkohtaisia pääsylistoja (access list). Listan avulla voidaan sulkea tilapäisesti tai pysyvästi erillisiä toimialueita, lähettäjiä, vastaanottajia, yksittäisiä verkko-osoitteita tai kokonaisia aliverkkoja, mikäli se on välttämätöntä muun liikenteen turvaamiseksi tai yksittäisen henkilön häirinnältä suojaamiseksi.

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: ”550 Mail from <lähettäjä> rejected as spam” tai ”550 Access Denied”

5 Liikennemääriin perustuva suodatus

Liikenneanalyysisuodatuksessa voidaan esimerkiksi sähköpostipalvelimen lokeja reaaliaikaisesti tarkkailemalla huomata poikkeamat normaalissa postinkulussa. Tällaisia roskapostitukseen viittaavia poikkeamia voivat olla epätavallisen pitkät yhteysajat postipalvelimeen, poikkeuksellinen määrä viestejä samasta isännästä tai suuri määrä vastaanottajia samassa viestissä. Liikennemääriä voi kontrolloida myös proaktiivisesti esimerkiksi hidastamalla yhteysnopeuksia tai rajoittamalla yhteysaikaa. Rajoituksia tulee kuitenkin aina käyttää harkiten, jotta esimerkiksi sähköpostilistojen toiminta ei häiriytyisi.

6 Viestien koko ja liitetiedostojen määrä

Ammattikorkeakoululla on oikeus rajoittaa välittämiensä viestien kokoa ja niiden mahdollisesti sisältämien liitetiedostojen määrää. **Tiedon viestin kokoon ja liitetiedostojen määrään liittyvistä rajoituksista tulee olla julkisesti saatavilla**.

7 Haittaohjelmien poistaminen

Ammattikorkeakoulu poistaa välittämistään viesteistä haittaohjelmat mahdollisuuksiensa mukaan tai tarpeen vaatiessa tuhoaa koko haittaohjelman sisältävän viestin.

8 Liitetiedostojen tiedostotyypit

Ammattikorkeakoululla on oikeus olla vastaanottamatta/välittämättä riskialttiita, haittaohjelmien kuljetukseen tyypillisesti käytettäviä tiedostotyyppejä sisältäviä viestejä.

ESTETYT TIEDOSTOTYYPIT

Kaksipäätteiset tiedostotyypit esimerkiksi:

- tiedosto.txt.(exe|vbs|pif|scr|bat|cmd|com|dll)

Muita esimerkkejä tiedostotyypeistä:

*.ade, *.adp, *.bas, *.bat, *.chm, *.cmd, *.com, *.cpl, *.crt, *.dll, *.docm, *.exe, *.hlp, *.hta, *.inf, *.ins, *.isp, *.js, *.jse, *.lnk, *.mdb, *.mde, *.msc, *.msi, *.msp, *.mst, *.ocx, *.pcd, *.pif, *.reg, *.scr, *.sct, *.shs, *.url, *.vb, *.vbe, *.vbs, *.wsc, *.wsf, *.wsh

Ajantasainen lista tiedostotyypeistä, joita ammattikorkeakoulun postipalvelin ei vastaanota/välitä, tulee aina olla julkisesti saatavilla.

9 Viivästäminen

Ammattikorkeakoululla on oikeus tarvittaessa viivästää viestien toimittamista kohtuullisen ajan tunnistaakseen mahdolliset liikenteen mukana tulevat haittaohjelmat.

Ammattikorkeakoulu käyttää greylisting eli harmaalistaus ominaisuutta, joka torjuu viestit jo lähettäjän koneella. Postipalvelimen edustalla toimiva ohjelmisto tarkistaa ennen viestin vastaanottamista harmaalistauspalvelimen tietokannasta viestin lähettäjän sähköposti- ja ip-osoitteen sekä vastaanottajan sähköpostiosoitteen. Jos jokin näistä kolmesta on tuntematon, kieltäydytään viestin vastaanottamisesta ja pyydetään lähettävää palvelinta yrittämään hetken kuluttua uudelleen.

Oikein toimivat sähköpostipalvelimet jättävät lähtevän viestin omaan jonoon ja yrittävät uudelleen muutamien minuuttien kuluttua. Tavalliselle postipalvelimelle tämä ei aiheuta vaivaa, mutta roskapostittajille massiivisen lähetysjonon ylläpitäminen on ongelma johtuen postitusten rajallisesta ajasta.

10 Muuta

Ammattikorkeakoulun tulee palomuurikonfiguraatiossaan tai muutoin, mahdollisuuksiensa mukaan, estää sähköpostin lähettäminen muihin toimialueisiin muiden kuin virallisten postipalvelimiensa kautta.

Ammattikorkeakoulun tulee huolehtia siitä, että sähköpostitoimialueen ylläpitoon liittyvät sähköpostiosoitteet ovat olemassa ja että ne ohjautuvat oikealle taholle. Tällaisia osoitteita ovat mm. postmaster (at) turkuamk.fi ja abuse (at) turkuamk.fi.

Tiedon ammattikorkeakoulun käyttämistä suodatusmenetelmistä tulee aina olla julkisesti saatavilla.

Lisätietoa saa osoitteesta postmaster (at) turkuamk.fi