

Tietohallinto
Tietoturva, ohje
24.1.2017
Julkinen

Sähköpostin suodatusohje

Ver- sio	pvm	Muutokset	Henkilö
1.0	13.05.2016	Dokumentti luotu	Esa Mätäsaho
1.0	4.1.2017	Dokumentti lokalisoitu REDU:lle	Marko Keisu
1.0	19.01.2017	Dokumentti käsitelty REDU johtoryhmässä	
1.0	19.01.2017	Dokumentti käsitelty yt-toimikunnassa	
1.0	24.01.2017	Vahvistettu kehitysjohtajan päätöksellä	Veli-Pekka Laukkanen

<i>Sähköpostin suodatusohje</i>	<i>1</i>
<i>1 Yleistä</i>	<i>1</i>
<i>2 SUODATUSMENETELMÄT</i>	<i>1</i>
2.1 Third party open relay -esto, eli releointihyökkäysten esto Rovaniemen koulutuskuntayhtymän koneiden kautta.....	1
2.2 Postin välitys tuntemattomista toimialueista tai koneista	1
2.3 Mustat listat (Black Lists)	1
2.4 Postin välitys sellaisista postikoneista, joiden kautta tunnetusti lähetetään roskapostia.....	2
2.5 Postin välitys sellaisista koneista, joilla on dynaamisesti varattu verkko-osoite	2
2.6 Palvelinkohtainen pääsyylista	2
2.7 Liikennemääriin perustuva suodatus.....	2
2.8 Viestien koko ja liitetiedostojen määrä	2
2.9 Haittaohjelmien poistaminen	2
2.10 Liitetiedostojen tiedostotyytit	3
<i>3 Sähköpostin sisältöön perustuva suodatus</i>	<i>3</i>
<i>4 Viivästäminen</i>	<i>3</i>
<i>5 Muuta</i>	<i>3</i>

1 YLEISTÄ

Sähköpostin käsittelysäännöissä määritellään periaatteet, joilla sähköpostia välitetään. Tässä ohjeessa täsmennetään, miten sähköpostiviestejä Rovaniemen koulutuskuntayhtymässä suodatetaan. Suodatuksen tulee aina tapahtua ohjelmallisesti ja viestintäsalaisuuden säilyttäen.

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 määrääjäksi, 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 käyttäjystävällinen kuvaus virheestä silloin, kun se on mahdollista.

2 SUODATUSMENETELMÄT

2.1 THIRD PARTY OPEN RELAY -ESTO, ELI RELEOINTIHYÖKKÄYSTEN ESTO ROVANIEMEN KOULUTUSKUNTAYHTYMÄN KONEIDEN KAUTTA

Rovaniemen koulutuskuntayhtymä ei välitä sellaisia viestejä, jotka eivät ole lähtöisin Rovaniemen koulutuskuntayhtymän osoitevaruudesta tai joiden vastaanottajan osoite ei ole Rovaniemen koulutuskuntayhtymän sähköpostiosoite. Lisäksi Rovaniemen koulutuskuntayhtymä estää palomuurikonfiguraatioissaan SMTP-yhteydet muihin kuin pääasiallisiin postipalvelimiinsa internetistä käsin.

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: "550 Relaying denied"

2.2 POSTIN VÄLITYS TUNTEMATTOMISTA TOIMIALUEISTA TAI KONEISTA

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

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

2.3 MUSTAT LISTAT (BLACK LISTS)

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

Esimerkkejä:

DSBL (Distributed Sender Blackhole List)
NJABL (Not Just Another Bogus List)
SCBL (SpamCop Blocking List)
SPAMHAUS (The Spamhaus Project)

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta:
"550 Rejected. <käytettävä mustalista>-listed host - see http://www.käytettävä_musta_lista.domain"

2.4 POSTIN VÄLITYS SELLAISISTA POSTIKONEISTA, JOIDEN KAUTTA TUNNETUSTI LÄHETETÄÄN ROSKAPOSTIA

Rovaniemen koulutuskuntayhtymä ei välitä postia sellaisista koneista, joiden kautta tunnetusti lähetetään roskapostia tai joita ylläpitävä organisaatio tunnetusti tukee roskapostittajia. Tähän organisaatio saa käyttää apunaan kansainvälisten, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja. Esimerkiksi NJABL-tietokantaa (Not Just Another Bogus List).

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta:
"550 Rejected. NJABL-listed host – see <http://njabl.org/cgi-bin/lookup.cgi?<lähde ip-osoite>>"

2.5 POSTIN VÄLITYS SELLAISISTA KONEISTA, JOILLA ON DYNAAMISESTI VARATTU VERKKO-OSOITE

Rovaniemen koulutuskuntayhtymällä on oikeus olla välittämättä postia sellaisista koneista, joiden verkko-osoite kuuluu dynaamisesti varattaviin osoiteavaruuksiin. Rovaniemen koulutuskuntayhtymä saa käyttää tarkastuksessa apunaan kansainvälisiä, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja, esimerkiksi NJABL Dynablock.

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta:
"550 Rejected. NJABL-listed host – see <http://njabl.org/cgi-bin/lookup.cgi?<lähde ip-osoite>>"

Kohdissa 3, 4 ja 5 Rovaniemen koulutuskuntayhtymä 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 Rovaniemen koulutuskuntayhtymä voi ylläpitää omaa kopiotaan tietokannoista, jota kuitenkin tulee päivittää kohtuullisin väliajoin.

2.6 PALVELINKOHTAINEN PÄÄSYLISTA

Rovaniemen koulutuskuntayhtymä käyttää tarvittaessa haittapostin torjumiseen itse ylläpitämiään palvelinkohtaisia pääsyylistoja (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 rejected as spam" tai "550 Access Denied"

2.7 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.

2.8 VIESTIEN KOKO JA LIITETIEDOSTOJEN MÄÄRÄ

Rovaniemen koulutuskuntayhtymällä on oikeus rajoittaa välittämiensä viestien kokoa ja niiden mahdollisesti sisältämien liitetiedostojen määrää. Tiedon viestin kokoon ja liitetiedostojen määrään liittyvistä rajoituksista saa lisätietoa Rovaniemen koulutuskuntayhtymän [www-sivuilla](http://www.sivuilla) tai palvelupisteestä..

2.9 HAITTAOHJELMIEN POISTAMINEN

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

2.10 LIITETIEDOSTOJEN TIEDOSTOTYYPIT

Rovaniemen koulutuskuntayhtymällä on oikeus olla vastaanottamatta / välittämättä riskialttiita, haittaohjelmien kuljetukseen tyypillisesti käytettäviä tiedostotyyppisiä sisältäviä viestejä. Esimerkkejä tiedostotyypeistä.

eg, chm, cnf, hta, ins, jse, lnk, mad, maf, mag, mam, maq, mar, mas, mat, mav, maw, pif, scf, sct, shb, shs, vbs, vbe, wsc, wsf, wsh, xnk, com, exe, scr, bat, cmd, cpl, mhtml

Välittämättä jätettävät tiedostot voidaan eristää määräajaksi karanteenialueelle, jolloin ne saatetaan vastaanottajan tai lähettäjän tietoon ennen niiden tuhoamista. Tällöin tiedosto voidaan toimittaa vastaanottajalle tämän sitä pyytäessä, edellyttäen että tiedosto ei sisällä esim. haitalliseksi katsottua koodia.

3 SÄHKÖPOSTIN SISÄLTÖÖN PERUSTUVA SUODATUS

Rovaniemen koulutuskuntayhtymä voi suodattaa roskapostia ohjelmallisesti sisällölliseen automaattiseen analyysiin perustuen, esimerkiksi pisteytykseen perustuvilla suodatusohjelmilla (esim. Spam Assassin, IMF).

Sisällöllisessä analyysissä roskapostiksi luokiteltu viesti tulee aina merkitä roskapostiksi ja toimittaa vastaanottajan sähköpostilaatikkoon, suodattaa erilliselle karanteenialueelle, josta se on vastaanottajan luettavissa, tai muutoin saattaa vastaanottajan tietoon kohtuullisen ajan kuluessa viestin vastaanottamisesta.

4 VIIVÄSTÄMINEN

Rovaniemen koulutuskuntayhtymällä on oikeus tarvittaessa viivästyttää viestien toimittamista kohtuullisen ajan tunnistaakseen mahdolliset liikenteen mukana tulevat haittaohjelmat.

5 MUUTA

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

Postin suodatusta on mahdollista tehdä sähköpostiohjelmaan asennettavassa lisäohjelmassa, keskitetyssä suodatuspalvelimessa tai yhdyskäytävässä. Suodatusohjeen kohdat 1–8 suositellaan tehtäväksi jo sähköpostiyhdyskäytävässä, kohta 9 keskitetyssä suodatuspalvelimessa ja käyttäjän työasemalla, kohta 10 keskitetyssä suodatuspalvelimessa sekä kohta 11 keskitetyssä suodatuspalvelimessa ja / tai käyttäjän työasemalla.

Rovaniemen koulutuskuntayhtymän huolehtii siitä, että sähköpostitoimialueen ylläpitoon liittyvät sähköpostiosoitteet ovat olemassa ja että ne ohjautuvat oikealle taholle. Tällaisia osoitteita ovat mm. postmaster@redu.fi ja abuse@redu.fi.

Lisätietoa saa ICT-palvelupisteestä osoitteesta servicedesk@luc.fi.