

**MÄÄRÄYKSEN 11 PERUSTELUT JA SOVEL-
TAMINEN**

**SÄHKÖPOSTIPALVELUJEN TIETOTURVAS-
TA JA TOIMIVUUDESTA**

Sisällys

1	LAINSÄÄDÄNTÖ.....	2
1.1	MÄÄRÄYKSEN LAINSÄÄDÄNTÖPERUSTA.....	2
1.2	MUUT ASIAAN LIITTYVÄT SÄÄNNÖKSET.....	2
2	MÄÄRÄYKSEN TARKOITUS JA MUUTOSHISTORIA	3
2.1	MÄÄRÄYKSEN TARKOITUS	3
2.2	KESKEISET MUUTOKSET JA MUUTOSHISTORIA.....	3
3	PYKÄLÄKOHTAISET PERUSTELUT JA SOVELTAMISOHJEET	4
3.1	1 § SOVELTAMISALA	4
3.2	2 § MÄÄRITELMÄT	4
3.2.1	<i>Sähköpostipalvelu.....</i>	4
3.2.2	<i>Sähköpostin välityspalvelu.....</i>	5
3.2.3	<i>Toissijainen sähköpostin välityspalvelu.....</i>	5
3.2.4	<i>Avoin sähköpostipalvelin.....</i>	6
3.2.5	<i>Haitallinen sähköpostiliikenne</i>	6
3.2.6	<i>Suodattaminen</i>	6
3.3	3 § AVOIMET SÄHKÖPOSTIN VÄLITYSPALVELIMET	6
3.4	4 § SAAPUVAN SÄHKÖPOSTILIIKENTEEEN KÄSITTELY	7
3.4.1	<i>Haitallisen sähköpostiliikenteen tunnistaminen</i>	7
3.4.2	<i>Sähköpostiliikenteen suodatus ja merkitseminen.....</i>	10
3.4.3	<i>Saapuvan sähköpostiliikenteen suodatusperiaatteista tiedottaminen.....</i>	11
3.5	5 § LÄHTEVÄN SÄHKÖPOSTILIIKENTEEEN KÄSITTELY	12
3.6	6 § ASIAKKAAN JA SÄHKÖPOSTIPALVELIMEN VÄLINEN YHTEYS.....	13
3.7	7 § SÄHKÖPOSTIPALVELUJEN TOIMIVUUDEN JA LAADUN SEURANTA.....	14
3.8	8 § SÄHKÖPOSTIOSOITTEIDEN HALLINTA	15
3.8.1	<i>Sähköpostiosoitteiden hallinnan kuvaus asiakkaille.....</i>	15
3.8.2	<i>Asiakkaalta vapautuneen sähköpostiosoitteen uudelleen käyttö.....</i>	15
3.8.3	<i>Harhauttavien sähköpostiosoitteiden ongelmatilanteiden hallinta</i>	16
3.9	9 § SÄHKÖPOSTIPALVELUNTARJOAJAN YHTEYSTIEDOT.....	16
3.10	10 § VOIMAANTULO JA SIIRTYMÄSÄÄNNÖKSET	16
4	MUUT SUOSITUKSET.....	17
4.1.1	<i>Palvelinten välisten yhteyksien suojaaminen.....</i>	17
5	VIITELUETTELO.....	17
6	LYHENNELUETTELO	18

1 LAINSÄÄDÄNTÖ

Tämän luvun tarkoituksena on antaa määräyksen käyttäjälle kokonaiskuva siitä, mihin säädöksiin määräys perustuu. Lisäksi luvussa listataan aihepiiriin liittyvä muu oleellinen säädäntö.

1.1 Määräyksen lainsäädäntöperusta

Viestintäviraston määräys perustuu viestintämarkkinalain (VML) [1] 128 ja 129 §:iin sekä sähköisen viestinnän tietosuojalain (SVTsL) [2] 19 ja 20 §:iin. VML tuli voimaan 25.7.2003 ja sillä pantiin osaltaan täytäntöön EY:n helmikuussa 2002 hyväksymät sähköisen viestinnän puite- [3], valtuutus- [4], käyttöoikeus- [5] ja yleispalveludirektiivit [6]. SVTsL tuli voimaan 1.9.2004 ja sillä pantiin osaltaan täytäntöön EY:n heinäkuussa 2002 hyväksymä sähköisen viestinnän tietosuojadirektiivi [7].

Viestintävirasto voi SVTsL:n 19 §:n 4 momentin nojalla antaa teleyritykselle tarkempia määräyksiä pykälän 1 - 3 momenteissa tarkoitettusta palvelun tietoturvasta. Pykälän 1 momentin mukaan teleyrityksen on huolehdittava palvelujensa tietoturvasta. Pykälän 2 momentin mukaan velvollisuus huolehtia tietoturvasta koskee myös laissa määritellyt tunnistamistietojen säilyttämisvelvollisuuden toteuttamiseksi tarvittavaa tietojen käsittelyä. Pykälän 3 momentin mukaan teleyritys vastaa tilaajille ja käyttäjille 1 ja 2 momentissa tarkoitettusta tietoturvasta myös sellaisen kolmannen osapuolen osalta, joka kokonaan tai osittain toteuttaa verkkopalvelun, viestintäpalvelun, tietojen säilyttämisen tai lisäarvopalvelun.

Viestintävirasto voi SVTsL:n 20 §:n nojalla antaa teleyritykselle tarkempia määräyksiä pykälässä tarkoitettusta palvelun tietoturvaloukkausten teknisestä torjumisesta ja tietoturvaan kohdistuvien häiriöiden poistamisesta. Pykälän mukaan teleyrityksen ja lisäarvopalvelun tarjoajan on oikeus ryhtyä välittömiin toimiin 19 §:ssä tarkoitettun tietoturvan varmistamiseksi.

Määräys liittyy VML:n 128 §:n 1, 4, 5, 7 ja 12 kohdissa säädettyihin vaatimuksiin, joiden mukaan yleiset viestintäverkot ja viestintäpalvelut sekä niihin liitettävät viestintäverkot ja viestintäpalvelut on suunniteltava, rakennettava ja ylläpidettävä siten, että:

- 1) televiestintä on tekniseltä laadultaan hyvää;
- 4) käyttäjien tai muiden henkilöiden tietosuoja, tietoturva tai muut oikeudet eivät vaarannu;
- 5) käyttäjien tai muiden henkilöiden terveydelle tai omaisuudelle ei aiheudu vaaraa;
- 7) ne toimivat yhdessä ja ne voidaan tarvittaessa liittää toiseen viestintäverkkoon;
- 12) teleyritys kykenee muutoinkin täyttämään sille kuuluvat tai tämän lain nojalla asetetut velvollisuudet.

Tässä määräyksessä tarkennetaan edellä mainittuja 128 §:n teknisiä vaatimuksia lain 129 §:n 2, 3, 4, 5, 10,15,16, 20 ja 21 kohtien nojalla, joiden mukaan viestintäviraston määräykset voivat koskea

- 2) viestintäverkon rakennetta;
- 3) viestintäverkon ja viestintäpalvelun suorituskykyä;
- 4) yhteenliittämistä, yhteentoimivuutta ja merkinantoa;
- 5) viestintäverkon liityntäpisteen teknisiä ominaisuuksia
- 10) viestintäverkon turvallisuutta ja häiriöttömyyttä;
- 15) käyttäjille tarjottavia palveluita;
- 16) suorituskyvyn ylläpitoa ja seurantaa sekä verkonhallintaa;
- 20) noudatettavia standardeja
- 21) muita näihin verrattavia viestintäverkolle tai viestintäpalvelulle asetettavia teknisiä vaatimuksia.

1.2 Muut asiaan liittyvät säännökset

Tässä kappaleessa kuvataan Viestintäviraston antamat tämän määräyksen aihepiiriin liittyvät muut määräykset. Kappaleen tarkoituksena on antaa määräyksen käyttäjälle parempi mahdollisuus viestintäverkkoja ja -palveluita koskevien velvoitteiden kokonais kuvan hahmottamiseen.

Määräys 9 tietoturvaloukkausten sekä vika- ja häiriötilanteiden ilmoittamisvelvollisuudesta yleisessä teletoiminnassa [8]. Määräystä sovelletaan teleyritysten yleiseen teletoimintaan ja siinä käytettäviin

telelaitteisiin. Määräystä sovelletaan myös viranomaisverkoissa tapahtuvaan teletoimintaan ja niissä käytettäviin laitteisiin.

Määräys 13 internet-yhteyspalvelujen tietoturvasta ja toimivuudesta [9]. Määräystä sovelletaan yleisissä viestintäverkoissa tarjottavien Internet-yhteyspalvelujen tuottamiseen sekä teleyrityksen näihin toimintoihin käyttämiin järjestelmiin, viestintäverkkoihin ja viestintäpalveluihin. Internet-yhteyspalvelulla tarkoitetaan määräyksessä Internet-liikenteen välittämistä. Määräystä sovelletaan Internet-yhteyspalvelujen tuottamisessa soveltuvin osin myös sekä verkkoyrityksissä että palveluyrityksissä.

Määräys 47 teleyritysten tietoturvasta [10]. Määräystä sovelletaan teleyritysten yleisten viestintäpalvelujen toteuttamiseen liittyvään toimintaan sekä teleyritysten yleiseen teletoimintaan käyttämiin järjestelmiin, viestintäverkkoihin ja -palveluihin ja siinä määrätään lähinnä tietoturvallisuuden liittyvien asioiden hoidosta teleyrityksessä.

Määräys 53 tunnistamistietojen tallentamisvelvollisuudesta [11]. Määräyksessä säädetään tietyille teleyrityksille velvollisuus tallentaa tunnistamistietoja. Määräyksellä ei aseteta teleyrityksille velvoitetta tallentaa mitään uutta tietoa, vaan tarkoituksena on ollut ainoastaan pidentää teleyrityksen jo nykyisellään omaa käyttöään varten tallentamien tietojen säilytysaikaa.

Määräys 54 Viestintäverkkojen ja -palvelujen varmistamisesta [12]. Määräyksen tarkoituksena on viestintäverkkojen ja -palvelujen toimintavarmuuden, tietosuojaan ja tietoturvan takaaminen normaalioloissa, normaaliolojen häiriötilanteissa ja poikkeusoloissa. Tästä syystä määräys asettaa teleyrityksille minimivelvoitteet muun muassa viestintäverkkojen ja -palvelujen toteutuksessa käytettyjen laitteiden tehonsyötön varmistukselle, laitteiden fyysiselle suojaamiselle sekä laitteiden ja yhteyksien varmistamiselle.

Esitetty lista vastaa tämän dokumentin julkaisuhetken tilannetta. Kaikki Viestintäviraston määräykset on julkaistu Viestintäviraston Internet-sivuilla osoitteessa www.ficora.fi.

2 MÄÄRÄYKSEN TARKOITUS JA MUUTOSHISTORIA

Tämän luvun tarkoituksena on antaa määräyksen käyttäjälle tieto määräyksen tavoitteista ja tarkoituksesta. Luvussa käsitellään myös merkittävimmät muutokset määräystä edeltäneisiin velvoitteisiin ja suosituksiin.

2.1 Määräyksen tarkoitus

Määräyksen tarkoituksena on asettaa sähköpostipalveluntarjoajille minimivelvoitteet viestintäpalvelun tietoturvan ja toimivuuden varmistamiseksi.

Määräyksen tavoitteena on varmistaa kuluttajien käyttämän sähköpostipalvelun toiminta. Kuluttajille viestintäpalvelun tietoturvan ja toimivuuden arviointi on vaikeaa. Koska kuluttajilla ei ole juurikaan mahdollisuutta vaikuttaa viestintäpalveluiden toimintavarmuuteen, on toimintavarmuudesta huolehdittava määräysteitse asettamalla sähköpostipalveluntarjoajille minimivelvoitteet sähköpostipalvelun olennaisille teknisille ominaisuuksille.

Sähköpostipalvelun merkitys myös koko yhteiskunnan toiminnan kannalta on kasvanut. Tästä johdun määräyksessä on asetettu palveluntarjoajien velvoitteet sähköpostiliikenteen käsittelystä, sähköpostipalvelimien ja -osoitteiden hallinnoinnista ja palvelun laadun seurannasta.

2.2 Keskeiset muutokset ja muutoshistoria

Määräyksessä on edelliseen määräysversioon nähden eriytetty sähköpostipalveluntarjoajan ja Internet-yhteyspalveluntarjoajan roolit ja tehtäväalueet sähköpostipalvelun osalta. Tässä määräyksessä keskitytään sähköpostipalveluntarjoajaa koskeviin velvollisuuksiin ja tehtäviin. Internet-yhteyspalveluita tai -liittymiä tarjoavia palveluntarjoajia koskevat vaatimukset ja suositukset on siirretty määräyksen 13: määräys Internet-yhteyspalvelujen tietoturvasta ja toimivuudesta.

Määräyksen pykälärakennetta on uudistettu edellisestä määräyksestä. Edellisen määräyksen 5 §:n (kuluttajaliittymään saapuvan liikenteen reititys), 6 §:n (kuluttajaliittymästä lähtevän liikenteen

reititys) ja 7 §:n (haittaohjelmaliikenteen havaitseminen ja suodattaminen) sähköpostipalveluntarjoajia koskevat vaatimukset on tässä määräyksessä koottu kahden pykälän (4 § saapuvan sähköpostiliikenteen käsittely ja 5 § lähtevän sähköpostiliikenteen käsittely) alle. Muutoksen tarkoituksena on selkiyttää määräyksen sisältöä ja asiakokonaisuuksia.

Määräyksen 6 §:ssä sähköpostipalveluntarjoajille on annettu uusi velvoite suojattujen yhteyksien tarjoamiseen ensisijaisena yhteytenä asiakkaan ja sähköpostilaatikon sekä asiakkaan ja sähköpostin lähetyspalvelimen välillä.

Toisena uutena aihealueena määräyksessä on 8 §:n mukainen sähköpostiosoitteiden hallinta. Pykälän tarkoituksena on yhtenäistää palveluntarjoajien erilaisia käytäntöjä hallita sähköpostiosoitteita sekä velvoittaa palveluntarjoajia tarjoamaan kuluttajille tietoa sähköpostiosoitteiden hallintaperiaatteistaan. Sähköpostipalvelun käytettävyydestä huolehtimisen veloitteet on sijoitettu muiden pykälien ja uudistettavana olevan verkonhallintamääräyksen alle.

3 PYKÄLÄKOHTAISET PERUSTELUT JA SOVELTAMISOHJEET

Tässä luvussa käydään läpi pykäläkohtaisesti pykälän perustelut sekä sen soveltamissuosituksukset.

3.1 1 § Soveltamisala

Määräyksen soveltamisalana on yleisissä viestintäverkoissa tarjottavien sähköpostiviestin lähettäm-, välittäm- tai vastaanottopalveluiden tarjoaminen kuluttaja- ja yritysasiakkaille, sekä näihin toimintoihin käytetyt järjestelmät. Määräystä sovelletaan sähköpostipalveluiden tarjontaan riippumatta siitä, missä muodossa toimintaa harjoitetaan. Siten määräys soveltuu myös esimerkiksi julkisyhteisön tai yhdistyksen kaikille halukkaille palvelun käyttäjille tarjoamaan palveluun. Määräystä ei kuitenkaan sovelleta rajatulle käyttäjäpiirille tarjottuihin sähköpostipalveluihin kuten yrityksen tai kunnan työntekijöilleen tarjoamaan sähköpostipalveluun.

Määräystä sovelletaan myös välityspalveluiksi luettaviin viestien uudelleenohjauspalveluihin. Tällaisiin palveluihin ei kuitenkaan sovelleta tämän määräyksen pykälä 5 ja 6.

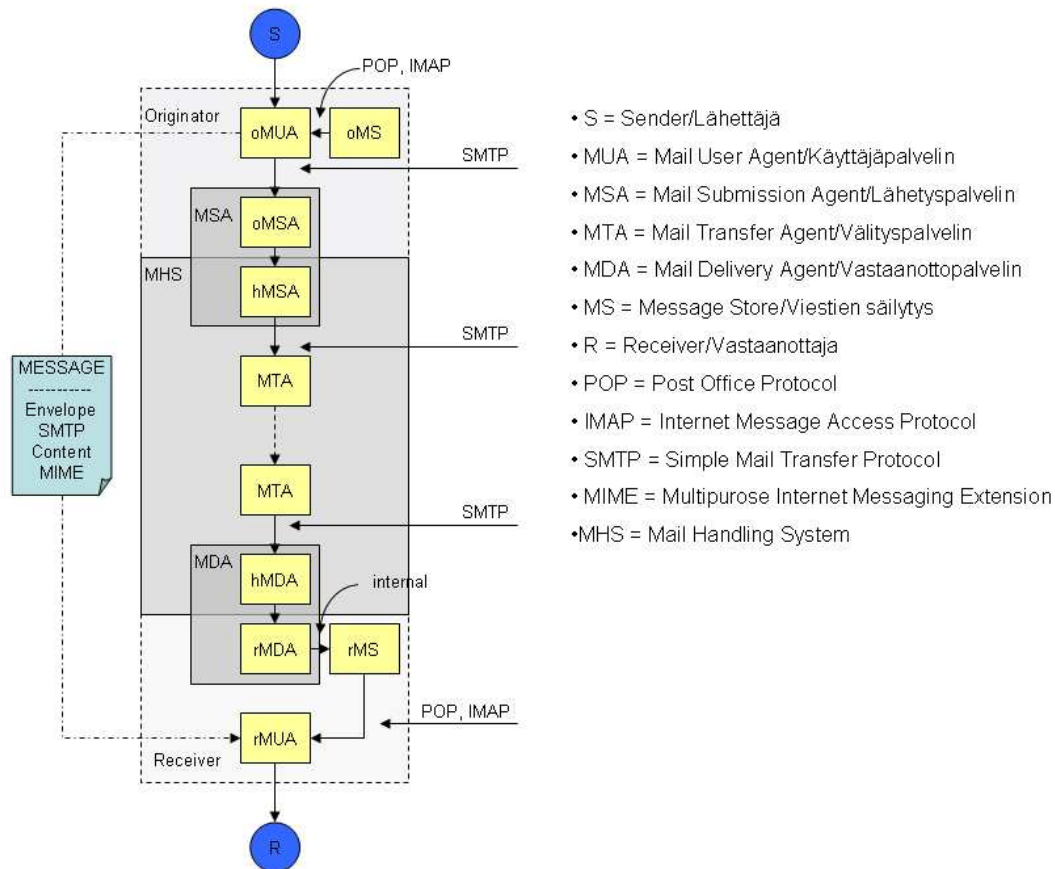
Sähköpostipalvelu ja sähköpostin välityspalvelu on määritelty tarkemmin kappaleessa 3.2. Määritelmät (kappaleet 3.2.1, 3.2.2 ja 3.2.3).

3.2 2 § Määritelmät

Tässä kappaleessa kuvataan määräyksessä käytetyt määritelmät.

3.2.1 Sähköpostipalvelu

Sähköpostipalvelulla tarkoitetaan tässä määräyksessä sähköpostiviestien lähettäm-, välittäm- tai vastaanottopalvelua. Sähköpostipalvelun periaatekuva, eri toiminnot ja toimintojen välillä käytettäviä protokollia on esitetty kuvassa 1. Sähköpostin lähettämispalvelulla tarkoitetaan palvelua, jossa asiakas lähettää viestin palveluntarjoajan lähetyspalvelimen (MSA) kautta. Välittämispalvelulla tarkoitetaan palvelua, jossa sähköpostiviesti vastaanotetaan, (käsitellään) ja lähetetään edelleen asiakkaan kanssa sovittuun kohteeseen. Vastaanottopalvelulla tarkoitetaan palvelua, jossa asiakkaan sähköpostiviestit vastaanotetaan vastaanottopalvelimelle (MDA) ja toimitetaan asiakkaan sähköpostilaatikkoon.



Kuva 1: Sähköpostipalvelun periaatekuva

Lähtevällä sähköpostiliikenteellä tarkoitetaan tässä määräyksessä sähköpostipalveluntarjoajan asiakkailta lähteviä sähköpostiviestejä, jotka välitetään palveluntarjoajan lähetyspalvelimien (MSA) kautta sähköpostin välityspalvelimille (MTA).

Saapuvalla sähköpostiliikenteellä tarkoitetaan tässä määräyksessä sähköpostipalveluntarjoajan asiakkaille saapuvia sähköpostiviestejä, jotka välitetään palveluntarjoajan vastaanottopalvelimien (MDA) kautta asiakkaiden sähköpostilaatikoihin (MS).

Sähköpostin toimivuudella tarkoitetaan palvelun tasoa, jolla asiallisten sähköpostiviestien lähetyks, välitys ja vastaanotto toimii ilman merkittäviä viiveitä tai käyttökatkoksia ja asialliset sähköpostiviestit toimitetaan vastaanottajille.

Sähköpostipalvelun käytettävyydellä tarkoitetaan sähköpostipalvelun käyttäjien kokemaa palvelun laatua ja toimivuutta. Palvelun käytettävyyteen voivat vaikuttaa esimerkiksi palvelun häiriötilanteet ja haitallisten sähköpostiviestien määrä.

3.2.2 Sähköpostin välityspalvelu

Sähköpostiviestien välityspalvelulla tarkoitetaan tässä määräyksessä sähköpostipalveluntarjoajan tarjoamaa palvelua, jossa se välittää tai uudelleenohjaa viestejä ominen sähköpostipalvelimiensa kautta.

3.2.3 Toissijainen sähköpostin välityspalvelu

Toissijaisella sähköpostin välityspalvelimella tarkoitetaan tässä määräyksessä asiakkaan omaa sähköpostipalvelua varmistavaa sähköpostin välityspalvelinta. Palvelussa asiakkaan ensisijaiseksi mx-tietueeksi tai -tietueiksi on määritelty asiakkaan oma sähköpostipalvelin tai palvelimet. Tällöin asiakkaalle saapuvaa sähköpostiliikennettä välitetään sähköpostipalveluntarjoajan toissijaisten

sähköpostin välityspalvelinten kautta vain niissä tilanteissa kun asiakkaan omat palvelimet eivät ole saavutettavissa.

3.2.4 Avoin sähköpostipalvelin

Avoimella sähköpostipalvelimella tarkoitetaan tässä määräyksessä sellaista viestien välitysjärjestelmää, jota kolmas osapuoli voi oikeudettomasti käyttää sähköpostiviestien välittämiseen. Välitysjärjestelmällä tarkoitetaan määräyksessä esimerkiksi sähköpostipalvelinta, www-välityspalvelinta tai www-palvelimelle asennettavia ohjelmistoja joita käytetään sähköpostiviestien välittämiseen.

3.2.5 Haitallinen sähköpostiliikenne

Haitallisella sähköpostiliikenteellä tarkoitetaan tässä määräyksessä sellaista sähköpostiliikennettä, joka saattaa aiheuttaa vaaraa viestintäverkon tai -palvelun tietoturvalle. Palvelun tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla (Toimivuus), ettei tietoja voida muuttaa muun kuin siihen oikeutetun toimesta (Luottamuksellisuus) ja että tiedot ja tietojärjestelmät ovat niihin oikeutettujen hyödynnettävissä (Käytettävyyys). Haitalliseksi sähköpostiliikenteeksi määritellään tässä määräyksessä myös sellainen sähköpostiliikenne, joka aiheuttaa haittaa vastaanottajan päätelaitteiden tietoturvalle. Tällaisen liikenteen katsominen haitalliseksi on välttämätöntä, koska viestinnän osapuolten päätelaitteisiin kohdistuvat tietoturvauhat vaarantavat välillisesti myös teleyrityksen tarjoaman viestintäpalvelun tietoturvan.

Sähköpostiliikenteen haitallisuutta on tarkasteltava sekä sähköpostipalveluntarjoajan että asiakkaan näkökulmista. Käytännössä tällä tarkoitetaan sitä, että viestintäpalvelun käytettävyyttä voi edellyttää toimia sekä sähköpostipalveluntarjoajan tarjoaman palvelun välityskyvystä huolehtimiseksi että myös käyttäjälle välitettävän palvelutason ylläpitämiseksi. Teoriassa valtaosa sähköpostipalveluun kohdistuvista tietoturvauhista voitaisiin ratkaista kasvattamalla sähköpostipalvelun käytettävissä olevaa välityskapasiteettia. Tällaiset toimenpiteet eivät kuitenkaan välttämättä suoranaisesti vaikuta sähköpostipalvelun käyttäjän kokemaan palvelun käytettävyyteen, sillä palvelun käyttö voi estyä käytännössä kokonaan esimerkiksi suuresta roskapostimäärästä johtuen.

Arvioitaessa haitallisena pidettävää sähköpostiliikennettä käytännössä oleellista on se, onko sähköpostiviesti määriteltävissä haitalliseksi yleisillä käytössä olevilla haitallisen sähköpostiliikenteen tunnistus- ja suodatusmekanismeilla.

3.2.6 Suodattaminen

Suodattamisella tarkoitetaan tässä määräyksessä sähköpostiviestien välittämisen tai vastaanottamisen estämistä, tietoturvaa vaarantavien haittaohjelmien poistamista viesteistä tai muita näihin rinnastettavia teknisuonteisia toimia.

3.3 3 § Avoimet sähköpostin välityspalvelimet

Avoimia sähköpostin välityspalvelimia käytetään yleisesti haitallisen sähköpostiliikenteen välittämiseen. Tunnistamalla avoimena toimivat sähköpostipalvelimet ja estämällä kolmansien osapuolien sähköpostipalvelimien käyttö sähköpostiviestien välitykseen voidaan vähentää välitettyä haitallisen sähköpostiliikenteen määrää.

Sähköpostipalveluntarjoajan on huolehdittava siitä, että sen hallinnoimat sähköpostijärjestelmät eivät toimi avoimena sähköpostin välityspalvelimina. Järjestelmien ja palvelujen käyttöönoton, ja muutosten yhteydessä suoritettavat testaus-toimenpiteet sekä asetusten huolellinen määrittely ovat esimerkkejä sähköpostijärjestelmien käyttöturvallisuudesta huolehtimisesta.

Sähköpostipalveluntarjoajan tulee säännöllisesti testata kaikki hallinnoimansa sähköpostijärjestelmät varmistuakseen siitä etteivät järjestelmät toimi avoimena sähköpostin välityspalvelimina. Mikäli yritys ei ole hankkinut omaa testausjärjestelmää, se voi käyttää testaamiseen Internetissä yleisesti saatavilla olevia julkisia palveluita.

Internet-yhteyspalveluntarjoajan Internet-liittymään kuuluvan sähköpostin lähetyspalvelimen osalta tällä velvollisuudella tarkoitetaan sitä, että sähköpostien lähettäminen on mahdollista ilman tunnistusta vain kyseisen ISP:n omasta verkosta.

3.4 4 § Saapuvan sähköpostiliikenteen käsittely

Saapuvan sähköpostiliikenteen käsittelyllä tarkoitetaan tässä määräyksessä toimenpiteitä, joita voidaan toteuttaa sähköpostipalveluntarjoajan vastaanottopalvelimien (MDA) tai välityspalvelimien kautta asiakkaille saapuville sähköpostiviesteille. Näitä toimenpiteitä ovat haitallisen sähköpostiliikenteen lähteiden ja haitallisen sähköpostiliikenteen tunnistaminen, haitalliseksi tunnistetulle liikenteelle tehtävät suodatus- ja merkitsemistoimenpiteet sekä liikenteen toimittaminen asiakkaille.

3.4.1 Haitallisen sähköpostiliikenteen tunnistaminen

Sähköpostiliikenteen lähteiden perusteella voidaan tunnistaa merkittävä osa tunnetuista oikeutettujen sähköpostiviestien lähteistä sekä tunnetuista haitallisen sähköpostiviestien lähteistä. Oikeutettujen lähteiden tunnistamisella voidaan välttää asianmukaisen sähköpostiliikenteen suodatus johtuen virheellisestä tunnistuksesta. Tunnistamalla haitallisen sähköpostiliikenteen lähteet, voidaan näistä lähteistä vastaanotettujen viestien toimitus sähköpostilaatikkoon estää tai sähköpostiviesti voidaan merkitä epäilyttäväksi ennen asiakkaan sähköpostilaatikkoon toimittamista.

Sähköpostilähteiden tunnistus voi perustua oikeutettujen lähettäjien, oikeudettomien lähettäjien tai molempien tunnistamiseen. Tunnistus voidaan tehdä esimerkiksi lähettäjän verkko-osoitteen, verkkotunnuksen tai lähettäjän sähköpostipalvelimen perusteella. Haitallisuuden määrittäminen perustuu ennalta saatuihin tai kerättyihin tietoihin lähteen kautta välitetyistä viesteistä tai viestin sisällön analysointiin.

Perustelut

Merkittävä osa sähköpostiliikenteestä saapuu ennalta tunnetuista verkko-osoitteista tai sähköpostipalvelimilta. Osa näistä voidaan kokemuksen, seurannan tai ulkopuolisen tilastoinnin perusteella tunnistaa haitallisen sähköpostiliikenteen lähteiksi jo SMTP:n yhteydenottovaiheessa. Samoin merkittävä osa asiallisesta sähköpostiliikenteestä vastaanotetaan toistuvasti käytetyistä ennalta tunnetuista oikeutetuista sähköpostilähteistä, jotka voidaan tunnistaa jo yhteydenottovaiheessa. Haitallisen sähköpostiliikenteen lähteiden tunnistaminen jo yhteydenottovaiheessa mahdollistaa sen, että sähköpostipalveluntarjoajan ei tarvitse edes ottaa kyseistä liikennettä vastaan. Tämä vähentää sähköpostipalveluun kohdistuvaa kuormitusta ja parantaa asiallisten sähköpostiviestien läpimenoa asiakkaille.

Haitallisen sähköpostiliikenteen tunnistaminen on edellytys kaikille sähköpostipalveluntarjoajan tekemille suodatus- ja merkitsemistoimenpiteille. Sähköpostipalveluntarjoaja voi kuitenkin havaita vain osan haitallisesta sähköpostiliikenteestä sähköpostin lähteiden perusteella. Siksi palvelun tarjoajalla on oltava käytössään myös muita menetelmiä haitallisen sähköpostiliikenteen havaitsemiseksi.

Monet näistä menetelmistä voivat kuitenkin aiheuttaa sähköpostipalveluntarjoajalle merkittäviä kustannuksia. Tiukempi tunnistuskriteeristö on myös herkempi virheellisille tulkinnoille. Valitsemallaan perustason tunnistusmenetelmillä sähköpostipalveluntarjoaja voi vähentää haitallisen sähköpostiliikenteen aiheuttamia vaikutuksia parantaen palvelun tietoturvaa ja toimivuutta sekä käyttäjien kokemaa palvelunlaatua ja käytettävyyttä. Sähköpostipalveluntarjoajalle on kuitenkin edellä mainituista syistä haluttu jättää mahdollisuus valita tarjoamaansa palveluun parhaiten soveltuvat haitallisen sähköpostiliikenteen tunnistusmekanismit.

Soveltaminen

Sähköpostipalveluntarjoajalla on oltava käytössä ajantasaiset ja luotettavat mekanismit sähköpostiliikenteen lähteiden tunnistamiseksi ja sähköpostiliikenteen haitallisuuden määrittämiseksi. Sähköpostipalveluntarjoaja voi valita järjestelmässään käytettävät mekanismit useista eri vaihtoehdoista siten, että **merkittävä** osa sisään tulevasta haitallisesta sähköpostiliikenteestä tulee tunnistetuksi vaarantaen mahdollisimman vähän asiallisten viestien läpimenoa. Kaikille asiakkaille käytössä olevien edellä mainitut kriteerit täyttävien perustason tunnistusmekanismien lisäksi sähköpostipalveluntarjoaja voi tarjota asiakkailleen myös edistyneempiä ja pitemmälle räätälöityjä haitallisen liikenteen tunnistus- ja käsittelymekanismeja esimerkiksi erillisellä sopimuksella.

Käytettäessä sähköpostiliikenteen suodatusmekanismeja SMTP-yhteydenottovaiheessa, tulee sähköpostipalveluntarjoajalla olla käytössään myös toimiva mekanismi tärkeimpien tunnettujen asial-

listen sähköpostilähteiden tunnistamiseksi. Määräyksen julkaisuhetkenä tällä tarkoitetaan pääsyylistojen käyttöä.

Sähköpostilähteiden tunnistamiseen ja haitallisuuden määrittämiseen on useita vaihtoehtoisia menetelmiä. Jo yhden käytössä olevan menetelmän avulla on mahdollista tunnistaa merkittävä osa haitallisesta sähköpostiliikenteestä. Haitallisen liikenteen tunnistamisen tulokset kuitenkin paranevat usein käytettäessä useita toisiaan täydentäviä menetelmiä yhtäaikaaisesti. Jokainen menetelmä tarjoaa omia etuja toisiin menetelmiin nähden, mutta valitettavasti kuhunkin menetelmään liittyy myös ongelmia. Sähköpostipalveluntarjoajan tulee olla tietoinen käyttämiensä menetelmien eduista ja haitoista ja arvioitava näiden vaikutukset ennen menetelmien käyttöönottoa.

Estolistaus

Estolistojen (blacklist) avulla voidaan tunnistaa ja suodattaa tai merkitä tunnetuista oikeudettomista sähköpostilähteistä saapuvat yhteydet tai sähköpostiviestit. Estolistalla tarkoitetaan yleisimmin tietokantaa tunnetuista haitallisen sähköpostiliikenteen lähteistä, joka koostuu usein verkko-osoitteista. Lista voi koostua myös yksittäisistä roskapostin lähetykseen käytetyistä sähköpostiosoitteista, verkkotunnuksista tai sähköpostipalvelimista. Estolista voi olla sähköpostipalveluntarjoajan itsensä ylläpitämä, kolmannen osapuolen ylläpitämä tai käyttäjän henkilökohtainen.

Sähköpostijärjestelmissä käytetään tavallisesti kolmannen osapuolen ylläpitämiä keskitettyjä estolistoja. Estolistojen käytössä ja valinnassa tulee käyttää erityistä huolellisuutta virheellisten tulkin-tojen välttämiseksi. Staattiset estolistat ovat usein epäluotettavia, sillä haitallisen sähköpostiliikenteen lähteet vaihtuvat tiheään ja mahdollinen staattinen väärä tieto estolistalla estää pitkäkestoisesti asiallista sähköpostiliikennettä. Tiedon poistaminen staattiselta estolistalta vaati aina käsin tehtävää työtä. Dynaamisesti ylläpidetyt estolistat sen sijaan päivittyvät nopeasti ja virheelliset listaukset tyyppillisesti poistuvat listoilta säännöllisesti.

Oman estolistan rakentaminen ei ole yleensä järkevää listan tietosisällön jatkuvan muuttumisen vuoksi. Estolistoja käytettäessä on syytä välttää tiettyjä suuria verkkoalueita yksittäisten käyttäjien toimenpiteiden perusteella listaavia estolistoja, jotta sähköpostipalvelun käytettävyydestä voidaan varmistua. Lisäksi sellaisia estolistoja tulee välttää, jossa listalle joutumisen perusteet ovat epäselvät, listalta poispääsyyn ei ole selkeitä menettelyjä tai listan käyttöä ei suositella suurille palveluntarjoajille.

Kolmannen osapuolen ylläpitämää estolistaa valitessa sähköpostipalveluntarjoajan tulee kiinnittää erityistä huomiota seuraaviin listan ominaisuuksiin:

- Listausperiaatteiden julkaiseminen
- Listalta poisto on yksinkertaista ja hyvin opastettua
- Listan ylläpitäjän yhteystiedot on julkaistu
- Listaus ei perustu yhteen virheelliseen viestiin
- Listaa päivitetään säännöllisesti

Estolistoja käytettäessä on huomioitava, että listat saattavat sisältää myös virheellistä tietoa ja näin ollen estää asiallista sähköpostiliikennettä. Käytettäessä kolmannen osapuolen ylläpitämää listaa tulee listan toimintaa seurata jatkuvasti. Eri listat sisältävät yleensä eri lähteitä, joten useamman listan yhtäaikaainen käyttö antaa usein parhaan tuloksen. Sähköpostin vastaanottopalvelimelle eri lähteistä tulevan haitallisen liikenteen tunnistusprosentti kasvaa, kun eri listat tunnistavat eri haitallisia lähteitä. Estolistoja voidaan käyttää myös osana sähköpostilähteen haitallisuuden pisteytystä heuristisessa suodatuksessa. Tällöin yksittäinen virheellinen listaus ei aiheuta asiallisen viestin suodatusta.

Käyttäessään estolistoja sähköpostipalveluntarjoajalla tulee olla käytössään toimiva mekanismi tunnettujen tärkeimpien asiallisten sähköpostilähteiden tunnistamiseksi. Määräyksen julkaisuhetkenä tällä tarkoitetaan pääsyylistojen käyttöä. Sähköpostipalveluntarjoajan tulee listata olennaiset yhteistyökumppaninsa ja luotettavat kotimaiset palveluntarjoajat sähköpostijärjestelmässä estolistan ohittavien osoitteiden listalle (pääsyylistalle) estolistan mahdollisesti aiheuttamien häiriöiden vaikutusten pienentämiseksi.

Pääsyylistaus

Pääsyylistalla (whitelist) merkitään viestien vastaanotto sallituksi tiettyjen verkko-osoitteiden, sähköpostipalvelimien tai sähköpostiosoitteiden kautta, jotka tiedetään yleisesti luotetuiksi asiallisten

viestien lähettäjinä. Tällaisiin voivat kuulua muun muassa tunnetut sähköpostipalveluntarjoajat ja yhteistyökumppanit.

Pääsyylistan käyttö on käytännössä välttämätöntä käytettäessä muita sähköpostilähteeseen perustuvia esto- tai suodatusmenetelmiä. Pääsyylistan avulla voidaan varmistaa viestien läpimeno luotetuista lähteistä, mikäli viestit tulisivat muuten suodatetuiksi esimerkiksi virheellisen estolistauksen seurauksena.

Pääsyylistaa käytettäessä on huomioitava, että myös luotettujen tahojen kautta voidaan välittää haitallista sähköpostiliikennettä, joten myöskään pääsyylistalla oleviin lähteisiin ei voi luottaa ehdotta. Lisäksi esimerkiksi pääsyylistattuja osoitteita voidaan väärentää haitallisen sähköpostiliikenteen viesteihin edistämään haitallisen sähköpostiliikenteen läpimenoa. Ongelmien välttämiseksi myös pääsyylistalla olevien lähteiden lähettämien viestien sisältöä tulee seurata.

Pääsyylista on usein hyvin staattinen lista verkko-osoitteita. Palveluntarjoajan tulee huolehtia, että listalla olevat tiedot ovat ajantasaisia, jotta vanhentuneiden tietojen aiheuttamilta ongelmilta vältytään. Viestintäviraston CERT-FI ylläpitää keskitettyä pääsyylistaa suomalaisten tahojen sähköpostipalvelimista. Sähköpostipalveluntarjoajat lähettävät muuttuneet palvelintietonsa CERT-FI:lle, joka jakaa päivitetyn listan säännöllisesti listan käyttäjille. Mikäli yritys haluaa CERT-FI:n pääsyylistan käyttöönsä tai päästä CERT-FI:n ylläpitämälle listalle, tulee asiasta olla yhteydessä CERT-FI yksikköön. Toinen vaihtoehto keskitetysti ylläpidetylle pääsyylistalle on esimerkiksi DNS Whitelist (<http://www.dnswl.org/>).

Harmaalistaus

Harmaalistaus (greylisting) perustuu haitallista sähköpostiliikennettä lähettävien ohjelmistojen toimintaan. Tavallisesta sähköpostijärjestelmästä poiketen nämä ohjelmistot eivät yritä lähettää viestiä uudestaan, vaikka viestin toimitus olisi epäonnistunut. Harmaalistauksessa tilastoidaan automaattisesti tiettyjä parametreja (saapuvan sähköpostin lähettäjän IP-osoite/osoitteen C-luokka, SMTP-lähettäjä ja SMTP-vastaanottaja) tai näistä muodostettu hash-taulu. Tuntemattomalta lähettäjältä/tietyillä parametreilla saapuvan viestin vastaanotosta kieltäydytään. Kun lähde yrittää viiveen jälkeen uutta lähetystä, viesti vastaanotetaan. Jatkossa ko. lähteestä viestit vastaanotetaan ilman viivettä.

Harmaalistauksen ongelmana on sen aiheuttama viive asiallisille sähköpostiviesteille jotka saapuvat ennalta tuntemattomista lähteistä. Lisäksi harmaalistauksen toiminta perustuu haitallisen sähköpostiliikenteen lähettäjien yhden lähetyskerran periaatteeseen. Mikäli haitallisen liikenteen lähettäjät alkavat harmaalistauksen kiertääkseen yrittämään viestien lähetystä uudelleen, ei harmaalistaus enää toimi. Lisäksi sähköpostiviestien uudelleenlähetykset aiheuttavat lisää sähköpostiliikennettä, mikä kuormittaa sekä verkkoja että sähköpostipalvelimia.

Mainejärjestelmät

Mainejärjestelmät perustuvat viestin lähteen aiempaan lähetystahojen historiaan. Sähköpostilähteiden (esim. lähettäjän IP-osoite ja SMTP-lähettäjä) lähettämiä viestejä seurataan, tilastoidaan ja vertaillaan lähteen aiempaan viestihistoriaan. Tilastoinnissa ja vertailussa kiinnitetään huomiota siihen lähettääkö lähde asianmukaisia sähköpostiviestejä vai haitallisia sähköpostiviestejä. Sähköpostilähteitä voidaan myös tarkkailla palvelimelta lähtevien viestien määrän perusteella. Tietoja hyödynnetään määrittämään sähköpostilähteen mainetaso pisteytyksen perusteella lähettäjän aiemman lähetys- ja viestihistorian perusteella. Mainetason perusteella tehdään päätös, toimitetaanko lähteestä tuleva viesti asianmukaisesti vastaanottajalle, toimitetaanko viesti vastaanottajalle alemmalla prioriteetilla vai estetäänkö viestin toimitus vastaanottajalle.

Mainejärjestelmien etuna on se, että ne hyödyntävät pitkäaikaista lähteiden seuranta, eikä viestien suodatusta tapahdu yksittäisten asiattomien viestien perusteella. Mainejärjestelmät tukevat hyvin muita suodatusjärjestelmiä ja osana heuristista suodatusta vähentää muun kriteeristön tekemiä virheitä. Mainejärjestelmissä on kuitenkin otettava huomioon, ettei järjestelmän pisteytys välttämättä ehdi reagoida nopeaan haitallisen liikenteen tulvaan.

Kolmansien osapuolten ylläpitämät mainejärjestelmät keräävät pisteytyksen muodostamiseen tarvittavia tietoja omilta asiakkailtaan. Laajalti saaduista tiedoista kootaan yhtenäinen tietokanta pisteytystä varten mainetason määrittämiseksi. Esimerkki kolmannen osapuolen ylläpitämästä mainejärjestelmä implementaatiosta on TrustedSource (<http://www.trustedsource.org/>) ja yksittäisen

tunnistusjärjestelmän apuna toimivasta mainejärjestelmästä spammassassin AWL (<http://wiki.apache.org/spamassassin/AutoWhitelist>).

Heuristinen analyysi

Sähköpostipalveluntarjoaja voi toteuttaa viestien haitallisuuden määrittämisen ja suodattamisen myös sähköpostiviestin sisältöön perustuvan analyysin avulla tai käyttää näitä menetelmiä sähköpostilähteiden tunnistamiseen käytettyjen menetelmien lisänä sähköpostiviestien suodatuksessa.

Haitallisten sähköpostiviestien sisältö yleensä täyttää tietyt ennalta tunnetut kriteerit. Viestin sisältöön perustuva suodattaminen voi tapahtua esimerkiksi vertaamalla viestistä laskettua tarkistussummaa tunnettuihin haitallisista viesteistä laskettuihin tarkistussummiin tai etsimällä viestistä haitallisuuteen viittaavia elementtejä, kuten tiettyjä sanoja, muotoiluja, liitetiedostoja, kuvia tai linkkejä. Sähköpostiviestistä voidaan myös etsiä asiallisen sähköpostiviestin piirteitä. Sisältöön perustuvaan suodattamiseen voidaan yhdistää myös esimerkiksi estolistoihin perustuvia suodatusmenetelmiä. Useita mekanismeja yhdisteessä kukin käytetty menetelmä joko lisää tai vähentää viestin haitallisuuden pistetasoa. Viestin saaman loppupistemäärän perusteella tehdään päätös onko viesti haitallinen vai ei. Suoritetun analyysin perusteella suodatusohjelmisto joko estävät viestin välityksen, merkitsevät viestin todennäköisesti haitalliseksi tai välittävät viestin eteenpäin sellaisenaan.

Muita mekanismeja

Edellä mainittujen mekanismien lisäksi sähköpostipalveluntarjoajalla on mahdollisuus valita lukuisia muita menetelmiä sähköpostilähteiden tunnistamiseen ja uusia keinoja tulee esille jatkuvasti. Uusimpiin keinoihin kuuluvat mm. Sender Policy Framework (SPF) [13] ja Domain Keys Identified Mail (DKIM) [14], joiden avulla voidaan tunnistaa että sähköpostiviesti on lähtenyt sähköpostiosoitteen osoittamalta sähköpostipalvelimelta. Kuten muissakin haitallisen sähköpostiliikenteen torjuntakeinoissa, myös näissä mekanismeissa on joukko heikkouksia, jotka tulee ottaa huomioon otettaessa menetelmiä käyttöön. Asiaa on kuvattu muun muassa RFC:ssä 4686 [15]. Koska esimerkiksi sähköpostin välityspalvelut, verkkopostikortit ja Internetyhteyspalveluntarjoajien lähetykset rikkovat näiden mekanismien toimintaa, soveltuvat mekanismit parhaiten vain lähteen positiiviseen tunnistamiseen.

Ennen uusien mekanismien käyttöönottoa tulee sähköpostipalveluntarjoajan perehtyä tarkoin menetelmän toimintaperiaatteisiin ja riskeihin virheellisten asiallisten sähköpostiviestien suodattamisen välttämiseksi. Usein yksittäisten mekanismien toimintatarkkuus on epävarmaa, mikäli mekanismin antamaan oikeudellinen/oikeudeton tulkintaan luotetaan varauksettomasti. Sen sijaan käytettäessä useita mekanismeja yhtäaikaista osana pisteytysjärjestelmää voidaan saada hyvinkin täsmällisiä suodatustuloksia pienellä virhemarginaalilla.

Suosituks

Sähköpostipalveluntarjoajia suositellaan tekemään haitallisen sähköpostiliikenteen lähteiden tunnistamista jo SMTP-yhteydenottovaiheessa. Näin suuri osa haitallisesta sähköpostiliikenteestä on mahdollista estää jo ennen sen pääsyä sähköpostijärjestelmään. Toimenpiteellä on mahdollista vähentää merkittävästi haitallisen sähköpostiliikenteen aiheuttamaa kuormitusta sähköpostipalvelimilla.

Haitallisen sähköpostiliikenteen tunnistamisessa suositellaan käytettäväksi useita menetelmiä samanaikaisesti. Näin voidaan parantaa haitallisen sähköpostiliikenteen tunnistustarkkuutta ja käyttää siten myös esimerkiksi tiukempia suodatuskriteereitä.

Pääsyylojen käyttöä suositellaan väriin tulkintojen välttämiseksi, kun sähköpostipalveluntarjoajalla on käytössään esto- ja suodatusmenetelmiä. Sähköpostipalveluntarjoajia suositellaan ottamaan käyttöön esimerkiksi Viestintäviraston CERT-FI:n ylläpitämän pääsyylojen tai vastaavan pääsyylojen.

3.4.2 Sähköpostiliikenteen suodatus ja merkitseminen

Saapuvan sähköpostiliikenteen suodatuksella tarkoitetaan asiakkaille saapuvan tunnistetun haitallisen sähköpostiliikenteen pääsyn estämistä asiakkaiden sähköpostilaatikkoon. Suodattamalla haitalliset sähköpostiviestit voidaan vähentää sähköpostipalvelimien kuormitusta ja asiakkaiden sähköpostilaatikkoon päätyvän haitallisten sähköpostiviestien määrää ja näin helpottaa asiallisten viestien läpikäymistä. Samalla ehkäistään haitallisen sähköpostiviestien vaikutuksia esimerkiksi

asiakkaiden avatessa sähköpostiviestien sisältämiä liitetiedostoja tai asiakkaiden ohjautuessa viestin linkin osoittamalle haittaohjelman sisältävälle sivustolle. Sähköpostiliikenteen suodatuksella voidaan parantaa asiakkaiden kokemaa palvelun laatua ja palvelun tietoturva.

Perustelut

Merkittävä osuus saapuvasta sähköpostiliikenteestä on nykyään tulkittavissa haitalliseksi sähköpostiliikenteeksi. Mahdollisimman varhaisessa vaiheessa tunnistetut ja suodatut haitalliset sähköpostiviestit vähentävät sähköpostijärjestelmän kuormitusta ja asiallisten viestien läpimeno parantuu. Estämällä haitallisen sähköpostiliikenteen pääsy sähköpostipalvelimille voidaan myös ennalta ehkäistä järjestelmään kohdistettuja haitallisia vaikutuksia esimerkiksi palvelunestohyökkäystapa-uksissa. Haitallisia sähköpostiviestejä suodattamalla palvelun tietoturva ja toimivuus parantuvat.

Suodattamalla haitallisia sähköpostiviestejä estetään asiakkaan tietoturvalle ja sitä kautta myös viestintäverkoille haitallisen sisällön pääsy tämän sähköpostilaatikkoon ja käsiteltäväksi. Lisäksi suodattamalla haitallista sähköpostiliikennettä vähennetään saapuneiden sähköpostiviestien määrää asiakkaan sähköpostilaatikossa. Asiakkaan sähköpostiviestien käsittely helpottuu, kun asiallisia viestejä ei tarvitse erotella haitallisista viesteistä. Samalla asiakkaiden kokemaa palvelunlaatu ja käytettävyyttä parantuvat.

Sähköpostiliikenteen suodatus voi perustua haitallisten sähköpostilähteiden tunnistusmekanismeihin ja/tai heuristisiin suodatusjärjestelmiin. Koska osa sähköpostipalvelun asiakkaista haluaa varmistua itse siitä, että virheellistä suodatusta ei tapahdu, on sähköpostipalveluntarjoajille annettu mahdollisuus merkitä haitalliseksi havaitsemansa liikenne sen suodattamiseen sijaan. Asiakkaan pyynnöstä ja erillisellä sopimuksella sähköpostipalveluntarjoaja voi jättää myös merkitsemisen suorittamatta.

Soveltaminen

Sähköpostipalveluntarjoajan on merkittävä tai suodatettava saapuvasta sähköpostiliikenteestä sellainen sähköpostiliikenne, jonka se on käytössään olevien haitallisen sähköpostiliikenteen tai sen lähteiden tunnistusmekanismien avulla määritellyt haitalliseksi. Automaattisen haitalliseksi havaitun liikenteen suodattamisen sijasta sähköpostipalveluntarjoaja voi myös esimerkiksi ohjata osan tai kaikki haitallisiksi havaitsemistaan ja merkitsemistään viesteistä erilliseen haitalliselle sähköpostille tarkoitettuun käyttäjäkohtaiseen kansioon, jossa viestejä voidaan säilyttää esimerkiksi tietty määrä tai tietyn ajan käyttäjän tarkastettavana. Sähköpostipalveluntarjoaja voi myös poistaa viesteistä haitalliseksi tunnistamansa sisällön ennen viestin toimittamista asiakkaalle.

Palveluntarjoajalle annettulla mahdollisuudella sopia asiakkaan kanssa erikseen siitä, että haitalliseksi tunnistettua liikennettä ei suodateta tai merkitä haitalliseksi tarkoitetaan asiakkaan pyynnöstä erikseen tehtävää sopimusta. Sähköpostipalveluntarjoaja ei siis voi sisällyttää tätä vaihtoehtoa vakiosopimuksiinsa.

Kaikista edellä mainituista poikkeuksista huolimatta sähköpostipalveluntarjoajan on kuitenkin aina suodatettava sellainen haitalliseksi tunnistettu sähköpostiliikenne, joka vaarantaa sähköpostipalvelun tuottamiseen käytettävien järjestelmien toimivuutta.

3.4.3 Saapuvan sähköpostiliikenteen suodatusperiaatteista tiedottaminen

Haitallisen sähköpostiliikenteen tunnistaminen ja suodattaminen tai merkitseminen on välttämätöntä sähköpostipalvelun toimivuuden ja käytettävyyden turvaamiseksi. Tiedottamalla asiakkaita käytössä olevista sähköpostiliikenteen suodatuksen peruseriaatteista voidaan välttää väärinkärsityksiä ja turhia asiakasvalituksia.

Perustelut

Asiakkaalla on oikeus saada tietoa hänelle tarjottavan palvelun ominaisuuksista ja siten myös sähköpostipalveluntarjoajan käyttämistä suodatusperiaatteista. Lisäksi sähköpostipalveluntarjoajan suorittama saapuvan sähköpostiliikenteen suodatus aiheuttaa usein asiakastiedusteluja palveluntarjoajalle, mikäli asiallisia sähköpostiviestejä tulee virheellisesti suodatetuksi tai asiakkaan sähköpostilaatikkoon saapuvan haitallisen sähköpostiliikenteen määrä kasvaa merkittävästi.

Soveltaminen

Kun sähköpostipalveluntarjoaja suodattaa asiakkaidensa sähköpostiliikennettä, sähköpostipalveluntarjoajan on kuvattava asiakkaalle käyttämänsä yleiset suodatusperiaatteet. Kuvauksen tarkoituksena on kertoa asiakkaalle yleisellä tasolla käytettävistä suodatusmenetelmistä ja niiden vaikutuksesta asiakkaan liikennöintiin. Suodatusperiaatteiden kuvaaminen asiakkaalle ei saa vaarantaa viestintäpalvelun tietoturvasuutta, eli kuvauksen ei tarvitse olla tarpeettoman yksityiskohtainen ja kertoa tarkkoja perusteita esimerkiksi miksi yksittäinen sähköpostiviesti tulkitaan sisällön perusteella haitalliseksi liikenteeksi.

Esimerkiksi estolistoja käytettäessä sähköpostipalveluntarjoajan ei tarvitse luetella suodatuksessa käytettäviä estolistoja yksityiskohtaisesti, sillä käytettävät listat saattavat vaihdella tilanteesta riippuen.

3.5 5 § Lähtevän sähköpostiliikenteen käsittely

Lähtevän sähköpostiliikenteen käsittelyllä tarkoitetaan tässä määräyksessä toimenpiteitä, jotka voidaan suorittaa lähtevän sähköpostipalvelimen (MSA) kautta välitettävälle sähköpostiviesteille. Näitä toimenpiteitä ovat oikeutettujen lähettäjien tunnistaminen sekä MSA:n kautta lähtevän haitalliseksi tunnistetun sähköpostiliikenteen suodattaminen.

Perustelut

Lähtevän sähköpostiliikenteen käsittelyn tarkoituksena on vähentää sähköpostipalveluntarjoajan palvelimien kautta lähtevän haitallisen sähköpostiliikenteen ja roskapostiliikenteen määrää ja parantaa sähköpostipalveluntarjoajan sähköpostipalvelimien mainetta sekä edistää palveluntarjoajan asiakkailta lähtevien asiallisten sähköpostiviestien läpimenoa. Samalla edistetään käyttäjien kokemaa palvelun laatua.

Haitallisen sähköpostiliikenteen vaikutuksia voidaan vähentää merkittävästi, mikäli haitalliset sähköpostiviestit tunnistetaan ja niiden välitys estetään mahdollisimman varhaisessa vaiheessa. Siksi palveluntarjoajan on rajattava sähköpostin lähetysoikeus vain lähettämiseen oikeutetuille tahoille sekä suodatettava haitalliseksi tunnistettua sähköpostiliikennettä ennen kuin haitalliset sähköpostiviestit pääsevät kuormittamaan tietoliikenneverkkoja ja vastaanottavia sähköpostipalvelimia.

Näillä toimenpiteillä palveluntarjoaja voi vähentää oman palvelimensa kautta lähtevien haitallisten sähköpostiviestien määrää ja parantaa näin omaa mainettaan viestien vastaanottajien näkökulmasta sekä edistää sähköpostipalveluntarjoajan oikeutettujen käyttäjien lähettämien asiallisten viestien välitystä ja läpimenoa.

Lisäksi haitallisen liikenteen tunnistamisella ja liikenteen lähteen selvittämisellä voidaan palveluntarjoajan asiakasta tiedottaa asiakkaan tietokoneen sisältämästä haittaohjelmasta ja neuvoa, kuinka asiakas voi poistaa haittaohjelman ja näin ollen estää haitallisten viestien lähetys asiakas-koneelta jatkossa.

Soveltaminen

Sähköpostipalveluntarjoajalla on oltava käytössä ajantasaiset ja luotettavat mekanismit haitallisen lähtevän sähköpostiliikenteen tunnistamiseksi ja suodattamiseksi. Haitallisen sähköpostiliikenteen tunnistaminen voi perustua esimerkiksi oikeudettoman lähteen tunnistamiseen, lähtevän liikenteen virussuodatukseen, käyttäjän poikkeavaan lähtevän sähköpostiliikenteen määrään tai viestin otsikotietojen Internet-standardien mukaisuuden tarkistamiseen.

Sähköpostipalveluntarjoaja voi valita järjestelmässään käytettävät mekanismit eri vaihtoehdoista siten, että **merkittävä** osa lähtevästä haitallisesta sähköpostiliikenteestä tulee tunnistetuksi ja suodatetuksi vaarantaen mahdollisimman vähän asiallisten viestien läpimenoa.

Mikäli sähköpostipalveluntarjoaja havaitsee, että oikeutetun käyttäjän päätelaitetta käytetään haitallisen sähköpostiliikenteen välitykseen, tulee sähköpostipalveluntarjoajan suodattaa asiakkaalta lähtevä haitallinen sähköpostiliikenne tai estää asiakkaan sähköpostiliikenne sekä ottaa mahdollisuuksien mukaan yhteyttä asiakkaaseen.

Poikkeava liikennemäärä

Poikkeavan liikennemäärän tunnistamiseksi sähköpostipalveluntarjoajan tulisi asettaa normaalikäytön raja-arvot. Mikäli lähtevän sähköpostiliikenteen määrä ylittää normaaliksi määritellyn lähetysrajan, voi sähköpostipalveluntarjoaja estää asiakkaan sähköpostiliikenteen väliaikaisesti. Lisäksi sähköpostipalveluntarjoajan on mahdollisuuksien mukaan otettava yhteyttä asiakkaaseen, jolloin asiakas voi tehdä tarvittavat toimenpiteet saastuneen koneen puhdistamiseksi ja tilanteen korjaamiseksi.

Asiakastiedotus

Sähköpostipalveluntarjoajan on kuvattava asiakkaille yleiset lähtevän sähköpostiliikenteen suodatusperiaatteet. Suodatusperiaatteisen tiedottamisessa sovelletaan kappaleessa 3.4.3 kuvattuja toimintaperiaatteita.

3.6 6 § Asiakkaan ja sähköpostipalvelimen välinen yhteys

Asiakkaan ja sähköpostipalvelimen välisellä yhteydellä tarkoitetaan tässä määräyksessä asiakkaan (MUA) ja sähköpostilaatikon (MS) välistä yhteyttä sekä asiakkaan (MUA) ja sähköpostin lähetyspalvelimen (MSA) välistä yhteyttä.

Asiakkaan ja sähköpostipalvelimen sekä asiakkaan ja sähköpostilaatikon välisien yhteyksien suojaamisella tarkoitetaan asiakkaan tunnistamista sekä edellä mainittujen asiakkaan ja palvelun välisten liikenteen salaamista.

Perustelut

Asiakkaan ja sähköpostipalvelimen välillä välitetään käyttäjätunnuksia ja salasanoja. Asiakkaan ja palvelimen välisten yhteyksien suojaamisella voidaan estää näiden tietojen päätyminen kolmannen osapuolen tietoon sekä estää palvelun väärinkäyttöä ja parantaa palvelun tietoturvaa. Lisäksi asiakkaan ja palvelimen välisen yhteyden suojaamisella voidaan varmistaa asiakkaiden viestien säilyminen luottamuksellisena asiakkaan ja palvelimen välisessä liikenteessä. Yhteyden suojaamisella voidaan lisäksi tarjota asiakkaille turvallinen tapa käyttää sähköpostipalvelua liityntäverkkoriippumattomasti ja parantaa asiakkaiden kokemaa palvelun luottamuksellisuutta.

Asiakkaita on kuitenkin syytä tiedottaa siitä, että asiakkaan ja palvelimen välisen yhteyden suojaaminen ei kuitenkaan aina varmista yhteyden luottamuksellisuutta viestintätapahtuman päästä päähän, lähettäjältä vastaanottajalle.

Selainpohjaisten sähköpostipalveluiden (webmail) tyypillisten käyttötapojen vuoksi on perusteltua, että yhteydet ovat aina suojattuja.

Soveltaminen

Sähköpostipalveluntarjoajan on tarjottava asiakkaille ensisijaisena vaihtoehtona suojattu yhteys asiakkaan ja sähköpostilaatikon sekä asiakkaan ja lähtevän liikenteen sähköpostipalvelimen välillä. Velvoite koskee myös muita kuin selainpohjaisia sähköpostipalveluja.

Tällä velvollisuudella tarkoitetaan sitä, että teleyrityksen on tarjottava kaikille sähköpostiasiakkailleen mahdollisuus suojattujen yhteyksien käyttöön, ja että suojattujen yhteyksien käyttö ohjeistetaan asiakkaille joko ensisijaisena tai ainoana vaihtoehtona asiakkaille jaettavassa ja asiakkaiden saatavilla olevassa käyttöohjeistuksessa.

Oikeutettujen käyttäjien tunnistamiseksi ja suojatun asiakasyhteyden muodostamiseksi asiakkaalta sähköpostin välityspalvelimelle suositellaan käytettäväksi SMTP-AUTH [16] protokollaa.

Asiakkaan ja sähköpostilaatikkopalvelimen välillä tähän tarkoitukseen voidaan käyttää esimerkiksi SSL/TLS:llä protokolla suojattuja IMAP tai POP yhteyksiä (IMAPS/POPS [17], [18]).

Selainpohjaisten sähköpostipalveluiden asiakasyhteydet on suojattava aina. Muistion kirjoittamishetkellä suositeltava suojausmenetelmä on HTTPS-protokolla [19].

3.7 7 § Sähköpostipalvelujen toimivuuden ja laadun seuranta

Perustelut

Sähköpostipalvelusta on kehittynyt koko yhteiskunnan toiminnan kannalta tärkeä viestintäpalvelu, jonka toiminnan turvaaminen on välttämätöntä. Jotta ongelmatilanteet voidaan havaita ajoissa ja niiden korjaaminen voidaan aloittaa varhaisessa vaiheessa, on palvelun toimivuuden ja laadun jatkuva seuranta välttämätöntä.

Teleyrityksen on seurattava jatkuvasti yleisten sähköpostipalvelujen tuottamiseen ja sähköpostin välittämiseen liittyvän toimintansa laatua ja palveluvarmuutta. Palveluiden toimivuuden ja laadun seurantamenettelyt on tarkoitettu ensisijaisesti palveluiden ylläpito- ja kehittämisprosessien tueksi sekä palveluiden toiminnan turvaamiseksi.

Soveltaminen

Sähköpostipalveluntarjoajan on jatkuvasti seurattava yleisten sähköpostipalveluun liittyvien toimintojen laatua ja palveluvarmuutta. Seurantaan kuuluu palvelun toimivuuden ja laadun reaaliaikainen seuranta sekä pitkäaikainen tilastointi.

Toimintojen laadun ja palveluvarmuuden jatkuva seuranta

Sähköpostipalveluntarjoajalla on oltava tarkoituksenmukaiset ja riittävät mekanismit merkittävien palvelun toimintaan vaikuttavien ongelmien havainnoimiseksi ja niihin reagoimiseksi. Tällaisilla ongelmilla tarkoitetaan tilanteita, joissa sähköpostipalvelun käytettävyyttä tai tietoturvasuoritus on vaarantunut esimerkiksi poikkeuksellisen sähköpostiliikenteen tai ohjelmisto-/laitteistovian vuoksi.

Yli 10 000 asiakkaan sähköpostipalveluntarjoajalla näiden mekanismien on oltava käytössä ympärivuorokautisesti. Ongelmatilanteisiin on kuitenkin reagoitava aina ilman aiheetonta viivytystä ongelman vakavuus huomioon ottaen. Ongelmatilanteisiin reagoinnilla tarkoitetaan esimerkiksi tässä määräyksessä lueteltujen suodatustoimenpiteiden käyttöönottoa, automaattisten hallintamekanismien käyttöä sähköpostipalvelua tuottavassa järjestelmässä sekä sähköpostiliikenteen uudelleenohjausta ruuhkatilanteissa tai palveluiden häiriötilanteissa.

Yllä kuvattujen ongelmien havainnoimiseen soveltuvia jatkuvaluonteisia mittareita ovat muun muassa sähköpostin läpimenoaika ja sähköpostipalvelun kuormitus- ja jonotilanne.

Sähköpostiviestin läpimenoaika

Sähköpostiviestin läpimenoaikaan seurannalla sähköpostipalveluntarjoajan omassa järjestelmässä tarkoitetaan läpimenoajan mittaamista sähköpostiviestin välittyessä palveluntarjoajan omassa järjestelmässä. Uloslähtevän sähköpostiliikenteen osalta voidaan mitata läpimenoaika siitä hetkestä kun viesti otetaan asiakasliittymästä tai sähköpostisovellukselta kuten webmail-sovellukselta välitettäväksi siihen hetkeen, kun viestiä yritetään toimittaa eteenpäin. Viestiä ei voida toimittaa eteenpäin esimerkiksi tapauksissa, joissa vastaanottava sähköpostipalvelin on tilapäisesti ruuhkautunut ja pyytää palvelinta lähettämään viestin myöhemmin uudelleen.

Sisään tulevan sähköpostiliikenteen osalta voidaan mitata läpimenoaika siitä hetkestä kun ulkopuolinen sähköpostijärjestelmä avaa yhteyden viestin välittämiseksi teleyrityksen sähköpostijärjestelmään siihen hetkeen, kun viesti on toimitettu teleyrityksen omassa järjestelmässä sijaitsevan vastaanottajan sähköpostilaatikkoon tai viestiä yritetään toimittaa eteenpäin teleyrityksen järjestelmän ulkopuoliselle vastaanottajalle. Viesti voi kulkea teleyrityksen omassa järjestelmässä useamman palvelimen kautta, esimerkiksi ulkopuolisesta järjestelmästä tulevan liikenteen sähköpostipalvelimen kautta postilaatikkopalvelimelle. Läpimenoaika voidaan seurata järjestelmän kokonaisviiveenä tai yksittäisen palvelinkomponentin sisäisenä viiveenä.

Sähköpostipalvelun kuormitus- ja jonotilanne

Kuormitus- ja jonotilanteen seurannalla tarkoitetaan palvelinjärjestelmien kuormituksen ja sähköpostiliikenteen jonojen tilannetietojen seuranta. Kuormitustilanteen seurannalla tarkoitetaan esimerkiksi käyttöjärjestelmätason resurssien seuranta sähköpostipalvelun tuottamiseen käytettävistä järjestelmistä. Jonotilanteen seurannalla tarkoitetaan esimerkiksi sähköpostipalvelun tuotta-

miseen käytettävien järjestelmien sähköpostijonojen automaattista seurantaan vikatilanteiden nopeaksi havaitsemiseksi ja tilanteeseen reagoimiseksi.

Tilastointi

Sähköpostipalvelun kehittämistä, palvelun toimintavarmuuden turvaamista ja viranomaisia varten sähköpostipalveluntarjoajan on seurattava ja tilastoiva ainakin seuraavia parametreja:

- haitalliseksi liikenteeksi tunnistetun, merkityn ja suodatetun sähköpostiliikenteen määrä
- lähetetyn ja vastaanotetun sähköpostiliikenteen määrä
- sähköpostipalvelun kuormitustilanne
- asiakasmäärä

Suodatusmekanismien toiminnan seuraaminen

Käytettyjen suodatusmekanismien toiminnan seuraamisella tarkoitetaan sähköpostipalvelun tuottamiseen käytettävissä järjestelmissä käytettävien suodattimien, kuten estolistojen tai sisällön-suodatusmekanismien, seuraamista mekanismien toiminnan ja suodatetun liikenteen määrän osalta. Seurannan perusteella teleyritys voi varmistua mekanismien toiminnasta, liikenteen suodattamisen perusteista epäselvissä tapauksissa sekä seurata suodatetun liikenteen määrää tietyllä aikajaksolla.

Suodatusmekanismien toimintaa voidaan seurata esimerkiksi raportoimalla estolistojen toiminnan perusteella estetyt viestit sähköpostilokissa, kirjaamalla viestisisällön perusteella merkityt tai estetyt viestit sähköpostilokiin sekä seuraamalla näistä arvoista tehtyjä tilastoja. Toimintaa voidaan testata myös lähettämällä suodatusmekanismien suojaamien järjestelmien kautta haitallisia komponentteja sisältäviä testiviestejä. Suodatetun liikenteen määrää voidaan seurata esimerkiksi tilastoimalla häiritseviksi, muuten haitalliseksi tai normaaliksi liikenteeksi luokiteltavaa liikennettä. Häiritsevien osalta teleyritys voi esimerkiksi tehdä summatason tilastointia erityyppisten häiritsevien esiintymistiheydestä sähköpostiliikenteessä. Seurannan perusteella teleyritys voi tarvittaessa ryhtyä jatkotoimenpiteisiin, esimerkiksi tehostettujen suodatusmenetelmien käyttöönottamiseksi.

3.8 8 § Sähköpostiosoitteiden hallinta

Sähköpostiosoitteiden hallinta on osa sähköpostipalvelun toimivuutta ja käytettävyyttä. Erilaiset sähköpostiosoitteiden hallintakäytännöt, samankaltaiset ja/tai harhauttavat sähköpostiosoitteet sekä käytöstä poistuneiden sähköpostiosoitteiden uudelleen käyttöönnotto ovat aiheuttaneet ongelmatilanteita. Yhtenäistämällä eri palveluntarjoajien käytäntöjä ja kuvaamalla asiakkaille sähköpostiosoitteiden hallintaa voidaan ennaltaehkäistä näitä asiakkaiden kokemia ongelmatilanteita. Valmiiden toimintamallien avulla voidaan puolestaan nopeuttaa ongelmatilanteiden ratkaisua.

3.8.1 Sähköpostiosoitteiden hallinnan kuvaus asiakkaille

Perustelut

Sähköpostiosoitteiden hallinnointikäytännöt vaihtelevat eri palveluntarjoajien kesken. Lisäksi ongelmatilanteita tulkitaan eri tavalla myös palveluntarjoajien sisällä. Yhteisten hallinnointikäytäntöjen määrittelyllä ja kuvaamisella asiakkaille voidaankin välttää väärinkäsityksiä ja nopeuttaa ongelmatilanteiden ratkaisua.

Soveltaminen

Sähköpostipalveluntarjoajan on määriteltävä ja kuvattava asiakkaille käyttämänsä sähköpostiosoitteiden hallinnointikäytännöt. Kuvauksen avulla asiakkaan tulee saada selville, kuinka hän voi saada uuden sähköpostiosoitteen käyttöönsä, muokata sähköpostipalvelun asetuksia ja poistaa sähköpostiosoite käytöstä. Lisäksi sähköpostipalveluntarjoajan on kuvattava asiakkailleen samankaltaisiin ja harhauttaviin sähköpostiosoitteisiin liittyvät käytössä olevat toimintamallit ja rajoitukset.

3.8.2 Asiakkaalta vapautuneen sähköpostiosoitteen uudelleen käyttö

Perustelut

Sähköpostiosoitteeseen tulee usein viestejä myös kyseisen osoitteen sulkemisen jälkeen. Mikäli vapautunut osoite on annettu välittömästi tai pian käytöstä poistumisen jälkeen toisen asiakkaan käyttöön, voi uusi asiakas saada vanhalle asiakkaalle osoitettuja sähköpostiviestejä. Sähköpostiviestien luottamuksellisuuden ja sähköpostiosoitteiden väärinkäytön estämiseksi tulee käytöstä poistetun sähköpostiosoitteen olla karanteenissa ennen kuin sitä on mahdollista vapauttaa uudelleen käyttöön.

Soveltaminen

Sähköpostipalveluntarjoaja ei saa luovuttaa asiakkaalta vapautunutta sähköpostiosoitetta toiselle asiakkaalle ennen kuin kolme kuukautta on kulunut sähköpostiosoitteen vapautumisesta. Mikäli sähköpostiosoitteen entinen haltija haluaa vapautuneen sähköpostiosoitteesen takaisin käyttöönsä kolmen kuukauden sisällä osoitteen vapautumisesta, on asiakkaalla oikeus saada sähköpostiosoite takaisin käyttöönsä, mikäli sähköpostipalvelun asiakassuhdetta ei ole katkaistu. Oikeus sähköpostiosoitteen takaisinsaamiseen ei kuitenkaan itsessään velvoita palveluntarjoajaa säilyttämään sähköpostitilin sisältämiä sähköpostiviestejä tilin sulkemisen jälkeen. Tällainen velvoite voi kuitenkin johtua esimerkiksi osapuolten välisestä sopimuksesta.

3.8.3 Harhauttavien sähköpostiosoitteiden ongelmatilanteiden hallinta**Perustelut**

Harhauttavat sähköpostiosoitteet luodaan harhauttamaan toista osapuolta luulemaan osoitteen omistajaa toiseksi henkilöksi/tahoksi. Harhauttavalla sähköpostiosoitteella tarkoitetaan esimerkiksi toisen henkilön tai yrityksen nimellä, yritystunnuksella tai yleisesti tiedossa olevalla ylläpito-osoitteella (esimerkiksi postmaster, webmaster tai asiakaspalvelu) rekisteröityä sähköpostiosoitetta. Ennalta laaditut toimintamallit nopeuttavat ja selkiyttävät tapauksien käsittelyä.

Soveltaminen

Mikäli sähköpostipalveluntarjoaja havaitsee tai saa tietoonsa verkkotunnukseensa rekisteröidyn harhauttavan sähköpostiosoitteen, tulee sähköpostipalveluntarjoajan puuttua ongelmaan. Sähköpostipalveluntarjoajalla on oikeus poistaa käytöstä osoitteet, jotka on perustettu harhauttavassa tarkoituksessa. Sähköpostiosoite voi olla myös toisen henkilön henkilötieto. Henkilötietoja koskee henkilötietolain mukainen virheettömyysvaatimus ja siihen liittyvä henkilötiedon korjaamisen velvollisuus. Toisen henkilötietojen käyttö hyötymistarkoituksessa voi olla myös rikosoikeudellisesti rangaistavaa.

Viestintävirasto suosittelee, että sähköpostipalveluntarjoajat eivät myönnä asiakkailleen sähköpostipalveluntarjoajan omaan verkkotunnukseen liittyviä RFC 2142:ssa [20] määriteltyjä harhauttavia sähköpostiosoitteita tai näiden suomenkielisiä vastineita.

3.9 9 § Sähköpostipalveluntarjoajan yhteystiedot

Sähköpostipalveluntarjoajan on huolehdittava siitä, että sen omissa ja sähköpostipalvelujen tarjoamiseen käytettävissä verkkotunnuksissa on oltava postmaster- ja abuse-osoitteet, johon saapuvia viestejä seurataan säännöllisesti.

Tällä vaatimuksella pyritään huolehtimaan siitä, että teleyrityksellä on käytössä yhteydenottopiste mahdollisten toiminnan tai käytön häiriöiden ilmoittamiseksi teleyritykselle, riippumatta ilmoittajan sijainnista.

Postmaster- ja abuse-osoitteiden levinneisyyden vuoksi ne keräävät usein asiatonta viestintää ja teleyrityksen onkin syytä järjestää osoitteen seuranta siten että osoitteisiin tulevien asiallisten yhteydenottojen käsittely ei viivästy haitallisen sähköpostiliikenteen suuren määrän vuoksi. Mikäli teleyrityksen hallussa on suuri määrä verkkotunnuksia, teleyrityksen hallussa olevien verkkotunnusten postmaster- ja abuse-osoitteisiin tulevat viestit on syytä ohjata soveltuviin yhteydenottopisteisiin. Teleyritys voi siirtää yhteydenottojen seurannan myös verkkotunnuksesta vastaavalle osapuolelle.

3.10 10 § Voimaantulo ja siirtymäsäännökset

Tämä määräys tulee voimaan 1 päivänä marraskuuta 2008.

Mikäli määräyksen 6 §:ssä annetun veloitteen (suojattujen yhteyksien tarjoamisesta) toteuttaminen vaatii muutoksia sähköpostipalveluntarjoajien tietojärjestelmiin ja asiakastiedotukseen, tälle veloitteelle on annettu siirtymäaikaa 1.3.2009 saakka.

4 MUUT SUOSITUKSET

Tässä luvussa on kuvattu muut sähköpostipalveluntarjoajille annettavat ei-velvoittavat suositukset, jotka eivät liity suoraan mihinkään tämän määräyksen pykälään.

4.1.1 Palvelinten välisten yhteyksien suojaaminen

Sähköpostin lähetys-, välitys- ja vastaanottopalvelimien välisten yhteyksien suojaaminen edesauttaa sähköpostipalvelun tietoturvaa ja luotettavuutta. Käytettäessä suojattua yhteyttä palvelimien välillä, palvelimet tunnistavat toisensa yhteyden muodostamisvaiheessa. Tunnistamisella voidaan todeta viestinnän toinen osapuoli luotettavaksi tahoksi. Palvelimen välisten yhteyksien suojaamisella voidaan estää myös sähköpostiviestien päätyminen kolmannen osapuolen tietoon

Sähköpostipalveluntarjoajien ja käyttäjien on kuitenkin huomioitava, että kaikki palvelimien väliset yhteydet eivät ole suojattuja.

Suositus

Sähköpostiliikenteen luottamuksen turvaamiseksi suositellaan, että mikäli sähköpostipalvelin (MSA, MTA tai MDA) tukee suojatun yhteyden käyttöä, on tämä ominaisuus mahdollisuuksien mukaan otettava käyttöön.

5 VIITELUETTELO

[1] Viestintämarkkinalaki (393/2003 muutoksineen, VML), ajantasainen versio:

<http://www.finlex.fi/fi/laki/ajantasa/2003/20030393>

[2] Sähköisen viestinnän tietosuojalaki (516/2004 muutoksineen, SVTsL), ajantasainen versio:

<http://www.finlex.fi/fi/laki/ajantasa/2004/20040516>

[3] Euroopan parlamentin ja neuvoston direktiivi 2002/21/EY, annettu 7 päivänä maaliskuuta 2002, sähköisten viestintäverkkojen ja -palvelujen yhteisestä sääntelyjärjestelmästä (puitedirektiivi)

http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fi&type_doc=Directive&an_doc=2002&nu_doc=21

[4] Euroopan parlamentin ja neuvoston direktiivi 2002/20/EY, annettu 7 päivänä maaliskuuta 2002, sähköisiä viestintäverkkoja ja -palveluja koskevista valtuutuksista (valtuutusdirektiivi)

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0020:FI:NOT>

[5] Euroopan parlamentin ja neuvoston direktiivi 2002/19/EY, annettu 7 päivänä maaliskuuta 2002, sähköistenviestintäverkkojen ja niiden liitännäistoimintojen käyttöoikeuksista ja yhteenliittämisestä (käyttöoikeusdirektiivi)

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0019:FI:NOT>

[6] Euroopan parlamentin ja neuvoston direktiivi 2002/22/EY, annettu 7 päivänä maaliskuuta 2002, yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alla (yleispalveludirektiivi)

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:FI:NOT>

[7] Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi)

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:FI:NOT>

- [8] Viestintäviraston määräys 9 B/2004 M, Tietoturvaloukkausten sekä vika- ja häiriötilanteiden ilmoittamisvelvollisuudesta yleisessä teletoiminnassa,
http://www.ficora.fi/attachments/suomi_R_Y/5jTIBwnxP/Files/CurrentFile/Viestintavirasto09B2004M.pdf
- [9] Viestintäviraston määräys 13 A/2008 M Internet-yhteyspalvelujen tietoturvasta ja toimivuudesta,
http://www.ficora.fi/attachments/suomi_R_Y/5AWLt8K4m/Files/CurrentFile/Viestintavirasto13A2008M.pdf
- [10] Viestintäviraston määräys 47 B/2004 M, Teleyritysten tietoturvasta,
http://www.ficora.fi/attachments/suomi_R_Y/1158858986420/Files/CurrentFile/Viestintavirasto47B2004M.pdf
- [11] Viestintäviraston määräys 53/2008 M Tunnistamistietojen tallentamisvelvollisuudesta,
http://www.ficora.fi/attachments/suomi_R_Y/5yk2y1H7z/Files/CurrentFile/Viestintavirasto532008M.pdf
- [12] Viestintäviraston määräys 54/2008 M, Viestintäverkkojen ja -palvelujen varmistamisesta,
http://www.ficora.fi/attachments/suomi_R_Y/5vB4GW4xt/Files/CurrentFile/Viestintavirasto542008M.pdf
- [13] RFC 4408, Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1, <http://www.ietf.org/rfc/rfc4408.txt>
- [14] RFC 4871, DomainKeys Identified Mail (DKIM) Signatures, <http://www.ietf.org/rfc/rfc4871.txt>
- [15] RFC 4686, Analysis of Threats Motivating DomainKeys Identified Mail (DKIM),
<http://www.ietf.org/rfc/rfc4686.txt>
- [16] RFC 2554, SMTP Service Extension for Authentication, <http://www.ietf.org/rfc/rfc2554.txt>
- [17] RFC 2595, Using TLS with IMAP, POP3 and ACAP, <http://www.ietf.org/rfc/rfc2595.txt>
- [18] RFC 4616, The PLAIN Simple Authentication and Security Layer (SASL) Mechanism,
<http://www.ietf.org/rfc/rfc4616.txt>
- [19] RFC 2818, HTTP Over TLS, <http://www.ietf.org/rfc/rfc2818.txt>
- [20] RFC 2142 Mailbox names for Common Services, Roles and Functions,
<http://www.ietf.org/rfc/rfc2142.txt>

6 LYHENNELUETTELO

CERT-FI	Computer Emergency Response Team - Finland
DNS	Domain Name Server
IMAP	Internet Message Access Protocol
IMAPS	Secure IMAP
IP	Internet Protocol
ISP	Internet Service Provider
MDA	Message Delivery Agent
MSA	Message Submission Agent
MTA	Mail Transfer Agent
MX	mail exchange
POP	Post Office Protocol
POPS	Secure POP
RFC	Request for Comments
SMTP	Simple Mail Transfer Protocol
SMTP-AUTH	SMTP Authentication
SSL	Secure Socket Layer
SVTsL	sähköisen viestinnän tietosuojalaki
TLS	Transport Layer Security
VML	viestintämarkkinalaki