

**MÄÄRÄYKSEN 13 PERUSTELUT JA  
SOVELTAMINEN**

**INTERNET-YHTEYSPALVELUJEN  
TIETOTURVASTA**

**SISÄLLYS**

<b>SISÄLLYS</b> .....	<b>1</b>
<b>1 LAINSÄÄDÄNTÖ</b> .....	<b>2</b>
1.1 MÄÄRÄYKSEN LAINSÄÄDÄNTÖPERUSTA.....	2
1.2 MUUT ASIAAN LIITTYVÄT SÄÄNNÖKSET.....	3
1.3 VIESTINTÄVIRASTON TULKINNAT.....	4
<b>2 MÄÄRÄYKSEN TARKOITUS JA MUUTOSHISTORIA</b> .....	<b>6</b>
2.1 MÄÄRÄYKSEN TARKOITUS.....	6
2.2 KESKEISET MUUTOKSET JA MUUTOSHISTORIA.....	6
<b>3 1 § SOVELTAMISALA</b> .....	<b>7</b>
<b>4 2 § MÄÄRITELMÄT</b> .....	<b>7</b>
4.1 INTERNET-YHTEYSPALVELU.....	7
4.2 ASIAKASLIITTYMÄ.....	7
4.3 ASIAKASLIITTYMÄN PALVELUT.....	8
4.4 HAITALLINEN LIIKENNE.....	8
4.5 SUODATTAMINEN.....	8
<b>5 3 § ASIAKASLIITTYMIEN TIETOTURVALLISUUS</b> .....	<b>8</b>
5.1 KÄYTTÄJIEN LIIKENTEEN EROTTAMINEN TOISISTAAN.....	8
<b>6 4 § TIEDOTTAMINEN</b> .....	<b>9</b>
6.1 TIEDOTTAMINEN ASIAKKAALLE.....	9
6.2 ASIAKASTIEDOTUS LIITTYMÄN TEKNISTEN RAJOITUSTEN OSALTA.....	10
<b>7 5 § KULUTTAJALIITTYMÄSTÄ LÄHTEVÄN SÄHKÖPOSTILIIKENTEEN OHJAUS JA REITITYS</b> .....	<b>11</b>
7.1 KULUTTAJALIITTYMÄSTÄ LÄHTEVÄN RAJOITAMATTOMAN SMTP-LIIKENTEEN ESTÄMINEN.....	11
7.2 KULUTTAJALIITTYMÄSTÄ LÄHTEVÄN SMTP-LIIKENTEEN SALLIMINEN ERITYISTAPAUKSISSA.....	11
<b>8 6 § HAITALLISEN LIIKENTEEN HAVAITSEMINEN</b> .....	<b>12</b>
8.1 HAITALLISEN LIIKENTEEN HAVAITSEMINEN.....	12
<b>9 7 § HAITALLISEN LIIKENTEEN SUODATTAMINEN</b> .....	<b>12</b>
9.1 LIIKENTEEN TILAPÄISEN SUODATTAMISEN PROSESSIT JA TOIMINTAMALLIT.....	12
9.2 VIRHEELLISIÄ LÄHDEOSOITTEITA SISÄLTÄVÄN LIIKENTEEN SUODATTAMINEN.....	13
9.3 KÄYTTÄJÄN TUNNISTAMINEN.....	14
9.4 OSOITE- JA REITTISUODATUS.....	14
9.5 SUODATUSOIMENPITEIDEN TOTEUTTAMINEN.....	15
<b>10 8 § LIITTYMÄN IRTIKYTKEMINEN</b> .....	<b>15</b>
10.1 ASIAKASLIITTYMIEN IRTIKYTKEMINEN.....	15
10.2 IRTIKYTKENTÄPROSESSIN OHJEISTUS.....	15
<b>11 9 § TIETOTURVALOUKKAUSTAPAUSTEN KÄSITTELY JA TILASTOINTI</b> .....	<b>16</b>
11.1 TIETOTURVALOUKKAUSTEN KÄSITTELY.....	17
11.2 TIETOTURVALOUKKAUSILMOITUSTEN TILASTOINTI.....	17
<b>12 10 § VOIMAANTULO JA SIIRTYMÄSÄÄNNÖKSET</b> .....	<b>19</b>
<b>13 VIITELUETTELO</b> .....	<b>19</b>

## 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 sähköisen viestinnän tietosuojalakiin (516/2004 muutoksineen, SVTsL) [1], joka tuli voimaan 1.9.2004 ja jolla panttiin osaltaan täytäntöön EY:n heinäkuussa 2002 hyväksymä sähköisen viestinnän tietosuojadirektiivi [2].

Lisäksi Viestintäviraston määräys perustuu viestintämarkkinalakiin (393/2003 muutoksineen, VML [3]), joka tuli voimaan 25.7.2003 ja jolla panttiin osaltaan täytäntöön EY:n helmikuussa 2002 hyväksymät sähköisen viestinnän puite-, valtuutus-, käyttöoikeus- ja yleispalveludirektiivit.

SVTsL:n 19 §:n 1 momentin nojalla teleyrityksen on huolehdittava palvelujensa tietoturvasta. Palvelun ja käsittelyn tietoturvasta huolehtiminen tarkoittaa toimia toiminnan turvallisuuden, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden sekä tietoaineistoturvallisuuden varmistamiseksi. Tietoturvasta huolehtimiseksi tehtävät toimet on suhteutettava uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin. SVTsL:n 19 §: 3 momentin nojalla teleyritys vastaa tilaajille ja käyttäjille 1 momentissa tarkoitetusta tietoturvasta myös sellaisen kolmannen osapuolen osalta, joka kokonaan tai osittain toteuttaa verkkopalvelun, viestintäpalvelun, tietojen säilyttämisen tai lisäarvopalvelun.

Viestintävirasto voi SVTsL:n 19 §:n 4 momentin nojalla antaa teleyrityksille tarkempia määräyksiä muun muassa pykälän 1 ja 3 momentissa tarkoitetusta palvelun tietoturvasta.

SVTsL:n 20 §:n 1 momentin nojalla teleyrityksellä sekä sen lukuun toimivalla on oikeus ryhtyä 2 momentissa tarkoitettuihin välttämättömiin toimiin tietoturvasta huolehtimiseksi:

- 1) viestintäverkkojen tai niihin liitettyjen palvelujen tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi;
- 2) viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi; tai
- 3) viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseksi.

SVTsL:n 20 §:n 2 momentin mukaan edellä 1 momentissa tarkoitetut toimet voivat käsittää:

- 1) viestin automaattisen sisällöllisen analyysin;
- 2) viestien välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen;
- 3) tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä;
- 4) muut näihin rinnastettavat teknisluonteiset toimenpiteet.

SVTsL:n 20 §:n 3 momentin mukaan jos viestin tyyppin, muodon tai muun vastaavan seikan perusteella on ilmeistä, että viesti sisältää haitallisen tietokoneohjelman tai käskyn eikä viestin automaattisella sisällöllisellä analyysillä pystytä turvaamaan pykälän 1 momentissa tarkoitettujen tavoitteiden toteutumista, yksittäisen viestin sisältöä saa käsitellä manuaalisesti. Manuaalisesta viestin sisällön käsittelystä on ilmoitettava viestin lähettäjälle ja vastaanottajalle, jollei ilmoittamisella todennäköisesti vaaranneta pykälän 1 momentissa tarkoitettujen tavoitteiden toteutumista.

SVTsL:n 20 §:n 4 momentin mukaan pykälässä tarkoitettujen toimenpiteiden toteuttaminen on huolellisesti ja ne on mitoitettava torjuttavan häiriön vakavuuteen. Toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä pykälän 1 momentissa tarkoitettujen tavoitteiden turvaamiseksi. Toimenpiteet on lopetettava, jos niiden toteuttamiselle ei enää ole tässä pykälässä säädettyjä edellytyksiä.

SVTsL:n 20 §:n 5 momentin mukaan Viestintävirasto voi antaa teleyrityksille tarkempia määräyksiä pykälässä tarkoitettujen toimenpiteiden teknisestä toteuttamisesta.

VML:n 128 §:n mukaan yleiset viestintäverkot ja viestintäpalvelut sekä niihin liitettävät viestintäverkot ja viestintäpalvelut on suunniteltava, rakennettava ja ylläpidettävä muun muassa siten, että

4) käyttäjien tai muiden henkilöiden tietosuoja, tietoturva tai muut oikeudet eivät vaarannu.

VML:n 129 §:n mukaan Viestintävirasto voi antaa 128 §:ssä tarkoitettuja viestintäverkkojen ja viestintäpalvelujen laatuvaatimuksia ja yhteensopivuutta koskevia määräyksiä. Määräykset voivat koskea muun muassa

10) viestintäverkon turvallisuutta ja häiriöttömyyttä,

16) suorituskyvyn ylläpitoa ja seurantaa sekä verkonhallintaa ja

17) teknistä dokumentointia.

## 1.2 Muut asiaan liittyvät säännökset

### 1.2.1 Viestintämarkkinalaki

*Viestintämarkkinalaki 67 § Viestintäpalvelusopimus.* Pykälään on valmisteilla muutos, jonka mukaan viestintäpalvelua koskevassa sopimuksessa on käsiteltävä aikaisempaa useampia asioita. Tähän on poimittu ehdotuksesta lisäykset, joilla voi olla merkitystä internet-yhteyspalvelun tarjonnassa:

Sopimuksessa on mainittava ainakin:

[...]

15) tiedot menettelyistä, joilla teleyritys mittaa ja muokkaa tietoliikennettä välttääkseen verkkoyhteyden ylikuormittumisen;

16) tiedot siitä, miten 15 kohdassa tarkoitettut menettelyt saattavat vaikuttaa palvelun laatuun;

[...]

18) toimitettavan päätelaitteen käyttöä koskevat rajoitukset;

[...]

21) millaisiin toimenpiteisiin teleyritys voi ryhtyä tietoturvan vaarantuessa.

*Viestintämarkkinalaki 131 § Velvollisuus korjata häiriö.* 1 momentin mukaan jos viestintäverkko tai laite aiheuttaa vaaraa tai häiriötä viestintäverkolle, laitteelle, viestintäverkon käyttäjälle tai muulle henkilölle, teleyrityksen tai muun viestintäverkon tai laitteen haltijan on välittömästi ryhdyttävä toimenpiteisiin tilanteen korjaamiseksi ja tarvittaessa irrotettava viestintäverkko tai laite yleisestä viestintäverkosta.

Viestintävirasto voi VML:n 131 §:n 1 momentissa tarkoitettussa tapauksessa määrätä korjaustoimenpiteistä sekä verkon tai laitteen irrottamisesta.

### 1.2.2 Viestintäviraston tekniset määräykset

Määräys 9 *tietoturvaloukkausten ilmoitusvelvollisuudesta yleisessä teletoiminnassa* [4]. Määräystä sovelletaan yleiseen teletoimintaan. Määräyksen tarkoituksena on määrittellä SVTSL:n 21 §:n mukaisten merkittävää tietoturvaloukkausta tai sen uhkaa koskevan ilmoituksen sisältö ja menettelytavat Viestintävirastolle ja asiakkaille tehtävissä ilmoituksissa.

Määräys 11 *sähköpostipalvelujen tietoturvasta ja toimivuudesta* [5]. Määräystä sovelletaan yleisissä viestintäverkoissa tarjottavien sähköpostipalvelujen tuottamiseen sekä sähköpostipalveluntarjoajan tähän tarkoitukseen käyttämiin järjestelmiin, viestintäverkkoihin ja -palveluihin. Määräyksen tavoitteena on varmistaa kuluttajien käyttämien sähköpostipalveluiden toiminta.

Määräys 28 *viestintäverkkojen ja -palveluiden yhteentoimivuudesta* [6]. Määräystä sovelletaan yleisiin viestintäverkkoihin ja -palveluihin sekä viranomaisverkkoihin. Määräyksen 2 lukua sovelletaan puhelinverkossa tarjottaviin viestintäpalveluihin. Määräyksen tarkoituksena on edistää eri teleyritysten viestintäverkkojen ja -palveluiden yhteenliitettävyyttä sekä viestintäpalveluiden päästä - päähän -yhteentoimivuutta.

Erityisesti määräykseen 13 liittyviä asioita ovat määräyksen 28 4 §:ssä virheellisiä lähdeosoitteita sisältävän liikenteen estämistä, virheellisten reittimainostusten suodattamista sekä IP-osoitelohkojen dokumentointia koskevat velvoitteet. Lisäksi samaan asiakokonaisuuteen liittyvät myös määräyksen 3 §:ssä annetut uudet velvoitteet asiakas- ja yhteenliittämisrajapintojen tietoturvasta sekä häiriöiden sietämisestä ja estämisestä.

Määräys 47 *teleyritysten tietoturvasta* [7]. Määräystä sovelletaan teleyritysten yleisten verkko- ja viestintäpalvelujen toteuttamiseen liittyvään toimintaan. Määräyksen soveltamisala kattaa esimerkiksi internet-yhteyspalveluiden, sähköpostipalveluiden ja viestintämarkkinalain mukaisten puhepalveluiden tarjonnan. Määräyksessä asetetaan teleyrityksille toimintaa järjestettäessä huomioitavia tietoturva vaatimuksia.

Määräys 57 *viestintäverkkojen ja -palvelujen ylläpidosta sekä menettelystä vika- ja häiriötilanteissa* [8]. Määräystä sovelletaan kaikkiin yleisiin viestintäverkkoihin ja niissä tarjottaviin viestintäpalveluihin. Määräyksen tarkoitus on parantaa teleyritysten vika- ja häiriötilanteisiin varautumista sekä niihin liittyviä menettelyvalmiuksia.

### 1.3 Viestintäviraston tulkinnat

Viestintävirasto on antanut useita tulkintoja SVTSL 20 §:n soveltumistilanteista. Osa tulkinnoista on julkaistu CERT-FI:n verkkosivuilla Ohjeet-osiossa <http://www.cert.fi/ohjeet.html>. Osiota täydennetään säännöllisesti uusilla tulkinnoilla.

#### 1.3.1 Tunnistamistietojen käsittely tietoturvasta huolehtimiseksi (387/64/2009)

Teleyritykset ovat saattaneet Viestintäviraston tietoon tulkintaongelmia SVTSL:n muutoksen vaikutuksista tunnistamistietojen käsittelyyn tietoturvasta huolehtimiseksi. Tulkintaongelmat koskevat tilanteita, joissa teleyrityksen on tietoturvasyistä pystyttävä tunnistamaan tiettyä IP-osoitetta käyttänyt asiakas DHCP-lokiin tallentuneita tunnistamistietoja käsittelemällä. Asiakkaan tunnistaminen on välttämätöntä tietoturvatyökalujen kohdistamiseksi oikeaan asiakasliittymään.

Viestintäviraston tulkinnan mukaan teleyritys saa käsitellä tarvittaessa tunnistamistietoja sekä 20 §:n 1 momentissa määritellyissä tilanteissa että käyttäessään pykälän 2 momentissa tarkoitettuja keinoja. Viestintäviraston tulkinnan mukaan teleyritys saa käsitellä tunnistamistietoja varsinaisen 20 §:ssä tarkoitetun toimenpiteen suorittamisen lisäksi myös toimenpiteen suorittamiseksi välttämättömien valmistelevien toimenpiteiden suorittamiseksi. Tällainen valmisteleva toimenpide voi olla esimerkiksi tiettyä IP-osoitetta käyttäneen asiakkaan tunnistaminen DHCP-lokiin tallentuneita tunnistamistietoja käsittelemällä.

#### 1.3.2 Haittaohjelmaliikenteen estäminen (46/64/2009)

CERT-FI on saanut tietoonsa useita satoja Conficker/Downadup -matotartuntaepäilyjä suomalaisista verkoista. Maailmalla matotartunnan saaneita koneita arvioidaan olevan useita miljoonia. Verkkomadon toimintaa tutkittaessa on saatu selville madon päivittämiseen käytettävä tapa. Tartunnan jälkeen mato luo päivämäärän perusteella satunnaisia verkkotunnuksia, joihin se yrittää ottaa yhteyttä päivittääkseen itsensä. Osa tartunnan saaneista päätelaitteista on pystytty selvittämään rekisteröimällä joitakin madon käyttämiä verkkotunnuksia ja seuraamalla niihin suuntautuvaa verkkoliikennettä. Tiedot tartunnan saaneiden päätelaitteiden osoitteista on toimitettu verkkojen ylläpitäjille.

Viestintäviraston tulkinnan mukaan teleyritykset voivat pienentää merkittävästi matotartuntojen aiheuttamaa tietoturvauhkaa estämällä madon liikennöinti sen päivittämiseen käytettäviin verkkotunnuksiin. Liikennöinnin estäminen tekee madon päivittämisestä ja murretun järjestelmän hyödyntämisestä merkittävästi vaikeampaa. Viestintäviraston tulkinnan mukaan liikenteen estämistä haittaohjelman päivittämisverkkotunnuksille voidaan pitää SVTSL:ssa tarkoitettuna välttämättömänä toimena verkkopalvelujen tai viestintäpalvelujen turvaamiseksi.

Jos teleyritys haluaa tunnistaa sen verkossa olevat saastuneet päätelaitteet, voi liikenteen estäminen tapahtua esimerkiksi antamalla muokattu vastaus saastuneen päätelaitteen teleyrityksen resolver-nimipalvelimille tekemään nimipalvelukyselyyn. Muokatun vastauksen IP-osoitteeksi voidaan valita esimerkiksi vapaa IP-osoite teleyrityksen omasta IP-osoiteavaruudesta.

Viestintäviraston tulkinnan mukaan teleyrityksillä on oikeus tallentaa haittaohjelman päivittämiseen käytettäviin verkkotunnuksiin suuntautuvan liikenteen lähdeosoitteet ja selvittää lähdeosoitetta käyttävä tilaaja. Tilaajan selvittämiseksi teleyritys saa käsitellä myös muussa yhteydessä kertyneitä tunnistamistietoja. Kerätyt tunnistamistiedot on tuhottava heti, kun niiden

käsittelylle ei ole enää perustetta. Tunnistamistietoja voidaan luovuttaa kolmansille osapuolille ainoastaan laissa yksilöidyillä perusteilla.

### 1.3.3 Saastuneen päätelaite muodostaa aina tietoturvauhan (46/64/2009)

Viestintäviraston vakiintuneen tulkinnan mukaan teleyrityksen verkossa olevat saastuneet päätelaitteet vaarantavat teleyrityksen palveluiden tietoturvaa. Siten haittaohjelmartunnan saaneiden päätelaitteiden selvittämistä voidaan pitää välttämättömänä palvelun toteuttamiseksi ja sen tietoturvasta huolehtimiseksi.

### 1.3.4 Liikenteen suodattaminen (1952/64/2009)

CERT-FI:n tietoon on tullut tapauksia, joissa suomalaisten verkkopankkiasiakkaiden verkkoliikennettä on ohjattu käyttäjän tietämättä kolmannen osapuolen ylläpitämälle www-palvelimelle. Ohjaus on toteutettu muokkaamalla DNS-asetuksia käyttäjän päätelaitteelle asentuneella haittaohjelmalla. Muokkaamisen jälkeen päätelaite käyttää verkkotunnusten IP-osoitteiden selvittämiseen haittaohjelman ylläpitäjän määrittelemiä DNS-palvelimia. Toimenpiteeseen on todennäköisesti käytetty DNS changer -tyyppistä haittaohjelmaa (esimerkiksi Zlob).

Viestintäviraston tulkinnan mukaan teleyritykset voivat SVTsL:n nojalla suodattaa teknisessä liitteessä yksilöidyille verkkoalueille suuntautuvan liikenteen viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseksi. Suodattaminen on perusteltua myös tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi.

SVTsL:n mukaan tunnistamistietoja saa käsitellä siinä määrin kuin se on tarpeen verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun toteuttamiseksi ja käyttämiseksi sekä laissa säädetyllä tavalla tietoturvasta huolehtimiseksi. Teleyrityksen verkossa olevat saastuneet päätelaitteet vaarantavat teleyrityksen palveluiden tietoturvaa. Siten haittaohjelmartunnan saaneiden päätelaitteiden selvittämistä voidaan pitää välttämättömänä palvelun toteuttamiseksi ja sen tietoturvasta huolehtimiseksi.

Viestintäviraston tulkinnan mukaan teleyritykset voivat kerätä liitteessä yksilöityihin verkkoalueisiin suuntautuvan liikenteen lähdeosoitteet ja selvittää lähdeosoitetta käyttävä tilaaja DHCP-lokiin (tai vastaavaan lokiin) tallentuneista tiedoista.

### 1.3.5 Kolmannen osapuolen palvelussa häiriköivän käyttäjän tunnistaminen (268/64/2010)

Teleyritykset ovat tiedustelleet Viestintävirastolta kolmannen osapuolen palvelussa häiriköivän asiakkaan tunnistamisoikeudesta tunnistamistietoja käsittelemällä. Häiriköivä asiakas käyttää usein vaihtuvan IP-osoitteen avulla toteutettua viestintäpalvelua. Vaihtuva osoite estää häiriköinnin kohteeksi joutuvaa palveluntarjoajaa kohdistamasta rajoitustoimia häiriköijään verkko-osoitteen perusteella. Vastaavasti tällaisen käyttäjän tunnistamisen teleyrityksen toimesta pelkästään asiakastietoja käsittelemällä on mahdotonta.

Viestintäviraston arvion mukaan muiden käyttäjien viestintäpalvelun käyttämahdollisuuksia merkittävästi ja välittömästi rajoittavan käyttäjän toimia voidaan pitää SVTsL:ssa tarkoitettuna tietoturvatoinenpiteisiin ryhtymiseen oikeuttavana viestintäpalvelulle haittaa aiheuttavana häiriönä. Tietoturvatoinenpiteisiin ryhtymistä voidaan pitää perusteltuina myös viestintäpalvelun muiden käyttäjien viestintämahdollisuuksien turvaamiseksi.

Arvioitaessa käyttämahdollisuuksien rajoittumisen merkittävyyttä, on huomiota kiinnitettävä ainakin siihen, että toimilla saavutettavan hyödyn on oltava olennaisesti luottamuksellisen viestin suojalle aiheuttavaa haittaa suurempi. Arvioinnissa on syytä kiinnittää huomiota ainakin kohteena olevan palvelun merkittävyyteen sekä mahdollisten rajoitustoimien todennäköisyyteen ja vaikuttavuuteen käyttäjien keskuudessa.

Arvioitaessa käyttämahdollisuuksien rajoittumisen välittömyyttä, on huomiota kiinnitettävä rajoitustoimenpiteiden toteutumisen todennäköisyyteen. Välittömyyden arviointi perustuu tyypillisesti käsittelytarvetta arvioivan toimijan omaan kokemukseen rajoitustoimenpiteiden

todennäköisyydestä. Jo aloitettujen rajoitustoimenpiteiden osalta ei välittömyysarviointia tarvitse tehdä.

Viestintäviraston tulkinnan mukaan kolmannen osapuolen palvelussa häiriköivät käyttäjät voidaan tunnistaa tunnistamistietoja käsittelemällä yllä kuvatut reunaehdot huomioiden. Tunnistamistietojen käsittelyn edellytyksenä on kuitenkin aina se, että käsittelyn tavoitetta ei voida saavuttaa millään muulla tavoin. Viestintämahdollisuuksien rajoittamista lievempänä toimenpiteenä käyttäjä voidaan vain tunnistaa yhteydenottoa varten.

### 1.3.6 Viestin määritelmä SVTsL:n kannalta

SVTsL:ssa viestillä tarkoitetaan viestillä viestintäverkossa osapuolten välillä tai vapaasti valikoituville vastaanottajille välitettävää puhelua, sähköpostiviestiä, tekstiviestiä, puheviestiä ja muuta vastaavaa sanomaa. Viestintäviraston tulkinnan mukaan kaikki viestintäverkoissa liikkuvat viestit ja sanomat ovat SVTsL:ssa tarkoitettuja viestejä riippumatta siitä, ovatko kysymyksessä luonnollisten henkilöiden vai erilaisten järjestelmien toisilleen lähettämät viestit.

## 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

Tämän määräyksen tarkoituksena on edistää internet-yhteyspalvelujen tietoturvaa. Tavoitteena on ennaltaehkäistä internet-yhteyspalveluihin liittyviä tietoturvaongelmia ja edistää uusien tietoturvapalvelujen käyttöönottoa. Määräyksellä on tarkoitus varmistaa, että teleyritykset pitävät huolta internet-yhteyspalvelujen tietoturvasta ja parantaa siten viestintäpalvelujen toimintavarmuutta ja luotettavuutta .

Määräyksen ja sen ohessa annettavien suositusten tarkoituksena on lisäksi edistää teleyritysten hyväksi katsomia ratkaisuja. Yhtenäinen internet-yhteyspalvelujen perustietoturvaso on alan toimijoiden ja teleyritysten asiakkaiden etu.

### 2.2 Keskeiset muutokset ja muutoshistoria

Määräyksestä 13 A/2008 M on siirretty IP-yhdysliikennekysymyksiin liittyvät veloitteet ja suositukset määräykseen 28 H/2010 M.

Määräyksen 13 A/2008M 3 § on ryhmitelty uudestaan. Tietoturvariskeihin liittyvät tiedotusveloitteet on siirretty 4 § alle.

Määräyksen 13 A/2008 M 4 § säädökset kuluttajaliittymään suuntautuvan SMTP-liikenteen estämisestä on poistettu kokonaan. Säädös on käytännössä estänyt kuluttajaliittymien takana sijaitsevat SMTP-palvelimet. Määräyksen voimaanjäävät säädökset kuluttajaliittymästä lähtevän sähköpostiliikenteen ohjauksesta ja reitityksestä tarjoavat riittävän mahdollisuuden roskapostiliikenteen havaitsemiseen ja rajoittamiseen. Muutoksen jälkeen kuluttajaliittymien takana sijaitseville SMTP-palvelimille ei ole säädöksistä johtuvista rajoitusvelvoitteista aiheutuvia esteitä.

Määräyksen haitallisen liikenteen havaitsemiseen, suodattamiseen ja irtikytkemiseen liittyvät säädökset on ryhmitelty uudestaan 6-8 § alle. Velvoitteisiin on lisätty teleyritysten viestintäverkkoja koskeva havainnointikyky viestintäverkon ja -palvelun tietoturvalle vaaraa aiheuttavan liikenteen havaitsemiseksi ja virheellisiä lähdeosoitteita sisältävän liikenteen jäljittämiseksi.

Internet-yhteyspalvelujen toimivuuden ja laadun seurantaan liittyvät veloitteet on poistettu tästä määräyksestä. Veloitteet ovat siirtyneet määräykseen 58/2009 M.

Määräyksen 9 § täsmentää tietoturvaloukkaustapausten käsittely- ja rekisteröintivelvoitetta. Uutena velvoitteena on teleyritysten käsittelemien tietoturvaloukkaustapausten ja niiden johdosta

suorittujen toimenpiteiden tilastointi. Lisäksi pykälä edellyttää teleyrityksiltä asianmukaisten yhteysosoitteiden ylläpitoa tietoturvaloukkausten ilmoittamista varten.

### 3 1 § SOVELTAMISALA

Määräystä sovelletaan yleisissä viestintäverkoissa tarjottavien internet-yhteyspalvelujen tuottamiseen sekä teleyrityksen näihin toimintoihin käyttämiin järjestelmiin, viestintäverkkoihin ja viestintäpalveluihin. Määräystä ei siten sovelleta esimerkiksi internet-yhteyspalvelun kautta tarjottaviin sähköposti- tai pikaviestipalveluihin. Määräystä sovelletaan sähköposti- ja pikaviestipalvelujen toteuttamiseen tarvittavaan IP-yhteystason palveluun.

Määräystä sovelletaan internet-yhteyspalvelujen tuottamisessa soveltuvin osin sekä verkkoyrityksissä että palveluyrityksissä.

### 4 2 § MÄÄRITELMÄT

Tässä kappaleessa kuvataan määräyksessä käytetyt määritelmät. Määräyksessä ei määritellä uudestaan laissa esiteltyjä määritelmiä.

#### 4.1 Internet-yhteyspalvelu

*Internet-yhteyspalvelulla* tarkoitetaan tässä määräyksessä viestintäpalvelua, jonka avulla voidaan muodostaa yhteys internetiin ja käyttää internetissä tarjolla olevia palveluita.

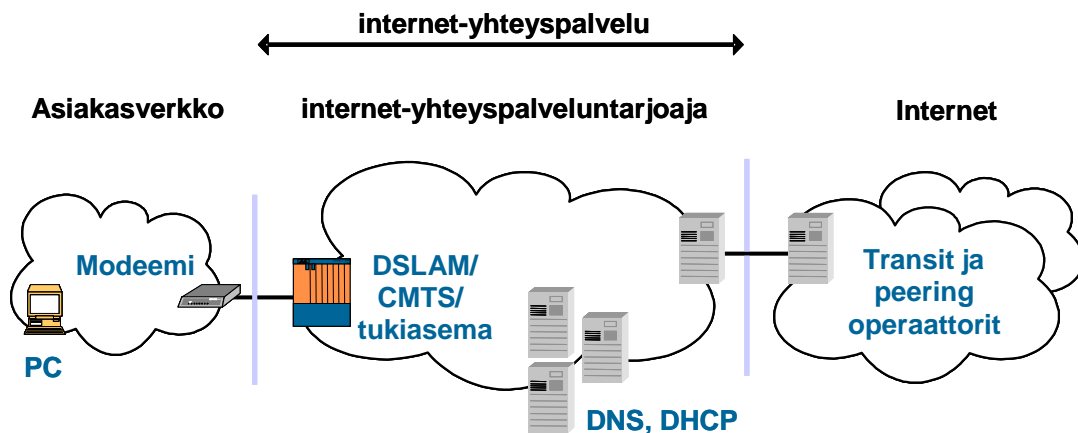
#### 4.2 Asiakasliittymä

*Asiakasliittymällä* tarkoitetaan tässä määräyksessä sekä kuluttaja- että yrityskäyttöön tarkoitettua asiakasverkon ja internet-verkon välistä loogista rajapintaa. Liittymän tilaaja kytketään asiakasliittymän kautta yleisen viestintäverkon ja sen palvelujen käyttäjäksi.

Asiakasliittymän ja internet-verkon välisellä rajapinnalla tarkoitetaan tässä määräyksessä loogista rajapintaa, jolla erotetaan kaksi eri verkkoa tai yksittäinen käyttäjä ja verkko. Teknisesti rajapinta sijaitsee esimerkiksi asiakasverkon ja verkkoyrityksen verkon sekä verkkoyrityksen verkon ja palveluyrityksen verkon välillä. Looginen rajapinta voi sijaita myös asiakkaan virtuaaliverkon ja julkisen internet-verkon välillä.

Asiakasliittymän toteutuksessa voidaan käyttää useita vaihtoehtoisia tekniikoita, kuten esimerkiksi analogista modeemiyhteyttä, radioverkkoa, langatonta lähiverkkoyhteyttä, kaapelidataverkkoa tai DSL-tekniikkaa.

Asiakasliittymän toteutukseen liittyviä rajapintoja on havainnollistettu seuraavassa kaaviokuvassa.



Kuva 1. Esimerkki verkon rajapinnoista asiakasliittymään

### 4.3 Asiakasliittymän palvelut

*Asiakasliittymän palveluilla* tarkoitetaan tässä määräyksessä teleyrityksen asiakkailleen asiakasliittymän kautta tarjoamia internet-liikenteen välittämiseen tarvittavia palveluita.

Asiakasliittymän kautta tarjottavia internet-liikenteen välittämiseen tarvittavia palveluita ovat esimerkiksi nimipalvelu (DNS), internet-osoitteiden jakamiseen käytetty palvelu (DHCP), sähköpostin välityspalvelu (SMTP) sekä www-välityspalvelu (proxy).

### 4.4 Haitallinen liikenne

*Haitallisella liikenteellä* tarkoitetaan tietoliikennettä, joka aiheuttaa vaaraa viestintäverkon tai -palvelun tietoturvalle. Haitallista liikennettä on tyypillisesti palvelunestohyökkäyksistä, roskapostista sekä verkkomatojen leviämisestä aiheutuva liikenne.

### 4.5 Suodattaminen

*Suodattamisella* tarkoitetaan tässä määräyksessä internet-liikenteen estämistä tai rajoittamista ennalta määriteltyjen sääntöjen mukaisesti.

Suodattamisella voidaan tarkoittaa esimerkiksi asiakasliittymästä lähtevän, väärennettyjä lähdeosoitteita käyttävän internet-liikenteen hylkäämistä. Osoitteet voidaan todeta väärennetyiksi vertaamalla osoitteita asiakkaalle myönnettyihin osoiteavaruuksiin.

Suodattamisella voidaan tarkoittaa myös tietyn tyyppisen internet-liikenteen kapasiteetin rajoittamista liittymäkohtaisesti tai liikennöinnissä käytettyyn sovellusprotokollaan perustuen.

Liikenteen suodattaminen ilman palvelun käyttäjän antamaa suostumusta on mahdollista, mikäli toimenpiteet ovat tarpeen viestintäverkon tai -palvelun tietoturvaan kohdistuvan uhan torjumiseksi tai palvelun tietoturvasta huolehtimiseksi. Suodatustoimenpiteitä toteutettaessa teleyrityksen tulee ottaa huomioon SVTSL:n 5 luvun lisäksi myös muun muassa VML:ssa asetetut vaatimukset.

## 5 3 § ASIAKASLIITTYMIEN TIETOTURVALLISUUS

### 5.1 Käyttäjien liikenteen erottaminen toisistaan

Määräyksen mukaan *teleyrityksen on erotettava asiakasliittymien liikenne siten, etteivät eri asiakasliittymien käyttäjät voi oikeudettomasti seurata toistensa liikennettä. Teleyrityksen tulee varmistaa, että liikenteen oikeudeton uudelleenohjaus liittymien välillä ei ole mahdollista.*

*Sen estämättä, mitä 1 momentissa määrätään, teleyritys voi tarjota salaamattomia WLAN-yhteyksiä ilman radiorajapinnassa tapahtuvaa liikenteen erottamista.*

#### Perustelut

Jaettua kapasiteettia tilaajien kesken käytäviä internet-liittymiä on käytetty esimerkiksi taloyhtiöverkkoja toteutettaessa. Näissä verkkototeutuksissa taloyhtiöön tuotava internet-yhteys jaetaan taloyhtiön käyttäjien kesken käyttämällä joko taloyhtiön tai teleyrityksen verkkolaitteita. Vastaavanlaisia jaettua kapasiteettia käytäviä verkkototeutuksia käytetään esimerkiksi kaupunkiverkoissa, joissa palvelun käyttö on avointa kaikille verkon kantaman oleskeleville käyttäjille.

Salaamattomat WLAN-yhteydet ovat yleisesti käytössä erityisesti paikoissa jossa on paljon liikkuvia tilaajia. WLAN-yhteyksien salaaminen on teknisesti mahdollista, mutta salauksen toteuttaminen, erityisesti salausavainten hallinta, vaikeuttaisi palvelun tarjoamista merkittävästi. Tästä syystä salaamattomista WLAN-yhteyksistä on säädetty erityinen poikkeus salaamattomien WLAN-yhteyksien sallimiseen ilman radiorajapinnassa tapahtuvaa liikenteen erottamista.

#### Soveltaminen

Tilaaajien liikenteen erottaminen toisistaan voidaan toteuttaa käytännössä esimerkiksi liikenteen fyysisellä erottamisella omiin johtoihinsa tai erottamalla liittymien liikenne loogisesti liittymäkohtaisten VLAN:ien taikka liikenteen salauksen avulla. Tilaaajien liikenteen erottamiseen voidaan myös käyttää DSLAM-keskittimien tai kytkimien port isolation -toiminnetta, etenkin tapauksissa joissa käytetään ryhmä-VLAN -tunnistetta.

WLAN-yhteyksillä tarkoitetaan IEEE-standardin 802.11 mukaisia langattomia lähiverkkoyhteyksiä.

## **6 4 § TIEDOTTAMINEN**

### **6.1 Tiedottaminen asiakkaalle**

Määräyksen mukaan *teleyrityksen on tiedotettava asiakkaalle viimeistään asiakasliittymää käyttöönotettaessa liittymän käyttämiseen liittyvistä yleisistä ja liittymätyyppikohtaisista tietoturvariskeistä sekä asiakkaan käytettävissä olevista toimenpiteistä tietoturvasta huolehtimiseksi.*

#### Perustelut

Teleyrityksen asiakkaihin kohdistamalla yleisellä tietoturvatiedotuksella lisätään asiakkaiden tietoisuutta internet-yhteyksien ja -palveluiden yleisistä tietoturvariskeistä. Merkittävä osa raportoiduista asiakkaiden tietoturvaongelmista voidaan välttää, jos asiakas on asianmukaisesti huolehtinut päätelaitteiden perustietoturvasta ja internet-palveluja käytetään tietoturvauhat huomioiden.

Huonosti ylläpidetyt päätelaitteet ja huolimaton internet-palvelujen käyttö vaarantavat asiakkaan oman päätelaitteen tietoturvan lisäksi myös muiden internet-käyttäjien ja internet-palveluja tarjoavan teleyrityksen palveluiden tietoturvan.

Lisäksi on tärkeää, että asiakkaille on mahdollisuus liittymätyyppikohtaisilta tietoturvauhilta suojautumiseen. Tämän vuoksi teleyrityksen tuleekin pitää huolta siitä, että asiakas saa tiedon liittymätyyppikohtaisista tietoturvariskeistä sekä käytettävissä olevista toimenpiteistä tietoturvasta huolehtimiseksi ennen liittymän kytkemistä.

#### Soveltaminen

##### *Tiedottaminen yleisistä tietoturvariskeistä*

Tiedottaminen voi tapahtua käytettävästä palvelusta riippuen esimerkiksi liittymää tilattaessa tai viimeistään asiakkaan aloittaessa liittymän käyttämisen. Ratkaisevaa on se, että tiedot on toimitettu asiakkaalle ennen liittymän aktiivisen käyttämisen aloittamista.

Teleyritys voi täyttää tiedottamisvelvollisuutensa esimerkiksi liittämällä tarvittavat tiedot sopimusasiakirjojen yhteyteen. Tiedottaminen voi kuitenkin tapahtua myös muutoin, mikäli käytettävä palvelu sen mahdollistaa. Siten tiedottaminen on mahdollista järjestää myös esimerkiksi yhteyden käyttöönoton mahdollistavalla kirjautumissivulla tai sähköisen sopimuksen toimittamisen yhteydessä. Teleyrityksen verkkosivuilla oleva yleinen tietoturvatiedotus, johon asiakasta ei liittymää käyttöönotettaessa nimenomaisesti ohjata tutustumaan, ei täytä kohdassa asetettuja vaatimuksia. Asiakas ei välttämättä tule edes vierailleeksi mainitulla sivustolla.

Viestintävirasto ylläpitää verkkosivua yleisimmistä tietoturvauhkista. Teleyritys voi huolehtia asiakastiedotuksesta myös ohjaamalla asiakas Viestintäviraston ylläpitämälle sivustolle.

Tiedottamisen pääasiallisen sisällön tulee painottua asiakkaan tai asiakasliittymän käyttäjän käytettävissä oleviin keinoihin oman päätelaitteensa tietoturvallisuudesta huolehtimiseksi. Tällaisia keinoja ovat esimerkiksi liikenteen salaaminen, käyttäjien liikenteen eriyttäminen, ohjelmistopalomuurin käyttöönotto ennen tietokoneen liittämistä verkkoon, virustorjunnan hankkiminen ja käyttöjärjestelmän sekä muiden ohjelmistojen päivittämisestä huolehtiminen.

##### *Tiedottaminen liittymätyyppikohtaisista tietoturvariskeistä*

Liittymätyyppikohtaisilla tietoturvariskeillä tarkoitetaan liittymän teknisestä toteutustavasta johtuvia erityisiä riskejä. Esimerkkinä riskistä voidaan mainita internet-yhteyspalvelun tarjoaminen salaamattoman WLAN-yhteyden avulla. Tällaisissa tilanteissa teleyrityksen on tiedotettava liittymän käyttämiseen liittyvistä viestinnän luottamuksellisuuden kohdistuvista erityisistä riskeistä.

Tiedottamisvelvoite tulee sovellettavaksi myös esimerkiksi silloin kun teleyritys tarjoaa liittymiä yhteisötilaajille, jotka sitten tarjoavat liittymiä edelleen omille loppukäyttäjilleen. Esimerkkinä tällaisesta palvelusta voidaan mainita taloyhtiöiden asukkailleen hankkimat tietoliikenneyhteydet. kuten. Teleyrityksen tulee tiedottaa asiakkaalleen kapasiteetin jakoon liittyvistä tietoturvariskeistä.

## 6.2 Asiakastiedotus liittymän teknisten rajoitusten osalta

Määräyksen mukaan *teleyrityksen on määriteltävä sekä kuvattava asiakkaalle keskeiset asiakasliittymän käyttöön vaikuttavat pysyväisluonteiset tekniset rajoitukset. Nämä voivat koskea käytettäviä tietoliikenneportteja, -protokollia tai liikennemäärää. Kuvauksesta on myös käytävä ilmi periaatteet, joilla puututaan viestintäpalvelujen tietoturvaa vaarantavaan liittymän tai palvelujen käyttöön.*

### Perustelut

Asiakasliittymän käyttöön vaikuttavat tekniset rajoitukset ovat liittymän keskeisiä perusominaisuuksia. Rajoitukset vaikuttavat muun muassa siihen, millaisiin tietoturvariskeihin asiakkaan on syytä varautua itse ja mitä palveluja asiakas voi liittymän kautta käyttää. Tämän takia rajoitusten asianmukainen kuvaaminen on tärkeää.

### Soveltaminen

Pysyväisluonteisilla teknisillä rajoituksilla tarkoitetaan erikseen asetettuja rajoitteita tai operaattorin verkon ominaisuuksista johtuvia tekijöitä, jotka vaikuttavat liittymän käyttöön. Tällaisia ovat esimerkiksi:

- tuettavat IP-protokollaversiot
- tietoliikenneportit joihin liikennöinti on estetty tai liikennettä on rajoitettu
- mahdolliset sovellusprotokolla- tai sovelluskohtaiset rajoitukset
- mahdollinen liittymäraja- tai rajapinnassa toteutettava osoitemuunnos (NAT)
- liikenteen priorisointiperiaatteet, esimerkiksi liikenteen priorisointi tietyn liikennemäärän ylityttyä
- suurin sallittu MTU-koko, mikäli se on alle 1500 tavua

Tämän lisäksi teleyrityksen on kuvattava periaatteet, joilla puututaan viestintäpalvelujen tietoturvaa vaarantavaan liittymän tai palvelujen käyttöön.

Liikennöintirajoja koskevan kuvauksen ei tarvitse olla niin yksityiskohtainen, että se itsessään vaarantaisi teleyrityksen palvelun tietoturvaa esimerkiksi antamalla liian yksityiskohtaisen kuvan käytettävistä suodatusmenetelmistä, Kuvaus on mahdollista toteuttaa esimerkiksi palvelukuvauksen yhteydessä tai teleyrityksen www-sivustolla.

Väliaikaisia teknisiä rajoituksia ei tarvitse kuvata. Tällaisia väliaikaisia rajoituksia voivat olla esimerkiksi akuutin tietoturvatilanteen selvittämisen yhteydessä tehtävät toimenpiteet.

Asetettaessa uusia tai muutettaessa olemassa olevia käyttörajoituksia liittymäsopimuksen voimassaoloaikana, on teleyrityksen otettava huomioon liittymäsopimuksen antama liikkumavara. Jos uudet rajoitukset voidaan katsoa liittymäsopimuksen yksipuoliseksi muuttamiseksi, tulee noudattaa lainsäädännössä sopimuksen muuttamiselle asetettuja menettelytapoja. Kuluttaja-asiakkaiden osalta vakiosopimusehdoista ja sopimuksen muuttamisesta on pakottavia säännöksiä VML:ssa.

## **7 5 § KULUTTAJALIITTYMÄSTÄ LÄHTEVÄN SÄHKÖPOSTILIIKENTEEN OHJAUS JA REITITYS**

### **7.1 Kuluttajaliittymästä lähtevän rajoittamattoman SMTP-liikenteen estäminen**

Määräyksen mukaan *internet-liittymiä tarjoavan teleyrityksen on estettävä kuluttajaliittymistä lähtevä rajoittamaton SMTP-liikenne muuten kuin sovittujen lähtevälle SMTP-liikenteelle tarkoitettujen palvelimien kautta.*

#### Perustelut

Rajoittamaton SMTP-liikenne (portti 25) liittymästä internet-verkkoon mahdollistaa haittaohjelmille roskasähköpostiviestien lähettämisen. Sallimalla lähtevä sähköpostiliikenne vain teleyrityksen lähtevälle SMTP-liikenteelle tarkoitettujen palvelimien kautta voidaan tehokkaasti rajoittaa haittaohjelmien tuottamien roskapostiviestien lähettämistä. Rajoitus ei vaikuta käyttäjien viestintämahdollisuuksiin, koska sähköpostia on mahdollista lähettää internet-liittymän tarjoavan teleyrityksen postipalvelimen kautta, tunnistettua sähköpostin lähetystä (Mail Submission, RFC 4409 [9] ) käyttäen tai www-pohjaisten sähköpostipalveluiden käyttöliittymien kautta.

Määräyksellä vahvistetaan IETF:n dokumentissa RFC 5068 [10] kuvatut parhaat käytännöt sähköpostin lähetysmenetelmistä.

#### Soveltaminen

Rajoittamattoman SMTP-liikenteen estämisellä tarkoitetaan teleyrityksen kuluttajaliittymille tarkoittamasta verkkoavaruudesta muiden kuin teleyrityksen lähtevälle SMTP-liikenteelle tarkoitettujen palvelinten tietoliikenneporttiin 25 suuntautuvan liikenteen estämistä.

Määräyksen mukaisesti toteutetulla rajoittamattoman SMTP-liikenteen estolla ei saa olla vaikutusta muita tietoliikenneportteja käyttävään sähköpostiliikennöintiin, kuten käyttäjätunnistusta tai salausta käyttäviin sähköpostiprotokolliin. Erityisesti tulee huolehtia, että rajoitus ei koske liikennettä IETF:n dokumentissa RFC 4409 [9] kuvattuun Mail Submission -palvelun käyttämään porttiin 587. Näin internet-liittymiä tarjoavan teleyrityksen asiakkailta on mahdollisuus liikennöidä turvallisesti ja tunnistetusti myös toisen palveluntarjoajan hallinnassa olevaan sähköpostijärjestelmään.

### **7.2 Kuluttajaliittymästä lähtevän SMTP-liikenteen salliminen erityistapauksissa**

Määräyksen mukaan *sen estämättä, mitä 1 momentissa määrätään, teleyritys voi sallia rajoittamattoman SMTP-liikenteen muutenkin kuin sovittujen lähtevälle SMTP-liikenteelle tarkoitettujen palvelimien kautta. Tällöin teleyrityksen on tiedotettava liittymän tilaajalle avoimeen liikennöintiin liittyvistä riskeistä. Teleyrityksellä on oltava myös valmiudet reagoida nopeasti häiriötilanteisiin.*

#### Perustelut

Rajoittamattoman SMTP-liikenteen salliminen tarkoittaa sitä, että teleyrityksen kuluttajaliittymälle tarkoittamasta verkkoavaruudesta voi lähettää teleyrityksen verkon ulkopuolelle SMTP-liikenteelle varattuun tietoliikenneporttiin 25 suuntautuvaa liikennettä.

Joillakin kuluttaja-asiakkailta voi olla perusteltuja tarpeita suoralle SMTP-liikenteelle kuluttajaliittymästä minne tahansa teleyrityksen verkon ulkopuolelle. Tällainen tarve on esimerkiksi kuluttaja-asiakkaan hallitessa SMTP-liikennettä oman palvelimensa kautta.

#### Soveltaminen

Teleyrityksen on kerrottava liittymän tilaajalle avoimeen liikennöintiin liittyvistä tietoturvariskeistä. Teleyrityksellä on oltava myös valmiudet reagoida nopeasti häiriötilanteisiin.

## **8 6 § HAITALLISEN LIIKENTEEN HAVAITSEMINEN**

### **8.1 Haitallisen liikenteen havaitseminen**

Määräyksen mukaan *teleyrityksen on seurattava ja tarpeen mukaan selvitettävä oman viestintäverkkonsa tapahtumia sellaisen liikenteen havaitsemiseksi, joka aiheuttaa vaaraa viestintäverkon tai -palvelun tietoturvalle. Teleyrityksellä on oltava valmius virheellisiä lähdeosoitteita sisältävän liikenteen jäljittämiseen.*

*Teleyrityksen on myös varustettava viestintäverkkonsa asianmukaisella havainnointikyvyllä 1 momentissa määrättyjen toimenpiteiden mahdollistamiseksi.*

#### Perustelut

Velvoitteen tarkoituksena on varmistaa, että teleyrityksillä on tarvittavat toimintamenetelmät ja järjestelmät haitallisen liikenteen ja erilaisten häiriötilanteiden havaitsemiseksi. Esimerkkejä havainnointikykyä vaativista tilanteista voivat olla nopeasti leviävän haittaohjelman aiheuttama tiettyyn tietoliikenneporttiin suuntautuva liikenne, palvelunestohyökkäys tai verkon reitityksen häiriö. Teleyrityksen viestintäverkkoon suuntautuvan haitallisen liikenteen tai haitallisten tapahtumien havaitseminen mahdollistaa viestintäverkon tietoturvasta huolehtimisen.

Virheellisiä lähdeosoitteita sisältävää liikennettä käytetään tyypillisesti palvelunestohyökkäyksissä. Tämäntyyppisen liikenteen lähteen selvittämisellä pyritään siihen, että haitallisen liikenteen vaikutuksia palvelun tai käyttäjän tietoturvalle voidaan rajoittaa tai torjua.

#### Soveltaminen

Teleyrityksen on varustettava viestintäverkkonsa järjestelmällä, joka mahdollistaa haitallisen liikenteen havaitsemisen. Järjestelmän tulee kyetä tarvittaessa seuraamaan viestintäverkon liikennettä tarkoituksenmukaisella näytteenottotarkkuudella.

Teleyrityksen viestintäverkon tietoliikenteen suuren volyymin vuoksi haitallisen liikenteen havaitsemisen mahdollistavaa järjestelmää ei useinkaan voida toteuttaa vaikuttamatta merkittävästi verkon suorituskykyyn. Tällöin tiedon kerääminen voi perustua liikenteestä otettuihin näytteisiin, jolloin tarkastellaan vain osaa verkossa välitettävistä paketeista. Näytteenottotarkkuus on valittava sellaiseksi, että näytteiden avulla saadaan riittävän tarkka kuva verkon liikenteestä.

Teleyritys voi käyttää esimerkiksi verkon liikennemääriä tai poikkeuksellisia tapahtumia seuraavaa automaattista hallintajärjestelmää, jolloin ennalta määritettyjen raja-arvojen ylittyessä välittyy hälytys tapahtumien valvontajärjestelmään. Lisäksi verkon tietoturvatapahtumien hallinnassa voidaan käyttää esimerkiksi tunkeutumisen havaitsemis- ja estojärjestelmiä.

Teleyrityksellä on oltava ennalta suunnitellut ja harjoitellut toimintamallit ja käytännöt, jotka mahdollistavat haitallisen liikenteen alkuperän selvittämisen myös siinä tapauksessa, että haitallinen liikenne sisältää virheellisiä lähdeosoitteita. Haitallisen liikenteen lähde on pystyttävä viipymättä tunnistamaan teleyrityksen omassa verkossa asiakasliittymän tarkkuudella. Yhteenliittämisrajapintoihin liittyvistä velvoitteista on säädetty Viestintäviraston määräyksessä 28 [6].

## **9 7 § HAITALLISEN LIIKENTEEN SUODATTAMINEN**

### **9.1 Liikenteen tilapäisen suodattamisen prosessit ja toimintamallit**

Määräyksen mukaan *teleyrityksellä on oltava prosessit ja toimintamallit, joiden mukaisesti liikennettä suodatetaan tilapäisesti tilanteissa, jotka aiheuttavat vaaraa viestintäverkon tai -palvelun tietoturvalle. Teleyrityksellä tulee olla tekninen valmius näihin toimenpiteisiin.*

#### Perustelut

Teleyrityksellä tulee olla valmiit prosessit ja toimintamallit haitallisen liikenteen tilapäiseen suodattamiseen, jotta se saadaan suodatettua mahdollisimman nopeasti viestintäverkosta pois. Teleyrityksen tulee huolehtia, että prosessit ja toimintamallit ovat ajan tasalla.

Liikenteen suodattamisella voidaan esimerkiksi rajoittaa sellaisten palvelunestohyökkäysten vaikutusta, joissa käytetään tietyn tyyppistä hallintaliikennettä kuormittamaan verkossa olevia järjestelmiä. Lisäksi toimenpiteillä voidaan rajoittaa tiettyyn porttiin liikennöivän haittaohjelman liikennettä.

### Soveltaminen

Viestintäverkon tai -palvelun tietoturvaa vaarantavassa tilanteessa teleyritys voi joutua ottamaan käyttöön tilapäisiä toimenpiteitä esimerkiksi kyseiseen tietoliikenneporttiin asiakasliittymiin ja asiakasliittymistä suuntautuvan liikenteen estämiseksi tai liikenteen rajoittamiseksi asiakasliittymistä tiettyihin kohdeosoitteisiin.

Suodatustoimenpiteet tulee keskeyttää, kun viestintäverkon tai -palvelun tietoturvaa vaarantava uhkatilanne on päättynyt.

Teknisellä valmiudella suodattamiseen tarkoitetaan esimerkiksi sitä, että internet-palveluntarjoajan verkkoelementit tukevat liikennemäärien protokolla-, osoite-, portti- ja verkkoliityntäkohtaista rajoitusta. Liikennemäärien rajoitus tulee voida toteuttaa verkon käytettävyyttä tarpeettomasti vaarantamatta. Lisäksi tekninen valmius edellyttää, että teleyrityksen verkon operointikeskuksella on kyky käynnistää tarvittavat suodatustoimet.

Liikennemääriä rajoittavien verkkoelementtien tulee tarvittaessa pystyä tallentamaan tarkoituksenmukaiset tapahtumatiedot suodatustapahtumista. Tällaisia tietoja voivat olla esimerkiksi liikenteen lähde- ja kohdeosoitteet, lähde- ja kohdeportit sekä tieto mitä liikenteelle tehtiin. Tarkoituksenmukaisuutta arvioitaessa tulee huomioida esimerkiksi riittävä näytteenottotarkkuus. Tapahtumatiedot ovat tarpeellisia esimerkiksi ongelmanselvitystä, verkkohyökkäysten selvitystä tai tunnistamista varten. Verkkoelementin tulee tukea myös tapahtumatietojen ajantasaisia analyysejä. Tapahtumatiedot tulee aikaleimata ja ajastuksessa tulee käyttää keskitettyä oikea-aikaista aikalähdettä.

## **9.2 Virheellisiä lähdeosoitteita sisältävän liikenteen suodattaminen**

Määräyksen mukaan *teleyrityksen on suodatettava sellainen asiakasliittymästä viestintäverkkoon suuntautuva liikenne, jonka lähdeosoite ei ole kyseiselle asiakasliittymälle osoitettu. Teleyrityksen on toteutettava suodatus asiakasrajapintaa lähimpänä olevassa verkkoelementissä, jossa suodatus on teknisesti tarkoituksenmukaisinta toteuttaa.*

### Perustelut

Hajautetuissa palvelunestohyökkäyksissä pyritään usein vaikeuttamaan hyökkääjän löytämistä käyttämällä liikennöinnissä väärennettyjä lähdeosoitteita. Liikenteen lähteeksi voidaan väärentää esimerkiksi hyökkäykseen liittymätön ulkopuolinen verkko tai satunnaisesti valittu kohdeverkon osoite. Väärennetyt lähdeosoitteet saattavat olla myös satunnaisesti valittuja osoitteita yksityiseen käyttöön tai erityisiin tarkoituksiin varatuista osoiteavaruuksista.

Vaatimuksilla pyritään rajoittamaan väärennettyjä IP-lähdeosoitteita käyttävien hyökkäysten aiheuttamia ongelmia.

### Soveltaminen

Väärennettyjä lähdeosoitteita käyttävän liikennöinnin estämiseksi asiakasliittymiä tarjoavan teleyrityksen on suodatettava sellainen asiakasliittymästä viestintäverkkoon suuntautuva liikenne, jonka lähdeosoite ei ole kyseiselle asiakasliittymälle osoitettu. Teleyrityksen on tarvittaessa pystyttävä selvittämään asiakasliittymä, josta verkkoon suuntautuvassa liikenteessä käytetään väärennettyjä lähdeosoitteita.

Suodatus voidaan toteuttaa esimerkiksi vertaamalla jokaisen rajapinnassa vastaanotetun paketin lähdeosoitetta hyväksyttävien osoiteavaruuksien listaan ja hylkäämällä jokainen paketti, jonka lähdeosoite ei kuulu listalla oleviin osoiteavaruuksiin.

Esimerkiksi ADSL-yhteyden tapauksessa suodatus voidaan toteuttaa keskittimen DSLAM-verkkoelementissä, DSL-verkon yhteyksien terminointilaitteessa tai runkoverkon reitittimessä. Suodatuksen tarkoituksenmukainen toteutuspiiste riippuu verkkolaitteiden tekniikan suodatuskyvystä tai teleyrityksen käytännöistä toteuttaa suodatus.

### 9.3 Käyttäjän tunnistaminen

Määräyksen mukaan *liikenteen suodattamista lievempänä toimenpiteenä asiakkaaseen voidaan ottaa yhteyttä tietoturvaa vaarantavan tilanteen selvittämistä varten.*

#### Perustelut

SVTSL:n mukaan teleyritys voi estää tai rajoittaa viestien välittymisen asiakkaan päätelaitteeseen estääkseen viestintäverkkoihin tai niihin liitettyihin palveluihin kohdistuvia tietoturvauhkia ja häittää aiheuttavia häiriöitä. Viestintäviraston tulkinnan mukaan on selvää, että liikenteen rajoitustoimenpiteitä lievempänä toimenpiteenä teleyritys voi selvittää tietoturvauhan tai häiriön aiheuttavan käyttäjän henkilöllisyyden ja olla käyttäjään tai tämän edustajaan yhteydessä uhkan tai häiriön poistamiseksi. Jos käyttäjää tai tämän edustajaa ei kuitenkaan tavoiteta tai uhkaa ei muuten saada poistettua, voi teleyritys ryhtyä liikenteen rajoitustoimenpiteisiin.

#### Soveltaminen

Teleyrityksen oikeus käsitellä tunnistamistietoja asiakkaan tunnistamiseksi on kuvattu kappaleessa 1.3.1. Toimenpiteet on toteutettava huolellisesti ja ne on mitoitettava torjuttavan häiriön vakavuuteen. Toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä tunnistamistietojen käsittelyn tavoitteen turvaamiseksi.

### 9.4 Osoite- ja reittisuodatus

Määräyksen mukaan, *mikäli teleyritys käyttää erityisiin tarkoituksiin varattuihin tai käyttämättömiin osoiteavaruuksiin perustuvaa suodatussäännöstöä liikenteen tai reititystiedon suodattamiseen, on teleyrityksen huolehdittava käytettävän suodatussäännöstön ajantasaisuudesta.*

#### Perustelut

Suodatuslistoja käytettäessä tulee kiinnittää erityistä huomiota suodatussäännöstön ajantasaisuuteen, jotta vanhentunut suodatussäännöstö ei rajoita jo myönnettyjen IP-verkkoresurssien asianmukaista käyttöä. Teleyrityksen tulee tarkistaa suodatussäännöstön ajantasaisuus säännöllisesti.

#### Soveltaminen

Suodatusta voidaan tehdä sekä käyttämättömien osoiteavaruuksien kaappauksen estämiseksi reittimainostuksista että palvelunestohyökkäysliikenteen rajoittamiseksi liikenteen lähdeosoitteista. Koska palvelunestohyökkäyksissä käytetään säännöllisesti myös puhtaasti väärennettyjä, mutta reitittyviä lähdeosoitteita, osoitesuodatuksen tarvetta ja päivitysmekanismeja kannattaa harkita huolella.

Reititystiedon tai liikenteen suodatusta tehtäessä teleyrityksen vastuu on huolehtia suodatuslistan ajantasaisuudesta, jotta voidaan välttää esimerkiksi juuri käyttöön otetun osoiteavaruuden suodattuminen.

Suodatettavia osoiteavaruuksia voivat olla ns. bogon-prefixit, joilla tarkoitetaan yksityiseen käyttöön (RFC 1918) tai erityisiin tarkoituksiin varattuja osoiteavaruuksia, joita ei ole tarkoitettu käytettäväksi avoimesti internet-verkossa. Lisäksi suodatettavia osoiteavaruuksia voivat olla

IANAn (Internet Assigned Numbers Authority) tai paikallisten internet-osoiterekistereiden toistaiseksi käyttöön luovuttamattomat verkot.

Bogon-suodatusta tehtäessä voidaan käyttää esimerkiksi luotettavien tahojen tarjoamaa BGP (Border Gateway Protocol) -reititystietoa, jossa osoiteavaruuksien käytössä tapahtuvat muutokset tehdään suodatustunnusmerkistöön keskitetyksi.

Laitteiden mukana tulevia default-bogon listoja ei tule käyttää, koska ne ovat vanhentuneita.

## 9.5 Suodatustoimenpiteiden toteuttaminen

On huomattava, että SvTSL 20 §:n 4 momentin mukaan suodatustoimenpiteet on toteutettava huolellisesti ja ne on mitoitettava torjuttavan häiriön vakavuuteen. Toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä toimenpiteelle asetettujen tavoitteiden turvaamiseksi. Toimenpiteet on lopetettava, jos niiden toteuttamiselle ei enää laissa säädettyjä edellytyksiä.

## 10 8 § LIITTYMÄN IRTIKYTKEMINEN

### 10.1 Asiakasliittymien irtikytkeminen

Määräyksen mukaan *teleyrityksen on kytkettävä asiakasliittymä tai sen palvelu irti yleisestä viestintäverkosta, jos viestintäpalvelun tietoturva oleellisesti vaarantuu liittymästä johtuvista syistä.*

#### Perustelut

Asiakasliittymän toiminta voi vaarantaa olennaisesti viestintäpalvelun tietoturvaa esimerkiksi tilanteissa, jossa liittymän takana oleva haittaohjelmartunnan saanut järjestelmä lähettää liittymästä suuria määriä roskapostia tai haittaohjelmia. Teleyrityksen verkkoon liitetyt saastuneet päätelaitteet vaarantavat aina teleyrityksen palveluiden tietoturvaa siinä määrin, että teleyrityksellä on oikeus aloittaa toimenpiteet saastuneen päätelaitteen aiheuttaman uhkan poistamiseksi.

#### Soveltaminen

Asiakasliittymän palvelun irtikytkemisellä yleisestä viestintäverkosta tarkoitetaan tässä määräyksessä esimerkiksi niiden tietoliikenneporttien tilapäistä sulkemista asiakasliittymästä, joihin suuntautuva liikenne vaarantaa viestintäpalvelun tietoturvaa. Vastaavasti teleyritys voi joutua rajoittamaan tiettyjen sovellusprotokollien liikennöintiä asiakasliittymästä, mikäli liikenne vaarantaa viestintäpalvelun tietoturvaa. Asiakasliittymästä johtuvilla syillä ei tyypillisesti tarkoiteta sitä, että asiakasliittymä tai asiakasliittymän kautta verkkoon kytketty www-palvelu on esimerkiksi palvelunestohyökkäyksen kohteena ja näin vastaanottaa poikkeuksellisen paljon liikennettä tiettyssä tilanteessa.

Tietoturvasta huolehdittaessa ja irtikytkemistilanteissa on syytä kiinnittää huomiota siihen, että viestinnän tunnistamistietoja on oikeus käsitellä ainoastaan viestintäverkkoihin ja -palveluihin kohdistuvissa tietoturvauhka tai -loukkaustilanteissa. Teleyrityksellä ei siten ole oikeutta käsitellä tunnistamistietoja esimerkiksi estääkseen liittymän käyttämisen palvelun tietoturvaa vaarantamattoman rikoksen suorittamiseen. Poikkeuksen tähän sääntöön muodostaa kuitenkin SVTsL:n 20 §:n 1 momentin 3 kohdassa tarkoitettu maksuvälinepetoksen valmistelu.

### 10.2 Irtikytkentäprosessin ohjeistus

Määräyksen mukaan *liittymän irtikytkeminen ja takaisinkytkeminen on toteutettava teleyrityksen ennalta määrittelemien prosessien ja toimintaohjeiden mukaisesti. Toimenpiteitä toteutettaessa voidaan ottaa huomioon liittymätyypistä johtuvat erityisolosuhteet ja tietoturvauhan vakavuusaste.*

#### Perustelut

Liittymän irtikytkeminen estää asiakasta käyttämästä kyseistä liittymää. Tästä syystä irtikytkemisprosessi on suunniteltava ja ohjeistettava yksityiskohtaisesti. Tehtyjen toimenpiteiden

ja käydyin viestinnän asianmukaisella kirjauksella varmistetaan teleyrityksen ja teleyrityksen asiakkaiden oikeusturva.

### Soveltaminen

Mikäli mahdollista, asiakkaaseen tulee olla yhteydessä ennen liittymän irtikytkemistä yleisestä viestintäverkosta esimerkiksi puhelimitse tai sähköpostitse. Asiakkaan kuuleminen ei saa kuitenkaan tarpeettomasti vaarantaa palvelun tietoturvasuudesta huolehtimista.

Irtikytkemiseen liittyvät toimenpiteet tulee toteuttaa ennalta määriteltyjen prosessien mukaisesti. Tehdyt toimenpiteet ja erityisesti syy liittymän irtikytkemiseen tulee kirjata tilanteen mahdollista jälkikäteen tapahtuvaa selvittämistä varten.

Irtikytkemiseen liittyvien toimintaohjeiden tulee sisältää tarpeelliset menettelyt asiakasliittymän takaisinkytkemiseksi viestintäverkkoon, kun teleyritys on todennut että viestintäpalveluun kohdistuva tietoturvaohje on poistunut. Esimerkiksi haittaohjelman aiheuttaman haitallisen liikennöinnin yhteydessä liittymä voidaan kytkeä takaisin viestintäverkkoon asiakkaan otettua yhteyttä teleyritykseen ja ilmoitettua poistaneensa haittaohjelman järjestelmästä.

Palvelu- ja verkko-operaattori sopivat keskenään irtikytkemisen käytännön toteuttamiseen liittyvät periaatteet. Molemmilla osapuolilla tulee olla mahdollisuus toteuttaa tarvittavat toimenpiteet palvelunsa tai verkkonsa tietoturvasuudesta huolehtimiseksi. Irti- ja takaisinkytkemisestä on ilmoitettava toiselle osapuolelle viipymättä.

Toimenpiteitä toteutettaessa voidaan ottaa huomioon liittymätyypistä johtuvat erityisolosuhteet. Esimerkiksi palveluntarjoajille suunnatuissa liittymätyypeissä häiriötilanteiden toimintamalleista voidaan sopia siten, että palveluiden tarjoamiselle aiheutuvat haitat olisivat mahdollisimman vähäiset. Esimerkiksi matkaviestinliittymien mobiilidatapalveluihin liittyvissä tietoturvaongelmissa matkaviestinliittymästä voidaan estää vain mobiilidatapalvelun käyttö kunnes tietoturvaongelma on selvitetty.

Mikäli asiakasliittymät ovat automaattivalvonnan piirissä, asiakasliittymien tai asiakasliittymän tiettyjen palvelujen irtikytkeminen viestintäverkosta tapahtuu tyypillisesti tarvittaessa automaattisesti esimerkiksi puolen tunnin ajaksi ilman operaattorin toimenpiteitä haitalliselle liikennöinnille asetettujen raja-arvojen ylityksessä. Liittymän ollessa irtikytkettynä asiakkaan liikenne voidaan ohjata palveluun, jossa asiakkaalle kerrotaan irtikytkemisen syy sekä mahdolliset asiakkaan toimenpiteet asiakkaan laitteen korjaamiseksi. Lisäksi asiakkaalla voi olla mahdollisuus liikennöidä tarvittaville sivustoille esimerkiksi virustorjunnan asentamiseksi ja käyttöjärjestelmän ohjelmistopäivitysten suorittamiseksi. Tämä toimintamalli vähentää tarvetta asiakasliittymien pysyvämpään irtikytkemiseen.

Käytettäessä automaattisia järjestelmiä asiakasliittymien sulkemiseen ja avaamiseen palvelun tietoturva huolehtimiseksi, asiakkaalle tulee kertoa liittymän tilapäiseen sulkemiseen ja avaamiseen liittyvät periaatteet.

## **11 9 § TIETOTURVALOUKKAUSTAPAUSTEN KÄSITTELY JA TILASTOINTI**

### **11.1 Yhteysosoitteet tietoturvaloukkaustapausten ilmoittamista varten**

Määräyksen mukaan *teleyrityksen on huolehdittava, että sillä on käytössään yhteysosoitteet tietoturvaloukkaustapausten ilmoittamista varten. Yhteysosoitteet on julkaistava teleyrityksen verkkosivuilla asianmukaisessa osiossa.*

### Perustelut

Asianmukaiset ja helposti löydettävissä olevat yhteysosoitteet helpottavat tietoturvaloukkaustapausten käsittelyä teleyrityksessä. Tieto tietoturvaloukkaustapauksesta voidaan ohjata suoraan kyseisiä tilanteita käsitteleville tahoille. Yhteysosoitteita tarvitaan myös abuse- ja irt-yhteystietojen rekisteröintiin alueelliseen verkkorekisteriin.

### Soveltaminen

Vähimmäistasona voidaan pitää sähköpostiosoitetta, johon lähetetyt viestit ohjautuvat teleyrityksen tietoturvaloukkauksia käsittelevälle taholle. Yleinen käytäntö on, että sähköpostiosoite on muotoa abuse@teleyrityksen\_verkkotunnus.

Tieto yhteysosoitteista on julkaistava tarkoituksenmukaisessa kohdassa teleyrityksen verkkosivuilla.

Teleyrityksen on otettava huomioon myös Viestintäviraston määräyksen 28 H/2010 M 4§ velvoitteet ja kyseiseen määräykseen liittyvän MPS 28 -dokumentin 6.3 -kohdan soveltamisohjeet IP-osoitelohkojen dokumentoinnista asiaankuuluvine abuse- ja irt-kontaktitietoineen internet-osoiterekisterin tietokantaan.

#### 11.1.1 Suosituksia

Tietoturvaloukkaustapauksiin ja tietoturvaan liittyvä ohjeistus ja yhteystiedot on suositeltavaa julkaista teleyrityksen www-palvelussa omana sivunaan, johon on koottu myös asiakkaan omatoimiseen tietoturvaloukkaustapausten selvittelyyn liittyvä ohjeistus.

Yhteystiedot on suositeltavaa julkaista myös englanniksi.

### 11.2 Tietoturvaloukkausten käsittely

Määräyksen mukaan *teleyrityksen on käsiteltävä ja rekisteröitävä sen tietoon tulleet teleyrityksen palveluita ja asiakkaita koskevat tietoturvaloukkaustapaukset asianmukaisesti.*

#### Perustelut

Teleyrityksen palvelun tietoturvasta huolehtiminen edellyttää teleyrityksen tietoon tulleiden teleyritysten palveluita ja asiakkaita koskevien tietoturvaloukkaustapausten tehokasta ja tarkoituksenmukaista käsittelemistä. Tapausten käsittelyn laiminlyönti vaarantaa teleyrityksen palveluiden ja asiakkaiden tietoturvaa ja välillisesti myös muiden viestintäverkkojen käyttäjien tietoturvaa.

Teleyritysten asiakkaiden oikeusturvan ja tapausten asianmukaisen selvittämisen prosessin varmistamiseksi teleyrityksen on rekisteröitävä kaikki käsittelemänsä tietoturvaloukkaustapaukset.

#### Soveltaminen

Teleyrityksen tulee määritellä viestintäverkon ja -palvelujen tietoturvasta vastaava taho, joka ottaa vastaan ilmoitukset tietoturvaa vaarantavista tapahtumista niiden selvittämistä varten. Teleyrityksen on tarkastettava ilmoitusten paikkansapitävyys tarkoituksenmukaisella tavalla.

Tietoturvaloukkaustapausten asianmukaisella käsittelemisellä tarkoitetaan tietoturvaloukkauksen luonteesta riippuen esimerkiksi tietoturvaloukkauksen selvittämistä ja siitä aiheutuvien vahinkojen minimoimista. Jos tietoturvaloukkaus ei kohdistu teleyrityksen omaan asiakkaaseen tai teleyritys ei muuten pysty selvittämään tietoturvaloukkausta omilla toimenpiteillään, voidaan asia siirtää sellaisen toimijan selvittettäväksi, joka pystyy loukkaukseen vaikuttamaan. Tällainen toimija voi olla esimerkiksi toinen teleyritys tai CERT-toimija, kansallisella tasolla Viestintäviraston CERT-FI.

Tietoturvaloukkaustapausten asianmukaisella rekisteröinnillä tarkoitetaan kaikkien teleyrityksen käsittelemien tietoturvaloukkaustapausten asianmukaista kirjaamista. Lisäksi teleyrityksen on kirjattava kaikki tapausten selvittämiseksi tehdyt toimenpiteet.

### 11.3 Tietoturvaloukkausilmoitusten tilastointi

Määräyksen mukaan *teleyrityksen on tilastoitava käsittelemänsä tietoturvaloukkaustapaukset ja niiden vuoksi suoritettavat toimenpiteet tyypeittäin. Tilastosta on käytävä ilmi ainakin seuraavat asiat:*

- *teleyrityksen käsittelemien tietoturvaloukkaustapausten kokonaismäärä*
- *tietoturvaloukkaustapausten aiheuttamien jatkotoimenpiteiden määrä toimenpidetyypeittäin*
- *kuinka moni teleyrityksen tilaaja on joutunut tietoturvaloukkaustapausten aiheuttamien jatkotoimenpiteiden kohteeksi asiakasryhmittäin*

### Perustelut

Teleyritysten suorittamien toimenpiteiden riittävyyden ja tarkoituksenmukaisuuden valvomiseksi teleyrityksen on tilastoitava käsittelemänsä tietoturvaloukkaustapaukset ja ne toimenpiteet, joihin teleyritys on tietoturvaloukkausten selvittämiseksi ryhtynyt.

Viestintävirasto tulee pyytämään valvontatehtävänsä suorittamiseksi tarpeellisia tietoja teleyrityksiltä säännöllisesti. Viestintäviraston tiedonsaantioikeus perustuu SVTsL:n 33 §:n 1 momenttiin, jonka mukaan sillä on oikeus saada teleyritykseltä sekä näiden lukuun toimivilta SVTsL:ssa säädettyjen tehtäviensä hoitamiseksi välttämättömät tiedot salassapitosäännösten tai muiden tietojen luovuttamista koskevien rajoitusten estämättä niiden harjoittamasta SVTsL:ssa tarkoitettua toiminnasta.

Tilastointi palvelee myös teleyrityksen sisäistä prosessien toimivuuden ja verkon tietoturvaluustilanteen seurantaa.

### Soveltaminen

Teleyrityksen on muodostettava tilasto käsittelemistään tietoturvaloukkaustapauksista siten, että tilastosta käy ilmi:

- tapausten kokonaismäärä
- tapauksista aiheutuneiden jatkotoimenpiteiden määrä
  - yhteydenotto asiakkaaseen
  - liikenteen suodattaminen
  - liittymän tai palvelun irtikytkeminen
  - siirretty muulle toimijalle
  - aiheeton ilmoitus, ei toimenpiteitä
- kuinka moni teleyrityksen tilaaja on joutunut edellisessä kohdassa mainittujen toimenpiteiden kohteeksi liittymätyypeittäin tarkoituksenmukaisella tavalla jaoteltuna

Teleyrityksen omista tietoturvaloukkaushavainnoista tilastoidaan tapaukset, jotka liittyvät teleyrityksen asiakasliittymiin ja palveluihin.

Tilastoinnissa käytettävä tilastointijakso on kalenterivuosi.

Teleyritysten Viestintävirastolle toimittamat tiedot ovat lain viranomaisten toiminnan julkisuudesta (621/1999) nojalla salassa pidettäviä.

### Suositus

Tilastointi voi olla edellä kuvattua yksityiskohtaisempaa. Teleyrityksen käsittelemät tietoturvaloukkaustapaukset voidaan tilastoida myös havaitun tietoturvaongelman perusteella käyttäen esimerkiksi seuraavaa jaottelua:

- Roskasähköpostin levitys
- Palvelunestohyökkäykseen osallinen järjestelmä
- Havainto mahdollisesta asiakasliittymän takana sijaitsevan järjestelmän luvattomasta käytöstä / tietomurrosta (esimerkiksi www-palvelimen sisällön muuttaminen)
- Haittaohjelmahavainto liittymän takana sijaitsevasta järjestelmästä
- Botnet-verkon komentopalvelin
- Muu tietoturvaongelma.

## 12 10 § VOIMAANTULO JA SIIRTYMÄSÄÄNNÖKSET

Määräyksen mukaan *tämä määräys tulee voimaan 1 päivänä huhtikuuta 2011 ja on voimassa toistaiseksi. Määräyksellä kumotaan 19 päivänä syyskuuta 2008 annettu Viestintäviraston määräys 13 A/2008 M Internet-yhteyspalvelujen tietoturvasta ja toimivuudesta. Määräyksen 9 § 3 momentin tilastointivelvoite tulee voimaan 1.1.2012 alkaen.*

### Perustelut

Määräys tulee voimaan samanaikaisesti määräyksen 28 H/2010 M kanssa. Määräyksen 9 § 3 momentin tilastointivelvoite voi edellyttää muutostoinenpiteitä teleyritysten prosesseissa. Tästä syystä tilastointivelvoite säädetään alkamaan vuoden 2012 alusta.

## 13 VIITELUETTELO

[1] Sähköisen viestinnän tietosuojalaki (516/2004 muutoksineen, SVTsl), ajantasainen versio:  
<http://www.finlex.fi/fi/laki/ajantasa/2004/20040516>

[2] 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>

[3] Viestintämarkkinalaki (393/2003 muutoksineen, VML), ajantasainen versio:  
<http://www.finlex.fi/fi/laki/ajantasa/2003/20030393>

[4] Viestintäviraston määräys 9 /2009 Tietoturvaloukkausten ilmoitusvelvollisuudesta yleisessä teletoiminnassa.  
<http://www.ficora.fi/attachments/suomiry/5m3uFvOS8/Viestintavirasto09D2009M.pdf>

[5] Viestintäviraston määräys 11 A/2008 M Sähköpostipalvelujen tietoturvasta ja toimivuudesta,  
<http://www.ficora.fi/attachments/suomiry/5AWLwAxxQ/Viestintavirasto11A2008M.pdf>

[6] Viestintäviraston määräys 28 H/2010 M Viestintäverkkojen ja -palveluiden yhteentoimivuudesta, <http://www.ficora.fi/attachments/suomimq/5uSDGAGnh/M28H2010.pdf>

[7] Viestintäviraston määräys 47 C/2009 M, Teleyritysten tietoturvasta,  
<http://www.ficora.fi/attachments/suomiry/5jR9D3dp3/Viestintavirasto47C2009M.pdf>

[8] Viestintäviraston määräys 57/2009 M Viestintäverkkojen ja -palvelujen ylläpidosta sekä menettelystä vika- ja häiriötilanteissa,  
<http://www.ficora.fi/attachments/suomiry/5kfMxhxej/Viestintavirasto572009M.pdf>

[9] Internet Engineering Task Force (IETF) Request for Comments 4409: Message Submission for Mail  
<http://tools.ietf.org/pdf/rfc4409.pdf>

[10] Internet Engineering Task Force (IETF) Request for Comments 5068: Email Submission Operations: Access and Accountability Requirements - BCP 134  
<http://tools.ietf.org/pdf/rfc5068.pdf>