

**MÄÄRÄYKSEN 9 PERUSTELUT JA  
SOVELTAMINEN**

**TIETOTURVALOUKKAUSTEN  
ILMOITUSVELVOLLISUUDESTA  
YLEISESSÄ TELETOIMINNASSA**

## 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 .....	2
1.2.1 <i>Muu lainsäädäntö .....</i>	<i>2</i>
1.2.2 <i>Viestintäviraston tekniset määräykset .....</i>	<i>3</i>
1.2.3 <i>Ilmoitettujen tietojen käsittely Viestintävirastossa .....</i>	<i>3</i>
<b>2 MÄÄRÄYKSEN TARKOITUS JA MUUTOSHISTORIA .....</b>	<b>5</b>
2.1 Määräyksen tarkoitus .....	5
2.2 Keskeiset muutokset ja muutoshistoria .....	5
<b>3 PYKÄLÄKOHTAISET PERUSTELUT JA SOVELTAMISOHJEET.....</b>	<b>6</b>
3.1 1 § Soveltamisala .....	6
3.1.1 <i>Perustelut ja soveltaminen.....</i>	<i>6</i>
3.2 2 § Tilaajalle tehtävä ilmoitus .....	7
3.2.1 <i>Perustelut.....</i>	<i>7</i>
3.2.2 <i>Soveltaminen.....</i>	<i>7</i>
3.3 3 § Viestintävirastolle tehtävä ilmoitus .....	8
3.3.1 <i>Perustelut.....</i>	<i>8</i>
3.3.2 <i>Soveltaminen.....</i>	<i>8</i>
<b>4 MUUT SUOSITUKSET .....</b>	<b>11</b>
4.1 Suositus yhteistoiminnasta tietoturvaloukkaustilanteissa.....	11
4.2 Suositus tietoturvatilanteiden ilmoittamisesta Viestintävirastolle .....	11
4.3 Suositus muihin kuin teleyrityksiin kohdistuvien loukkausten ilmoittamisesta .....	11
<b>5 VIITELUETTELO .....</b>	<b>12</b>

## 1 LAINSÄÄDÄNTÖ

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

### 1.1 Määräyksen lainsäädäntöperusta

Viestintäviraston määräys perustuu sähköisen viestinnän tietosuojalain (516/2004, SVTsL) [1] 21 §:ään. SVTsL tuli voimaan 1.9.2004 ja sillä panttiin osaltaan täytäntöön EY:n heinäkuussa 2002 hyväksymä sähköisen viestinnän tietosuojadirektiivi [2].

SVTsL:n 21 §:n 1 momentin nojalla teleyritys on velvollinen ilmoittamaan palvelun tietoturvaan kohdistuvasta uhkasta viipymättä tilaajalle ja kerrottava samalla:

- tilaajan ja käyttäjän käytettävissä olevista toimenpiteistä uhkan torjumiseksi; sekä
- niiden todennäköisistä kustannuksista.

SVTsL:n 21 §: 2 momentin nojalla teleyrityksen on ilmoitettava Viestintävirastolle verkkopalvelun ja viestintäpalvelun merkittävistä tietoturvaloukkauksista ja sellaisista niihin kohdistuvista tietoturvauhkista, joista teleyritys on tietoinen. Samalla sen on ilmoitettava toimenpiteistä, joilla tällaisten tietoturvaloukkausten ja niiden uhkien toistuminen pyritään estämään. Torjuttuaan palveluunsa kohdistuneen merkittävän tietoturvaloukkauksen tai -uhkan taikka poistettuaan häiriön teleyrityksen on tiedotettava tarkoituksenmukaisella tavalla toteuttamistaan toimista ja niiden mahdollisista vaikutuksista palvelun käyttöön.

Viestintävirasto voi SVTsL:n 21 §:n 4 momentin nojalla antaa teleyrityksille:

- määräyksiä tietoturvaan kohdistuvasta erityisestä uhkasta tilaajille tehtävien ilmoitusten sisällöstä ja muodosta;
- määräyksiä palveluun kohdistuvista merkittävistä tietoturvaloukkauksista ja tietoturvauhkista Viestintävirastolle tehtävien ilmoitusten sisällöstä, muodosta ja toimittamisesta; sekä
- ohjeita merkittävän tietoturvaloukkauksen tai -uhkan poistamisen jälkeisen tiedottamisen sisällöstä ja muodosta.

### 1.2 Muut asiaan liittyvät säännökset

#### 1.2.1 Muu lainsäädäntö

*SVTsL:n 19 § Velvollisuus huolehtia tietoturvasta.* Pykälän mukaan teleyrityksen on huolehdittava palvelujensa tietoturvasta. Palvelun tietoturvasta huolehtiminen tarkoittaa toimia toiminnan turvallisuuden, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden sekä tietoaineistoturvallisuuden varmistamiseksi. Nämä toimet on suhteutettava uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin. Tietoturvasta huolehtimisvelvollisuus koskee myös tunnistamistietojen säilytysvelvollisuuden toteuttamiseksi tarvittavaa tietojen käsittelyä. Teleyritys vastaa tilaajille ja käyttäjille tietoturvasta myös sellaisen kolmannen osapuolen osalta, joka kokonaan tai osittain toteuttaa verkkopalvelun, viestintäpalvelun, tietojen säilyttämisen tai lisäarvopalvelun.

*SVTsL:n 20 § Toimenpiteet tietoturvan toteuttamiseksi.* Pykälän mukaan teleyrityksellä ja sen lukuun toimivalla on oikeus ryhtyä laissa tarkoitettuihin välttämättömiin toimiin tietoturvasta huolehtimiseksi seuraavissa tilanteissa:

- 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 \[3\] 37 luvun 11 §:ssä](#) tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseksi.

Tietoturvasta huolehtimiseksi välttämättömät 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 tekniluonteiset toimenpiteet.

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 SVTsL:n 20 §:ssä asetettujen tavoitteiden toteutumista, yksittäisen viestin sisältöä saa käsitellä manuaalisesti. Manuaalisesta viestin sisällön käsittelystä on ilmoitettava viestin lähettäjälle ja vastaanottajalle, jollei ilmoittamisella todennäköisesti vaaranneta tavoitteiden toteutumista. Teleyritysten on toteutettava toimenpiteet huolellisesti ja ne on mitoitettava torjuttavan häiriön vakavuuteen. Toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä käsittelyn tavoitteiden turvaamiseksi. Toimenpiteet on lopetettava, jos niiden toteuttamiselle ei enää ole tässä pykälässä säädettyjä edellytyksiä.

*Viestintämarkkinalain (393/2003, VML) [4] 131 § Velvollisuus korjata häiriö.* Pykälän mukaan teleyrityksen tai muun viestintäverkon tai laitteen haltijan on välittömästi ryhdyttävä toimenpiteisiin tilanteen korjaamiseksi ja tarvittaessa irrotettava viestintäverkko tai laite yleisestä viestintäverkosta, jos viestintäverkko tai laite aiheuttaa vaaraa tai häiriötä viestintäverkolle, laitteelle, viestintäverkon käyttäjälle tai muulle henkilölle.

#### 1.2.2 Viestintäviraston tekniset määräykset

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 13 *internet-yhteyspalvelujen tietoturvasta ja toimivuudesta* [6]. Määräystä sovelletaan yleisissä viestintäverkoissa tarjottavien internet-yhteyspalvelujen tuottamiseen sekä teleyrityksen näihin toimintoihin käyttämiin järjestelmiin, viestintäverkkoihin ja viestintäpalveluihin. Internetyhteyspalvelulla tarkoitetaan määräyksessä internet-liikenteen välittämistä. Määräystä sovelletaan internet-yhteyspalvelujen tuottamisessa soveltuvin osin myös sekä verkkoyrityksissä että palveluyrityksissä.

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. Määräystä sovelletaan myös merkitykseltään vähäiseen teletoimintaan. 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.

Esitetty lista vastaa tämän dokumentin julkaisuhetken tilannetta. Kaikki Viestintäviraston määräykset on julkaistu Viestintäviraston internet-sivuilla osoitteessa [www.ficora.fi](http://www.ficora.fi).

#### 1.2.3 Ilmoitettujen tietojen käsittely Viestintävirastossa

Viestintävirasto käsittelee SVTsL:n 21 §:n nojalla ilmoitettuja tietoja luottamuksellisesti. Tiedot ovat *viranomaisen toiminnan julkisuudesta annetun lain* (621/1999, Julkisuuslaki) [9] nojalla salassa pidettäviä.

- *Julkisuuslain 24 §:n 1 momentin 7 kohdan* mukaan salassa pidettäviä viranomaisen asiakirjoja ovat, jollei erikseen toisin säädetä henkilöiden, rakennusten, laitosten, rakennelmien sekä tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat ja niiden

toteuttamiseen vaikuttavat asiakirjat, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna turvajärjestelyjen tarkoituksen toteutumista.

- *Julkisuuslain 24 §:n 1 momentin 20 kohdan* mukaan salassa pidettäviä ovat myös asiakirjat, jotka sisältävät tietoja yksityisestä liike- tai ammattisalaisuudesta, samoin kuin sellaiset asiakirjat, jotka sisältävät tietoja muusta vastaavasta yksityisen elinkeinotoimintaa koskevasta seikasta, jos tiedon antaminen niistä aiheuttaisi elinkeinonharjoittajalle taloudellista vahinkoa, ja kysymys ei ole kuluttajien terveyden tai ympäristön terveellisyyden suojaamiseksi tai toiminnasta haittaa kärsivien oikeuksien valvomiseksi merkityksellisistä tiedoista tai elinkeinonharjoittajan velvollisuuksia ja niiden hoitamista koskevista tiedoista.

*SVTsL:n 34 a §:n* mukaan Viestintävirastolla on oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan tunnistamistietoja tietyin edellytyksin niille teleyrityksille, lisäarvopalvelun tarjoajille ja yhteisötilaajille, joita on käytetty hyväksi tietoturvaloukkauksessa, jotka ovat joutuneet tietoturvaloukkauksen kohteiksi tai joihin todennäköisesti voi kohdistua tietoturvaloukkaus. Lisäksi Viestintävirastolla on oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan tunnistamistietoja muussa valtiossa toimivalle viranomaiselle tai muulle taholle, jonka tehtävänä on ennalta ehkäistä tai selvittää viestintäverkkoihin ja -palveluihin kohdistuvia tietoturvaloukkauksia.

Viestintävirastolla on kuitenkin oikeus luovuttaa tunnistamistietoja ainoastaan siinä laajuudessa kuin se on tarpeen tietoturvaloukkausten ehkäisemiseksi ja selvittämiseksi. Tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

## **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 määritellä sähköisen viestinnän tietosuojalain 21 §:n mukaisten merkittävää tietoturvaloukkausta tai sen uhkaa koskevan ilmoituksen sisältö ja menettelytavat Viestintävirastolle ja asiakkaille tehtävissä ilmoituksissa.

### **2.2 Keskeiset muutokset ja muutoshistoria**

Määräysten uusi ryhmittely:

Määräysuudistuksen yhteydessä vuoden 2010 alussa määräyksestä 9 eriytetään teleyritysten vika- ja häiriötilanteiden ilmoitusvelvollisuutta koskevat säännökset erilliseksi määräykseksi 57 viestintäverkkojen ja -palvelujen ylläpidosta sekä menettelystä vika- ja häiriötilanteissa.

Määräykseen 9 jäävään tietoturvaloukkauksia koskevaan ilmoitusvelvollisuuteen ei tehdä merkittäviä muutoksia. Tilaajille ja Viestintävirastolle tehtävä tiedottaminen on kuitenkin eriytetty omiksi pykälikseen. Lisäksi määräyksen perustelut ja soveltaminen -muistioon on lisätty suositus teleyritysten yhteistoiminnasta tietoturvaloukkaustilanteissa.

### 3 PYKÄLÄKOHTAISET PERUSTELUT JA SOVELTAMISOHJEET

Tässä luvussa käydään läpi pykäläkohtaisesti pykälän perustelut sekä sen soveltamissuositukset.

#### 3.1 1 § Soveltamisala

##### 3.1.1 Perustelut ja soveltaminen

###### Yleinen teletoiminta:

Määräystä sovelletaan teleyritysten yleiseen teletoimintaan. Yleisellä teletoiminnalla tarkoitetaan verkkopalvelun tai viestintäpalvelun tarjoamista käyttäjäpiirille, jota ei ole etukäteen rajattu. Verkkopalvelulla tarkoitetaan verkkoyrityksen tarjoamaa palvelua, joka on yrityksen omistaman tai muulla perusteella hallussa olevan viestintäverkon tarjoamista käytettäväksi viestien siirtoon, jakeluun tai tarjolla pitoon. Viestintäpalvelulla taas tarkoitetaan palveluyrityksen tarjoamaa palvelua, joka on viestien siirtämistä yrityksen hallussa olevassa tai verkkoyritykseltä käyttöön saadussa viestintäverkossa taikka viestien jakelemista tai tarjolla pitämistä joukkoviestintäverkossa.

Viestintäverkko määritellään *VML 2 §:ssä* ja sillä tarkoitetaan sekä kohdeviestintään että joukkoviestintään tarjottavia verkkoja. Määräys soveltuu siten esimerkiksi kiinteään ja langattomaan puhelin- ja dataverkkoon, kaapelitelevisioverkkoon, ja tietysti edellytyksin maanpäälliseen digitaaliseen televisioverkkoon ja analogiseen radioon. Yleisen viestintäverkon määritelmässä on olennaista se, että verkkoa tarjotaan ennalta rajoittamattomalle käyttäjäpiirille. Viestintäpalvelun määritelmässä olennaista on se, että teleyritys osallistuu palveluntarjoajana teknisesti viestien siirtoon tai tarjolla pitoon.

Määräystä sovelletaan myös merkitykseltään vähäiseen teletoimintaan, josta ei ole *VML 13 §:n* mukaista teletoimintailmoitusvelvollisuutta. Määräys ei kuitenkaan koske sisältöpalveluita tai ennalta rajatulle käyttäjäpiirille tarjottavia palveluita.

###### Joukkoviestintäverkkoja koskeva soveltamisrajaus:

SVTsL:ia eikä siten määräystäkään sovelleta joukkoviestintäverkossa välitettävään viestiin, jos viestiä ei voi yksittäisessä tapauksessa yhdistää sitä vastaanottavaan tilaajaan tai käyttäjään. Siten määräystä sovelletaan joukkoviestintäverkkoihin vain, jos niitä käytetään muuhun kuin televisio- tai radiotoimintaan.

Viestintämarkkinalain mukaan joukkoviestintäverkolla tarkoitetaan viestintäverkkoa, jota pääasiassa käytetään televisio- ja radio-ohjelmistojen tai muun kaikille vastaanottajille samanlaisena välitettävän aineiston lähettämiseen tai tarjolla pitoon. Viestillä tarkoitetaan viestintäverkossa osapuolten välillä tai vapaasti valikoituville vastaanottajille välitettävää puhelua, sähköpostiviestiä, tekstiviestiä, puheviestiä ja muuta vastaavaa sanomaa. Viestejä ovat myös sellaiset sisällölliset sanomat, jotka välitetään vapaasti valikoituville vastaanottajille, kuten televisio-ohjelmat ja radio-ohjelmat sekä kaikki sähköisten viestintäverkkojen yleisölle avointen sivustojen avulla välitettävät tiedot.

###### Viranomaisverkot:

Määräystä ei sovelleta myöskään *viranomaistoimintaan* viestintämarkkinalaissa tarkoitettussa viranomaisverkossa tai muussa yleiseen järjestykseen ja turvallisuuteen, maanpuolustukseen, pelastustehtäviin, väestönsuojeluun tai maaliikenteen, meriliikenteen, raideliikenteen taikka ilmaliikenteen turvallisuuteen liittyvien tarpeiden vuoksi rakennetussa viestintäverkossa. *VML:ssa* viranomaisverkolla tarkoitetaan yleiseen järjestykseen ja turvallisuuteen, pelastustehtäviin tai väestönsuojeluun liittyvien tarpeiden vuoksi rakennettua viestintäverkkoa, jonka liittymiä voidaan tarjota viranomaisten lisäksi myös muulle, edellä mainittujen tehtävien hoitamisen kannalta välttämättömälle käyttäjäryhmälle. *VML:n* mukainen viranomaisverkko voi olla niin sanottu puhdas erillisverkko, tai se voi olla liitetty yleiseen viestintäverkkoon, jolloin viranomaisverkosta voidaan esimerkiksi soittaa yleiseen puhelinverkkoon.

Määräystä kuitenkin sovelletaan muuhun yleiseen teletoimintaan kuin viranomaistoimintaan viranomaisverkoissa.

### 3.2 2 § Tilaaajalle tehtävä ilmoitus

#### 3.2.1 Perustelut

Teleyritysten tarjoamien palveluiden tilaajien ja käyttäjien toimintaedellytysten turvaaminen edellyttää tilaajilla ja käyttäjillä olevaa tietoisuutta palveluun kohdistuvista tietoturvariskeistä. Sähköisen viestinnän tietosuojalain mukaan *jos palveluun kohdistuu sellainen erityinen uhka, jota palvelujen tarjoajat eivät kykene välttämään omin toimin tai yhdessä muiden toimijoiden kanssa, tulee palvelun tarjoajan ilmoittaa ilman viivytystä asiasta tilaajilleen. Samalla teleyrityksen on kerrottava tilaajan ja käyttäjän käytettävissä olevista toimenpiteistä uhkan torjumiseksi sekä toimenpiteiden todennäköisistä kustannuksista.*

#### 3.2.2 Soveltaminen

##### *Erityisen uhkan arviointi*

Tilaaajille tiedotettavia erityisiä tietoturvauhkia voivat olla esimerkiksi:

- internetin käyttöön liittyvät päätelaitteisiin ja ohjelmistoihin liittyvät kulloinkin ajankohtaiset tietoturvauhkat ja niiltä suojautuminen
  - uhkat, jotka liittyvät haittaohjelmiin ja niiden leviämiseen esimerkiksi sähköpostin, internet-sivujen, matkaviestimien ja vertaisverkkojen välityksellä
  - modeemipohjaisen internet-liikenteen soittotiedon uudelleenohjaukset
- yleisesti käytössä olevissa järjestelmissä ja ohjelmistoissa havaitut vakavat tietoturvan puutteet, esimerkiksi korjaamattomat, yleisesti tiedossa olevat haavoittuvuudet ohjelmistoissa tai järjestelmissä (tieto julkistettu esimerkiksi CERT-tiedotteena tai järjestelmätoimittajan toimesta)
- viestintäpalveluiden käyttöön liittyvät ajankohtaiset tietoturvauhkat, jotka vaativat viestintäpalvelujen käyttäjiltä erityishuomiota
  - laajamittaiset haittaohjelmaepidemiat, jotka vaativat asiakkaalta välittömiä toimenpiteitä
  - roskapostiviestien määrän huomattava kasvu, jolla on vaikutusta sähköpostipalvelujen käytettävyydelle
  - muut sellaiset viestintäverkoissa sattuneet tapahtumat, jotka vaarantavat merkittävästi tilaajien tietoturvaa tai -suoja
- viestintäpalveluiden kansainvälisestä luonteesta johtuvat erityiset uhkat
  - suomalaisille käyttäjille suunnattuun viestintäpalveluun kohdistuvat tietoturvauhkat, jotka johtuvat palvelun toteuttamisesta osittain tai kokonaan Suomen ulkopuolella ja joita teleyritys ei voi omin toimenpitein ehkäistä

Tiedotusta ohjelmistohaavoittuvuuksista suositellaan erityisesti, jos korjaamaton haavoittuvuus yleisesti käytössä olevissa ohjelmistoissa on erityisen helposti hyödynnettävissä ja siten uhkaamassa verkkojen ja palvelujen tietoturvaa yleisesti.

##### *Ilmoituksen ajoittaminen*

Osa teleyrityksen palveluun kohdistuvista uhkista on sellaisia, joiden korjaaminen ei ole välittömästi mahdollista. Julkinen tiedottaminen tällaisista uhkista olisi omiaan vaarantamaan viestinnän luottamuksellisuuden tai mahdollistaisi laajamittaisia taloudellisia väärinkäytöksiä. Tällaisten uhkien osalta on syytä ensin pyrkiä tietoturva-aukon korjaamiseen, jolloin vältytään myös tilaaajille aiheutuvista lisävahingoista.

SVTsL:n mukaan *torjuttuaan palveluunsa kohdistuneen merkittävän tietoturvaloukkauksen tai -uhkan teleyrityksen on tiedotettava tarkoituksenmukaisella tavalla toteuttamistaan toimista ja niiden mahdollisista vaikutuksista palvelun käyttöön.* Tiedottaminen on luonteeltaan yleistä ja nimenomaan jälkikäteistä. Toimenpiteistä on kuitenkin tiedotettava niin reaaliaikaisina kuin mahdollista. Jälkikäteisellä tiedottamisella mahdollistetaan tietoturvaloukkauksen tai -uhkan

kohteeksi joutuneen toimijan reagointimahdollisuudet jälkikäteisiä toimenpiteitä vaativissa tilanteissa.

### *Ilmoitusmenettely*

Asiakastiedotukseen voidaan käyttää esimerkiksi teleyrityksen internet-sivuja, laskunvälitiedotteita ja sähköpostiviestejä. Internet-sivujen ja laskunvälitiedotteiden soveltuvuus on erittäin hyvä esimerkiksi sellaisissa tapauksissa joissa uhka ei ole kriittinen eikä vaadi välittömiä toimenpiteitä tilaajalta. Tällaisia ovat muun muassa tiedotteet, jotka koskevat yleisiä internetin käyttöön liittyviä uhkia ja niiden torjumiseksi käytettävissä olevia toimenpiteitä. Internet-sivut soveltuvat hyvin myös tiedottamiseen kriittisemmistä uhkista, esimerkiksi viestintäverkoissa äkillisesti kasvavasta vaarallisesta haittaohjelmaliikenteestä. Sähköpostitse tapahtuva tiedottaminen soveltuu esimerkiksi tapauksiin, joissa uhka koskee vain rajattua joukkoa teleyrityksen tilaajista ja joissa tiedottaminen muille kuin asianosaisille saattaisi vaarantaa tilaajien tietoturvaa tai -suoja. Laajamittaisissa kriittisissä tilanteissa myös joukkoviestintävälineiden käyttö tiedotuskanavana voi olla perusteltua.

Perusohjeistus-tyyppinen asiakastiedotus tyypillisen internet-käyttäjän tietojärjestelmän suojaamiseksi yleisimmiltä internet-käytön uhkatekijöiltä on syytä liittää liittymän avaamisen yhteydessä asiakkaalle toimitettavaan materiaaleihin ja uusia säännöllisesti, esimerkiksi kerran vuodessa, muun asiakkaalle toimitettavan oheisviestinnän yhteydessä.

Teleyrityksen on syytä ilmoittaa tilaajalle, mikäli hänen liittymänsä on kytketty irti liittymässä esiintyneiden tietoturvaongelmien vuoksi. Tilaajaa tulee informoida sekä teleyrityksen toimenpiteistä tilanteen korjaamiseksi sekä myös niistä toimenpiteistä, joita teleyritys odottaa tilaajalta liittymän tietoturvan korjaamiseksi.

### *Suositus*

Lisäksi Viestintävirasto suosittaa, että teleyritys tiedottaa asiakkailleen tyypillisimmistä viestintäpalveluiden käyttöön liittyvistä huijaus/petosyrityksistä ja oikeasta tavasta reagoida niihin, esimerkiksi:

- tekstiviesteillä tuntemattomasta numerosta saapuvat pyynnöt soittaa tyypillisesti lisämaksullisiin numeroihin;
- takaisinsoittoon tähtäävät haamusoitot lisämaksullisista tai ulkomaalaisista puhelinnumeroista; sekä
- ajankohtaiset phishing-hyökkäyskampanjat

## **3.3 3 § Viestintävirastolle tehtävä ilmoitus**

### 3.3.1 Perustelut

Tietoturvaloukkausilmoituksessa pyydettyjä tietoja tarvitaan kootun, ajantasaisen ja analysoidun tilannekuvan muodostamiseksi valtakunnallisesta viestintäverkkojen ja -palvelujen tietoturvatilanteesta. Tiedot mahdollistavat vastatoimien suuntaamista ja painottamista ajantasaisen tiedon perusteella. Lisäksi ilmoituksen laatiminen auttaa organisaatiota seuraamaan omaa tietoturvallisuuden hallintaprosessia ja muodostamaan organisaatiokohtaista tietoturvatilannekuvaa. Ilmoitettavat tiedot ovat tietoturvaloukkaustapausta analysoitaessa tarvittavia perustietoja.

### 3.3.2 Soveltaminen

SVTsL:n mukaan *teleyrityksen on ilmoitettava Viestintävirastolle verkkopalvelun ja viestintäpalvelun merkittävistä tietoturvaloukkauksista ja sellaisista niihin kohdistuvista tietoturvauhkista, joista teleyritys on tietoinen. Samalla teleyrityksen on ilmoitettava Viestintävirastolle toimenpiteistä, joilla tällaisten tietoturvaloukkausten ja niiden uhkien toistuminen pyritään estämään.*

### *Merkittävyyden arviointi*

Loukkauksen, sen uhkan ja vian tai häiriön merkittävyyttä arvioitaessa on kiinnitettävä SVTsL:n perustelujen mukaan huomiota tilaajien ja käyttäjien oikeuksien suojaan, palvelun käytettävyyteen ja maantieteellisten vaikutusten laajuuteen. Ilmoitus on tehtävä välittömästi, kun asian merkittävyys on todettu. Ilmoituksesta on käytävä selkeästi ilmi, mihin toimiin asian johdosta on ryhdytty ja mahdollisuuksien mukaan myös se, miten ongelma voidaan tulevaisuudessa estää. Jos tulevaisuudessa toteutettavia toimia ei kyetä ilmoituksen yhteydessä kertomaan, ilmoitusta tulee täydentää ilman aiheetonta viivytystä.

Luettelossa kuvataan esimerkkejä sellaisista tapaustyypeistä, joista ilmoitus on tehtävä. Luettelo ei ole tyhjentävä, vaan sen tarkoitus on kuvata ilmoituskynnyksen vakavuustaso. Viestintävirastolle ilmoitettavia tietoturvaloukkauksia ovat esimerkiksi:

- tietomurrot teleyrityksen tietojärjestelmiin
- teleyrityksen tietojärjestelmiin kohdistuneet tietoturvaloukkaukset
  - tunnistamis-, asiakas- tai määrittelytietojen joutuminen väriin käsiin
  - verkon dokumentaatiotietojen tai rakennekuvausten joutuminen väriin käsiin
  - asiaton pääsy järjestelmän pääkäyttäjäksi
  - asiaton pääsy järjestelmään käyttäjätunnuksella, jolla on pääsy viestinnän sisältöön tai tunnistamistietoihin tai mahdollisuus asiattomasti muuttaa teleyrityksen tietojärjestelmien tai viestintäverkkojen määrittelyjä
- tietoturvaloukkaukset, joilla on huomattavaa vaikutusta viestintäverkon tai -palveluiden käytettävyyteen
  - palvelunestohyökkäykset
  - roskasähköpostiliikenteen äkillinen kasvu
  - viestintäverkon liikenteen reititykseen vaikuttavat hyökkäykset
- haittaohjelmien (esimerkiksi tietokonevirukset, takaporttiohjelmat, ”troijalaiset hevoset” vakoiluohjelmat tai verkkoliikenteen tarkkailuohjelmat) aktivoituminen teleyrityksen tietojärjestelmissä
- yritykset saada teleyrityksen tai sen asiakkaiden tietoturvasuutta vaarantavia tietoja teleyrityksen henkilöstöltä (nk. ”social engineering”)
- havaitut salakuuntelu, tarkkailulaitteet ja -kytkennät sekä ohjelmistot viestintäverkossa tai teleyrityksen tietojärjestelmissä tai tiloissa

Luettelossa kuvataan esimerkkejä sellaisista tapaustyypeistä, joista ilmoitus on tehtävä. Luettelo ei ole tyhjentävä, vaan sen tarkoitus on kuvata ilmoituskynnyksen vakavuustaso. Viestintävirastolle ilmoitettavia tietoturva-uhkia ovat esimerkiksi:

- Havaitut merkittävät tietomurtoyrietykset
  - järjestelmälliset, tavallisesta verkkokäytöstä poikkeavat yritykset selvittää teknisin menetelmin tietoja esimerkiksi viestintäverkkojen ja -palvelujen seuraavista ominaisuuksista
    - verkon fyysinen ja looginen topologia
    - laitteisto ja ohjelmistoversiot
    - mahdolliset järjestelmissä olevat haavoittuvuudet
  - järjestelmälliset vihamieliset kirjautumisyrietykset teleyrityksen tietojärjestelmiin
  - tietomurtoyrietyt Viestintäviraston viestintäverkkojen ja -palvelujen varmistamisesta antaman määräyksen 54/2008 M tärkeysluokkaan 1 tai 2 kuuluvaan teleyrityksen komponenttiin
- havaittu tavallisesta poikkeava verkkoliikenne
  - huomattava käyttämättömiin verkko-osoitelohkoihin kohdistuva liikenne
  - huomattava liikennevolyyymi tuntemattomilla tai harvoin käytetyillä protokollatyypeillä
  - äkillinen liikenteen kasvu harvinaisiin ulkomaansuuntiin
- teleyrityksen tietojärjestelmissä ja ohjelmistoissa havaitsemat huomattavat tietoturvan puutteet, joita ei ole julkistettu esimerkiksi CERT-tiedotteena tai järjestelmätoimittajan toimesta
  - tietoturva-aukot, joita käyttäen on mahdollista päästä asiattomasti pääkäyttäjäksi järjestelmään

- tietoturva-aukot, joita käyttäen on mahdollista päästä asiattomasti viestinnän sisältöön tai tunnistamistietoihin tai muuttaa teleyrityksen tietojärjestelmien tai viestintäverkon määrittelyjä
- haittaohjelmien laajamittainen, merkittävää uhkaa teleyrityksen palveluille tai asiakkaille aiheuttava leviäminen tai aktivoituminen viestintäverkossa
- viestintäpalveluiden kansainvälisestä luonteesta johtuvat erityiset uhkat
  - havaittaessa suomalaisille käyttäjille suunnattuun viestintäpalveluun kohdistuva tietoturva-uhka, joka johtuu palvelun toteuttamisesta osittain tai kokonaan Suomen ulkopuolella ja jota teleyritys ei voi omin toimenpitein ehkäistä

### *Ilmoitusmenettely*

Jos tietoturvaloukkaus tai tietoturvaloukkauksen uhka on vakava, ilmoituksen tekoon käytettävässä sanomanvälitysjärjestelmässä epäillään tietoturvaloukkausta tai tilanne vaatii välittömiä Viestintäviraston toimenpiteitä, on ensimmäinen ilmoitus syytä tehdä välittömästi olemassa olevin tiedoin esimerkiksi puhelimitse. Täydentävä kirjallinen ilmoitus voidaan tehdä, kun tilanteesta on tarkempi kokonaiskuva. Pitkäaikaisissa tapauksissa teleyrityksen on pidettävä Viestintävirasto ajan tasalla tilanteen kehittymisestä. Sellainen sähköisesti toimitettu ilmoitus, joka voidaan saattaa kirjalliseen ja luettavaan muotoon, katsotaan kirjalliseksi.

Suosittelava ilmoitustapa on käyttää liitteen 1 lomaketta tietoturvaloukkausten ja tietoturvaloukkausten uhkien ilmoittamiseen. Ilmoitus voidaan tehdä myös esimerkiksi sähköpostilla vapaamuotoista tekstiä käyttäen, jos siinä välitetään lomakkeen tietosisältö.

Teleyrityksiä pyydetään ilmoittamaan Viestintävirastolle ja pitämään ajan tasalla yhteystietonsa tietoturvaloukkausten käsittelytoimintojen osalta liitteen 2 mukaisella lomakkeella.

### *Yhteystiedot*

SÄHKÖPOSTI: [CERT@FICORA.FI](mailto:CERT@FICORA.FI)

Tiedot CERT-FI-yksikön PGP-avaimista sähköpostiviestin salaamiseksi on saatavissa internet-osoitteesta <https://www.cert.fi/palvelut/yhteystiedot/rooliavaimet.html>

Puhelin: 09 6966 510

Faksi: 09 6966 515

Postiosoite:  
Viestintävirasto  
CERT-FI  
PL 313  
00181 HELSINKI

## **4 MUUT SUOSITUKSET**

### **4.1 Suositus yhteistoiminnasta tietoturvaloukkaustilanteissa**

Viestintävirasto suositaa, että teleyritykset toimivat tiiviissä yhteistoiminnassa sekä keskenään että Viestintäviraston CERT-FI -yksikön kanssa tietoturvaloukkausten ja niiden uhkien selvittämiseksi.

Teleyritysten verkonhallinnan ja tietoturvaloukkauksia selvittävien vastuuyksiköiden suositellaan tiedottavan myös muita teleyrityksiä sellaisista tietoturvaloukkauksista ja -uhkista, jotka vaikuttavat tai voivat vaikuttaa toisen teleyrityksen viestintäverkkoon tai -palveluun.

### **4.2 Suositus tietoturvatilanteiden ilmoittamisesta Viestintävirastolle**

Viestintävirasto suositaa, että toimijat ilmoittavat harkintansa mukaan CERT-FI:lle myös merkittävää vähäisemmistä tietoturvaloukkauksista ja niiden uhkista. Tiedot tukevat kansallisen tietoturvallisuuden tilannekuvan muodostamista ja auttavat CERT-FI:tä kehittämään palveluitaan paremmin toimijoiden tarpeita vastaaviksi.

### **4.3 Suositus muihin kuin teleyrityksiin kohdistuvien loukkausten ilmoittamisesta**

Viestintävirasto suositaa, että myös muut toimijat kuin teleyritykset ilmoittavat niihin kohdistuneet tietoturvaloukkaukset ja tietoturvaloukkausten uhkat Viestintäviraston CERT-FI-yksikölle. CERT-FI voi muun muassa tukea ja auttaa loukkauksen kohteeksi joutunutta toimijaa loukkauksesta toipumisessa ja tarvittavissa vastatoimissa. Lisäksi CERT-FI:llä on käytettävissään erittäin laaja kansainvälinen yhteistyöverkosta, joka mahdollistaa nopean ja tehokkaan puuttumisen myös kansainvälisiin tietoturvatilanteisiin.

## 5 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] Rikoslaki (39/1889 muutoksineen), ajantasainen versio:  
<http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001>

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

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

[6] Viestintäviraston määräys 13 A/2008 M Internet-yhteyspalvelujen tietoturvasta ja toimivuudesta,  
<http://www.ficora.fi/attachments/suomiry/5AWLt8K4m/Viestintavirasto13A2008M.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] Laki viranomaisten toiminnan julkisuudesta (621/1999 muutoksineen, julkisuuslaki), ajantasainen versio: <http://www.finlex.fi/fi/laki/ajantasa/1999/19990621>