Määräys teletoiminnan tietoturvasta

Annettu Helsingissä 4 päivänä maaliskuuta 2015.

Viestintävirasto on määrännyt 7 päivänä marraskuuta 2014 annetun tietoyhteiskuntakaaren (917/2014) 244 §:n, 247 §:n ja 272 §:n nojalla:

Luku 1 Yleiset säännökset

1 § Määräyksen tarkoitus

Tämän määräyksen tarkoituksena on:
1) edistää yleisten viestintäverkkojen ja -palvelujen tietoturvaa,
2) turvata sähköisen viestinnän luottamuksellisuutta ja yksityisyyden suojan toteutumista sekä
3) varmistaa, että tietoturvan toteuttaminen teleyrityksissä on kattavaa, suunnitelmallista ja tehokasta.

2 § Soveltamisala

Tätä määräystä sovelletaan yleiseen teletoimintaan.

Tässä määräyksessä määrätään:
luvussa 2 tietoturvatoimenpiteistä kaikissa viestintäverkoissa ja -palveluissa,
luvussa 3 rajapintojen erityisistä tietoturvavaatimuksista,
luvussa 4 internetyhteyspalvelujen erityisistä vaatimuksista,
luvussa 5 sähköpostipalvelujen erityisistä vaatimuksista ja
luvussa 6 asiakkaille tietoturvatiedottamisesta.

Teleyritykselle määräyksen 3 luvun 9 §:n 1 momentissa määrätyt velvoitteet koskevat myös viranomaisverkkoa siltä osin kuin viranomaisverkko yhteenliitetään yleiseen viestintäverkkoon.

Tämän määräyksen 5 ja 6 luvun soveltamista rajoitetaan siten, että:
1) 18 §:n 2 momentin 3 kohtaa, 20 §:ää ja 23 §:ää ei sovelleta sähköpostiviestien välityspalveluun eli palveluun, jossa teleyritys välittää tai uudelleenohjaa viestejä omien sähköpostipalvelimiensa kautta ja
2) 18 §:n 2 momentin 1 ja 2 kohtia ei sovelleta toissijaiseen sähköpostin välityspalveluun eli asiakkaan omaa sähköpostipalvelua varmistavaan sähköpostin välityspalvelimeen.

3 § Määritelmät

Tässä määräyksessä tarkoitetaan:
1) *asiakasrajapinnalla* rajapintaa, jolla teleyrityksen asiakkaan viestintäverkko, päätelaite tai sovellus liitetään yleiseen viestintäverkkoon;
2) *avoimella sähköpostipalvelimella* sellaista sähköpostiviestien välitysjärjestelmää, jota kolmas osapuoli pystyy oikeudettomasti käyttämään sähköpostiviestien välittämiseen;
3) *haitallisella liikenteellä* sähköisiä viestejä, jotka aiheuttavat vaaraa viestintäverkon tai -palvelun tietoturvalle;
4) *suodattamisella* haitallisen liikenteen estämistä, rajoittamista, tietoturvaa vaarantavien haitallisten tietokoneohjelmien poistamista sähköisistä viesteistä tai muita näihin rinnastettavia teknisluonteisia toimia;
5) *sähköpostipalvelulla* sähköpostiviestien lähettämis-, välittämis- tai vastaanottopalvelua, joka hyödyntää internetin nimipalvelua viestien välittämisessä;
6) *viestintäverkon tai -palvelun komponentilla* verkkoelementtiä, laitetta tai tietojärjestelmää, joista viestintäverkko tai -palvelu muodostuu tai jota se hyödyntää;
7) *yhteenliittämisrajapinnalla* teleyritysten viestintäverkkojen- tai palvelujen välistä rajapintaa.

Luku 2 Kaikkien verkkojen ja palvelujen yleiset vaatimukset

4 § Tietoturvallisuuden huomioiminen

Teleyrityksen on otettava viestintäverkkojen ja -palvelujen elinkaaren eri vaiheissa huomioon:
1) hallinnollinen tietoturvallisuus;
2) henkilöstöturvallisuus;
3) laitteisto-, ohjelmisto- ja tietoliikenneturvallisuus;
4) tietoaineisto- ja käyttöturvallisuus;
5) fyysinen turvallisuus.

Teleyrityksen on dokumentoitava ja ylläpidettävä kuvaus siitä, miten se huomioi toiminnassaan momentin 1 mukaiset tekijät.

5 § Riskien hallinta

Teleyrityksen on tunnistettava teletoiminnan jatkuvuuden kannalta tärkeät toiminnot, tiedot ja järjestelmät sekä arvioitava ja käsiteltävä säännöllisesti niihin kohdistuvat tietoturvariskit.

Riskien hallinnan prosessit ja vähintään viimeisimmän käsittelykerran tulokset on dokumentoitava.

6 § Tietoaineistot

Teleyrityksessä on oltava käytössä teletoiminnan kannalta tärkeiden tietoaineistojen luokitusjärjestelmä ja luokitteluun liittyvä tietoaineistojen käsittelymenettely. Luokituskriteereistä ja käsittelymenettelyistä on laadittava ja ylläpidettävä ajantasainen dokumentaatio.

7 § IP-osoitteiden dokumentointi

Teleyrityksen on huolehdittava, että sille osoitetut ja sen mainostamat IP-osoitteet on asianmukaisesti dokumentoitu osoiteavaruuden myöntäneen internetosoiterekisterin tietokantaan.

8 § Hallintaverkon ja hallintayhteyksien liikenne

Teleyrityksen on asianmukaisesti suojattava viestintäverkon tai -palvelun komponenttien hallintaliikenne siten että viestintäverkon tai -palvelun komponentteihin ei pääse oikeudettomasti tekemään muutoksia.

Luku 3 Rajapintojen erityiset vaatimukset

9 § Yhteenliittämis- ja asiakasrajapintojen häiriöiden estäminen ja niiltä suojautuminen

Teleyrityksen on pidettävä huolta, että sen viestintäverkon tai -palvelun komponentit eivät aiheuta häiriötä muiden teleyritysten viestintäverkoille tai -palveluille. Teleyrityksellä on oltava tarkoituksenmukaiset mekanismit näiden häiriöiden estämiseksi.

Teleyrityksen on suojattava oma verkkonsa yhteenliittämis- ja asiakasrajapinnoista tulevalta haitalliselta liikenteeltä toteuttamalla verkossaan tarvittavat suojausmekanismit.

10 § Tarpeettomien palvelujen ja protokollien sulkeminen

Teleyrityksen on pidettävä huolta, että sen verkon yhteenliittämis- ja asiakasrajapinnoissa olevissa viestintäverkon tai -palvelun komponenteissa tai näiden porteissa ei ole päällä tarjotun viestintäpalvelun kannalta tarpeettomia palveluja tai protokollia.

11 § IP-liikenteen estäminen yhteenliittämisrajapinnoissa

Teleyrityksen on estettävä IP-yhteenliittämisrajapinnoissa sellainen sen viestintäverkkoon suuntautuva IP-liikenne, jossa vastaanotetun IP-paketin lähdeosoite:

1) kuuluu teleyrityksen itsensä hallinnoimaan tai mainostamaan IP-osoiteavaruuteen tai
2) kuuluu IP-osoiteavaruuteen, joka on varattu ei-julkiseen käyttöön tai
3) ei kuulu sen liikennettä välittävän teleyrityksen toisille teleyrityksille mainostamiin reitteihin.

Teleyrityksen on hylättävä IP-yhteenliittämisrajapinnoissa vastaanotettavista reittimainostuksista sellaiset reitit, jotka kuuluvat teleyrityksen omiin tai sellaisiin teleyrityksen asiakkaalle toimittamiin osoitelohkoihin, joiden ei voida olettaa mainostuvan muilta teleyrityksiltä.

Edellä 1 momentissa määritelty liikenne voidaan kuitenkin välittää tai 2 momentissa kuvatut reittimainostukset yksittäisten verkkojen osalta sallia, jos sellaisesta on erityisesti sovittu.

12 § IP-liikenteen estäminen asiakasrajapinnassa

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.

Momentissa 1 tarkoitettua liikenteen suodattamista lievempänä toimenpiteenä asiakkaaseen voidaan ottaa yhteyttä tietoturvaa vaarantavan tilanteen selvittämistä varten.

Luku 4 Internetyhteyspalvelujen erityiset vaatimukset

13 § Internetyhteyspalvelujen liikennöinnin eriyttäminen

Teleyrityksen on erotettava eri asiakkaiden liikenne toisistaan siten, etteivät eri liittymien käyttäjät voi oikeudettomasti seurata toistensa liikennettä. Teleyrityksen on varmistettava, 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.

14 § Kuluttajaliittymistä lähtevän sähköpostiliikenteen ohjaus

Teleyrityksen on estettävä kuluttajaliittymistä lähtevä rajoittamaton SMTP-liikenne muuten kuin sovittujen lähtevälle SMTP-liikenteelle tarkoitettujen palvelimien kautta.

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.

15 § Haitallisen liikenteen suodatusvelvollisuus

Teleyrityksellä on oltava tekninen valmius tilapäisesti suodattaa haitallista liikennettä.

Teleyrityksen on säännöllisesti seurattava käytössä olevien suodatustoimenpiteiden soveltuvuutta niiden käyttötarkoitukseen ja huolehdittava suodatussäännöstön ajantasaisuudesta.

Teleyrityksen on ylläpidettävä ajantasaista dokumentaatiota viestintäverkoissa ja -palveluissa käytössä olevista suodatustoimenpiteistä.

16 § Internetyhteyspalveluliittymän irtikytkeminen

Teleyrityksen on kytkettävä asiakasliittymä irti yleisestä viestintäverkosta, jos viestintäpalvelun tietoturva oleellisesti vaarantuu liittymään kohdistuvan tai liittymästä lähtevän liikenteen johdosta eikä tämän määräyksen 15 §:n mukaisilla tai muilla irtikytkemistä lievemmillä toimenpiteillä pystytä huolehtimaan viestintäpalvelun tietoturvasta.

Irtikytkeminen ja takaisinkytkeminen on toteutettava teleyrityksen ennalta määrittelemien prosessien ja toimintaohjeiden mukaisesti. Toimenpiteitä toteutettaessa voidaan ottaa huomioon liittymätyypistä johtuvat erityisolosuhteet ja tietoturvauhan vakavuusaste.

Luku 5 Sähköpostipalvelujen erityiset vaatimukset

17 § Sähköpostipalvelujen yhteystiedot ja osoiteresurssien hallinta

Sähköpostipalvelua tarjoavan teleyrityksen on huolehdittava, että sähköpostipalvelujen tarjoamiseen käytettävissä verkkotunnuksissa on postmaster- ja abuse-sähköpostiosoitteet tai muut abuse-kontaktitiedot, johon saapuvia viestejä seurataan säännöllisesti.

Sähköpostipalvelua tarjoava teleyritys ei saa luovuttaa asiakkaalta vapautunutta sähköpostiosoitetta toiselle asiakkaalle ennen kuin kolme kuukautta on kulunut sähköpostiosoitteen vapautumisesta.

18 § Sähköpostipalvelujen erityinen suodatusvelvollisuus

Sähköpostipalveluja tarjoavalla teleyrityksellä on oltava käytössä ajantasaiset ja luotettavat mekanismit haitallisen sähköpostiliikenteen tunnistamiseksi ja käsittelemiseksi.

Sähköpostipalveluja tarjoavan teleyrityksen on:
1) suodatettava sellainen saapuva haitallinen liikenne, joka vaarantaa sähköpostipalvelun tuottamiseen käytettävien järjestelmien toimivuutta;
2) merkittävä tai suodatettava saapuvasta sähköpostiliikenteestä haitalliseksi tunnistettu liikenne, mikäli asiakkaan kanssa ei ole erikseen toisin sovittu ja
3) suodatettava lähtevästä sähköpostiliikenteestä haitalliseksi tunnistettu liikenne.

19 § Avoimet sähköpostin välityspalvelimet

Sähköpostipalveluja tarjoavan teleyrityksen on huolehdittava siitä, että sen hallinnoimat sähköpostijärjestelmät eivät toimi avoimina sähköpostin välityspalvelimina.

20 § Asiakkaan ja sähköpostipalvelimen välinen yhteys

Sähköpostipalvelua tarjoavan teleyrityksen on tarjottava asiakkaille ensisijaisena vaihtoehtona suojattu yhteys asiakkaan ja sähköpostilaatikon sekä asiakkaan ja lähtevän liikenteen sähköpostipalvelimen välillä. Suojaus on toteutettava siten, että palvelun käyttäjä todennetaan ja liikenne salataan. Velvoite koskee myös muita kuin selainpohjaisia sähköpostipalveluja.

Selainpohjaisten sähköpostipalvelujen asiakasyhteydet on suojattava.

Luku 6 Asiakkaille tiedottaminen

21 § Yleinen tiedotusvelvollisuus tietoturvatoimenpiteistä

Teleyrityksen on kuvattava asiakkaalle periaatteet, joilla puututaan viestintäpalvelujen tietoturvaa vaarantavaan liittymän tai palvelujen käyttöön.

22 § Internetyhteyspalvelun erityiset tiedotusvelvollisuudet

Teleyrityksen on tiedotettava asiakkaalle viimeistään internetyhteyspalveluliittymää käyttöönotettaessa liittymän käyttämiseen liittyvistä yleisistä ja liittymätyyppikohtaisista tietoturvariskeistä sekä asiakkaan käytettävissä olevista toimenpiteistä tietoturvasta huolehtimiseksi.

23 § Sähköpostipalvelun erityiset tiedotusvelvollisuudet

Sähköpostipalvelua tarjoavan teleyrityksen on kuvattava asiakkaille yleiset saapuvan ja lähtevän sähköpostiliikenteen suodatusperiaatteet ja sähköpostiosoitteiden hallinnointia koskevat käytännöt.

Luku 7 Voimaantulosäännökset

24 § Voimaantulo

Tämä määräys tulee voimaan 4.3.2015 ja on voimassa toistaiseksi.

25 § Tiedonsaanti ja julkaiseminen

Tämä määräys on julkaistu Viestintäviraston määräyskokoelmassa ja se on saatavissa Viestintäviraston asiakaspalvelusta:

Käyntiosoite	Itämerenkatu 3 A, Helsinki
Postiosoite	PL 313, 00181 Helsinki
Puhelin	0295 390 100
Faksi	0295 390 270
WWW-sivusto	http://www.viestintävirasto.fi/
Y-tunnus	0709019-2

Helsingissä 4 päivänä maaliskuuta 2015

Asta Sihvonen-Punkka
Pääjohtaja

Kirsi Karlamaa
Johtaja