Antopäivä:	Voimaantulopäivä:	Voimassa:
[pp.kk.vvvv]	[pp.kk.vvvv]	toistaiseksi

Säädösperusta
Laki sähköisen viestinnän palveluista (917/2014) 244, 247 ja 272 §

Määräyksen vastaisen toiminnan seuraamuksista säädetään:
Laki sähköisen viestinnän palveluista (917/2014) 330–332, 340 ja 349 §

Täytäntöönpantava EU-lainsäädäntö:
Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/1972 40 artikla
Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY 4 artikla

Muutostiedot:
Kumoaa Viestintäviraston 4.3.2015 teletoiminnan tietoturvasta antaman määräyksen 67 A/2015 M

Määräys teletoiminnan tietoturvasta

Sisällys

Luku 1 Soveltamisala ja määritelmät

1 Soveltamisala

1. Tätä määräystä sovelletaan yleiseen teletoimintaan.

2. Määräyksen 15 kohdan 1 alakohtaa sovelletaan myös viranomaisverkkoon ja viranomaisviestintään liittyvään viestintäpalveluun siltä osin kuin nämä yhteenliitetään yleiseen viestintäverkkoon tai yleisesti saatavilla olevaan viestintäpalveluun.

3. Tässä määräyksessä määrätään:
   - luvussa 2 tietoturvatoimenpiteistä kaikissa yleisissä viestintäverkoissa ja yleisesti saatavilla olevissa viestintäpalveluissa,
   - luvussa 3 rajapintojen erityisistä vaatimuksista,
   - luvussa 4 internetyhteyspalvelujen erityisistä vaatimuksista,
   - luvussa 5 tekstiviesti- ja multimediaviestipalvelujen erityisistä vaatimuksista ja
   - luvussa 6 sähköpostipalvelujen erityisistä vaatimuksista.

2 Määritelmät

1. Tässä määräyksessä tarkoitetaan:

   1) *asiakasrajapinnalla* rajapintaa, jolla teleyrityksen asiakkaan viestintäverkko, päätelaite tai sovellus liitetään yleiseen viestintäverkkoon;

   2) *avoimella sähköpostin välityspalvelimella* sellaista sähköpostiviestien välitysjärjestelmää, jota kolmas osapuoli pystyy oikeudettomasti käyttämään sähköpostiviestien välittämiseen;

   3) *haitallisella liikenteellä* sähköisiä viestejä, (a) jotka aiheuttavat vaaraa viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle, (b) joihin voidaan kohdistaa toimia sähköisen viestinnän palveluista annetun lain 272 §:n 1 momentin 2 kohdassa tarkoitetulla tavalla viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi, tai (c) joita käytetään viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmisteluun;

   4) *suodattamisella* haitallisen liikenteen estämistä, rajoittamista, tietoturvaa vaarantavien haitallisten tietokoneohjelmien poistamista sähköisistä viesteistä tai muita näihin rinnastettavia teknisluonteisia toimia, mukaan lukien viestin merkitseminen haitalliseksi liikenteeksi;

   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;

   8) *tekstiviestipalvelulla* lyhytsanomien välittämispalvelua matkaviestinverkon tekstiviestikeskuksen välityksellä; ja

   9) *multimediaviestipalvelulla* multimediaobjekteja kuten kuvia, ääntä, videota ja muotoiltua tekstiä sisältävien lyhytsanomien välittämispalvelua matkaviestinverkon multimediaviestikeskuksen välityksellä.

2. Lisäksi tässä määräyksessä käytetään sähköisen viestinnän palveluista annetun lain (917/2014) 3 §:n määritelmiä.

Luku 2 Yleiset tietoturvavaatimukset

3 Tietoturvallisuuden huomioiminen

1. Teleyrityksen on otettava viestintäverkkojen ja -palvelujen elinkaaren eri vaiheissa huomioon:

   1) tietoturvallisuuden ja riskien hallinta;

   2) henkilöstöturvallisuus;

   3) tietojärjestelmä- ja tietoliikenneturvallisuus sekä fyysinen turvallisuus;

   4) tietoturvallinen operointi ja muutoshallinta;

   5) tietoturvaa häiritsevien tai uhkaavien tilanteiden havaitseminen ja hallinta;

   6) jatkuvuudenhallinta;

   7) havainnointi, testaus ja tietoturvallisuuden arvioinnit; ja

   8) uhkatietoisuuden ylläpito sekä tilaajien ja käyttäjien tiedottaminen.

2. Teleyrityksen on dokumentoitava ja ylläpidettävä ajantasainen kuvaus siitä, miten se toteuttaa toiminnassaan 1 alakohdan mukaiset tekijät ja muut jäljempänä tässä luvussa mainitut vaatimukset.

4 Tietoturvallisuuden ja riskien hallinta

1. Teleyrityksen on otettava tietoturvallisuuden ja riskien hallinta huomioon toteuttamalla vähintään seuraavat vaatimukset:

   1) Teleyrityksellä on oltava asianmukainen tietoturvapolitiikka ja sitä tarkentavat toimintaperiaatteet, joita sen on ylläpidettävä säännöllisesti huomioiden vähintään toimintaympäristön muutokset, havaitut poikkeamat, harjoitukset sekä ennakoitavissa olevat muutokset tietoturvan uhkaympäristöön.

   2) Teleyrityksen on tunnistettava teletoiminnan jatkuvuuden kannalta tärkeät toiminnot, tiedot ja järjestelmät sekä arvioitava ja käsiteltävä jatkuvana prosessina niihin kohdistuvat tietoturvariskit. Toimitusketjujen, virtualisointiympäristöjen ja reunalaskentayksiköiden riskien arviointiin tulee kiinnittää erityistä huomiota.

   3) Teleyrityksen on määriteltävä asianmukaiset tietoturvaroolit ja -vastuut tietoturvapolitiikan ja sitä tarkentavien toimintaperiaatteiden mukaisesti. Teleyrityksen on estettävä tietoturvaa vaarantavien vastuu- ja tehtäväkokonaisuuksien syntyminen tai, jos se ei ole mahdollista, hallittava muutoin niistä aiheutuvat riskit.

   4) Teleyrityksen on määriteltävä toimittajasuhteita ja toimittajasopimuksia koskevat asianmukaiset tietoturvavaatimukset ja laadittava tarkentavat toimintaperiaatteet ja riskienhallintaprosessit, joilla varmistetaan viestintäverkkojen ja -palvelujen tietoturva koko toimitusketjussa.

2. Edellä 1 alakohdan luetelmakohdan 2 riskienkäsittelynprosessin tulokset on säilytettävä vähintään kolmen vuoden ajan tai kolmelta viimeisimmältä käsittelykerralta, sen mukaan kumpi säilytysaika on pitempi.

5 Henkilöstöturvallisuus

Teleyrityksen on otettava henkilöstöturvallisuus huomioon toteuttamalla vähintään seuraavat vaatimukset:

1) Teleyrityksen on toteutettava asianmukaiset selvitykset käyttämänsä henkilöstön luotettavuudesta varmistumiseksi, jos se on henkilön tehtävien ja vastuiden kannalta tarpeen.

2) Teleyrityksen on huolehdittava, että henkilöstöllä on riittävä tietoturvaosaaminen ja että tietoturvakoulutusta järjestetään säännöllisesti henkilöstön osaamisen ylläpitämiseksi. Teleyrityksen on huolehdittava siitä, että sen henkilöstö on tietoinen määräyksen kohdassa 4.1.1 tarkoitetusta tietoturvapolitiikasta ja toimintaperiaatteista sekä niiden tavoitteista ja vaikutuksista omien työtehtäviensä osalta.

3) Teleyrityksellä on oltava asianmukaiset menettelytavat henkilöstössä tai henkilöstön tehtävissä tapahtuvista muutoksista aiheutuvien tietoturvariskien hallitsemiseksi.

4) Teleyrityksellä on oltava asianmukaiset menettelytavat tietoturvaa koskevien toimintaperiaatteiden ja menettelyjen noudattamista koskeviin henkilöstön toiminnasta johtuviin poikkeamiin puuttumiseksi sekä henkilöstön toiminnasta johtuvien tietoturvaloukkauksien käsittelemiseksi.

6 Tietojärjestelmä- ja tietoliikenneturvallisuus sekä fyysinen turvallisuus

1. Teleyrityksen on otettava tietojärjestelmä- ja tietoliikenneturvallisuus huomioon toteuttamalla vähintään seuraavat vaatimukset:

   1) Teleyrityksen viestintäverkkoon ja tietojärjestelmiin pääsyä ja käyttöoikeuksien hallinnointia varten on oltava käytössä asianmukaiset menettelyt, joita ylläpidetään pääsynhallintaa koskevien kohdennettujen toimintaperiaatteiden mukaisesti.

   2) Teleyrityksen on huolehdittava viestintäverkkojen ja -palvelujen, henkilöstön käytössä olevien päätelaitteiden ja tietojärjestelmien eheydestä ja suojattava niitä haitallisen koodin lisäykseltä sekä haittaohjelmilta, jotka voisivat muuttaa järjestelmien toimintoja.

   3) Teleyrityksen on suojattava viestintäverkkojen ja -palvelujen kannalta keskeiset järjestelmät palvelunestohyökkäyksiä vastaan. Suojaustoimenpiteet tulee mitoittaa ajantasaisen riskiarvion mukaisesti.

   4) Teleyrityksellä on oltava kohdennetut toimintaperiaatteet ja asianmukaiset menettelyt kryptografian ja salauksen käytöstä välitystietojen, viestien, sijaintitietojen, ohjausliikenteen ja teletoiminnassa käytettyjen teleyrityksen tietoaineistojen säilytyksen ja siirtämisen aikana. Toimintaperiaatteissa on määriteltävä tietoturvariskeihin nähden ainakin salausta edellyttävät tietoaineistot ja liikennetapaukset sekä käytettävät salaustekniikat ja -käytännöt, salausavainten hallinta ja poikkeukset salauksen käytöstä. Teleyrityksen on käytettävä asianmukaista salausta aina, kun se on teknisesti mahdollista ja oikeasuhteista tietojen säilyttämiseen tai siirtämiseen liittyviin tietoturvariskeihin ja salauksesta aiheutuviin kustannuksiin nähden.

5) Teleyrityksellä on oltava asianmukaiset toimintaperiaatteet ja menettelyt salausavainmateriaalien ja todentamisessa käytettävien salaisten tietojen suojaamiselle ja hallinnalle.

6) Virtualisointiympäristössä toteutetut viestintäverkkojen ja -palvelujen komponentit on toteuttava siten, että vain niiden toiminnan kannalta välttämättömät toiminnallisuudet ja pääsyoikeudet on sallittu.

2. Teleyrityksellä on oltava asianmukaiset toimintaperiaatteet ja menettelyt tietojärjestelmien, laitteiden, tietoaineistojen ja toimitilojen fyysisestä turvallisuudesta sekä laitteiden ympäristöolosuhteista huolehtimiselle. Laitetilojen fyysisestä suojaamisesta määrätään myös Liikenne- ja viestintäviraston määräyksessä viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista.

7 Tietoturvallinen operointi ja muutoshallinta

1. Teleyrityksen on toteutettava viestintäverkkojen ja -palvelujen operointi ja muutoshallinta siten, että siinä otetaan huomioon vähintään seuraavat vaatimukset:

   1) Teleyrityksellä on oltava asianmukaiset toimintaperiaatteet ja menettelyt viestintäverkon tai -palvelun komponenttien käytölle (operoinnille).

   2) Teleyrityksellä on oltava asianmukaiset muutoksenhallintamenettelyt, joilla pienennetään muutoksista johtuvien tietoturvahäiriöiden todennäköisyyttä tai tarvittaessa palautetaan muutosta edeltänyt tai muu toimiva tila.

   3) Teleyrityksellä on oltava asianmukaiset toimintaperiaatteet ja menettelyt omaisuuden ja konfiguraatioiden hallintaa varten.

2. Muutoshallinnasta määrätään lisäksi Liikenne- ja viestintäviraston teletoiminnan häiriötilanteista antaman määräyksen 9 §:ssä.

8 Testaaminen ja tietoturvallisuuden arvioinnit

Teleyrityksen on toteuttava viestintäverkkojen ja -palvelujen tietoturvallisuuden testaus ja arviointi siten, että niissä otetaan huomioon vähintään seuraavat vaatimukset:

1) Teleyrityksellä on oltava asianmukaiset toimintaperiaatteet ja menettelyt viestintäverkkojen ja -palvelujen komponenttien tietoturvallisuuden testaamiseksi ja tarvittaessa riskiarvion mukaan niitä koskevien turvallisuusarviointien suorittamiseksi.

2) Teleyrityksellä on oltava asianmukaiset toimintaperiaatteet ja menettelyt, joilla se seuraa tietoturvapolitiikkansa ja toimintaperiaatteidensa sekä toimintaansa kohdistuvien tietoturvavaatimusten toteutumista (tietoturvallisuuden arviointi). Vähintään viimeisimmän arvioinnin tulokset on säilytettävä.

9 Uhkatiedon ylläpito

Teleyrityksellä on oltava asianmukaiset menettelyt viestintäverkkojen ja -palvelujen tietoturvaan liittyvien uhkatietojen keräämiseksi ja uhkien arvioimiseksi.

10 Standardien noudattaminen

1. Matkaviestinverkon teleyrityksellä on oltava tarkoituksenmukaiset menettelyt, joilla varmistetaan liitteessä 1 mainittujen teknisten määritysten (standardien) turvallisuusvaatimusten toteuttaminen LTE-tekniikalla toteutetussa neljännen sukupolven matkaviestinverkossa, viidennen sukupolven matkaviestinverkossa sekä IP-pohjaisessa yleisessä

puhelinpalvelussa. Standardista on käytettävä uusinta 3GPP:n hyväksymää versiota, joka vastaa teleyrityksen viestintäverkossaan tai -palvelussaan toteuttamaa toiminnallisuutta.

2. Teleyritys voi jättää 1 alakohdassa tarkoitetun turvallisuusvaatimuksen toteuttamatta, jos sen toteuttaminen ei ole tarkoituksenmukaista ottaen huomioon sen merkitys kyseisessä tapauksessa viestintäverkon tai -palvelun tietoturvalle ja muut asiaan liittyvät toimenpiteet tietoturvasta huolehtimiseksi.

3. Teleyrityksen on ylläpidettävä kuvaus siitä, miten se huomioi toiminnassaan 1 alakohdan. Turvallisuustoiminnon tai mekanismin toteuttamatta jättäminen 2 alakohdan perusteella ja toteuttamatta jättämisen perusteet tulee dokumentoida kunkin turvallisuusvaatimuksen osalta erikseen.

11 Tietoaineistot

Teleyrityksessä on oltava käytössä teletoiminnan kannalta tärkeiden tietoaineistojen luokitusjärjestelmä, luokituskriteerit ja luokitteluun liittyvä tietoaineistojen käsittelymenettelyt.

12 Asiakkaan tunnistaminen tietoturvasta huolehtimiseksi

Teleyrityksellä on oltava asianmukaiset toimintaperiaatteet ja menettelyt tilaajan tai käyttäjän tunnistamiseksi asioinnin riskitasoon nähden riittävän luotettavalla tavalla ennen kuin asiakkaan palveluun tehdään olennaisia viestintäpalvelun tietoturvaan vaikuttavia muutoksia taikka tilaajalle tai käyttäjälle annetaan luottamuksellisia tietoja.

13 IP-osoitteiden dokumentointi

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

14 Hallintaverkon ja hallintayhteyksien liikenne

1. Teleyrityksellä tulee olla asianmukaiset verkonhallintaa ja hallintayhteyksiä koskevat toimintaperiaatteet ja menettelyt.

2. Teleyrityksen on asianmukaisesti suojattava ja tarvittaessa salattava viestintäverkon tai -palvelun komponenttien hallintaliikenne siten, että oikeudettomien muutosten tekeminen viestintäverkon tai -palvelun komponentteihin on toimintaperiaatteiden mukaisesti estetty.

3. Teleyrityksellä on oltava asianmukaiset menettelyt, joilla arvioidaan verkonhallintaan käytettävistä päätelaitteesta aiheutuvat tietoturvauhat ja hallitaan niistä johtuvat riskit.

Luku 3 Viestintäverkkojen ja -palvelujen rajapintojen erityiset vaatimukset

15 Rajapintojen häiriöiden estäminen ja niiltä suojautuminen

1. Teleyrityksen on huolehdittava, että sen viestintäverkon tai -palvelun komponentit eivät aiheuta häiriötä muille viestintäverkoille tai -palveluille. Teleyrityksellä on oltava tarkoituksenmukaiset mekanismit näiden häiriöiden estämiseksi.

2. Teleyrityksen on suojattava viestintäverkkonsa ja -palvelunsa yhteenliittämis-, sovellus- ja asiakasrajapinnoista tulevalta haitalliselta liikenteeltä toteuttamalla verkossaan tarvittavat suojausmekanismit.

16 Tarpeettomien porttien, palvelujen ja protokollien sulkeminen

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

17 IP-yhteenliittämisrajapintojen suojaaminen ja liikenteen suodattaminen

1. Teleyrityksen on IP-yhteenliittämisrajapintojen suojaamiseksi vähintään:

   1) havainnoitava reitityspoikkeamia;

   2) suojattava reittitietojen vaihtamiseen käytettävät istunnot aina, kun se on mahdollista;

   3) suodatettava viestintäverkkoonsa suuntautuvaa virheellisen IP-lähdeosoitteen sisältävää liikennettä, mukaan lukien liikenne, jossa vastaanotetun IP-paketin lähdeosoite

      i) kuuluu teleyrityksen itsensä hallinnoimaan tai mainostamaan IP-osoiteavaruuteen tai IP-osoiteavaruuteen, joka on varattu ei-julkiseen käyttöön taikka

      ii) ei kuulu sen liikennettä välittävän teleyrityksen toisille teleyrityksille mainostamiin reitteihin;

   4) hylättävä vastaanotettavista reittimainostuksista

      i) reitit, jotka kuuluvat teleyrityksen omiin tai sellaisiin teleyrityksen asiakkaalle toimittamiin osoitelohkoihin, joiden ei voida olettaa mainostuvan muilta teleyrityksiltä; ja

      ii) reittimainostukset, joiden ROA-tietue (Route Origin Authorization) on virheellinen; sekä

   5) luotava hallinnoimilleen verkkoalueille ROA-tietueet, jos se on teknisesti mahdollista, sekä huolehdittava niiden allekirjoittamisesta ja julkaisusta.

2. Edellä 1 alakohdan 3 luetelmakohdassa määritelty liikenne voidaan kuitenkin välittää ja 4 luetelmakohdassa kuvatut reittimainostukset yksittäisten verkkojen osalta sallia, jos sellaisesta on erityisesti sovittu toimijoiden kesken.

18 IP-liikenteen lähdeosoitteen väärentämisen estäminen asiakasrajapinnassa

1. 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.

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

19 Matkaviestinverkon rajapintojen suojaaminen

Teleyrityksen on suojattava matkaviestinverkon rajapinnat viestintäverkon ja -palvelun tietoturvan varmistamiseksi sekä liikenteen oikeudettoman uudelleenohjaamisen estämiseksi. Teleyrityksen on matkaviestinverkon rajapinnoissaan vähintään:

1) valvottava signalointirajapintojen tietoturvaa sekä suunniteltava, toteutettava ja ylläpidettävä ajantasaiseen uhkatietoon ja riskiarvioon pohjautuvat signalointirajapintojen tietoturvan hallintatoimenpiteet;

2) suojattava matkaviestinverkon viipaleen hallintaliittymä siten, että vain valtuutetut osapuolet voivat luoda, muuttaa tai poistaa viipaleita taikka saada tietoa viipaleen ominaisuuksista, tilaajista tai käyttäjistä;

3) toteutettava matkaviestinverkon ensisijaisen todennuksen lisäksi viipalekohtainen päätelaitteiden käyttöoikeustodennus ja valtuutus, jossa käytetään muita kuin ensisijaisessa todennuksessa käytettyjä tunnistetietoja, jos se on tarpeen ottaen huomioon kyseisen viipaleen käyttöön liittyvät tietoturvauhat ja tekniset mahdollisuudet käyttöoikeustodennuksen ja valtuutuksen toteuttamiseksi; sekä

4) suojattava viestintäverkot ja -palvelut reunalaskentayksikön niihin mahdollisesti kohdistamalta haitalliselta liikenteeltä toteuttamalla verkossa tarpeelliset suojausmekanismit.

Luku 4 Internetyhteyspalvelujen erityiset vaatimukset

20 Internetyhteyspalvelujen liikennöinnin eriyttäminen

1. 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.

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

21 Kuluttajaliittymistä lähtevän sähköpostiliikenteen ohjaus

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

2. Sen estämättä, mitä 1 alakohdassa 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 valmius reagoida nopeasti häiriötilanteisiin.

22 Haitallisen liikenteen suodatusvelvollisuus internetyhteyspalvelussa

1. Teleyrityksellä on oltava tarkoituksenmukaiset järjestelmät ja menettelytavat internetyhteyspalvelun haitallisen liikenteen tilapäiseen suodattamiseen.

2. Teleyrityksen on säännöllisesti seurattava käytössä olevien suodatustoimenpiteiden soveltuvuutta käyttötarkoitukseensa ja huolehdittava suodatussäännöstön ajantasaisuudesta.

3. Teleyrityksen on ylläpidettävä ajantasaista dokumentaatiota käytössä olevista suodatustoimenpiteistä.

23 Internetyhteyspalveluliittymän irtikytkeminen

1. Teleyrityksen on kytkettävä asiakasliittymä irti yleisestä viestintäverkosta, jos viestintäpalvelun tietoturva oleellisesti vaarantuu liittymään kohdistuvan tai liittymästä lähtevän liikenteen johdosta eikä tämän määräyksen 22 kohdan mukaisilla tai muilla irtikytkemistä lievemmillä toimenpiteillä pystytä huolehtimaan viestintäpalvelun tietoturvasta.

2. 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 Tekstiviesti- ja multimediaviestipalvelujen erityiset vaatimukset

24 Teksti- ja multimediaviestiliikenteen suodatus

1. Teleyrityksellä on oltava tarkoituksenmukaiset järjestelmät ja menettelytavat tekstiviesti- ja multimediaviestipalvelujen haitallisen liikenteen tilapäiseen suodattamiseen.

2. Teksti- ja multimediaviestipalveluita tarjoavan teleyrityksen on:

   1) merkittävä tai suodatettava saapuvasta viestiliikenteestä haitalliseksi tunnistettu liikenne, ellei asiakkaan kanssa ole erikseen toisin sovittu; sekä

   2) suodatettava lähtevästä viestiliikenteestä haitalliseksi tunnistettu liikenne.

3. Edellä 1 ja 2 alakohdassa määrättyä ei sovelleta multimediaviestipalveluun, jos teleyritys muutoin havainnoi tietoturvaa vaarantavia häiriötilanteita ja sillä on kyky reagoida niihin nopeasti.

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

Luku 6 Sähköpostipalvelujen erityiset vaatimukset

25 Sähköpostipalvelujen yhteystiedot ja osoiteresurssien hallinta

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

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

26 Sähköpostipalvelujen erityinen suodatusvelvollisuus

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

2. Sähköpostipalveluja tarjoavan teleyrityksen on:

   1) suodatettava sellainen saapuva haitallinen liikenne, joka vaarantaa sähköpostipalvelun tuottamiseen käytettävien järjestelmien tietoturvaa;

   2) merkittävä tai suodatettava saapuvasta sähköpostiliikenteestä haitalliseksi tunnistettu liikenne, ellei asiakkaan kanssa ole erikseen toisin sovittu ja

   3) suodatettava lähtevästä sähköpostiliikenteestä haitalliseksi tunnistettu liikenne.

27 Avoimet sähköpostin välityspalvelimet

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

28 Asiakkaan ja sähköpostipalvelimen välinen yhteys

1. 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.

2. Selainpohjaisten sähköpostipalvelujen asiakasyhteydet on suojattava.

Luku 7 Voimaantulosäännökset

29 Voimaantulo [ja siirtymäaika]

1. [Tämä määräys tulee voimaan kolme kuukautta määräyksen antamisesta.]

2. Tällä määräyksellä kumotaan 4.3.2015 annettu Viestintäviraston määräys 67 A/2015 M teletoiminnan tietoturvasta.

Helsingissä (pv) päivänä (kk)kuuta 20(vv)

Ratkaisija

Esittelijä

Liite 1 Noudatettavat tekniset standardit

3GPP TS 33.116, Security Assurance Specification (SCAS) for the MME network product class

3GPP TS 33.216, Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class

3GPP TS 33.226, Security assurance for IP Multimedia Subsystem (IMS)

3GPP TS 33.250, Security assurance specification for the PGW network product class

3GPP TS 33.326, Security Assurance Specification (SCAS) for the Network Slice-Specific Authentication and Authorization Function (NSSAAF) network product class

3GPP TS 33.511, Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class

3GPP TS 33.512, 5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)

3GPP TS 33.513, 5G Security Assurance Specification (SCAS); User Plane Function (UPF)

3GPP TS 33.514, 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class

3GPP TS 33.515, 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class

3GPP TS 33.516, 5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class

3GPP TS 33.517, 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class

3GPP TS 33.518, 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class

3GPP TS 33.519, 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class

3GPP TS 33.520, 5G Security Assurance Specification (SCAS); Non-3GPP InterWorking Function (N3IWF)

3GPP TS 33.521, 5G Security Assurance Specification (SCAS); Network Data Analytics Function (NWDAF)

3GPP TS 33.522, 5G Security Assurance Specification (SCAS); Service Communication Proxy (SCP)

3GPP TS 33.523, 5G Security Assurance Specification (SCAS); Split gNB product classes

3GPP TS 33.526, Security Assurance Specification for Management Function (MnF)

3GPP TS 33.527, Security Assurance Specification (SCAS) for 3GPP virtualized network products

3GPP TS 33.528, Security Assurance Specification (SCAS) for Policy Control Function (PCF)

3GPP TS 33.529, Security Assurance Specification (SCAS) for the Short Message Service Function (SMSF) network product class

3GPP TS 33.537, Security Assurance Specification (SCAS) for the Authentication and Key Management for Applications (AKMA) Anchor Function (AAnF)

[Yllä olevista valmisteluvaiheessa olevat standardit otetaan tähän liitteeseen, jos ne julkaistaan määräyksen aikataulun puitteissa.]