

**SUOSITUS MÄÄRÄYKSEN  
VIESTINTÄVIRASTO 13 A/2008 M  
SOVELTAMISESTA**

**INTERNET-YHTEYSPALVELUJEN  
TIETOTURVASTA JA TOIMIVUUDESTA**

## Sisällys

<b>1. SOVELTAMISALA</b> .....	<b>2</b>
<b>2. MÄÄRITELMÄT</b> .....	<b>2</b>
<b>3. ASIAKASLIITTYMIEN TIETOTURVALLISUUS</b> .....	<b>3</b>
3.1. TIEDOTTAMINEN ASIAKKAALLE .....	4
3.2. ASIAKASTIEDOTUS LIITTYMÄN TEKNISTEN RAJOITUSTEN OSALTA .....	4
<b>4. KULUTTAJALIITTYMÄÄN SUUNTAUTUVAN SÄHKÖPOSTILIIKENTEEN OHJAUS JA REITITYS</b> .....	<b>5</b>
<b>5. KULUTTAJALIITTYMÄSTÄ LÄHTEVÄN SÄHKÖPOSTILIIKENTEEN OHJAUS JA REITITYS</b> .....	<b>6</b>
<b>6. OSOITEPOHJAINEN SUODATUS ASIAKASLIITTYMISSÄ</b> .....	<b>7</b>
<b>7. HAITALLISEN LIIKENTEEN HAVAITSEMINEN JA SUODATTAMINEN ASIAKASLIITTYMISSÄ</b> .....	<b>7</b>
7.1. HAITALLISEN LIIKENTEEN HAVAITSEMINEN .....	7
7.2. LIIKENTEEN TILAPÄISEN SUODATTAMISEN PROSESSIT JA TOIMINTAMALLIT .....	8
7.3. ASIAKASLIITTYMIEN IRTIKYTKEMINEN .....	8
<b>8. RUNKOVERKON TIETOTURVALLISUUS</b> .....	<b>9</b>
<b>9. OSOITE- JA REITTISUODATUS RUNKOVERKOSSA</b> .....	<b>10</b>
9.1. REITTIMAINOSTUKSEN TARKASTAMINEN .....	10
9.2. VIRHEELLISIÄ LÄHDEOSOITTEITA SISÄLTÄVÄN LIIKENTEEN SUODATTAMINEN .....	11
9.3. SUUNNATTUJEN YLEISLEVITYSVIESTIEN VÄLITTÄMISEN ESTÄMINEN .....	11
9.4. MAINOSTETTUJEN VERKKOJEN DOKUMENTOINTI .....	11
9.5. KÄYTTÄMÄTTÖMIEN OSOITEAVARUUKSIEN SUODATTAMINEN.....	11
<b>10. HAITALLISEN LIIKENTEEN HAVAITSEMINEN JA SUODATTAMINEN RUNKOVERKOSSA</b> .....	<b>12</b>
<b>11. INTERNET-YHTEYSPALVELUJEN TOIMIVUUDEN JA LAADUN SEURANTA</b> .....	<b>12</b>
11.1. VIESTINTÄVERKON TAI –PALVELUN KÄYTETTÄVYYDEN KANNALTA MERKITTÄVÄT POIKKEUSTILAN TEET .....	12
11.2. VERKON KUORMITUSTILANNE.....	13
11.3. KÄYTTÖKATKOKSET INTERNET-YHTEYSPALVELUSSA JAOTELTUNA TYPPEITTÄIN.....	13
11.4. TODETUT VIKATILANTEET YKSITTÄISISSÄ ASIAKASLIITTYMISSÄ JAOTELTUNA TYPPEITTÄIN .....	13
11.5. TÄMÄN MÄÄRÄYKSEN PERUSTEELLA IRTIKYTKETTYJEN LIITTYMIEN MÄÄRÄ .....	13
<b>12. TELEYRITYKSEN YHTEYSTIEDOT YLEISISSÄ IP-OSOITEREKISTEREISSÄ</b> .....	<b>13</b>

## 1. SOVELTAMISALA

Määräystä sovelletaan yleisissä viestintäverkoissa tarjottavien Internet -yhteyspalvelujen tuottamiseen sekä teleyrityksen näihin toimintoihin käyttämiin järjestelmiin, viestintäverkkoihin ja viestintäpalveluihin. Internet-yhteyspalvelulla tarkoitetaan tässä määräyksessä Internet-liikenteen välittämistä.

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

Määräyksessä säädetyt tietoturvatoinenpiteet on sähköisen viestinnän tietosuojalain (516/2004) 19 §:n mukaisesti suhteutettava uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin.

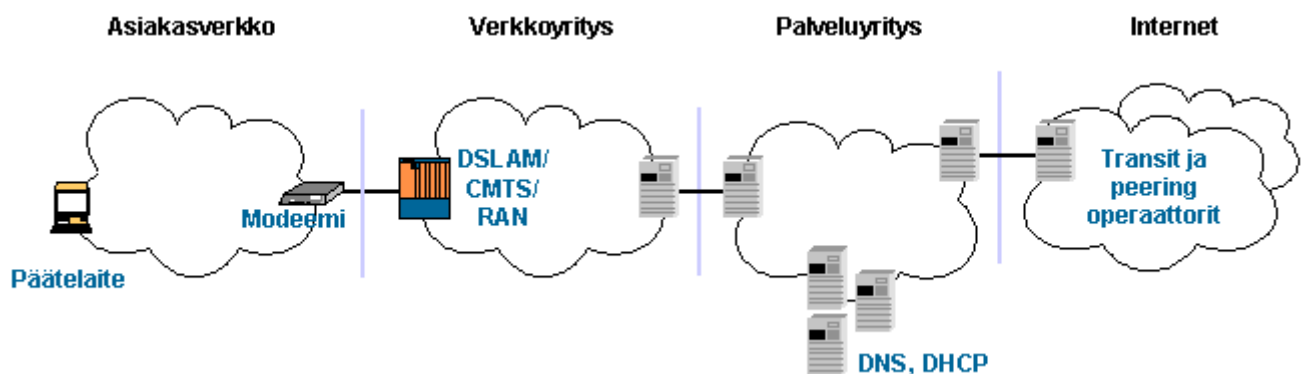
## 2. MÄÄRITELMÄT

*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 joilla 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 analogista modeemyhteyttä, radioverkkoa, langatonta lähiverkkoyhteyttä, kaapelidataverkkoa tai DSL-tekniikkaa käyttäen.

Asiakasliittymän toteutukseen liittyviä rajapintoja on havainnollistettu seuraavassa kaaviokuvassa.



Kuva 1. Esimerkki verkon rajapinnoista asiakasliittymään

*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), sähköpostipalvelu (SMTP) sekä www-välityspalvelu (proxy). Palvelut voivat olla joko liittymän lisäpalveluita tai liittymän käyttämisen kannalta välttämättömiä palveluita, kuten nimipalvelu.

*Transit-liikenteellä* tai *-palvelulla* tarkoitetaan tässä määräyksessä teleyrityksen asiakkailleen tai toiselle teleyritykselle tarjoamaa Internet-liikenteen vaihto- tai välityspalvelua.

Monet teleyritykset toimivat Internet-verkossa autonomisena järjestelmänä (AS) ja ovat liittyneet useisiin muihin vastaaviin verkkoihin erilaisten julkisten tai yksityisten liikenteen vaihto- tai välityssopimusten kautta. Verkot kommunikoivat keskenään Border Gateway-Protokollan (BGP) välityksellä.

Samankokoiset verkot voivat vaihtaa liikennettä keskenään tyypillisesti vastikkeetta peering-liikenteen kautta. Osa liikenteen vaihdosta taas tapahtuu maksullisena transit-liikennöintinä, jollaista on erityisesti liikenne, jossa kaikkia Internet-reittejä mainostetaan toiselle teleyritykselle.

Yhdysliikenne toteutetaan tyypillisesti useamman kuin yhden yhdysliikennepisteen kautta liikennöinnin varmistamiseksi.

*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 osoitevaruuksiin.

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 käytettävyyteen tai tietoturvaan kohdistuvan uhan torjumiseksi tai palvelun tietoturvaan huolehtimiseksi. Suodatustoimenpiteitä toteutettaessa teleyrityksen tulee ottaa huomioon sähköisen viestinnän tietosuojalain 5 luvun lisäksi myös kuluttajansuojalaissa (38/1978) ja viestintämarkkinalaissa (393/2003) asetetut vaatimukset.

### **3. ASIAKASLIITTYMIEN TIETOTURVALLISUUS**

Teleyrityksen on suoritettava asiakasliittymiä koskevat toteutus- ja ylläpitotoimenpiteet siten, että tietoturvanäkökohdat on otettu huomioon.

Kun teleyritys tarjoaa asiakasliittymää, jossa teleyritys jakaa liittymän kapasiteetin tilaajien kesken, teleyrityksen on erotettava tilaajien liikenne toisistaan siten, etteivät tilaajat oikeudettomasti voi seurata toistensa liikennettä. Teleyrityksen tulee varmistaa, että toisen tilaajan liikenteen oikeudeton uudelleenohjaus liittymien välillä ei ole mahdollista.

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. Vastavantalaisia jaettua kapasiteettia käyttäviä verkkototeutuksia käytetään esimerkiksi kaupunkiverkoissa, joissa palvelun käyttö on avointa kaikille verkon kantaman oleskeleville käyttäjille.

Taloyhtiöverkkojen osalta tilanne liikenteen estämisessä tilaajien kesken on yksinkertaisempi kuin esimerkiksi yritysverkoissa, sillä taloyhtiön käyttäjillä ei tyypillisesti ole tarvetta liikennöidä suoraan keskenään, vaan liikenne suuntautuu tavallisesti taloyhtiöverkon ulkopuolelle.

Tilaajien liikenteen erottaminen toisistaan voidaan toteuttaa käytännössä esimerkiksi määrittelemällä taloyhtiöverkon Ethernet tai homepna-kytkimien huoneistokohtaiset portit erillisiin Virtual LANeihin (VLAN). Vaihtoehtoisesti voidaan estää liikenne eri huoneistokohtaisten porttien välillä kytkimissä.

Teleyrityksen tulisi tiedottaa asiakkaalleen kapasiteetin jakoon liittyvistä tietoturvariskeistä, kun teleyritys ei itse toteuta liittymää, jossa verkon kapasiteetti jaetaan käyttäjien kesken. Tiedotta-

misvelvollisuus voi tulla kyseeseen esimerkiksi silloin kun teyryitys toteuttaa ainoastaan Internet-yhteyden taloverkkototeutuksessa ja kapasiteetin jakamisesta vastaa taloyhtiö yhteisötalajana.

Kun teyryitys toteuttaa Internet-liittymän käyttäen tekniikkaa (esimerkiksi hotspot-tyyppiset salaamattomat WLAN (Wireless Local Area Network)-toteutukset), joka ei oletusarvoisesti tue tilaajien liikenteen erottamista toisistaan, palvelun tietoturva on huolehdittava muulla tavoin, esimerkiksi tiedottamalla käyttäjille salaamattomaan liikennöintiin liittyvistä riskeistä.

Kuten edellä on todettu, esimerkiksi WLAN tekniikan osalta, kaikkia palveluun kohdistuvia tietoturvauhkia ei aina ole mahdollista poistaa. Tällöinkin uhkasta on tiedotusvelvollisuus asiakkaalle. Sähköisen viestinnän tietosuojalain 19 §:n mukaan teyryityksen viestintä- ja verkkopalvelun tietoturva huolehtimiseksi suoritettavat toimet on suhteutettava uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin.

### **3.1. Tiedottaminen asiakkaalle**

Teyryityksen on kerrottava asiakkaalle ennen asiakasliittymän kytkeästä liittymän käyttämiseen liittyvistä yleisistä ja liittymätyyppikohtaisista tietoturvariskeistä sekä käytettävissä olevista toimenpiteistä tietoturva huolehtimiseksi.

Tiedottamisen pääasiallisen sisällön tulee painottua asiakkaan tai asiakasliittymän käyttäjän käytettävissä oleviin toimenpiteisiin tietoturvallisuudesta huolehtimiseksi. Näitä ovat esimerkiksi ohjelmistopalomuurin käyttöönotto ennen tietokoneen liittämistä verkkoon, virustorjunnan hankkiminen ja käyttöjärjestelmän sekä muiden ohjelmistojen/verkkopalvelujen päivittämisestä huolehtiminen. Teyryitys voi olla tuotteistanut kyseiset tietoturvatkaisut esimerkiksi asiakkaalle tarjottavana tietoturvapalveluna, joka sisältää työasemapalomuurin ja virustorjuntaohjelmiston.

Lisäksi asiakkaalle tulee kertoa, ajankohtaisista käyttäjään vaikuttavista tietoturvauhkista sekä mistä saa lisätietoa liittymän käyttöön liittyvistä tietoturvakysymyksistä. Asiakkaalle tulee kertoa teyryityksen yhteystiedot ongelmatilanteissa esimerkiksi jos liittymä kytketään irti yleisestä viestintäverkosta tai liittymän käytössä ilmenee muita tietoturvaongelmia.

Asiakkaalle tiedottaminen voi tapahtua esimerkiksi asiakasliittymätyyppien palvelukuvauksissa, liittymää tilattaessa, liittymätyyppiä vaihdettaessa, toimitettaessa liittymän tilausvahvistus tai liittymää toimitettaessa. Oleellista tiedottamisessa on, että tieto tulee olla asiakkaalla, mielellään kirjallisessa muodossa, ennen liittymän kytkeästä viestintäverkkoon, viimeistään liittymän toimituksen yhteydessä. Yleinen tietoturvatiedotus esimerkiksi teyryityksen www-sivustolla ei täytä näitä vaatimuksia, sillä asiakkaan järjestelmä ehtii todennäköisesti saada haittaohjelmatartunnan ennen kuin asiakas pääsee lukemaan ohjeistusta.

Jos teyryitys tarjoaa asiakasliittymiä, joissa ei ole liikenteen rajoituksia, pitää asiakkaalle tiedottaa liittymän käyttöön liittyvistä erityisistä riskeistä. Erityisillä riskeillä tarkoitetaan tässä yhteydessä esimerkiksi palvelimen ylläpitoon liittyviä tietoturvariskejä.

Erityiset tietoturvariskit rajoittamattoman sisään tulevan liikenteen osalta liittyvät esimerkiksi palvelimen ylläpitoon liittyviin laitteisto- ja ohjelmistoturvallisuuden asioihin, kuten ohjelmistopäivityksiin, käyttöoikeuksien rajaamiseen ja palvelimen ylläpitoon. Rajoittamattoman lähtevän liikenteen osalta tietoturvariskit puolestaan liittyvät esimerkiksi haittaohjelmatartunnan saaneiden työasemien aikaansaamaan roskapostiliikenteeseen.

### **3.2. Asiakastiedotus liittymän teknisten rajoitusten osalta**

Teyryityksen on määriteltävä sekä kuvattava asiakkaalle asiakasliittymän osalta selkeät käyttö-säännöt. Kuvauksessa on lueteltava keskeiset asiakasliittymän käyttöön vaikuttavat tekniset rajoitukset, kuten käytettäviin tietoliikenneportteihin, protokollaan tai liikennemäärään liittyvät pysyväisluonteiset rajoitukset sekä asiakasliittymätyyppikohtaiset liikennöintirajoitukset. Kuvauksesta on myös käytävä ilmi toimenpiteet, joilla poikkeukselliseen liikennöintiin puututaan.

Protokollakohtaisilla liikennerajoituksilla voidaan tarkoittaa esimerkiksi sovellusprotokollatasolla tehtävää tiettyjen protokollien liikennemäärien rajoittamista tiettyyn osaan liittymän kapasiteetista.

Näillä ominaisuuksilla tarkoitetaan liittymätyypin perusominaisuuksia, jotka ovat oleellinen osa liittymää. Liittymän perusominaisuuksien lisäksi asiakasliittymän tietoturvallisuudesta on mahdollista huolehtia myös tilapäisiä toimenpiteitä toteuttaen. Näistä toimenpiteistä on kerrottu jäljempänä.

Kuluttajille suunnatut asiakasliittymät voidaan jaotella esimerkiksi seuraavasti:

- suojattuun liittymään, jossa sisään tulevat yhteydet on estetty ja uloslähtevästä liikenteestä estetty tiettyjä portteja
- teholiittymään, jossa sisään tulevasta liikenteestä on estetty tiettyjä portteja ja uloslähtevä liikenne pääasiassa sallittu
- suojaamattomaan liittymään jossa liikenne on pääasiassa sallittu rajoituksetta.

Liittymän perusominaisuudet, kuten liittymätyypissä oletusarvoisesti estetyt tietoliikenneportit tai tiettyjen sovellusprotokollien priorisointi, tulee kuvata asiakkaalle esimerkiksi liittymätyypin tuotekuvauksessa, jotta asiakas voi valita käyttöönsä sopivimman liittymän. Sovellusprotokollien priorisoinnin yhteydessä asiakkaalle tulee kuvata yleisellä tasolla, millä perusteella liikennettä priorisoidaan ja kuinka paljon kapasiteettia eri sovelluksille on käytettävissä.

Kuvaus on mahdollista toteuttaa esimerkiksi kertomalla liittymäsopimuksessa käytösäännöt ja sallittavaksi katsotut verkon käytön rajat sekä kuvaamalla erillisellä tiedotesivulla teleyrityksen www-sivustolla mahdolliset käytössä olevat muuttuvat käyttörajoitukset.

Käyttörajoituksia asetettaessa tai käyttörajoituksia muutettaessa liittymäsopimuksen kestäessä tulee ottaa huomioon liittymäsopimuksen sisältö sekä noudattaa lainsäädännössä asetettuja menettelytapoja, mikäli rajoitus voidaan katsoa liittymäsopimuksen yksipuoliseksi muuttamiseksi.

Käytösäännöissä tulee liikennöintirajoitusten lisäksi käydä ilmi toimenpiteet, joilla poikkeukselliseen liikennöintiin puututaan. Kun teleyritys käyttää automaattista järjestelmää liikenteen rajoittamiseksi, esimerkiksi asettamalla karanteeniin poikkeuksellisesti liikennöivät asiakasliittymät, asiakkaille tulee kuvata yleisesti minkä rajojen rikkomisesta karanteeniin joutuu, kuinka kauan liittymä on eristettynä sekä millä edellytyksillä liittymästä jälleen sallitaan normaali liikennöinti. Liikennöintirajojen määrittely ei saa vaarantaa viestintäpalvelun tietoturvaa, eli kuvauksen ei tule olla tarpeettoman yksityiskohtainen ja kertoa tarkkoja perusteita tiettyntyyppisen liikennöinnin tulkitsemisesta haitalliseksi.

#### **4. KULUTTAJALIITTYMÄÄN SUUNTAUTUVAN SÄHKÖPOSTILIIKENTEEN OHJAUS JA REITITYS**

Internet-liittymiä tarjoavan teleyrityksen on estettävä kuluttajaliittymään suuntautuva SMTP-liikenne (Simple Mail Transfer Protocol) muualta kuin sovittujen SMTP-liikenteelle tarkoitettujen palvelimien kautta. SMTP-liikenteen estämisellä tarkoitetaan esimerkiksi teleyrityksen verkon ulkopuolelta kuluttajaliittymille tarkoitettuun verkkoavaruuteen SMTP-liikenteelle varattuun tietoliikenneporttiin suuntautuvan liikenteen estämistä tai ohjaamista sovituille SMTP-liikenteelle tarkoitetuille palvelimille. Liikenteen estämistä voidaan toteuttaa myös teleyrityksen viestintäverkon sisällä eli liittymätyyppien välillä, esimerkiksi yritys- ja kuluttajaliittymien välillä.

Liikenteen estämisellä pyritään estämään mahdollisesti haittaohjelmien mukana asentuvien avoimien sähköpostipalvelimien käyttö kuluttajaliittymissä teleyrityksen verkon ulkopuolelta. Lisäksi liikenteen estämisellä pyritään estämään kuluttajaliittymissä mahdollisesti sijaitseviin haavoittuviin sähköpostipalvelimiin murtautuminen teleyrityksen verkon ulkopuolelta sähköpostisovellusten tai palvelimien haavoittuvuutta hyväksikäyttäen.

Joillakin kuluttaja-asiakkailta voi kuitenkin olla perusteltuja tarpeita suoralle SMTP-liikenteelle kuluttajaliittymään. Teleyritys voi sallia muualtakin kuin sovittujen SMTP-liikenteelle tarkoitettujen

palvelimien kautta liittymään suuntautuvan SMTP-liikenteen. Tällöin teleyrityksen on tiedotettava liittymän tilaajalle avoimeen liikennöintiin liittyvistä riskeistä sekä käyttäjän käytettävissä olevista toimenpiteistä riskien hallitsemiseksi.

Suoraa SMTP-liikennettä kuluttajaliittymään voidaan tarvita esimerkiksi tapauksissa, jossa kuluttajaliittymässä on teleyrityksen sallima sähköpostipalvelin ja kyseiseen sähköpostipalvelimeen ei voida reitittää sähköpostia teleyrityksen oman sähköpostijärjestelmän kautta. Koska kyseessä on palvelinjärjestelmä, joka ottaa vastaan sähköpostiliikennettä rajoittamattomasta verkkoavaruudesta, on palvelun tietoturvasuudesta huolehtiminen erityisen tärkeää. Tietoturvasuudesta huolehtimisella tarkoitetaan tässä yhteydessä esimerkiksi järjestelmän oikeaa määrittelyä ja ohjelmistopäivityksistä huolehtimista.

## **5. KULUTTAJALIITTYMÄSTÄ LÄHTEVÄN SÄHKÖPOSTILIIKENTEEN OHJAUS JA REITITYS**

Internet-liittymiä tarjoavan teleyrityksen on estettävä kuluttajaliittymistä lähtevä rajoittamaton SMTP-liikenne muuten kuin sovittujen lähtevälle liikenteelle tarkoitettujen palvelimien kautta. Rajoittamattoman SMTP-liikenteen estämisellä tarkoitetaan esimerkiksi teleyrityksen kuluttajaliittymille tarkoittamasta verkkoavaruudesta teleyrityksen verkon ulkopuolelle SMTP-liikenteelle varattuun tietoliikenneporttiin suuntautuvan liikenteen estämistä tai ohjaamista sovituille lähtevälle SMTP-liikenteelle tarkoitetuille palvelimille. Liikenteen estämistä voidaan toteuttaa myös teleyrityksen viestintäverkon sisällä eli liittymätyyppien välillä, esimerkiksi yritys- ja kuluttajaliittymien välillä.

Rajoittaminen voidaan toteuttaa esimerkiksi ohjelmistoilla, joilla teleyritys hallinnoi automaattisesti uloslähtevää SMTP-liikennettä esimerkiksi viivästämällä sähköpostiliikennettä tai estämällä liikennöinnin osittain tai kokonaan liittymistä, jotka lähettävät SMTP-liikennettä hallitsemattomasti. Tällaisella poikkeavalla liikennöinnillä tarkoitetaan esimerkiksi liikennemäärältään tai vastaanottajalukumäärältään huomattavan liikenteen välittämistä kuluttajaliittymästä.

Kun rajoittamaton uloslähtevä SMTP-liikenne reitittyy ulko verkkoon sovittujen SMTP-palvelimien kautta, näissä järjestelmissä voidaan kontrolloida tehokkaasti liikennemääriä.

Teleyrityksen sähköpostijärjestelmän ei tule estää muiden kuin teleyrityksen hallinnoimien verkkotunnusten käyttämistä sähköpostin lähettäjäosoitteen verkkotunnusosassa. Asiakkaiden tulee voida käyttää vapaasti myös kolmansien osapuolien verkkotunnuksia liikennöinnissään.

Määräyksen mukaisesti toteutetulla rajoittamattoman SMTP-liikenteen estolla ei saa olla vaikutusta muita tietoliikenneportteja käyttävään sähköpostiliikennöintiin, kuten käyttäjätunnistusta tai salausta käyttäviin sähköpostiprotokolliin. Näin Internet-liittymiä tarjoavan teleyrityksen asiakkailta on mahdollisuus liikennöidä turvallisesti myös toisen palveluntarjoajan hallinnassa olevaan sähköpostijärjestelmään.

Joillakin kuluttaja-asiakkailta voi olla perusteltuja tarpeita suoralle SMTP-liikenteelle kuluttajaliittymästä minne tahansa teleyrityksen verkon ulkopuolelle. Teleyritys voi sallia muualtakin kuin sovittujen lähtevälle SMTP-liikenteelle tarkoitettujen palvelimien kautta liittymästä lähtevän rajoittamattoman SMTP-liikenteen. Tällöin teleyrityksen on tiedotettava liittymän tilaajalle avoimeen liikennöintiin liittyvistä riskeistä sekä kiinnitettävä erityistä huomiota kuluttajaliittymästä lähtevän SMTP-liikenteen määrän seurantaan viestintäverkossaan. Tällöin teleyrityksellä on oltava myös valmiudet reagoida nopeasti häiriötilanteisiin.

Pääsääntöisesti lähtevä SMTP-liikenne myös kuluttajaliittymissä sijaitsevista sähköpostipalvelimista voidaan reitittää sovittujen lähtevälle SMTP-liikenteelle tarkoitettujen palvelimien kautta, mutta tietyissä tilanteissa suoralle liikennöinnille voi olla tarvetta. Kuluttajaliittymästä lähtevän SMTP-liikenteen seuraamisella tarkoitetaan tässä määräyksessä liikennemäärien ja – tavan automaattista seurantaa, sekä puuttumista liikennöintiin seurannan perusteella.

## 6. OSOITEPOHJAINEN SUODATUS ASIAKASLIITTYMISSÄ

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

Väärennetyjä 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 väärennettyä liikennettä lähettävä asiakasliittymä.

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

Asiakasliittymiä tarjoavan teleyrityksen tulisi myös suodattaa sellainen viestintäverkosta asiakasliittymään suuntautuva liikenne, jonka lähdeosoite on osoiteavaruudesta, johon kyseinen liittymä kuuluu. (RFC 3013, kohdat 4.3 ja 4.4 ja multihoming-verkkojen osalta RFC 3704).

Teleyrityksen on toteutettava suodatus asiakasrajapintaa lähimpänä olevassa verkkoelementissä, jossa suodatus on teknisesti tarkoituksenmukaisinta toteuttaa. Suodatus tulee mahdollisuuksien mukaan toteuttaa myös teleyrityksen asiakkaiden välillä.

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

## 7. HAITALLISEN LIIKENTEEN HAVAITSEMINEN JA SUODATTAMINEN ASIAKASLIITTYMISSÄ

### 7.1. Haitallisen liikenteen havaitseminen

Teleyrityksen on seurattava ja tarpeen mukaan selvitettävä oman viestintäverkkonsa tapahtumia sellaisen liikenteen havaitsemiseksi, joka aiheuttaa vaaraa viestintäverkon tai -palvelun tietoturvalle tai käytettävyydelle.

Teleyrityksen tulee määritellä viestintäverkon ja/tai palvelujen tietoturvasta vastaava ryhmä, jolle voidaan ohjata asiakasliittymien osalta asiakkaiden ja ulkopuolisten tahojen yhteydenotot tietoturvaa vaarantavista tapahtumista, viestintäverkon tapahtumien seuranta sekä tapahtumien selvitys.

Teleyritys voi saada tiedon viestintäpalvelun tietoturvaa tai käytettävyyttä vaarantavaa liikennettä lähettävästä asiakasliittymästä esimerkiksi viestintäverkkonsa liikennemääriä ja sen poikkeamia seuraavan automaattisen hallintajärjestelmän, teleyrityksen viestintäpalvelun häiriötilanteen, ulkopuolisen tahon ilmoituksen tai asiakasvalituksen kautta. Teleyrityksen on tarkastettava ilmoitusten paikkansapitävyys tarkoituksenmukaisella tavalla.

Teleyrityksen on määriteltävä menettelyt ja yhteydenottotavat, joiden mukaan viestintäverkon tietoturvasta huolehtiva ryhmä toimii yhteistyössä ja vaihtaa tarvittaessa tietoja viestintäpalvelun tietoturvallisuutta vaarantavista tapahtumista muiden Internet-palveluntarjoajien, asiakkaiden ja viranomaisten kanssa. Teleyrityksen tulee sopia ennalta turvalliset tietojenvaihtomenettelyt olenaisten yhteistyökumppanien kanssa.

## 7.2. Liikenteen tilapäisen suodattamisen prosessit ja toimintamallit

Teleyritys voi saada tiedon viestintäverkon tai –palvelun tietoturvaa tai käytettävyyttä uhkaavasta tilanteesta, kuten nopeasti leviävästä, haittaohjelman aiheuttamasta tiettyyn tietoliikenneporttiin suuntautuvasta liikenteestä edellä mainituilla tavoilla.

Tällaisessa tilanteessa teleyritys voi joutua ottamaan käyttöön tilapäisiä toimenpiteitä esimerkiksi kyseiseen tietoliikenneporttiin asiakasliittymiin ja asiakasliittymistä suuntautuvan liikenteen estämiseksi tai liikenteen rajoittamiseksi asiakasliittymistä tiettyihin kohdeosoitteisiin. Teleyrityksellä on oltava prosessit ja toimintamallit joiden mukaisesti asiakasliittymien liikennettä suodatetaan tilapäisesti tilanteissa, jotka aiheuttavat vaaraa viestintäverkon tai –palvelun tietoturvalle tai käytettävyydelle.

Toimenpiteistä tulee tiedottaa käyttäjille esimerkiksi Internet-palveluntarjoajan www-sivustolla. Suodatustoimenpiteet tulee keskeyttää, kun viestintäverkon tai –palvelun tietoturvaa tai käytettävyyttä vakavasti vaarantava uhkatilanne on päättynyt.

## 7.3. Asiakasliittymien irtikytkeminen

Teleyrityksen on kytkettävä asiakasliittymä tai asiakasliittymän palvelu irti yleisestä viestintäverkosta, jos viestintäpalvelun tietoturva tai käytettävyys vaarantuu oleellisesti liittymästä johtuvista syistä. Liittymän irtikytkeminen ja takaisin kytkeminen on toteutettava ennalta määriteltyjen prosessien ja toimintaohjeiden mukaisesti. Toimenpiteitä toteutettaessa voidaan ottaa huomioon liittymätyypistä johtuvat erityisolosuhteet.

Asiakasliittymän palvelun irtikytkemisellä yleisestä viestintäverkosta tarkoitetaan tässä määräyksessä esimerkiksi niiden tietoliikenneporttien tilapäistä sulkemista asiakasliittymästä, joihin suuntautuva liikenne vaarantaa viestintäpalvelun tietoturvaa tai käytettävyyttä. Vastaavasti teleyritys voi joutua rajoittamaan tiettyjen sovellusprotokollien liikennöintiä asiakasliittymästä, mikäli liikenne vaarantaa viestintäpalvelun tietoturvaa tai käytettävyyttä.

Asiakasliittymän toiminta voi vaarantaa olennaisesti viestintäpalvelun tietoturvaa tai käytettävyyttä esimerkiksi tilanteissa, jossa liittymän takana oleva haittaohjelmatartunnan saanut järjestelmä lähettää liittymästä suuria määriä roskapostia tai haittaohjelmia. Haittaohjelmatartunnan saanut järjestelmä voi vaarantaa olennaisesti viestintäpalvelun tietoturvaa tai käytettävyyttä myös, mikäli sitä käytetään esimerkiksi palvelunestohyökkäykseen ja järjestelmä lähettää viestintäpalvelun tietoturvaa vaarantavaa liikennettä tai liikennettä, jonka tarkoituksena on jonkin tahon viestintämahdollisuuksien estäminen.

Internet-liittymässä ylläpidettävän avoimen sähköpostin välityspalvelimen voidaan myös katsoa vaarantavan viestintäpalvelun tietoturvaa tai käytettävyyttä. Täten teleyritys on velvollinen kytkemään irti havaitsemansa tai tietoonsa saamansa yleisestä viestintäverkosta avoimena sähköpostin välityspalvelimena toimivan tietojärjestelmän, kun toimenpide on tarpeen tietoturvasta tai käytettävyydestä huolehtimiseksi.

Teleyritys voi saada tiedon avoimesta sähköpostipalvelimesta verkossaan esimerkiksi oman sähköpostijärjestelmänsä tai viestintäverkkonsa seurannan kautta, ulkopuolisen tahon ilmoituksen kautta tai asiakkaan ilmoituksen perusteella. Teleyrityksen on tarkoituksenmukaisella tavalla tarkistettava ilmoitusten paikkansapitävyys ennen järjestelmän irtikytkemistä yleisestä viestintäverkosta.

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. Tällaisiin tilanteisiin reagoidaan jäljempänä kuvattujen toimintamallien mukaisesti.

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 ole oikeutta yleisesti valvoa asiakkaan lähettämän liikenteen sisältöä taikka tunnistamistietoja muissa tapauksissa.

Mikäli teleyritys muuta kautta kuin luottamuksellisen viestinnän tunnistamistietoja käsittelemällä saa tietoonsa, että asiakkaan viestintä vaarantaa toisten henkilöiden oikeuksia esimerkiksi rikollisella tavalla, tulee tällaisissa tilanteissa noudattaa liittymän sopimusehtoja sekä sopimussuhteeseen soveltuvaa lainsäädäntöä.

Irtikytkemiseen liittyvät toimenpiteet tulee toteuttaa ennalta määriteltyjen prosessien mukaisesti. Tehdyt toimenpiteet ja erityisesti syy liittymän irtikytkemiseen tulee kirjata tilanteen mahdollista jälkikäteen tapahtuvaa selvitystä varten. Mikäli mahdollista, asiakkaaseen tulee olla yhteydessä ennen liittymän irtikytkemistä yleisestä viestintäverkosta esimerkiksi puhelimitse tai sähköpostitse. Yhteydenotto asiakkaaseen ei ole kuitenkaan välttämättä mahdollista tilanteissa, jotka vaativat nopeaa reagointia palvelun tietoturvan tai käytettävyyden ollessa vakavasti uhattuna. Näissä tilanteissa asiakkaan kuuleminen ei saa tarpeettomasti vaarantaa palvelun tietoturvallisuudesta tai käytettävyydestä huolehtimista.

Liittymän irtikytkeminen ja takaisinkytkeminen on toteutettava ennalta määriteltyjen prosessien ja toimintaohjeiden mukaisesti. Toimenpiteitä toteutettaessa voidaan ottaa huomioon liittymätyypeistä johtuvat erityisolosuhteet. Esimerkiksi palveluntarjoajille suunnatuissa liittymätyypeissä häiriötilanteiden toimintamalleista voidaan sopia siten, että palveluiden tarjoamiselle aiheutuvat haitat olisivat mahdollisimman vähäiset.

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

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

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 ylityessä. Liittymän ollessa irtikytkettynä asiakkaan liikenne voidaan ohjata rajatulle alueelle, 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 tietoturvasta ja käytettävyydestä huolehtimiseksi, asiakkaalle tulee jaksossa 3 kuvatulla tavalla kertoa liittymän tilapäiseen sulkemiseen ja avaamiseen liittyvät periaatteet.

## **8. RUNKOVERKON TIETOTURVALLISUUS**

Teleyrityksellä on oltava ohjeet ja toimintamallit palvelunestohyökkäystilanteita ja muita viestintäverkon tai -palvelun tietoturvaa tai käytettävyyttä vaarantavia tilanteita varten.

Teleyrityksen ohjeistuksen ja toimintamallien palvelunestohyökkäystilanteita ja muita viestintäverkon tai -palvelun tietoturvaa tai käytettävyyttä vaarantavia tilanteita varten tulee olla toteutettu

sillä tarkkuudella, että teyrytyksen henkilöstö voi reagoida tyypillisimpiin poikkeustilanteisiin ja toimia tilanteissa toimintamallien ja ohjeistuksen mukaisesti.

Teuryrytyksellä on oltava valmiudet ryhtyä toimenpiteisiin palvelunestohyökkäyksiin liittyvän liikenteen rajoittamiseksi ja virheellisiä lähdeosoitteita sisältävän liikenteen jäljittämiseksi.

Teuryrytyksen verkon tulee tukea liikennemäärien rajoittamista palvelun tietoturvasta ja käytettävyydestä huolehtimiseksi.

Liikenteen rajoitustoimenpiteillä tarkoitetaan esimerkiksi sitä, että Internet-palveluntarjoajan verkkoelementit tukevat liikennemäärien protokolla-, osoite-, portti- ja verkkoliityntäkohtaista rajoitusta. Näillä rajoitustoimenpiteillä voidaan ennaltaehkäistä palvelunestohyökkäyksiä sekä rajoittaa tiettyjen verkkohyökkäystapojen aiheuttamaa vahinkoa.

Liikenteen rajoitustoimenpiteillä voidaan esimerkiksi rajoittaa sellaisten palvelunestohyökkäysten vaikutusta, joissa käytetään tiettyntyyppistä hallintaliikennettä kuormittamaan verkossa olevia järjestelmiä. Lisäksi toimenpiteillä voidaan rajoittaa tiettyyn porttiin liikennöivän haaittaohjelman liikennettä.

Valmiudella liikenteen jäljittämiseen tarkoitetaan esimerkiksi sellaisten toimintamallien ja käytäntöjen luomista, jotka mahdollistavat virheellisiä lähdeosoitteita sisältävän liikenteen alkuperän selvittämisen. Toimenpiteet voivat sisältää esimerkiksi ohjeistusta ja tarvittavia muutoksia runkoverkkolaitteiden asetuksiin.

Virheellisiä lähdeosoitteita sisältävän liikenteen lähteen selvittämisellä pyritään tunnistamaan liikennettä lähettävä taho, jotta palvelunestohyökkäykseen liittyvän haaittaliikenteen palvelun tietoturvalle aiheuttamat häiriöt saadaan estettyä.

Liikennemääriä rajoittavien verkkoelementtien tulee tukea liikenteen rajoitusta sekä itse verkkoelementtiin kohdistuvan että verkkoelementin läpi menevän liikenteen osalta. Liikennemäärien rajoitus tulee voida toteuttaa verkon käytettävyyttä tarpeettomasti vaarantamatta. Esimerkiksi liikennettä rajoittavan verkkoelementin tulee pystyä toteuttamaan toimenpiteet, kuten IP-liikenteen suodatus, verkkoelementtiä kohtuuttomasti kuormittamatta.

Liikennemääriä rajoittavien verkkoelementtien tulee tarvittaessa pystyä kirjaamaan tarkoituksenmukaiset tapahtumatiedot suodatustapahtumista, esimerkiksi lähde- ja kohdeosoitteesta, lähde- ja kohdeportista sekä mitä kyseiselle paketille tehtiin. Tarkoituksenmukaisuutta arvioitaessa tulee huomioida esimerkiksi riittävä näytteenottotarkkuus, esimerkiksi joka kymmenennen paketin kirjaaminen suodatetusta liikenteestä voi riittää tietyissä tilanteissa. Kirjaus on tarpeellinen esimerkiksi ongelmanselvitystä, verkkohyökkäysten selvitystä tai tunnistamista varten. Verkkoelementin tulee tukea tapahtumatietojen toimittamista keskitetyille lokipalvelimelle. Tapahtumatiedot tulee aikaleimata ja ajastuksessa tulee käyttää keskitettyä aikalähdettä.

## **9. OSOITE- JA REITTI SUODATUS RUNKOVERKOSSA**

Teuryrytysten välisessä yhdysliikenteessä liikennettä vaihtavien teuryrytysten on estettävä sellaisen liikenteen välittäminen, jonka lähdeosoite ei ole lähettävän teuryrytyksen reittimainostuksessa.

Pääasiallisesti vastuu virheellisiä lähdeosoitteita sisältävän liikenteen välittämisen estämisessä on liikennettä lähettävällä teuryrytyksellä.

### **9.1. Reittimainostuksen tarkastaminen**

Vastaanotettavasta reittimainostuksesta tulee hylätä teuryrytyksen omiin verkkoihin kuuluvat reitit, jos yksittäisen verkon osalta ei ole muuta sovittu.

Minkään muun teleyrityksen ei pitäisi mainostaa teleyrityksen omia tai tarkempia (more specific) reittejä ilman erillistä sopimusta, esimerkiksi tietyt väliaikaiset moniliittymisratkaisut (multi-homing) voivat edellyttää tällaista mainostusta. Oikeudeton mainostus voi olla tahallista toimintaa liikenteen ohjaamiseksi hyökkääjän järjestelmään tai tahatonta. Oikeudettoman mainostuksen aiheuttamalta uhalta suojautumiseksi reittimainostuksia vastaanottavan teleyrityksen on suodatettava mainostuksesta pois virheelliset mainostukset.

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

Teleyrityksen on suodatettava viestintäverkkoonsa suuntautuva liikenne, jonka lähdeosoite on osoitettu kyseiselle teleyritykselle, mikäli kyseisen liikenteen välittämisestä ei ole erikseen sovittu. Suodatustoimenpiteet on tehtävä teknisesti tarkoituksenmukaisella tarkkuudella.

Virheellisiä lähdeosoitteita sisältävät paketit ovat väärennetyllä lähdeosoitteella lähetettyjä joko seurauksena virheellisestä tai tahallisesta lähdeosoitteen määrittelystä.

Joissain poikkeuksellisissa tilanteissa teleyritys saattaa sopia toisen teleyrityksen kanssa siitä että osaa teleyrityksen osoiteavaruudesta reititetään väliaikaisesti toisen verkosta lähtevänä.

## **9.3. Suunnattujen yleislevitysviestien välittämisen estäminen**

Teleyrityksen on estettävä julkiseen Internet-verkkoon liitetyissä verkkoelementeissään suunnattujen yleislevitysviestien (directed broadcast) välitys verkkoliityntärajapinnoissa. Broadcast-tyyppisiä verkkoja, joissa suunnattuja yleislevitysviestejä tyypillisesti käytetään, ovat esimerkiksi Ethernet-verkot.

## **9.4. Mainostettujen verkkojen dokumentointi**

Teleyrityksen on dokumentoitava mainostamiensa, kyseiselle teleyritykselle osoitettujen osoitteiden käyttö huolellisesti kirjaamalla verkot julkiseen Internet-reititystietokantaan (Internet Routing Registry, IRR).

Mainostettavien osoiteavaruuksien kirjaaminen on tärkeää, koska teleyritykset käyttävät näitä tietoja automaattisten reittisuodatuslistojen (prefix list) luomiseen. Reittisuodatuslistoilla huolehditaan siitä, että reittejä mainostava teleyritys mainostaa vain hallinnoimiaan osoiteavaruuksia. Lisäksi huolellisesti kirjatusta osoitetiedoista löytyy helposti vastaava yhteyshenkilö myös abuse-yhteydenotoissa.

Julkinen dokumentointi on suoritettava vähintään mainostettavien reittien tarkkuudella. Kirjaus suoritetaan RIPE -tietokantaan kulloinkin voimassaolevin menetelmin. Dokumentoimattomia osoiteavaruuksia ei saa mainostaa muille teleyrityksille.

Transit-palvelua tarjoavan teleyrityksen on huolehdittava mainostamiensa asiakasverkkojen kirjaamisesta julkiseen Internet-reititystietokantaan (Internet Routing Registry, IRR) suosituksen edellisessä kohdassa mainittujen periaatteiden mukaisesti.

Vaikka asiakasorganisaatiot ehkä hallinnoisivatkin itse osoiteavaruuksia tai reititystä, he eivät välttämättä ole tietoisia tästä määräyksestä ja suosituksesta sekä menetelmistä joiden mukaisesti osoiteavaruuksien käyttö on kirjattava Internet-reititystietokantaan. Transit-palvelua tarjoavalla teleyrityksellä on myös vastuu neuvoa asiakastaan tarvittaessa, jotta myös asiakasverkkojen kirjaaminen saadaan suoritettua oikein.

## **9.5. Käyttämättömien osoiteavaruuksien suodattaminen**

Kun teleyritys käyttää erityisiin tarkoituksiin varattuihin tai käyttämättömiin osoiteavaruuksiin perustuvaa suodatussäännöstöä liikenteen tai reititystiedon suodattamiseen, on teleyrityksen huolehdittava käytettävän suodatussäännösten ajantasaisuudesta.

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

Suodatettavia osoiteavaruuksia voivat olla ns. bogon-prefixit, joilla tarkoitetaan yksityiseen käyttöön (RFC 1918) tai erityisiin tarkoituksiin varattuja osoiteavaruuksia. Lisäksi suodatettavia osoiteavaruuksia voivat olla IANAn (Internet Assigned Numbers Authority) tai paikallisten Internet-osoiterekistereiden toistaiseksi allokoimattomat verkot.

Reititystiedon tai liikenteen suodatusta tehtäessä tulee huolehtia suodatuslistan ajantasaisuudesta, jotta voidaan välttää esimerkiksi juuri käyttöön otetun osoiteavaruuden suodattuminen. Bogon-suodatusta tehtäessä voidaan käyttää esimerkiksi luotettavien tahojen tarjoamaa BGP (Border Gateway Protocol) -reititystietoa, jossa osoiteavaruuksien käytössä tapahtuvat muutokset tehdään suodatustunnusmerkistöön keskitetysti.

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

## **10. HAITALLISEN LIIKENTEEN HAVAITSEMINEN JA SUODATTAMINEN RUNKOVERKOSSA**

Teleyrityksen on seurattava ja tarpeen mukaan selvitettävä runkoverkkonsa tapahtumia sellaisen liikenteen havaitsemiseksi, joka aiheuttaa vaaraa viestintäverkon tai –palvelun tietoturvalle tai käytettävyydelle.

Teleyrityksen tulee määritellä viestintäverkon ja/tai palvelujen tietoturvasta vastaava ryhmä, jolle ohjataan tietoturvaa vaarantavien tapahtumien seuranta ja selvitys runkoverkon osalta. Teleyritys voi saada tiedon viestintäpalvelun tietoturvaa vaarantavista tapahtumista, kuten runkoverkon välityksellä tehtävistä palvelunestohyökkäyksistä tai poikkeuksellisen paljon liikennettä aiheuttavista haittaohjelmista, oman seurantansa tai ulkopuolisten ilmoitusten kautta.

Teleyritys voi käyttää omassa tilanneseurannassaan esimerkiksi runkoverkon liikennemääriä tai poikkeuksellisia tapahtumia seuraavaa automaattista hallintajärjestelmää. Lisäksi runkoverkon tietoturvatapahtumien hallinnassa voidaan käyttää esimerkiksi tunkeutumisen havaitsemis- ja estojärjestelmiä.

Teleyrityksen on määriteltävä menetelmät, joiden mukaan runkoverkon tietoturvasta vastaava ryhmä toimii yhteistyössä ja vaihtaa tietoja viestintäpalvelun tietoturvaa vaarantavista tapahtumista asiakasliittymien tietoturvallisuudesta vastaavien tahojen, toisten Internet-palveluntarjoajien vastaavien ryhmien, viranomaisten, muiden tietoturvatoimijoiden sekä kansallisten CERT-toimijoiden kanssa. Teleyrityksen tulee muodostaa turvalliset tietojenvaihtomenettelyt olennaisten yhteistyökumppanien kanssa ongelmatilanteiden nopean ratkaisemisen mahdollistamiseksi.

## **11. INTERNET-YHTEYSPALVELUJEN TOIMIVUUDEN JA LAADUN SEURANTA**

Teleyrityksen on jatkuvasti seurattava tarjoamiensa Internet-yhteyspalvelujen laatua ja palveluvarmuutta. Palvelujen toiminnan ja laadun seurannalla tuetaan palvelujen hallinta- ja kehitysprosesseja sekä palvelujen toiminnasta varmistumista. Lisäksi palvelujen toiminnan ja laadun seuranta voidaan käyttää apuna osoittamaan asiakkaalle sovitun palvelunlaadun toteutuminen.

### **11.1. Viestintäverkon tai –palvelun käytettävyyden kannalta merkittävät poikkeustilan teet**

Viestintäverkon tai -palvelun käytettävyyden kannalta merkittävien poikkeustilanteiden seurannalla tarkoitetaan niiden palvelun käytettävyyteen tai tietoturvallisuuteen vaikuttavien tapahtumien raportointia ja tilastointia, jotka ovat aiheuttaneet merkittäviä poikkeamia viestintäverkon tai -

palvelun toimivuudessa. Tällaisia tapahtumia voivat olla esimerkiksi virhetilanteet verkon runko-laitteissa tai laajojen palvelunestohyökkäysten aiheuttamat merkittävät poikkeamat palvelujen laatussa.

### **11.2. Verkon kuormitustilanne**

Verkon kuormitustilanteen mittaamisella tarkoitetaan tietoliikenneverkon tilannetietojen seuranta kuormituksen määrittelyä ja raportointia. Verkon kuormitustilanteen seurannalla tarkoitetaan esimerkiksi runkoverkon tietoliikenneyhteyksien kapasiteetin tai liittymäkohtaisen kuormitustason seuranta. Lisäksi kuormitustason seurannalla voidaan tarkoitaa esimerkiksi yksittäisten ADSL-tilaajaliittymien kokonaisliikennemäärien seuraamista riittävän yhteyskapasiteetin varmistamiseksi.

### **11.3. Käyttökatkokset Internet-yhteyspalvelussa jaoteltuna tyypeittäin**

Internet-yhteyspalvelussa tapahtuvien käyttökatkosten seurannalla ja jaottelulla tyypeittäin tarkoitetaan suunnittelemattomien ja suunniteltujen poikkeuksellisten käyttökatkosten kirjaamista ennalta määritelyjen menettelytapojen mukaisesti.

Käyttökatkokset voidaan jaotella esimerkiksi seuraaviin tyypeihin:

- Laitteistoviat
- Ohjelmistovirheet
- Määrittelyvirheet
- Kuormituksesta aiheutuvat vikatilanteet
- Palvelunestohyökkäyksiä aiheuttavat häiriö- ja katkostilanteet

### **11.4. Todetut vikatilanteet yksittäisissä asiakasliittymissä jaoteltuna tyypeittäin**

Teleyrityksen toteamat vikatilanteet yksittäisten asiakasliittymien osalta voidaan jaotella tyypeittäin vastaavalla tavalla kuin koko Internet-yhteyspalvelussa. Yksittäisellä asiakasliittymällä voidaan tarkoitaa esimerkiksi yksittäistä tilaajakohtaista ADSL- tai kaapelimodeemiliittymää.

Vikatilanteita voidaan jaotella esimerkiksi seuraavasti:

- Laitteistoviat
- Ohjelmistovirheet
- Määrittelyvirheet
- Kaapeliviat

### **11.5. Tämän määräyksen perusteella irtikytkettyjen liittymien määrä**

Tämän määräyksen perusteella irtikytkettyjen liittymien määrän seuraamisella tarkoitetaan irtikytkettyjen asiakasliittymien tai muiden asiakasyhteyksien määrän seuraamista ja tilastointia. Vastaavasti voidaan seurata myös niiden asiakasliittymien määriä ja rajoitusmekanismeja, joihin on kohdistettu esimerkiksi poikkeamia seuraavan automaattisen liikenteenhallintajärjestelmän toimenpiteitä, koska näistä liittymistä on lähtenyt palvelun tietoturvasuutta vaarantavaa liikennettä.

Kyseisten liittymien ja toimenpiteiden seurannalla teleyritys voi mitata verkkonsa tilaa tietoturvasuuden osalta, tilastoida kyseisiä arvoja raportointia varten sekä tarvittaessa puuttua poikkeamiin. Irtikytkettyjen liittymien seurannan tulee liittyä teleyrityksen määrittelemiin irtikytkemisprosesseihin. Seurannassa tulee huomioida syy liittymän irtikytkemiseen tai rajoittamiseen, liittymän irtikytkemisaika, toimenpiteen suorittaja, toteutetut toimenpiteet, yhteydenotto asiakkaaseen sekä aika, jolloin liittymä on kytketty takaisin toimintaan.

## **12. TELEYRITYKSEN YHTEYSTIEDOT YLEISISSÄ IP-OSOITEREKISTEREISSÄ**

Teleyrityksen on huolehdittava siitä, että IP-osoitelohkon luovuttaneen alueellisen Internet-osoiterekisterin (RIR) WHOIS-tietokannassa on asianmukaiset yhteystiedot teleyrityksen tai te-

leyrityksen asiakkaiden hallussa olevien osoiteavaruuksien osalta, mukaan lukien abuse-kontaktitiedot.

Teleyrityksen on huolehdittava siitä, että abuse-kontaktitietojen perusteella teleyrityksen tai teleyrityksen asiakkaiden hallussa olevien osoiteavaruuksien hallinnasta vastuullisille tahoille tehdyt yhteydenotot rekisteröidään ja yhteydenottoja seurataan säännöllisesti.

Koska alueellisen Internet-osoiterekisterin tietokannassa sijaitsevat yhteystiedot ovat julkista tietoa, etenkin abuse-sähköpostiosoitteisiin tulee varsin paljon roskapostia ja muuta asiatonta viestiliikennettä. Tästä syystä yhteydenotot on syytä käsitellä automaattisella työkalulla, joka suodattaa viestiliikenteestä asiattomat viestit sekä rekisteröi ja kuittaa muut yhteydenotot. Näin yhteydenottojen perusteella tehtävä ongelmanselvitysprosessi yksinkertaistuu ja tehostuu.