Teletoiminnan tietoturvasta annetun määräyksen perustelumuistio

Sisällys

I. Määräyksen tausta ja säädösperusta

Määräys liittyy sähköisen viestinnän palveluista annetun lain (917/2014, SVPL) 29 lukuun, jossa säädetään viestintäverkon ja viestintäpalvelun laatuvaatimuksista, viestinnän välittäjän, kuten teleyrityksen, velvollisuudesta huolehtia palvelujensa, viestien, välitystietojen ja sijaintitietojen tietoturvasta sekä 33 lukuun, jossa taas säädetään tietoturvan ja häiriöiden hallinnasta sekä häiriöistä ilmoittamisesta.

Viestintäverkkojen ja viestintäpalvelujen laatuvaatimukset

Määräys liittyy SVPL 243 §:n 1 momentin 1, 2, 7, 9, 10, 11 ja 13 kohtiin, joiden mukaan yleiset viestintäverkot ja -palvelut sekä niihin liitettävät viestintäverkot ja -palvelut on suunniteltava, rakennettava ja ylläpidettävä siten, että:

1) sähköinen viestintä on tekniseltä laadultaan hyvää ja tietoturvallista;

2) ne kestävät normaalit odotettavissa olevat ilmastolliset, mekaaniset, sähkömagneettiset ja muut ulkoiset häiriöt sekä tietoturvauhat;

7) kenenkään tietosuoja, tietoturva tai muut oikeudet eivät vaarannu;

9) ne eivät aiheuta kohtuuttomia sähkömagneettisia tai muita häiriöitä taikka tietoturvauhkia;

10) ne toimivat yhdessä ja viestintäverkot voidaan tarvittaessa liittää toiseen viestintäverkkoon ja

11) niihin tehtävistä muutoksista ei aiheudu ennakoimatonta häiriötä muille viestintäverkoille ja viestintäpalveluille;

13) niistä vastaava toimija kykenee muutoinkin täyttämään sille kuuluvat tai tämän lain nojalla asetetut velvollisuudet.

Edellä 1, 2 ja 10 ja 11 kohdassa tarkoitetut laatuvaatimukset on SVPL 243 §:n 2 momentin mukaan suhteutettava viestintäverkkojen ja -palvelujen käyttäjämäärään, maantieteelliseen alueeseen, jota ne palvelevat, sekä niiden merkitykseen käyttäjille.

Toimenpiteet, joilla huolehditaan edellä luetelluissa kohdissa 1, 2, 7 ja 9 tarkoitetusta tietoturvasta, tarkoittavat SVPL 243 §:n 3 momentin mukaan toimia toiminnan turvallisuuden, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden sekä tietoaineistoturvallisuuden varmistamiseksi. Toimenpiteet on suhteutettava uhan vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin sekä käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.

Lisäksi kaikki lain 243 §:n 1 momentissa tarkoitetut laatuvaatimukset koskevat lain 243 §:n 4 momentin mukaan myös viestintäverkkoihin ja viestintäpalveluihin liittyviä merkittäviä liitännäistoimintoja ja liitännäispalveluja[1].

[1] SVPL 3 §:n 1 momentin 8 kohdan mukaan *liitännäispalvelulla* tarkoitetaan ehdollisen käyttöoikeuden järjestelmää, sähköistä ohjelmaopasta, numeronmuunnosjärjestelmää, tunnistamis-, paikantamis- ja tilatietopalvelua sekä muuta vastaavaa viestintäverkkoon tai viestintäpalveluun liittyvää palvelua, joka mahdollistaa viestintäverkon tai viestintäpalvelun tarjoamisen taikka tukee palvelun tarjoamista niiden kautta. Samaisen säännöksen 9 kohdan mukaan taas *liitännäistoiminnolla* tarkoitetaan liitännäispalvelua sekä rakennusta, rakennuksen sisääntuloa ja kaapelointia, kaapelikanavaa, mastoa sekä muuta vastaavaa viestintäverkkoon tai viestintäpalveluun liittyvää fyysistä rakennetta, toimintoa ja elementtiä, joka mahdollistaa viestintäverkon tai viestintäpalvelun tarjoamisen taikka tukee palvelun tarjoamista niiden kautta.

Tässä määräyksessä tarkennetaan edellä mainittuja 243 §:n teknisiä vaatimuksia lain 244 §:n 2, 3, 5, 8, 12, 13, 14 ja 16 kohtien nojalla, joiden mukaan Liikenne- ja viestintäviraston määräykset voivat koskea:

2) viestintäverkon ja siihen kuuluvan laitetilan sähköistä ja fyysistä suojaamista;

3) suorituskykyä, tietoturvallisuutta ja häiriöttömyyttä sekä niiden ylläpitoa, seurantaa ja verkonhallintaa;

5) viestintäverkon rakennetta ja sen liityntäpisteen teknisiä ominaisuuksia;

8) yhteenliittämistä, yhteentoimivuutta, merkinantoa ja synkronointia;

12) teknistä dokumentointia ja tilastointia sekä näihin liittyvien asiakirjojen muotoa ja tietojen säilyttämistä;

13) noudatettavia standardeja;

14) liitännäistoimintoja ja liitännäispalveluja siltä osin kuin niillä on vaikutusta 243 §:ssä säädettyihin viestintäverkkoa tai viestintäpalvelua koskeviin vaatimuksiin;

16) muita näihin verrattavia viestintäverkolle tai viestintäpalvelulle asetettavia teknisiä vaatimuksia.

Lain 247 §:ssä taas säädetään viestinnän välittäjän, kuten siis myös teleyrityksen, velvollisuudesta huolehtia tietoturvasta. Säännöksen 1 momentin mukaan viestinnän välittäjän on viestejä välittäessään huolehdittava palvelujensa, viestien välitystietojen ja sijaintitietojen tietoturvasta. 3 momentin mukaan toimenpiteet, joilla huolehditaan tietoturvasta, on suhteutettava uhan vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin sekä käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.

Lain 247 §:n 4 momentin nojalla Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä mm. edellä kuvatussa 1 momentissa tarkoitetusta tietoturvasta.

Välitystiedolla tarkoitetaan SVPL 3 §:n 40 kohdan mukaan (laissa 456/2016) oikeus- tai luonnolliseen henkilöön yhdistettävissä olevaa tietoa, jota käsitellään viestin välittämiseksi sekä tietoa radioaseman tunnisteesta ja radiolähettimen käyttäjästä sekä tietoa radiolähetyksen alkamisajankohdasta, kestosta ja lähetyspaikasta. SVPL 3 §:n 22 kohdan mukaan sähköisellä viestillä tarkoitetaan tietoa, jota välitetään tai jaetaan sähköisesti.

Tietoturvan ja häiriöiden hallinta

SVPL 272 §:ssä säädetään teleyritysten ja eräiden muiden tahojen toimenpiteistä tietoturvan toteuttamiseksi. Pykälän 1 momentin mukaan näillä tahoilla on oikeus ryhtyä pykälän 2 momentissa tarkoitettuihin välttämättömiin toimiin tietoturvasta huolehtimiseksi:

1) viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi;

2) viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi; tai

3) viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseksi.

Edellä eli 1 momentissa luetellut tarkoitetut toimet voivat käsittää:

1) viestin sisältöä koskevan automaattisen selvittämisen;

2) viestien välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen;

3) tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä;

4) muut 1–3 kohdassa tarkoitettuihin rinnastettavat teknisluonteiset toimenpiteet.

Pykälän 3 momentin mukaan, jos viestin tyypin, muodon tai muun vastaavan seikan perusteella on ilmeistä, että viesti sisältää haitallisen tietokoneohjelman tai käskyn eikä 2 momentin 1 kohdassa tarkoitetulla toimella pystytä turvaamaan 1 momentissa tarkoitettujen tavoitteiden toteutumista, yksittäisen viestin sisältöä saa käsitellä manuaalisesti. Manuaalisesta viestin sisällön käsittelystä on ilmoitettava viestin lähettäjälle ja vastaanottajalle, jollei ilmoittamisella todennäköisesti vaaranneta 1 momentissa tarkoitettujen tavoitteiden toteutumista.

Pykälässä tarkoitetut toimenpiteet on samaisen pykälän 4 momentin mukaan toteutettava huolellisesti ja ne on mitoitettava suhteessa torjuttavan häiriön vakavuuteen. Toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä 1 momentissa tarkoitettujen tavoitteiden turvaamiseksi. Toimenpiteet on lopetettava, jos niiden toteuttamiselle ei enää ole tässä pykälässä säädettyjä edellytyksiä.

Määräyksessä tarkennetaan SVPL 272 §:n 5 momentin nojalla edellä tarkoitettujen toimenpiteiden teknistä toteuttamista.

Määräys ja erityisesti sen internetyhteyspalvelun irtikytkemistä koskevat velvoitteet liittyvät myös SVPL 273 §:ään, jossa säädetään velvollisuudesta korjata häiriö. Pykälän 1 momentin mukaan, jos viestintäverkko, viestintäpalvelu tai laite aiheuttaa merkittävää haittaa tai häiriötä viestintäverkolle, viestintäpalvelulle, viestintäverkkoon liitetylle muulle palvelulle, laitteelle, viestintäverkon käyttäjälle tai muulle henkilölle, teleyrityksen tai muun viestintäverkon tai laitteen haltijan on välittömästi ryhdyttävä toimenpiteisiin tilanteen korjaamiseksi ja tarvittaessa irrotettava viestintäverkko, viestintäpalvelu tai laite yleisestä viestintäverkosta.

SVPL 273 §:n 2 momentin mukaan edellä tarkoitetut toimenpiteet on toteutettava huolellisesti ja ne on mitoitettava suhteessa torjuttavan häiriön vakavuuteen. Toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä 1 momentissa tarkoitettujen tavoitteiden turvaamiseksi. Toimenpiteet on lopetettava, jos niiden toteuttamiselle ei enää ole tässä pykälässä säädettyjä edellytyksiä.

Liikenne- ja viestintävirasto voi SVPL 273 §:n 1 momentissa tarkoitetussa tapauksessa päättää korjaustoimenpiteistä sekä verkon, palvelun tai laitteen irrottamisesta.

II. Asiaan liittyvät muut Liikenne- ja viestintäviraston määräykset ja suositukset

Tässä luvussa kuvataan tämän määräyksen aihepiiriin liittyvät muut Liikenne- ja viestintäviraston määräykset, suositukset ja ohjeet.[2]

[2] Määräykset, ohjeet ja julkiset suositukset löytyvät sivulta https://www.traficom.fi/fi/saadokset?group=kyberturvallisuus.

Määräyksessä *teletoiminnan häiriötilanteista* käsitellään erilaisia teletoiminnan häiriötilanteita. Määräys kattaa yhtäältä tilanteet, joissa teleyrityksen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus (*tietoturvahäiriö*), ja toisaalta tapahtumat, jotka estävät viestintäpalvelun toimivuuden tai häiritsevät sitä olennaisesti (*toimivuushäiriö*). Määräys asettaa velvoitteita teleyrityksille koskien niin tietoturva- kuin toimivuushäiriöiden havaitsemista ja hallintaa kuin niistä ilmoittamista ja tilastointia.

Määräyksessä *viestintäverkon kriittisistä osista* määrätään viestintäverkon kriittisten osien tunnistamisesta ja dokumentoinnista sekä annetaan lakia tarkempia määräyksiä viestintäverkon kriittisten osien määrittelystä.

Määräys *viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista* asettaa teleyrityksille minimivelvoitteet muun muassa viestintäverkkojen ja -palvelujen toteutuksessa käytettyjen laitteiden tehonsyötön varmistukselle, laitteiden ja yhteyksien varmistamiselle sekä laitteiden fyysiselle suojaamiselle.

Määräys *viestintäverkon sähköisestä suojaamisesta* sisältää velvoitteet yleisten viestintäverkkojen ja niihin liitettyjen laitteiden ja viestintäverkkojen suojaamisesta ilmastollista alkuperää olevilta ja sähkölaitteistojen aiheuttamilta ylijännitteiltä ja ylivirroilta.

Määräys *viestintäverkkojen ja -palvelujen laadusta ja yleispalvelusta* koskee viestintäverkkojen ja -palvelujen toimintavarmuuden, suorituskyvyn, luotettavuuden ja laadun mittaamista ja varmistamista. Määräyksessä on annettu tähän liittyen yleisiä kaikkiin yleisiin viestintäverkkoihin ja -palveluihin sovellettavia velvoitteita sekä puhelinpalveluja, internetyhteyspalveluja ja televisiopalveluja koskevia erityisvaatimuksia.

Määräys *hätäliikenteen teknisestä toteutuksesta ja varmistamisesta* sisältää vaatimukset, joilla yleisten viestintäverkkojen osalta varmistetaan hätäpuheluiden ja hätätekstiviestien sekä niihin liittyvän hätäpalvelun kannalta olennaisen informaation siirtyminen viestintäverkoista hätäkeskuksiin. Määräyksen vaatimukset myös varmistavat hätäpuheluille normaaleja puheluja paremmat onnistumismahdollisuudet erilaisissa viestintäverkon ruuhka- ja häiriötilanteissa.

Suositus *teletoiminnan varautumisesta* antaa teleyrityksille neuvoja lain varautumisvelvoitteiden täyttämiseen. Suositus, joka on osin salassa pidettävä, ei ole yleinen, kaiken kattava varautumis-, jatkuvuus- tai valmiussuunnittelua ja niiden toteuttamista koskeva ohje, vaan siinä on nostettu esiin asiakokonaisuuksia, joita Liikenne- ja viestintävirasto suosittelee teleyrityksiä ottamaan huomioon osana varautumisvelvollisuutta ja olemassa olevia varautumiskäytäntöjä.

Suositus *tiettyihin tietoliikenneportteihin suuntautuvan liikenteen tietoturvaperusteisesta suodattamisesta teleyritysten verkoissa* koskee internetyhteyspalveluissa tapahtuvaa liikenteen suodatusta.

Suositus *kansainvälisesti toteutetun palvelun tietoturvasta tiedottamisesta* koskee sitä, mitä ja miten käyttäjille on annettava tietoa kansainvälisen kytköksen sisältävästä viestintäpalvelusta. Osa teleyrityksistä toteuttaa viestintäpalvelunsa osin tai kokonaan Suomen ulkopuolella tai hyödyntäen ulkomaisten yritysten tarjoamia palveluja. Näin ollen palvelun toteutukseen saattaa kohdistua Suomen lainsäädännöstä poikkeavaa sääntelyä, josta palvelujen käyttäjien on syytä saada tietoa. Sen lisäksi, että teleyritys huolehtii palvelunsa tietoturvasta myös tällaisessa tilanteessa, tällaisen tiedon avulla käyttäjä voi itse arvioida, millaisia mahdollisia uhkia hänen viestintäänsä ja välitystietoihin kohdistuu.

Suositus *Common Nordic Recommendations on SS7 Security Issues* sisältää toimenpiteitä SS7-signaloinnin turvallisuuden parantamiseksi. Suositus on salassa pidettävä.

Ohje *välitystietojen käsittelyä koskevien tietojen tallentamisesta* sisältää ohjeita SVPL 145 §:n soveltamiseen. Pykälässä säädetään viestinnän välittäjän velvollisuudesta tallentaa yksityiskohtaiset tapahtumatiedot luottamuksellisuuden ja yksityisyyden suojan kannalta keskeisiä välitystietoja sisältävissä tietojärjestelmissä tapahtuvasta välitystietojen käsittelystä, jos se on teknisesti ja ilman kohtuuttomia kustannuksia mahdollista.

III. Määräyksen tavoite

Määräyksen tavoitteena 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.

Määräyksen vaatimukset tähtäävät näiden tavoitteiden saavuttamiseen, ja tavoitteet ohjaavat määräyksen soveltamista. Yllä mainitut tavoitteet on syytä pitää lähtökohtana kaikissa yleisen teletoiminnan tieturvallisuuden toteuttamista koskevissa asioissa.

Tietoturvalla tarkoitetaan SVPL 3 §:n 28 kohdan mukaan "hallinnollisia ja teknisiä toimia, joilla varmistetaan, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, että tietoja ei voi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä". Tietoturva tarkoittaa siis toimia viestinnän luottamuksellisuuden, eheyden ja käytettävyyden turvaamiseksi. Määräyksen tarkoitus on edistää näiden tavoitteiden toteutumista.

Määräyksessä määritellään tietoturvan toteuttamista koskevat vähimmäisvaatimukset. Määräyksellä pyritään siihen, että tietoturvan huomioiminen teleyrityksissä on osa jokapäiväistä toimintaa. Toisin sanoen määräyksellä pyritään varmistamaan, että tietoturvatekijät huomioidaan rutiininomaisesti ja tehokkailla prosesseilla osana viestintäverkkojen ja -palvelujen toteutusta.

IV. Muut toteuttamisvaihtoehdot

Tässä luvussa kuvataan määräyksen valmistelun yhteydessä harkitut muut vaihtoehtoiset toteuttamistavat.

Määräyksen soveltamisala

Aiemman määräyksen soveltamisala rajoittui yleiseen teletoimintaan lukuun ottamatta häiriöiden estämiseen liittyvää velvoitetta (9.1 §), jota sovellettiin lisäksi yleisiin viestintäverkkoihin liitettyihin viranomaisverkkoihin. Liikenne- ja viestintävirasto arvioi määräyksen valmistelun aikana tarvetta ulottaa soveltamisalan laajennus viranomaisverkkojen lisäksi esimerkiksi sellaisiin paikallisiin matkaviestinverkkoihin, jotka eivät olisi yleisiä viestintäverkkoja, tai ns. kriittisiin erillisverkkoihin, jotka on määritelty viestintäverkon kriittisistä osista annetussa määräyksessä. Työryhmäkäsittelyn aikana tälle ei kuitenkaan ilmennyt selkeää tarvetta. SVPL 273 §:ssä säädetään joka tapauksessa yleisestä velvollisuudesta häiriöiden korjaamiseen. Lisäksi yhteenliittämisestä sovittaessa on mahdollista ottaa huomioon tietoturvaan liittyvät vaatimukset. Tämän johdosta arvioitiin, että uuden määräyksen vastaavan kohdan (15.1) soveltamisalaa ei ole tarpeen laajentaa yksityisiin verkkoihin.

Soveltamisalan laajennuksessa otettiin kuitenkin huomioon Virve 2.0:n toteutusmalli, jossa perinteisen viranomaisverkon sijasta verkkopalvelun tuottaa teleyritys (viran-

omaisviestintää palveleva verkkopalvelu) ja palvelutuottaja viranomaisviestintään liittyvän viestintäpalvelun. Uuden määräyksen soveltaminen ulotettiin myös viimeksi mainittuihin, jotta määräyksen soveltamisala ei käytännössä rajoittuisi aiempaan nähden.

Tietoturvallisuuden huomiointia koskevien velvoitteiden tarkentaminen

Aiemmassa määräyksessä määriteltiin huomioitavat tietoturvallisuuden osa-alueet vain yleisellä tasolla. Vaikka määrittelytapa oli joustava, Liikenne- ja viestintäviraston kokemuksen mukaan sen ohjaava vaikutus jäi vastaavasti hyvin yleisluontoiseksi. Tämän johdosta Liikenne- ja viestintävirasto arvioi määräyksen valmistelun yhteydessä vaihtoehtoina aiemman määrittelytavan pysyttämistä, sen täydentämistä yksityiskohtaisemmilla kriteereillä tai määrittelytavan muuttamista kokonaan niin, että määräyksessä tukeuduttaisiin varsin suoraan Euroopan kyberturvallisuusvirasto ENISA:n määrittelemiin tietoturvan osa-alueisiin.[3]

Kesällä 2022 tehdyssä kyselyssä[4] asiasta näkemyksiä esittäneet lausunnonantajat katsoivat, ettei aiemman määräyksen velvoite ollut liian ylätasoinen. Lausunnoissa tuotiin esille, että velvoitteiden tulisi olla riittävän ylätasoisia niin, että teleyritys voi itse valita tietoturvaratkaisut.

Liikenne- ja viestintävirasto katsoo, että aiempaa tarkempi määrittely on kuitenkin tarpeellinen määräyksen tavoitteiden tukemiseksi ja määräyksen ohjaavan vaikutuksen parantamiseksi. Velvoitteiden suhteellisen yleinen aiempi määrittelytapa ei ole tukenut esimerkiksi valvonta- ja tarkastustoimintaa, kun määräyksessä ei asetettu yksityiskohtaisempia velvoitteita eri osa-alueille, joiden toteuttamista tarkastuksilla olisi voitu yksilöidysti valvoa. Virasto arvioi myös valintaa aiemman määrittelytavan täydentämisen sekä ENISA:n mukaisen lähestymistavan omaksumisen välillä. Liikenne- ja viestintävirasto katsoo, että ENISA:n lähestymistavan valintaa puoltaa se, että tällöin velvoitteiden toteuttamisessa voidaan tukeutua ENISA:n määrittelemiin ja suosittelemiin tietoturvakontrolleihin. Tällöin vaatimusten noudattamisen dokumentointi teleyrityksissä ja niiden valvonta viranomaisen näkökulmasta ovat molemmat yksinkertaisempia verrattuna siihen, jos teleyritysten olisi laadittava samoista tai samankaltaisista velvoitteista dokumentaatio eri tavalla jaoteltua määräystä vasten, mikä aiheuttaisi ylimääräistä työtä. Monikansallisten teleyritysten kannalta ENISA:n lähestymistavan valinnalla ja ENISA:n suosittelemia kontrolleja hyödyntämällä vältetään eriävien kansallisten vaatimusten muodostumista ja edistetään myös mahdollisuuksia saman dokumentaation hyödyntämiseen eri maissa.

Eräiden matkaviestinverkkoja koskevien standardien noudattaminen

Aiempaan määräysversioon ei sisältynyt standardien noudattamiseen liittyviä velvoitteita. Kaikkea teletoimintaa yleisesti koskevia turvallisuusstandardeja ei ole olemassa, mutta eri tekniikoille ja toiminnoille on olemassa standardeja, joihin nojautumalla voidaan varmistua yleisesti hyväksyttyjen käytäntöjen noudattamisesta.

5G-matkaviestinverkoilla ja niiden mahdollistamilla uusilla palveluilla tulee olemaan keskeinen rooli tietoyhteiskunnan ja talouden kannalta. 5G-verkon ohella LTE-teknologialla on vielä pitkään myös olennainen rooli matkaviestinverkon perusteknologiana.

[3] ENISA Guideline on security measures under the EECC, 4th Edition, July 2021 (jäljempänä ENISA:n suuntaviivat tai ENISA GL).
[4] Teletoiminnan tietoturvasta annetun määräyksen (67 A/2015 M) ajantasaistaminen: Kysely kokemuksista ja kehityskohteista, dnro Traficom/16241/09.09/2022.

Näiden verkkojen tietoturvasta huolehtiminen on siten korostetun tärkeää samaan aikaan, kun 5G-teknologian monimutkaisempi teknologiaympäristö asettaa aiempaa korkeammat riskienhallinnan vaatimukset.[5]

Matkaviestinverkkojen turvallisuuden varmistaminen osana yhteiskunnan kriittistä infrastruktuuria on siis entistäkin tärkeämpää. Standardointiorganisaatioiden yhteenliittymä (3GPP) on omalta osaltaan vastannut turvallisuuteen liittyviin huoliin laatimalla turvallisuusstandardeja, joiden avulla laitevalmistajat ja matkaviestinverkon teleyritykset voivat läpinäkyvästi todistaa ja todentaa tarpeellisten turvallisuustoimintojen toteutumisen järjestelmissään, viestintäverkoissaan ja -palveluissaan. Turvallisuusstandardit ovat kokoelmastandardeja, joihin on kerätty keskeisiä 4G- ja 5G-laitteiden turvallisuuteen liittyvät toimintoja.

Liikenne- ja viestintävirasto katsoo, että on perusteltua tarkastella, miten erityisesti uudempien matkaviestinverkkosukupolvien tietoturvallisuuteen keskittyviä standardeja voidaan hyödyntää määräyksessä ja teleyritysten omassa toiminnassa osana matkaviestinverkkojen kokonaisturvallisuuden toteutumista. Määräystyöryhmässä osa jäsenistä suhtautui kielteisesti esitettyihin velvoittaviin standardikohtaisiin viittauksiin, koska standardien yksityiskohtaisen toteuttamisen katsottiin rajoittavan teleyritysten toimintamahdollisuuksia turvallisuusratkaisujen ja mahdollisesti laitetoimittajien valinnassa. Lisäksi ongelmana nähtiin, että standardien päivittyessä yksityiskohtainen listaus vanhentuisi nopeasti, jolloin määräyspäivityksen yhteydessä laadittu lista ei enää vastaisi täysimääräisesti turvallisuustarpeisiin.

Liikenne- ja viestintävirasto on arvioinut matkaviestinverkon turvallisuusvaatimuksista huolehtimiseksi seuraavia toteutusvaihtoehtoja:

1. Ei viitata määräystasolla yksittäisiin standardeihin tai niiden turvallisuustoimintoihin. Vaihtoehtoa voi täydentää suosituksen luontoinen viittaus turvallisuusstandardeihin perustelumuistiossa.
2. Velvoitetaan määräyksellä noudattamaan matkaviestinverkkostandardien tiettyjä kohtia määräyksessä asiakohdittain.
3. Velvoitetaan määräyksellä noudattamaan lueteltuja standardeja yleisesti.

Liikenne- ja viestintävirasto katsoo, että 3GPP:n standardien hyödyntäminen on toimiva keino varmistaa, että verkkojen ja palvelujen toteutuksessa käytettävät komponentit täyttävät perustason kyberturvallisuusvaatimukset. Standardeihin viittaamalla voidaan huolehtia siitä, että valmiiksi määritellyt turvallisuustoiminnot tulevat mahdollisimman pitkälle asianmukaisesti toteutetuiksi ja käyttöön otetuksi. Tällaista tavoitetta ei täyttäisi pelkkä suositus standardien noudattamisesta, minkä takia vaihtoehtoa 1 ei valittu. Standardien noudattamista edellyttävään ratkaisuun on päädytty myös ainakin Itävallassa ja Saksassa, jossa on asetettu 3GPP:n standardien noudattamista koskevia vaatimuksia osana matkaviestinverkkojen turvallisuuden parantamista.[6]

Vaihtoehtoa 2 ei valittu, koska standardit ovat teknologiakohtaisia, eikä matkaviestinverkkoja koskeviin 3GPP:n standardeihin viittaaminen ole asianmukainen ratkaisu ylei-

[5] Ks. Selvitys 5G:n kyberturvallisuudesta, Yhteenveto, Traficomin julkaisuja, 14.05.2019, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Selvitys%205Gn%20kyberturvallisuudesta%20yhteenveto.pdf sekä Cybersecurity of 5G networks EU Toolbox of risk mitigating measures, NIS Cooperation Group, CG Publication 01/2020 (jäljempänä 5G Toolbox), s. 3–4.

[6] BSI Technical Guideline TR-03163: Security in Telecommunications Infrastructure sekä Verordnung der Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) über Verpflichtungen von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste im Zusammenhang mit Mindestsicherheitsmaßnahmen unter Berücksichtigung von 5G-Netzen sowie mit Informationspflichten bei Sicherheitsvorfällen – Telekom-Netzsicherheitsverordnung 2020 (TK-NSiV 2020) § 6(2) ja liite 1 (https://www.ris.bka.gv.at/eli/bgbl/II/2020/301/20200703).

sesti velvoittavien määräyskohtien kohdalla. Muutoinkin velvoittavat viittaukset yksittäisiin standardien kohtiin lisäisivät tarpeettomasti määräyksen monimutkaisuutta ja päivittämisen tarvetta.

Vaihtoehto 3 valittiin ja päädyttiin toteuttamaan se määräyksen standardiliitteellä, koska se oli vaihtoehdoista toteuttamiskelpoisin. Velvoitteen tarkoituksena ei ole edellyttää, että teleyritykset todentavat omin toimenpitein laitevalmistajien toimittamien komponenttien täyttävän asianomaiset vaatimukset, vaan että otetaan käyttöön asianmukaiset menettelyt, joilla teleyrityksen määrittämin tavoin huolehditaan siitä, että standardien kuvaamat turvallisuustoiminnot huomioidaan ja tarvittaessa toteutetaan teleyrityksen toiminnassa kyseisten järjestelmien koko elinkaaren ajan. Velvoitteella ei ole tarkoitus vaikuttaa laitetoimittajien tuotekehityssykliin, vaan varmistaa että teleyrityksen käyttöön ottamien toiminteiden versioille standardeissa määritetyt turvallisuustoiminnot huomioidaan täysimääräisesti tai niiden toteuttamatta jättäminen perustellaan ja riskit hallitaan muilla keinoin.

BGP-reititys

Aiemmassa määräysversiossa ei ollut kattavasti otettu kantaa BGP:n turvallisuustekijöihin. BGP on internetin keskeinen reititysprotokolla, johon kohdistuvat tahattomat tai tahalliset häiriöt voivat aiheuttaa vakaviakin seurauksia tietoturvalle. BGP-reititysprotokollassa ei ole sisäänrakennettuja turvallisuusominaisuuksia, mikä on johtanut tilanteeseen, jossa BGP:n turvallisuus hoidetaan lähinnä protokollan päälle jälkikäteen rakennetuilla turvallisuusominaisuuksilla. Määräykseen valitut turvallisuusominaisuudet pohjautuvat ENISA:n BGP-tietoturvasuosituksiin[7].

Liikenne- ja viestintävirasto selvitti kesällä 2022 teleyritysten BGP-turvallisuustekijöiden käyttöönoton tilaa. Kysely kohdistui ENISA:n tietoturvasuosituksiin[7] BGP:n turvallisuuteen liittyen.

Osa BGP:n tietoturvallisuutta parantavista tekijöistä on mainittu esimerkkeinä tässä perustelumuistiossa. Niiden käyttöön ei ole velvoitettu, sillä Liikenne- ja viestintävirasto ei ole katsonut niiden olevan välttämättömiä tämän määräyksen antamisen hetkellä. Välttämättömyyttä on arvioitu turvallisuusominaisuuksien vaikutusten pohjalta.

Ottaen huomioon sekä BGP:n keskeisen roolin internetin reitityksessä, että kyseisen protokollan sisäisen turvattomuuden, Liikenne- ja viestintävirasto on katsonut tarpeelliseksi määritellä teleyrityksille velvoitteita, jotka ylläpitävät ja parantavat BGP:n turvallisuuden tilaa.

Rajapintojen erityiset vaatimukset

Aiemmassa määräyksessä luku 3 koski yhteenliittämis- ja asiakasrajapintojen häiriöiden estämistä ja niiltä suojautumista, tarpeettomien palvelujen ja protokollien sulkemista ja IP-liikenteen estämistä yhteenliittämis- ja asiakasrajapinnoissa. Viestintäverkkojen kehitys, uudet käyttötapaukset ja palveluperusteiset arkkitehtuuriratkaisut (SBI) ovat lisänneet uusia rajapintoja teleyritysten viestintäverkkoihin. Lisäksi vanhempien verkkosukupolvien signalointiprotokollat ovat edelleen laajalti käytössä uusien signalointiprotokollien ohella.

Kesällä 2022 toteutetussa määräyksen laatimista edeltäneessä kyselyssä lausunnonantajat suhtautuivat edellytykseen suojata signalointirajapintoja vaihtelevasti. Osassa vastauksia ei nähty tarvetta tarkemmalle sääntelylle. Osa piti ajatusta hyvänä mutta

[7] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP), https://www.enisa.europa.eu/publications/7-steps-to-shore-up-bgp.

niin, että vaatimus tulisi pitää ylätasolla. Yhdessä lausunnossa tuotiin esille, että teleyrityksiltä tulisi edellyttää kaikkia niitä toimenpiteitä, joilla varmistetaan kriittisen viestinnän häiriöttömyys yleisissä viestintäverkoissa. Lausunnonantajat eivät nähneet tarvetta huomioida matkaviestinverkkojen viipaloinnin turvallisuuskysymyksiä uudessa määräysversiossa tai katsoivat, että ylätason viittaus olemassa oleviin suosituksiin olisi riittävää.

Liikenne- ja viestintävirasto on katsonut, että viestintäverkkojen kehityksen myötä rajapintojen suojaamisesta on tarpeen määrätä aiempaa yksityiskohtaisemmin. Määräys perustuu pitkälti olemassa olleisiin suosituksiin.

Haitallisen liikenteen suodattaminen matkaviestinverkon viestipalveluissa

Aiempaan määräykseen ei sisältynyt erityisiä SMS- tai MMS-palveluita koskevia tietoturvavelvoitteita. Viime vuosina näitä palveluita on kuitenkin käytetty laajasti haittaohjelmien ja huijausviestien levittämisessä, mikä on edellyttänyt teleyrityksiltä toimenpiteitä ongelman torjumiseksi.

Kesällä 2022 toteutetussa, määräyksen laatimista edeltäneessä kyselyssä lausunnonantajat suhtautuivat haitallisen liikenteen suodattamista koskevan velvollisuuden laajentamiseen SMS- tai MMS-palveluihin neutraalisti tai sitä pidettiin tarpeellisena.

Suodattamiseen käytössä olevat tekniset ratkaisut ja kyvykkyydet vaihtelevat jonkin verran mm. sen mukaan, onko kyse SMS- vai MMS-palvelusta. Liikenne- ja viestintävirasto katsoo, että asianmukaisen suodatuskyvykkyyden varmistamiseksi asiasta on tarpeen määrätä. Vaihtoehtoina virasto on harkinnut sisältöpohjaisen haitallisen liikenteen suodatuskyvykkyyden edellyttämistä sekä SMS- että MMS-palvelun osalta kaikissa tapauksissa sekä vaihtoehtoa, jossa tämän vaatimuksen soveltamista rajoitettaisiin vähemmän käytetyissä MMS-palveluissa, joissa tämän kaltaiseen suodatukseen ei ole yhtä vakiintuneita ratkaisuja kuin SMS-palvelun osalta. Kun otetaan huomioon MMS-palvelun suhteessa hyvin vähäinen käyttö, ei Liikenne- ja viestintävirasto katso perustelluksi edellyttää poikkeuksetta kykyä sisältöpohjaiseen suodatukseen tämän palvelun kohdalla, kun punnitaan tästä oletettavasti aiheutuvia kustannuksia suhteessa vaihtoehtoisiin keinoihin, joilla voidaan puuttua haittaohjelmien tai huijausviestien leviämiseen MMS-viestien avulla. Tämän johdosta määräykseen on valittu malli, jossa sisältöpohjaisen suodatuksen sijaan teleyritys voi eräissä tilanteissa käyttää muita keinoja.

Kuluttajaliittymistä lähtevän sähköpostiliikenteen suodatusta koskevat toimenpiteet

Liikenne- ja viestintävirasto on arvioinut rajoittamattoman sähköpostiliikenteen eli portin 25 suodatusvelvollisuuden a) säilyttämistä entisellään, b) velvollisuuden poistamista ja suodatustoimenpiteen jättämistä ns. *avoimen internetin asetuksen*[8] ja SVPL 272 §:n perusteella ratkaistavaksi sekä c) poikkeuksen lisäämistä suodatusvelvollisuuteen niitä tilanteita nähden, joissa kuluttaja pyytää suodatustoimenpiteen poistamista.

Liikenne- ja viestintävirasto selvitti syksyllä 2022 SMTP-liikenteen rajoittamisen tilannetta internetyhteyspalveluissa muissa Euroopan valtioissa. Muilta valvontaviranomaisilta saatujen, ei-kattavien tietojen perusteella etenkin kuluttajaliittymistä porttiin 25 lähtevää sähköpostiliikennettä suodatetaan useissa maissa, mutta on myös maita, joissa tätä liikennettä ei keskeisten operaattorien toimesta lainkaan suodateta. Silloin

[8] Euroopan parlamentin ja neuvoston asetus (EU) 2015/2120 avointa internetyhteyttä koskevista toimenpiteistä ja yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alalla annetun direktiivin 2002/22/EY sekä verkkovierailuista yleisissä matkaviestinverkoissa unionin alueella annetun asetuksen (EU) N:o 531/2012 muuttamisesta.

kun suodatusta tehdään, tuli pääsääntöisesti samalla esille, että kuluttajalla on kuitenkin mahdollisuus pyytää suodatustoimenpiteen poistoa. Muissa valtioissa tämä suodatus ei tiettävästi perustu velvoittavaan määräykseen kuten Suomessa.

Liikenne- ja viestintävirasto antoi vuonna 2022 päätöksen, joka määräyksestä poiketen koski vastaavaa suodatustoimenpidettä eräissä yritysliittymissä, joiden osalta määräys ei edellytä suodatusta.[9] Päätöksessä arvioitiin sitä, oliko teleyrityksellä perusteet soveltaa kuluttajien osalta pakollisena ollutta tietoliikenneporttiin 25 lähtevän sähköpostiliikenteen rajoitusta myös tiettyihin yritysliittymiin. Päätöksessä arvioidussa tilanteessa tälle ei ollut riittäviä perusteita, kun kyse oli sellaisista muista kuin kuluttajaliittymistä, jotka oli tarkoitettu tiedonsiirtoon matkaviestinverkossa ja joilla oli kiinteä IP-osoite. Päätöksessä ei otettu kantaa siihen, olisiko rajoitus perusteltu muissa tilanteissa yritysliittymissä.

Kesällä 2022 toteutetussa, määräyksen laatimista edeltäneessä kyselyssä kuluttajaliittymistä lähtevän rajoittamattoman SMTP-liikenteen suodatusta pidettiin edelleen tarpeellisena. Liikenne- ja viestintävirasto pyysi näkemyksiä myös siitä, pitäisikö määräystä kehittää niin, että teleyrityksen tulisi kuluttajan pyynnöstä poistaa rajoitus liittymästä. Kaksi asiasta lausunutta teleyritystä eivät pitäneet tätä perusteltuna. Eräässä lausunnossa tuotiin esille, että erillisten, omilla säännöillään toimivien kuluttajaliittymien tekeminen ei olisi hallinnallisesti tai kustannuksiltaan järkevää muutamaa käyttäjää varten.

Liikenne- ja viestintävirasto arvioi, että kuluttajaliittymiä koskevan, lähtökohtaisen suodatusvelvoitteen säilyttäminen määräyksessä on edelleen perusteltua tietoturvauhkien torjumiseksi. Toimenpiteellä puututaan päätelaitteelta roskapostia lähettämään pyrkivien haittaohjelmien tai väärin konfiguroitujen sähköpostipalvelinten aiheuttamaan haittaliikenteen uhkaan. Velvoitteen poistamisen arvioitaisiin lisäävän roskapostin määrää, joskin kuluttajaliittymistä lähtevän roskapostin leviämistä rajoittaa nykyisin yleistynyt DKIM- ja SPF-menetelmien käyttö sekä erilaisten maineperusteisten järjestelmien hyödyntäminen, jotka rajoittavat kuluttajaliittymien käytössä olevien IP-osoitteiden käyttämistä sähköpostin lähettämiseen.

Velvoitteen säilyttämisen kannalta on kiinnitettävä huomiota myös rajoituksen vaikutuksiin mahdollisuudelle tarjota sähköpostipalvelinta kuluttajaliittymästä. Voidaan arvioida, että kuluttajakäytössä suodatustoimenpide hyvin harvoin aiheuttaa merkittävää haittaa käyttäjille, vaikka se rajoittaa sähköpostipalvelimen toteuttamista liittymän avulla. Ei ole mahdollista tarkasti arvioida, kuinka suuri osuus kuluttajista olisi halukas käyttämään omaa sähköpostipalvelinta liittymässä tilanteessa, jossa suodatusta ei olisi käytössä. Kyseessä voidaan kuitenkin arvioida olevan jokseenkin pieni käyttäjäryhmä, mihin viittaa sekin, että Liikenne- ja viestintävirastolle on viime vuosina tullut vain muutamia tiedusteluja portin 25 suodatuksen haittavaikutuksista. Asiakkaiden saatavilla on lisäksi tyypillisesti sellaisia esimerkiksi yrityskäyttöön tarkoitettuja liittymiä, joissa suodatustoimenpiteitä ei ole käytössä.

Jos määräyksessä edellytettäisiin teleyrityksiä poistamaan suodatus käytöstä asiakkaan pyynnöstä, aiheutuisi tästä kustannuksia yrityksille. Teleyrityksen olisi tarpeen toteuttaa provisiointiympäristöön mahdollisuus muuttaa käytössä olevia suodatuksia liittymäkohtaisesti. Liittymätyypistä riippuen tämä ei välttämättä ole teknisesti kohtuullisesti toteuttavissakaan. Liikenne- ja viestintäviraston työryhmätyöskentelyn aikana saamien tietojen mukaan tämä olisi teleyrityksille työläs muutos. Muutoksella olisi kustannusvaikutuksia, jotka voisivat kohdistua koko asiakaskuntaan. Liikenne- ja viestintäviraston tiedossa ei ole kuitenkaan tarkkoja tietoja teleyrityksille tosiallisesti aiheutuvista kus-

[9] Yritysliittymästä lähtevän sähköpostiliikenteen rajoittaminen, dnro Traficom/9900/09.00.00/2021.

tannuksista. Lisäksi voidaan huomauttaa, että joissakin muissa valtioissa tällainen poikkeusmahdollisuus näyttäisi kuitenkin jo olevan olemassa. Kuitenkin kun otetaan huomioon edellä tietoturvasta ja rajoitusten vaikutuksista asiakkaisiin sanottu, vaikuttaa perustellulta arvioida mahdollisesta muutoksesta aiheutuvat haitat lähtökohtaisesti hyötyjä suuremmiksi. Asiaa voidaan arvioida uudelleen esimerkiksi seuraavan määräyspäivityksen yhteydessä.

Sähköpostiviestien välityspalvelua ja toissijaista sähköpostin välityspalvelua koskevat soveltamisrajoitukset

Liikenne- ja viestintävirasto arvioi soveltamisrajoitusten säilyttämistä aiemman mukaisina tai niiden poistamista määräyksestä. Arvion lopputuloksena soveltamisrajaukset on osittain poistettu määräyksestä tarpeettomina.

Suodatusvelvollisuuden piiristä ei ole viraston arvion mukaan ensinnäkään perusteltua rajata pois saapuvaa liikennettä, joka vaarantaa toissijaisen sähköpostin välityspalvelun tuottamiseen käytettävien järjestelmien tietoturvaa. Suodatusvelvollisuutta on perusteltua soveltaa lähtökohtaisesti myös muuhun saapuvaan haitalliseen liikenteeseen. Jo aiempi määräys mahdollisti tästä poikkeamisen asiakaskohtaisesti sopimalla, mikä on mahdollista myös jatkossa. Toiseksi lähtevän haitallisen liikenteen suodatusta koskevaa velvollisuutta on perusteltua soveltaa jatkossa lähtökohtaisesti myös sähköpostiviestien välityspalveluun, jotta myös tämän liikenteen tietoturvallisuudesta huolehditaan.

Liikenne- ja viestintäviraston saamien tietojen perusteella mukaan useissa tapauksissa sähköpostin välityspalvelussa sekä toissijaisessa välityspalvelussa käytettävät suodatukset ovatkin tällä hetkellä jo samoja, joita teleyritys muutenkin käyttää. Määräys joka tapauksessa jättää soveltamisen varaa sen suhteen, millä menetelmillä haitallista liikennettä on erilaisissa palveluissa perusteltua suodattaa. Tämän takia aiempaa määräystä vastaavien soveltamisalarajoitusten ottaminen tämän määräyksen 26 kohtaan ei ole enää tarpeen.

Tämän ja aiemman määräyksen mukaan sähköpostipalvelua tarjoavan teleyrityksen on tarjottava asiakkaille ensisijaisena vaihtoehtona suojattu yhteys asiakkaan ja sähköpostilaatikon sekä asiakkaan ja lähtevän liikenteen sähköpostipalvelimen välillä. Tätä velvollisuutta ei aiemmassa määräyksessä sovellettu sähköpostiviestien välityspalveluun. Tämä on tarkoittanut käytännössä sitä, että salattua yhteyttä ei ole tarvinnut tarjota sellaisille internetyhteyspalvelun käyttäjille, jotka ovat toisen sähköpostipalveluntarjoajan asiakkaita mutta jotka ovat halunneet käyttää porttia 25 sähköpostin lähettämiseen. Tällöin heidän on tullut tuota porttia koskevan suodatuksen (aiemman määräyksen 14.1 §, tämän määräyksen 21.1 kohta) käyttää internetyhteyspalveluntarjoajana toimivan teleyrityksen lähtevän SMTP-liikenteen sähköpostipalvelinta. TLS-salauksen käyttö ilman autentikointia portissa 25 on sinänsä teknisesti mahdollista, joskin Liikenne- ja viestintäviraston käsityksen mukaan tämän vaihtoehdon tarjoaminen vaihtelee käytännössä tällä hetkellä. Salauksen tarjoaminen tukisi määräyksen tavoitteita edistää viestintäpalvelujen tietoturvaa ja turvata sähköisen viestinnän luottamuksellisuutta. Tämän johdosta on arvioitu, tulisiko soveltamisalarajoitus poistaa niin, että yhteyden suojaamista olisi tarjottava myös käytettäessä porttia 25 sähköpostiviestien välityspalvelussa.

Kun asiakas käyttää toisen sähköpostipalvelutarjoajan palveluita päätelaitteen sähköpostisovelluksen avulla, ei portin 25 suodatus estä tätä käyttämästä sähköpostin lähettämiseen oman sähköpostipalveluntarjoajansa palvelinta esimerkiksi portissa 587 tai 465. Salauksen käyttöä toivova asiakas voi tässä tapauksessa joka tapauksessa käyttää suoraan oman sähköpostipalveluntarjoajansa palvelinta välityspalvelimen sijasta, jos muun kuin portin 25 käyttö on mahdollista. Sen sijaan Liikenne- ja viestintäviraston

käsityksen mukaan portin 25 suodatus käytännössä estää tavanomaisen sähköpostipalvelimen toteuttamisen kuluttajaliittymän avulla, ellei lähettämiseen käytetä oman internetyhteyspalveluntarjoajan SMTP-palvelinta välityspalvelimena (relay) viestien lähettämiseen. Tämän johdosta Liikenne- ja viestintävirasto arvioi, että on perusteltua jatkossa edellyttää teleyrityksiä tarjoamaan mahdollisuutta yhteyden suojaukseen myös sähköpostin välityspalvelinta käytettäessä. Tämän arvioidaan aiheuttavan vain vähäisiä kustannuksia tarvittavien asetusmuutosten tekemiseksi niiden palveluntarjoajien osalta, jotka eivät tätä mahdollisuutta vielä tarjoa.

Asiakkaille tiedottamista koskevat velvoitteet

Aiemman määräyksen asiakkaille tiedottamista koskeva luku 6 on poistettu määräyksestä. Liikenne- ja viestintävirasto arvioi, että kyseisten velvoitteiden tavoitteet saavutetaan asianmukaisesti jo soveltamalla lain ja asetuksen tasoisia säännöksiä, jolloin tarvetta antaa asiasta tarkempia velvoittavia määräyksiä ei ole.

Valtioneuvoston asetuksessa ennen viestintäpalvelusopimuksen tekemistä annettavista tiedoista (96/2021) säädetään tietojen antamisesta palveluntarjoajan toimista tietoturvan vaarantuessa tai tietoturvauhkien tai -haavoittuvuuksien ilmetessä (1 §:n 6 k.). Tämä vastaa olennaisesti aiemman määräyksen 21 §:ää, joka koski yleistä tiedottamista tietoturvatoimenpiteistä. Lisäksi valtioneuvoston asetuksessa säädetyn voidaan arvioida kattavan myös aiemman määräyksen 23 §:n säädetyn sähköpostipalvelun erityisen tiedotusvelvollisuuden sähköpostiliikenteen suodatusperiaatteista. Lisäksi suodatukseen liittyvästä välitystietojen käsittelystä on ilmoitettava SVPL 138.2 §:n nojalla. Sähköpostiosoitteiden hallinnointikäytäntöjen osalta arvioidaan, että aiemman velvoitteen alaan kuuluvien tietojen antaminen kuuluu nykyisin normaalien asiakaspalvelukäytäntöjen piiriin.

Internetyhteyspalvelun erityisiä tiedotusvelvollisuuksia koskeva aiemman määräyksen 22 § koski liittymän käyttöön liittyvistä tietoturvariskeistä ja niihin liittyvistä asiakkaan käytössä olevista toimenpiteistä tiedottamista. Perustelumuistiossa yhtenä esimerkkinä mainittiin internetyhteyspalvelun tarjoaminen salaamattoman WLAN-yhteyden avulla, jolloin teleyrityksen oli tiedotettava liittymän käyttämiseen liittyvistä viestinnän luottamuksellisuuteen kohdistuvista erityisistä riskeistä. Yleisesti saatavilla olevia viestintäpalveluita ei tiettävästi tällä hetkellä tarjota laajamittaisesti WLAN-yhteyksien avulla. Lisäksi HTTP-liikenteen salauksen ja VPN-yhteyksien käytön yleistyminen jossain määrin rajoittaa WLAN-yhteyden salauksen puuttumisesta aiheutuvia tietoturvariskejä. Sikäli kuin tietoturvariski voi kohdistua teleyritykseen, säädetään teleyrityksen käyttäjälle antamista ohjeista SVPL 246.3 §:ssä. Sen mukaan tilaajan on ylläpidettävä yleiseen viestintäverkkoon liitettävää laitetta tai järjestelmää teleyrityksen antamien ohjeiden mukaisesti siten, ettei se vaaranna yleisen viestintäverkon ja -palvelun tietoturvallisuutta. Lisäksi SVPL 274.2 §:ssä säädetään teleyrityksen velvollisuudesta kertoa käytettävissä olevista suojautumistoimenpiteistä, kun teleyritys ilmoittaa tilaajalle tai käyttäjälle teleyrityksen palveluun kohdistuvasta tietoturvaloukkauksesta tai sen uhasta.

Liikenne- ja viestintävirasto on siirtänyt pääosan aiemman määräyksen 6 luvusta suosituksiksi tämän perustelumuistion liitteen lukuun 7.

V. Määräyksen valmistelu

Liikenne- ja viestintävirasto aloitti määräysmuutoksen valmistelun tekemällä kesällä 2022 teleyrityksille ja muulle yleisölle kyselyn kokemuksista ja kehitysideoista.[10] Kyselyyn vastasivat DNA Oyj, Elisa Oyj, Telia Finland Oyj, Suomen Erillisverkot Oy ja Huawei

[10] Teletoiminnan tietoturvasta annetun määräyksen (67 A/2015 M) ajantasaistaminen: Kysely kokemuksista ja kehitysideoista, dnro Traficom/16241/09.09/2022: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=e80c3ac0-6941-4bba-bdcf-62c826646465&proposalLanguage=da4408c3-39e4-4f5a-84db-84481bafc744.

Technologies Oy (Finland) Co. Ltd sekä yksityishenkilö. Vastauksia hyödynnettiin määräysluonnoksen laatimisessa.

Liikenne- ja viestintävirasto pyysi tammikuussa 2023 teleyrityksiä nimeämään osallistujia määräystyöryhmään. Työryhmään ilmoittautui ja nimettiin seuraavien tahojen edustajat: Digita Oy, DNA Oyj, Elisa Oyj, FiCom ry, Finnet-liitto ry, Ikaalisten-Parkanon Puhelin, Karjaan Puhelin Oy, Line Carrier Oy, Telia Finland Oyj, Telia Inmics-Nebula Oy ja Ålands Telekommunikation Ab. Työryhmä kokoontui kahdeksan kertaa vuoden 2023 aikana. Työryhmän kokouksissa käsiteltiin määräyksen ja perustelumuistion luonnoksia.

Lausuntokierros järjestettiin […].

VI. Lausuntopalaute

[täydennetään käsittelyn aikana]

VII. Muutokset ja arvio määräyksen vaikutuksista

Tässä luvussa kuvataan määräykseen tehdyt keskeiset muutokset ja niiden vaikutukset.

<u>Määräyksen 1 luku</u>

- Määräyksen tavoitteet kuvataan jatkossa vain perustelumuistiossa.
- Määräyksen soveltamisalaa on muutettu niin, että sähköpostiviestien välityspalvelua ja toissijaista sähköpostin välityspalvelua koskevat soveltamisrajoitukset on poistettu määräyksestä. Lisäksi jo aiemman määräyksen sisältämä häiriöiden estämistä koskevan velvoitteen soveltamisalan laajennus viranomaisverkkoihin ulotettiin myös viranomaisviestintään liittyvään viestintäpalveluun.
- Määritelmiin on täydennetty haitallisen liikenteen määritelmää siten, että se aiempaa selvemmin kattaa samat tilanteet, joissa SVPL 272 § mahdollistaa viestinnän käsittelyyn liittyviä toimenpiteitä tietoturvan toteuttamiseksi.
- Avoimen sähköpostipalvelimen sijasta muutettiin määriteltäväksi asiaksi avoin sähköpostin välityspalvelin, jotta määritelmä vastaa määräyksen velvoitteissa käytettyä käsitettä.
- Määritelmiin on lisätty tekstiviestipalvelun ja multimediaviestipalvelun määritelmät, joita käytetään uudessa 5 luvussa.

<u>Määräyksen 2 luku</u>

- Tietoturvallisuuden huomioiminen kohtaa on laajennettu aiempaan määräykseen nähden. Huomioitavat osa-alueet vastaavat ENISA:n suuntaviivoissa noudatettua jaottelua tietoturvan 8 osa-alueeseen. Kutakin osa-aluetta täsmennetään uusissa kohdissa, joissa on hyödynnetty ENISA:n kullekin osa-alueelle määrittelemiä turvallisuustavoitteita ottaen kuitenkin huomioon, että turvallisuustavoitteista määrätään osittain myös muissa Liikenne- ja viestintäviraston määräyksissä. Määräyspäivityksen taustalla on tältä osin tarve ajantasaistaa määräystä sekä ottaa huomioon erityisesti 5G-verkkojen uudet arkkitehtuurimuutokset ja käyttötapaukset.

  Vaikka määräyksessä ei enää sellaisenaan käytetä aiemman määräyksen terminologian mukaista jaottelua hallinnolliseen tietoturvaan, henkilöstöturvallisuuteen,

laitteisto-, ohjelmisto- ja tietoliikenneturvallisuuteen, tietoaineisto- ja käyttöturvallisuuteen sekä fyysiseen turvallisuuteen, on määräyksen edelleen tarkoitus kattaa kaikki nämä osa-alueet.

Määräyksen aiempaa suurempi yksityiskohtaisuus aiheuttaa kuitenkin jonkin verran lisätyötä teleyrityksille, etenkin jos niiden on otettava uusia toimenpiteitä käyttöön ja dokumentoitava ne. Suhteellisesti vaikutukset ovat suurimmat pienempien teleyritysten osalta, joissa ei välttämättä ole aiemmin suuressa määrin hyödynnetty ENISA:n tuottamaa aineistoa. Toisaalta määräyksen tarkentaminen ohjaa aiempaa selkeämmin teleyrityksiä tarpeellisten tietoturvatoimenpiteiden toteuttamisessa, mikä myös jossain määrin yksinkertaistaa tarvittavien toimenpiteiden määrittämistä ja sitä kautta määräyksen soveltamista.

Muutoksella arvioidaan olevan selkeä tietoturvallisuutta vahvistava vaikutus, kun määräys ohjaa aiempaa selkeämmin tarkemmin määriteltyjen tietoturvatavoitteiden toteuttamiseen. Tietoturvatavoitteiden toteuttamisessa puolestaan on mahdollista käyttää mm. ENISA:n määrittelemiä tietoturvakontrolleja, jotka on helppo yhdistää määräyksen mukaisiin velvoitteisiin, mikä tukee myös dokumentointia.

Muutos edistää myös Liikenne- ja viestintäviraston valvonta- ja tarkastustoiminnan tehokkuutta ja ennakoitavuutta, kun määräyksen täytäntöönpanossa voidaan tukeutua selkeästi määriteltyihin ENISA:n tietoturvatavoitteisiin ja -kontrolleihin.

- Riskienkäsittelyn tulosten dokumentoinnin säilyttämisen velvollisuutta on pidennetty aiemmasta yhdestä edelliseen kolmeen käsittelykertaan. Aiempi yhden käsittelykerran dokumentaatio ei ole ollut riittävää riskienhallinnan jatkuvuuden toteamiseksi. ISO/IEC 27005 standardissa vaatimus kohdistuu kahteen käsittelykertaan. Koska useampien käsittelykerran tulosten säilyttämisestä ei aiheudu ratkaisevasti enempää lisätyötä, on vaatimus ulotettu määräyksessä kolmeen käsittelykertaan.

- Erityisen tärkeänä asiaryhmänä alihankintaan ja toimitusketjuihin liittyvistä tietoturvariskeistä huolehtiminen on nostettu määräyksen tasolle. Myös esimerkiksi uhkatiedon ylläpito on nostettu uutena asiana määräykseen.

- Matkaviestinverkkostandardien noudattamista koskevat menettelyt on tuotu uutena vaatimuksena määräykseen. Velvoite edellyttää teleyrityksiä ottamaan käyttöön menettelyt, joilla varmistetaan standardeissa kuvattujen turvallisuustoimintojen toteuttaminen teleyrityksen 4G- ja 5G-verkoissa. Määräys antaa kuitenkin mahdollisuuden jättää standardeissa kuvattu toiminto toteuttamatta, mikäli teleyrityksellä on tähän perusteltu syy ja riskit on muutoin hallittu. Tämä mahdollistaa teleyrityksille sen, että standardien turvallisuustoimintojen toteuttamisen vaihtoehtona on korvaavien toimenpiteiden määrittäminen ja dokumentointi.

  Velvoitteesta ei arvioida itsessään aiheutuvan matkaviestinverkon teleyrityksille merkittäviä lisäkustannuksia, sillä kyseessä olevia standardeja pyritään joka tapauksissa noudattamaan hankinnoissa ja laitevalmistajien toimesta. Menettelyjen sekä turvallisuustoimintojen huomioimisen ja mahdollisen toteuttamatta jättämisen ja korvaavien toimenpiteiden dokumentoinnista aiheutuu kuitenkin jonkin verran kustannuksia. Menettelyiden dokumentointivelvoitteesta seuraa, että teleyritysten on sisällytettävä kyseisten standardien seuranta osaksi dokumentaatio- ja muita prosessejaan, kuten konfigurointien hallintaa.

- Asiakkaan tunnistaminen tietoturvasta huolehtimiseksi on tuotu uutena kohtana määräykseen.

  Alan parhaita käytäntöjä noudattaville yrityksille ei arvioida aiheutuvan merkittäviä lisäkustannuksia, sillä kyseessä ovat toimenpiteet, joita jokaisen teleyrityksen on

muutenkin syytä noudattaa. Velvoitteella kuitenkin korostetaan jatkuvan kehittämisen tarvetta. Jos yrityksen käytännöt eivät ole aiemmin olleet riittävällä tasolla, tukee erityinen velvoite käytäntöihin kohdistuvaa valvontaa ja korostaa näiden yritysten tarvetta kehittää käytäntöjään.

- Hallintaverkon ja hallintayhteyksien suojaamista koskevaa kohtaa on tarkennettu. Kohtaan on lisätty vaatimus toimintaperiaatteiden ja menettelyjen laatimisesta sekä hallintaan käytettäviin päätelaitteisiin liittyvien riskien arvioimisesta ja hallinnasta.

Määräyksen 3 luku

- Rajapintojen häiriöiden estäminen ja niiltä suojautuminen -kohdan ensimmäinen alakohtaa on laajennettu niin, että koskee kaikille muille viestintäverkoille eikä vain yleisille viestintäverkoilla aiheutuvien häiriöiden estämistä. Toista alakohtaa on laajennettu sovellusrajapintoihin ja selkeytetty, että velvoite koskee sekä viestintäverkkoja että -palveluita.

- Yhteenliittämisrajapintojen suojaaminen ja liikenteen suodattaminen -kohtaa on laajennettu aiempaan määräykseen nähden. Kohta käsittelee lähinnä BGP-reititysprotokollan turvaamista, jota aiemmassa määräyksessä oli lähinnä reittimainostusten osalta. Velvoitteiden osa-alueiksi on nostettu ENISA:n suosituksien pohjalta keskeisimmät menettelyt.

  Määräyksen aiempaa suurempi yksityiskohtaisuus aiheuttaa osittain teleyrityksille lisätyötä. Suurin osa velvoitteista on jo ainakin jossain määrin otettu huomioon, ja määräys lähinnä vahvistaakin jo olemassa olevia käytänteitä. Määräyksen aiempaa suurempi yksityiskohtaisuus ohjaa teleyrityksiä toteuttamaan tarvittavia suojaus- ja suodatustoimenpiteitä BGP-reititykseen liittyen.

  Muutoksilla arvioidaan olevan BGP-reititysprotokollan turvallisuuteen vahvistava ja ylläpitävä vaikutus. Koska määräyksen osa-alueiksi on nostettu ENISA:n suositusten pohjalta keskeisimmät turvallisuusominaisuudet, katsotaan tämän myös helpottavan määräyksen täytäntöönpanoa. Pohjautuminen ENISA:n suosituksiin myös helpottaa Liikenne- ja Viestintäviraston tarkastustoimintaa sekä BGP-reititysprotokollaan liittyvien turvallisuusominaisuuksien seuraamista ja kehittymistä.

- Määräykseen on lisätty uusi matkaviestinverkkojen rajapintojen suojaamista koskeva velvoite. Matkaviestinverkkosukupolvien elinkaari on hyvin pitkä ja edelleen on käytössä esimerkiksi alun perin 1970-luvulla laadittu SS7-signalointiprotokolla, joka aikanaan kehitettiin hyvin erilaiseen uhkaympäristöön. Signalointiprotokollien turvallisuuspuutteita on sittemmin pyritty ehkäisemään toimintaohjeilla ja -suosituksilla tunnettujen heikkouksien torjumiseksi.

  Velvoitteesta ei arvioida aiheutuvan teleyrityksille lisäkustannuksia, mikäli teleyrityksen menettelyt ovat jo noudattaneet alan parhaita käytäntöjä ja suosituksia. 5G-verkon arkkitehtuurimuutosten myötä myös eri sovellusrajapintojen suojaamisen merkitys korostuu ja uusina erityisesti huomioitavina rajapintoina on keskeisten toiminnallisuuksien, kuten viipaloinnin ja reunalaskennan turvallisuus. Viipaloinnin osalta on tärkeää, että oikeudeton pääsy sekä viipaleen resursseihin ja hallintaliittymään estetään. Lisäksi on tärkeää, että radiorajapinnan pääsynhallintaa vahvistetaan tarpeen mukaan viipalekohtaisella pääsyn todentamisella. Hallintakäyttöliittymän ja radiorajapinnan suojaamisen parhaiden käytäntöjen mukaisesti ei arvioida tuovan teleyrityksille lisäkustannuksia.

Määräyksen 5 luku

- Määräykseen on uutena asiana lisätty teksti- ja multimediaviestiliikenteen suodatus. Velvoitteen ei arvioida pääsääntöisesti edellyttävän merkittäviä uusia investointeja teleyrityksiltä.

Määräyksen 6 luku

- Sähköpostiviestien välityspalvelua ja toissijaista sähköpostin välityspalvelua koskevat soveltamisalan rajoitukset on poistettu määräyksestä tarpeettomina. Muutokset edistävät tietoturvaa, mutta niillä ei arvioida olevan merkittäviä vaikutuksia teleyritysten toimintaan. Teleyrityksen käytännöistä riippuen ne eivät välttämättä edellytä muutoksia aiempiin käytäntöihin nähden. Joissakin tapauksissa voi olla tarpeen tehdä muutoksia sähköpostipalvelun asetuksiin.

Poistetut velvoitteet

- Aiemman määräyksen asiakkaille tiedottamista koskeva luku 6 on poistettu määräyksestä (ks. Muut toteuttamisvaihtoehdot). Luvussa käsitellyt asiat on siirretty tämän perustelumuistion liitteeseen, jota on muutoinkin täydennetty.

YKSITYISKOHTAISET PERUSTELUT JA SOVELTAMISOHJEET

Luku 1 Soveltamisala ja määritelmät

Tässä luvussa käsitellään määräyksen lukua 1 eli määräyksen soveltamisalaa ja määritelmiä.

1. Soveltamisala

1.1 Määräyksen yleinen soveltamisala

Määräys koskee yleistä teletoimintaa. Määräys velvoittaa siten kaikkia teleyrityksiä niiden tarjoaman palvelun tyypistä riippumatta. Määräystä sovelletaan myös merkityksettään vähäiseen teletoimintaan, josta ei ole SVPL 4 §:n mukaista teletoimintailmoitusvelvollisuutta.

SVPL 3 §:n 27 kohdan mukaan teleyrityksellä tarkoitetaan "sitä, joka tarjoaa verkkopalvelua tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille".

Verkkopalvelu määritellään SVPL 3 §:ssä, ja sillä tarkoitetaan palvelua, jossa teleyritys tarjoaa omistamaansa tai muulla perusteella hallussaan olevaa viestintäverkkoa käytettäväksi viestien siirtoon tai jakeluun. Verkkopalvelua tarjoavasta teleyrityksestä käytetään SVPL:ssä myös nimitystä *verkkoyritys*. *Viestintäverkkoja* ovat lain mukaan toisiinsa liitetyistä johtimista sekä laitteista muodostuvat järjestelmät, jotka on tarkoitettu viestien siirtoon tai jakeluun johtimella, radioaalloilla tai muulla sähkömagneettisella tavalla. Sellaiset viestintäverkot, joita käytetään viestintäpalvelujen tarjontaan ennalta rajaamattomalle käyttäjäpiirille, ovat lain mukaan *yleisiä viestintäverkkoja*. Ne viestintäverkot, joita käytetään pääasiassa televisio- ja radio-ohjelmistojen tai muun kaikille vastaanottajille samanlaisena välitettävän aineiston siirtoon tai lähettämiseen, ovat lain mukaan *joukkoviestintäverkkoja*.

Viestintäpalvelulla tarkoitetaan SVPL 3 §:n 37 kohdan (laissa 1207/2020) mukaan "palvelua, joka muodostuu kokonaan tai pääosin viestien siirtämisestä viestintäverkossa sekä siirto- ja lähetyspalvelua joukkoviestintäverkossa ja henkilöiden välisen viestinnän palvelua". Määräystä sovelletaan sekä numeroihin perustuviin että numeroista riippumattomiin henkilöiden välisen viestinnän palveluihin.

Määräyksen vaatimukset on jaettu kuuteen asiakokonaisuuteen:

- Luvussa 2 annetaan yleiset teletoiminnan tietoturvavaatimukset kaikille viestintäverkoille ja -palveluille.
- Luvussa 3 käsitellään yhteenliittämis-, sovellus- ja asiakasrajapinnoissa tehtäviä tietoturvatoimenpiteitä.
- Luvussa 4 annetaan erityisiä vaatimuksia internetyhteyspalvelujen tietoturvasta huolehtimiselle.
- Luvussa 5 annetaan erityisiä vaatimuksia SMS- ja MMS-viestipalvelujen tietoturvasta huolehtimiselle.
- Luvussa 6 käsitellään sähköpostipalvelujen erityisiä vaatimuksia.

Määräystä *ei sovelleta muuhun kuin yleiseen teletoimintaan*. Yleistä teletoimintaa eivät ole ennalta rajatulle käyttäjäpiirille tarjottavat verkko- tai viestintäpalvelut eivätkä sisältöpalvelut. Sisältöpalveluina soveltamisalan ulkopuolelle jäävät esimerkiksi internetsivujen sisällöt, keskustelupalstat sekä televisio- ja radio-ohjelmistojen sisältö.

Määräys ei siis koske muita *viestinnän välittäjiä* kuin teleyrityksiä eli *yhteisötilaajia* ja *muita viestinnän välittäjiä*.[11] Määräys ei aseta velvoitteita esimerkiksi yhteisötilaajille. Määräys ei sovellu yrityksen tai yhteisön sisäisen viestintäverkon hallintaan, koska tällöin käyttäjäpiiri on ennalta rajattu eikä kyse ole yleisestä teletoiminnasta. Yhteisötilaajat ovat SVPL:n tarkoittamia *tilaajia.* Vaikka palvelun tarjoava teleyritys ei vastaakaan yhteisön sisäisestä viestintäverkosta tai -palvelusta, teleyritys vastaa tilaajalle tarjoamastaan palvelusta.

1.2 Määräyksen soveltaminen viranomaisverkkoihin ja viranomaisviestintään liittyvään viestintäpalveluun

Vaikka määräystä sovelletaan muutoin vain teletoimintaan, määräyksen kohtaa 15.1 sovelletaan viranomaisverkkoihin ja viranomaisviestintään liittyvään viestintäpalveluun silloin, kun nämä on yhteenliitetty yleiseen viestintäverkkoon tai yleisesti saatavilla olevaan viestintäpalveluun eli teleyrityksen verkkoon tai palveluun. Muilta osin määräys ei koske viranomaisverkkoja.

Viranomaisverkolla tarkoitetaan SVPL 3 §:n 39 a kohdan (laissa 52/2019) mukaan valtion johtamiseen ja turvallisuuteen, maanpuolustukseen, yleiseen järjestykseen ja turvallisuuteen, rajaturvallisuuteen, pelastustoimintaan, meripelastustoimintaan, hätäkeskustoimintaan, maahanmuuttoon, sosiaali- ja terveydenhuollon päivystystoimintaan, raideliikenneturvallisuuteen tai väestönsuojeluun liittyvien tehtävien vuoksi rakennettua viestintäverkkoa. Esimerkiksi VIRVE-verkko on viranomaisverkko.

Viranomaisviestintään liittyvällä viestintäpalvelulla tarkoitetaan SVPL 3 §:n 39 c kohdassa tarkoitetun *viranomaisviestintään liittyvän viestintäpalvelun tarjoajan* palvelua eli viranomaisten aikakriittisen laajakaistaisen matkaviestinnän tieto- ja viestintäteknistä palvelua.[12]

Määräyksessä ei aseteta velvoitteita sellaisille paikallisverkoille, jotka eivät ole yleistä teletoimintaa. Toteutustavasta riippuen niihinkin voi kohdistua SVPL:ssä säädettyjä velvoitteita. Mikäli paikallisverkko on liitetty yleiseen viestintäverkkoon, tulee myös paikallisverkkojen suunnittelussa ja käytössä huolehtia tietoturvallisuudesta.[13]

2. Määritelmät

Tässä luvussa kuvataan määräyksessä käytetyt määritelmät. Määräyksessä ei määritellä uudestaan SVPL:ssä määriteltyjä käsitteitä. Määritelmät on laadittu niin, että ne eivät ole ristiriidassa lain määritelmien kanssa.

2.1 Asiakasrajapinta

Asiakasrajapinnalla tarkoitetaan tässä määräyksessä rajapintaa, jolla teleyrityksen asiakkaan viestintäverkko, päätelaite tai sovellus liitetään yleiseen viestintäverkkoon. Asiakkaan päätelaitteita ovat esimerkiksi tilaajan tai käyttäjän omistamat ja hallinnoimat modeemit, kytkimet ja tietokoneet. Englanniksi asiakasrajapinnasta käytetään nimitystä User to Network Interface (UNI-rajapinta).

[11] SVPL 3 §:n 36 kohdan mukaan viestinnän välittäjällä tarkoitetaan teleyritystä, yhteisötilaajaa ja sellaista muuta tahoa, joka välittää sähköistä viestintää muutoin kuin henkilökohtaisiin tai niihin verrattaviin tavanomaisiin yksityisiin tarkoituksiin (jäljempänä muu viestinnän välittäjä). *Yhteisötilaajalla* tarkoitetaan SVPL 3 §:n 41 kohdan mukaan viestintäpalvelun tai lisäarvopalvelun tilaajana olevaa yritystä tai yhteisöä, joka käsittelee itse viestintäverkossaan käyttäjien viestejä, välitystietoja tai sijaintitietoja.
[12] Määräystä sovelletaan sen yleisen soveltamisalan mukaisesti myös viranomaisviestintään liittyvään verkkopalveluun, mitä pidetään osana yleistä teletoimintaa (HE 226/2018 vp, s. 49).
[13] Liikenne- ja viestintävirasto: Ohje paikallisten matkaviestinverkkojen kyberturvallisuudesta ja riskienhallinnasta. Traficomin tutkimuksia ja selvityksiä 8/2023, s. 19–20, https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/ohje-paikallisten-matkaviestinverkkojen-kyberturvallisuudesta-ja-riskienhallinnasta.

2.2 Avoin sähköpostin välityspalvelin

Avoimella sähköpostin välityspalvelimella tarkoitetaan sellaista sähköpostiviestien välitysjärjestelmää, jota kolmas osapuoli pystyy oikeudettomasti käyttämään sähköpostiviestien välittämiseen. Välitysjärjestelmällä tarkoitetaan määräyksessä esimerkiksi sähköpostipalvelinta, www-välityspalvelinta tai www-palvelimelle asennettavia ohjelmistoja, joita käytetään sähköpostiviestien välittämiseen.

2.3 Haitallinen liikenne ja roskaposti

Haitallisella liikenteellä tarkoitetaan määräyksessä sähköisiä viestejä, jotka aiheuttavat vaaraa viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle, joihin voidaan kohdistaa toimia SVPL 272 §:n 1 momentin 2 kohdassa tarkoitetulla tavalla viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi taikka viestejä, joita käytetään viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmisteluun. Käsitettä käytetään muun muassa teksti- ja multimediaviestipalveluita sekä sähköpostipalveluita koskevissa määräyksen kohdissa, joissa asetetaan haitallisen liikenteen suodattamista koskevia velvoitteita. Käsitteen on tarkoitus kattaa kaikki ne tilanteet, joissa viestien ja välitystietojen käsittely on mahdollista SVPL 272 §:n nojalla tietoturvasta huolehtimiseksi.

Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, ettei tietoja voida muuttaa muun kuin siihen oikeutetun toimesta ja että tiedot ja tietojärjestelmät ovat niihin oikeutettujen hyödynnettävissä. Sähköinen viesti voi tarkoittaa tapauksesta riippuen esimerkiksi IP-pakettia, sähköpostia tai SMS-viestiä taikka verkon elementtien välistä ohjausliikennettä.

Haitallista liikennettä on siten esimerkiksi palvelunestohyökkäyksistä, roskapostista tai verkkomatojen leviämisestä aiheutuva liikenne. Liikenteen haitallisuutta on tarkasteltava sekä palveluntarjoajan että asiakkaan näkökulmista. Käytännössä tällä tarkoitetaan esimerkiksi sitä, että vaikkapa viestintäpalvelun käytettävyyden turvaaminen voi edellyttää toimia sekä palveluntarjoajan tarjoaman palvelun välityskyvystä huolehtimiseksi että käyttäjälle tarjottavan palvelutason ylläpitämiseksi. Kulloinkin sovellettavana olevasta velvoitteesta ja soveltamistilanteesta (kuten mikä viestintäpalvelu on kyseessä) riippuu, minkälaisen haitallisen liikenteen torjuminen tulee kyseeseen.

2.4 Suodattaminen

Suodattamisella tarkoitetaan edellä määritellyn haitallisen liikenteen estämistä tai rajoittamista. Suodattamista voi olla esimerkiksi asiakasliittymästä lähtevän, väärennettyjä lähdeosoitteita käyttävän internetliikenteen hylkääminen, tietyntyyppisen internetliikenteen kapasiteetin rajoittaminen liittymäkohtaisesti tai liikennöinnissä käytettyyn sovellusprotokollaan perustuen, tai sähköpostiviestien välittämisen tai vastaanottamisen estäminen.

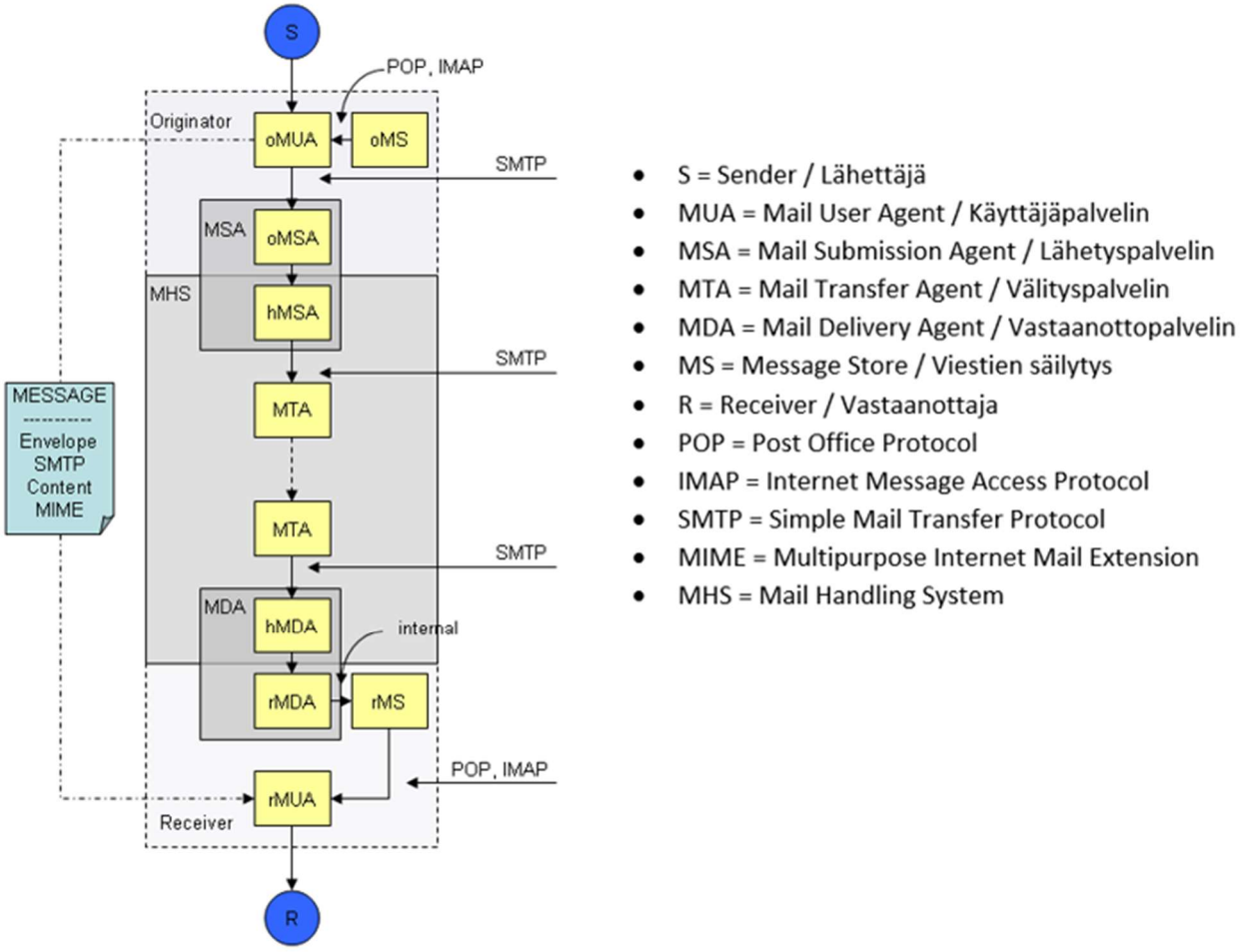
Suodattamisella tarkoitetaan myös tietoturvaa vaarantavien haitallisten tietokoneohjelmien poistamista viesteistä eli esimerkiksi sähköpostiviesteistä haittaohjelmien poistamista.

Edellisten lisäksi suodattaminen voi tarkoittaa myös muita teknisluonteisia toimia tietoturvaa vaarantavan liikennöinnin hallitsemiseksi.

2.5 Sähköpostipalvelu

Sähköpostipalvelulla tarkoitetaan sähköpostiviestien lähettämis-, välittämis- tai vastaanottopalvelua, joka hyödyntää internetin nimipalvelua eli DNS-palvelua viestien välittämiseen. Sähköpostipalvelun periaatekuva, eri toiminnot ja toimintojen välillä käytettäviä protokollia on esitetty kuvassa 1.

Sähköpostin lähettämispalvelulla tarkoitetaan palvelua, jossa asiakas lähettää viestin palveluntarjoajan lähetyspalvelimen (MSA) kautta. Välittämispalvelulla tarkoitetaan palvelua, jossa sähköpostiviesti vastaanotetaan, (käsitellään) ja lähetetään edelleen asiakkaan kanssa sovittuun kohteeseen. Vastaanottopalvelulla tarkoitetaan palvelua, jossa asiakkaan sähköpostiviestit vastaanotetaan vastaanottopalvelimelle (MDA) ja toimitetaan asiakkaan sähköpostilaatikkoon.



Kuva 1. Sähköpostipalvelun periaatekuva.

Lähtevällä sähköpostiliikenteellä tarkoitetaan asiakkailta lähteviä sähköpostiviestejä, jotka välitetään palveluntarjoajan lähetyspalvelimien (MSA) kautta sähköpostin välityspalvelimille (MTA).

Saapuvalla sähköpostiliikenteellä taas tarkoitetaan asiakkaille saapuvia sähköpostiviestejä, jotka välitetään palveluntarjoajan vastaanottopalvelimien (MDA) kautta asiakkaiden sähköpostilaatikoihin (MS).

Määräyksen soveltamisalaan kuuluvat myös *sähköpostiviestien välityspalvelu* ja *toissijainen sähköpostin välityspalvelu*, joita ei ole määräyksessä erikseen määritelty.[14]

Sähköpostiviestien välityspalvelulla tarkoitetaan sähköpostipalvelua tarjoavan teleyrityksen palvelua, jossa teleyritys välittää tai uudelleenohjaa viestejä omien sähköpostipalvelimiensa kautta (ns. viestien uudelleenohjauspalvelu).

Sähköpostia koskevia velvoitteita sovelletaan myös toissijaiseen sähköpostin välityspalveluun, millä tarkoitetaan asiakkaan omaa sähköpostipalvelua varmistavaa sähköpostin välityspalvelinta. Palvelussa asiakkaan ensisijaiseksi mx-tietueeksi tai -tietueiksi on määritelty asiakkaan oma sähköpostipalvelin tai palvelimet. Tällöin asiakkaalle saapuvaa sähköpostiliikennettä välitetään sähköpostipalveluntarjoajan toissijaisten sähköpostin välityspalvelinten kautta vain niissä tilanteissa, kun asiakkaan omat palvelimet eivät ole saavutettavissa. Saapuvan sähköpostiliikenteen suodattamista käsittelevät velvoitteet koskevat lähtökohtaisesti myös tällaista palvelua, mutta määräys jättää mahdollisuuden sopia asiasta toisin asiakkaan kanssa.

2.6 Viestintäverkon tai -palvelun komponentti

Viestintäverkon tai -palvelun komponentilla tarkoitetaan verkkoelementtiä, laitetta tai tietojärjestelmää, joista viestintäverkko tai -palvelu muodostuu tai jota se hyödyntää. Käsitettä käytetään useissa Liikenne- ja viestintäviraston määräyksissä.

Viestintäverkon tai -palvelun komponentteja ovat esimerkiksi matkaviestinkeskus, tukiasemaohjain, tukiasema, tekstiviestikeskus, laajakaistakeskitin, nimipalvelin, verkon pääsynhallinnasta vastaava palvelin, kytkin, reititin, SIP-sovelluspalvelin tai älyverkon komponentti. Viestintäverkon tai -palvelun komponentilla ei tarkoiteta siirtoteitä tai laitteen tai verkkoelementin osia, kuten matkaviestinkeskuksen prosessoriyksiköitä. Myöskään telepäätelaitteet eivät ole viestintäverkon tai -palvelun komponentteja.

Viestintäverkon tai -palvelun komponentti voidaan toteuttaa myös virtualisointiympäristössä (ks. perustelumuistion luku 6.6).

2.7 Yhteenliittämisrajapinta

Yhteenliittämisrajapinnalla tarkoitetaan tässä määräyksessä teleyritysten viestintäverkkojen tai -palvelujen välistä rajapintaa. Englanniksi yhteenliittämisrajapinnasta käytetään nimitystä Network to Network Interface (NNI-rajapinta).

2.8 Tekstiviestipalvelu ja multimediaviestipalvelu

Tässä määräyksessä *tekstiviestipalvelulla* tarkoitetaan SMS-viestien eli aakkosnumeerisia merkkejä ja erikoismerkkejä sisältävien tai binäärimuotoisten lyhytsanomien välittämispalvelua matkaviestinverkon tekstiviestikeskuksen välityksellä.

Multimediaviestipalvelulla tarkoitetaan määräyksessä MMS-viestien eli multimediaobjekteja kuten kuvia, ääntä, videota ja muotoiltua tekstiä sisältävien lyhytsanomien välittämispalvelua matkaviestinverkon multimediaviestikeskuksen välityksellä.

Luku 2 Yleiset tietoturvavaatimukset

Tässä luvussa käsitellään määräyksen luvussa 2 asetettuja kaikkia teleyrityksen viestintäverkkoja ja -palveluja koskevia vaatimuksia. Lisäksi määräyksen kohta 10 sisältää erityisiä vaatimuksia matkaviestinverkon teleyrityksille.

[14] Ks. kohta Muut toteuttamisvaihtoehdot tähän määräykseen tehdyistä muutoksista eräiden velvoitteiden soveltamisalassa.

3. Tietoturvallisuuden huomioiminen

3.1 Tietoturvallisuuden osa-alueet

Tietoturva on keskeinen osa teleyrityksen tarjoamien viestintäverkkojen ja -palvelujen laatua. Tietoturvallisuuden eri osa-alueiden huomioiminen teletoiminnassa on tärkeää kaikissa tarjottujen viestintäverkkojen ja -palvelujen elinkaaren eri vaiheissa: niitä suunniteltaessa, toteutettaessa, ylläpidettäessä sekä käytöstä poistettaessa. Jotta tietoturvasta huolehtiminen olisi rutiininomaista ja jokapäiväistä, on perusteltua edellyttää, että teleyritys määrittelee prosessit ja menettelyt tietoturvan toteuttamiselle.

Tietoturvallisuuden toteuttamisessa ja sitä kuvaavissa asiakirjoissa on huomioitava useita eri asioita. Määräyksen kohdassa 3.1 luetellaan huomioitavat asiakokonaisuudet, jotka vastaavat ENISA:n teledirektiivin mukaisia tietoturvatoimenpiteitä koskevissa suuntaviivoissa noudatettua jaottelua tietoturvan kahdeksaan osa-alueeseen (security domain).[15] Huomioitavat osa-alueet ovat:

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.

Eri osa-alueille asetetaan tarkempia vähimmäisvaatimuksia jäljempänä määräyksen kohdissa 4–9, joissa on puolestaan hyödynnetty ENISA:n kullekin osa-alueelle määrittelemiä turvallisuustavoitteita (security objective). Osa-alueisiin liittyviä vaatimuksia asetetaan myös muissa Liikenne- ja viestintäviraston määräyksissä, eikä tämä määräys aseta yksityiskohtaisia velvoitteita kaikille osa-alueille. Osa-alueisiin 5–6 sekä osittain osa-alueeseen 7 ja 8 liittyvät tarkemmat vaatimukset asetetaankin pääosin määräyksessä teletoiminnan häiriötilanteista, joka sisältää vaatimuksia mm. tietoturvaloukkausten havainnoinnista ja toipumismenettelyistä samoin kuin tietoturvaloukkaustapauksiin liittyvien ilmoitusten tekemisestä. Osa-alue 5 sisältää tietoturvaloukkausten hallinnan menettelyt, tietoturvaloukkausten havainnoinnin sekä tietoturvaloukkaustapauksiin liittyvien ilmoitusten käsittelyn menettelyt.[16] Osa-alue 6 tarkoittaa puolestaan teletoiminnan jatkuvuuden varmistamista erilaisissa vakavissa häiriötilanteissa, mikä sisältää esimerkiksi menettelyt toiminnan palauttamiseksi vakavissa häiriötilanteissa ja varmuuskopioinnin.[17] Osa-alueen 7 tarkoittama havainnointi sisältää määräyksen 8 kohdassa mainitun lisäksi tietoturvan kannalta merkittävien tapahtumien monitoroinnin erityisesti lokituksen avulla.[18] Osa-alue 8 kattaa määräyksessä käsitellyn teleyrityksen uhkatietoisuuden ylläpitämisen lisäksi tilaajien ja käyttäjien informoinnin tietoturvauhista, jotta nämä voivat ottaa käyttöön tarvittavia suojakeinoja ja siten edistää myös viestintäverkkojen ja -palvelujen tietoturvallisuutta.[19] Osa-aluetta koskevia, tilaajien ja käyttäjien

[15] ENISA Guideline on Security Measures under the EECC, 4th Edition, July 2021 (jäljempänä myös ENISA GL).
[16] ENISA GL SO18–SO20. Osa-alue 5 kattaa muun ohella mahdollisen tietoturvaloukkaustapausten koordinoidun ensivasteen toiminnon, ilmoitusyhteyspisteen ylläpidon sekä abuse-toiminnot eli internetpalvelujen tarjonnan yhteydessä asiakkaiden ja ulkoisten sidosryhmien tietoturvaloukkaustapauksiin liittyvien tapausten yhteys- ja palvelupisteeksi tarkoitetun toiminnon.
[17] ENISA GL SO21–SO22.
[18] ENISA GL, SO23.
[19] ENISA GL, SO29.

informointiin liittyviä suosituksia annetaan tämän perustelumuistion liitteen kohdassa 7.

Määräyksessä asetetaan useimmille tietoturvan eri osa-alueille keskeisimmät tietoturvatavoitteet ja -toimenpiteet mutta ei lähtökohtaisesti aseteta yksityiskohtaisia vaatimuksia siitä, miten tai mitä tietoturvatoimenpiteitä (kontrolleja) toteuttamalla nämä eri kokonaisuudet tarkalleen on kaikissa tilanteissa huomioitava. Tarkoituksenmukaiset toimenpiteet tietoturvan toteuttamiseksi vaihtelevat jossain määrin teleyrityksittäin mm. toiminnan laajuuden sekä tarjottavien verkkojen ja palvelujen ja niihin liittyvien erilaisten uhkien perusteella. Toimenpiteet on suhteutettava uhan vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin sekä käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka (SVPL 243.3 §).

ENISA:n laatima 5G-tietoturvatoimenpiteiden matriisi[20] sisältää sekä yleisiä, kaikkeen teletoimintaan soveltuvia kontrolleja, jotka pohjautuvat mm. ISO/IEC 27000 -standardisarjaan, sekä teknologiakohtaisia kontrolleja, jotka pohjautuvat 5G-verkon osalta mm. 3GPP:n TS 33.501 -standardiin. Matriisia voidaan hyödyntää myös määräyksen velvoitteiden toteuttamisessa. Määräyksen asiakokonaisuuksiin liittyviä vähimmäisvaatimuksia on käsitelty myös muissa Liikenne- ja viestintäviraston määräyksissä tai muualla lainsäädännössä, minkä lisäksi teletoiminnan tietoturvasta huolehtimiseen saattaa kohdistua myös esimerkiksi teleyrityskohtaisia, sopimuksista johtuvia vaatimuksia. Määräyksen kohdan 3.1 kannalta oleellista onkin se, että teleyritys tunnistaa omaan toimintaansa kohdistuvat vaatimukset ja niiden toteuttamiseen soveltuvat menettelyt. Tässä perustelumuistiossa esimerkkeinä mainittujen tietoturvakontrollien sijasta on mahdollista käyttää muitakin yhtä tehokkaita toimenpiteitä.

3.2 Tietoturvadokumentit

Määräyksen kohta 3.2 edellyttää, että teleyrityksellä on dokumentit siitä, miten se toteuttaa määräyksen 2 luvun tietoturvaa koskevat yleiset vaatimukset toiminnassaan. Dokumentit luovat perustan järjestelmälliselle tietoturvan kehittämiselle ja tietoturvan hallinnalle sekä auttavat tietoturvallisuuteen kohdistuvien investointien kohdentamisessa. Dokumentaation perusteella myös Liikenne- ja viestintävirasto voi tarvittaessa todentaa, että teleyritys noudattaa sitä koskevia tietoturvallisuudesta huolehtimisen velvoitteita.

Määräyksessä ei määritellä, mitä kaikkia eri dokumentteja teleyrityksellä on oltava, vaan asia jätetään teleyrityksen omaan harkintaan. Oleellista on, että dokumentointi on ajantasainen ja siitä pystyy toteamaan, että kaikki dokumentointivelvoitteen piiriin kuuluvat tietoturvan osa-alueet ja tarkemmat velvoitteet on huomioitu teleyrityksen toiminnassa.

4. Tietoturvallisuuden ja riskien hallinta

4.1 Tietoturvapolitiikka ja toimintaperiaatteet

Määräyksen kohta 4.1.1 edellyttää, että teleyritys laatii asianmukaiset tietoturvallisuuden ohjausasiakirjat, joita ovat tietoturvapolitiikka ja sitä tarkentavat toimintaperiaatteet. Tietoturvapolitiikalla teleyrityksen ylin johto sitoutuu tietoturvan toteuttamiseen sekä määrittää tietoturvallisuuden tahtotilan ja periaatteet viestintäverkkojen ja -palvelujen komponenttien ja muiden teletoimintaan liittyvien suojattavien kohteiden tietoturvan varmistamiseksi. Tietoturvallisuuden ohjausasiakirjoja laatiessaan teleyritys voi

[20] ENISA 5G Security Controls Matrix, May 24, 2023, https://www.enisa.europa.eu/publications/5g-security-controls-matrix.

tukeutua esimerkiksi yleisesti saatavilla oleviin tietoturvastandardeihin tai ENISA:n suosituksiin.[21] Tietoturvapolitiikkaa sekä yleisesti tietoturvallisuuden hallintajärjestelmää koskevia vaatimuksia on esitetty myös esimerkiksi standardissa ISO/IEC 27001.

Määräys edellyttää (kohta 4.1.1 ja osin kohta 3.2), että teleyritys tarkastelee säännöllisesti ja tarvittaessa ylläpitää (päivittää) tietoturvapolitiikkaansa sekä sitä toteuttavia toimintaperiaatteita. Tarkastelussa tulee määräyksen mukaisesti ottaa huomioon toimintaympäristön muutokset, havaitut poikkeamat, harjoitukset sekä ennakoitavissa olevat muutokset tietoturvan uhkaympäristöön. Arvioitaessa havaittujen poikkeamien mahdollisesti edellyttämiä muutoksia tietoturvapolitiikkaan tai toimintaperiaatteisiin on hyvä käytännössä ottaa huomioon, onko kyse tahallisesta rikkeestä vai johtuuko poikkeama esimerkiksi koulutuksen puutteesta, koska tämä vaikuttaa siihen, mitä käytännön toimia teleyrityksen on tapauksen johdosta järkevää toteuttaa.

4.2 Riskit

Riski on kielteisen seikan tai tapahtuman todennäköisyyden ja vaikutusten yhdistelmä.[22] Tietoturvariskeillä tarkoitetaan määräyksessä sellaista tahatonta tai tahallista tekijää, joka vaarantaa teletoiminnan luottamuksellisuutta, eheyttä tai käytettävyyttä. Tietoturvariski eroaa tietoturvauhasta siten, että sen todennäköisyyttä ja vaikutuksia on arvioitu.

Tietoturvariskit voivat aiheutua esimerkiksi:

- inhimillisistä virheistä
- henkilöstölle annettujen ohjeiden puutteista tai noudattamatta jättämisestä
- varkauksista tai ilkivallasta
- laitteiden, järjestelmien tai ohjelmistojen virheistä ja toimintahäiriöistä
- haittaohjelmien leviämisestä
- tietoaineistojen tuhoutumisesta
- tulipalosta tai tulvasta
- alihankkijan tai kumppanuusverkostoon kuuluvan toimijan virheistä ja laiminlyönneistä.

Riskien hallinta on prosessi, jonka tarkoitus on tunnistaa riskejä, vähentää niiden todennäköisyyttä ja/tai vaikutuksia hyväksyttävälle tasolle ja ylläpitää saavutettua tasoa. Riskien hallinnan tehtävänä on suojella organisaatiota ja sen kykyä suorittaa toimintojaan taloudelliset seikat huomioon ottaen.

Riskien hallinnan vaatimuksilla pyritään varmistamaan, että teleyritys on tietoinen riskien mahdollisen toteutumisen aiheuttamista seurauksista ja siitä, ovatko riskiä pienentävät toimenpiteet riittäviä. Riskien hallinnan tavoitteena on muun muassa:

- nopeuttaa tietoturvaongelmista toipumista
- vähentää tietoturvaongelmista aiheutuneita kustannuksia ja vahinkoja
- kohdentaa teletoiminnan tietoturvallisuutta parantavia investointeja
- parantaa teletoiminnan laatua ja tuottavuutta
- optimoida taloudellisesti teletoimintaan kohdistuvien riskien hallintaa
- ennaltaehkäistä riskien toteutumista.

Teleyritysten varautumisvelvollisuudesta säädetään SVPL 35 luvussa.

[21] Esim. ENISA GL ja ENISA 5G Supplement to the Guideline on Security Measures under the EECC, 2nd Edition, July 2021.
[22] Kokonaisturvallisuuden sanasto, TSK 50, Helsinki 2017.

Riskien tunnistaminen ja käsittely

Määräyksen kohta 4.1.2 edellyttää, että teleyritys tunnistaa ja hallitsee omaan teletoimintaansa ja sen jatkuvuuteen liittyvät riskit. Riskienhallinta tarkoittaa sitä, että teleyritys arvioi tietoturvariskit, käsittelee ne eli toteuttaa tarkoituksenmukaiset riskikontrollit ja hyväksyy mahdolliset jäännösriskit, samalla varmistaen, että toistuvat arvioinnit tuottavat verrattavia tuloksia. Käsittelyn tuloksena teleyritys määrittää toiminnalleen hyväksyttävän riskitason ja toteuttaa sen tarkoituksenmukaisin keinoin (usein ns. kontrollein eli erilaisin riskejä tai niiden realisoitumista lieventävin keinoin). Käytännössä riskien hallinnan tulee siis olla vastuutettua ja aikataulutettua. Lisäksi riskeille pitää määritellä asianmukainen omistaja, joka tarkistaa ja hyväksyy jäännösriskit. Jäännösriskien hyväksyntä tulee valtuuttaa teleyrityksen organisaation tasolle, hyväksytyn tietoturvapolitiikan mukaisesti.[23]

Määräyksessä ei aseteta velvoitetta tietyn riskien hallinnan standardin noudattamiselle, vaan teletoiminnan laajuudesta ja luonteessa riippuen voidaan soveltaa eritasoisia toimintamalleja. Riskien hallinnasta on laadittu mm. seuraavia standardeja ja julkaisuja: ISO/IEC 27005 ja NIST 800-30 Risk Management Guide. Riskienhallintamallit vaihtelevat yhtiöittäin, eikä yhtä jokaiselle sopivaa mallia ole olemassa.

Määräyksessä edellytetään, että riskien hallinta on jatkuva prosessi. Tämän mukaisesti riskejä ja niiden hallintakeinoja tulee arvioida aina olosuhteiden muuttuessa, kuten osana uusien palvelujen hankinta ja käyttöönottoprosessia, muutosten yhteydessä (ks. muutostenhallinnasta k. 7.2) tai mahdollisen riskin realisoitumisen jälkeen.

Matkaviestinverkon teleyrityksen kohdalla on keskeistä ottaa huomioon erityisesti 5G-verkkojen ja -palvelujen komponentteihin kohdistuvat sisäiset ja ulkoiset uhat, jotka ovat osittain uusia. Määräys edellyttää, että teleyrityksellä on riskienhallintaprosessi, jolla uhkien aiheuttamia riskejä muun muassa kyseisiin omaisuuseriin pyritään hallitsemaan ja lieventämään. Lisäksi esimerkiksi virtualisointiympäristöjen ja reunalaskentayksiköiden riskien arviointiin on perusteltua kiinnittää erityistä huomiota.

Prosessin ja tulosten dokumentointi

Teleyrityksen on määräyksen kohdan 4.2 mukaisesti riskien hallinnan jatkuvuuden ja vaatimusten noudattamisen valvomiseksi säilytettävä dokumentoidut riskienkäsittelyprosessin tulokset vähintään kolmen vuoden ajan tai kolmelta viimeisimmältä käsittelykerralta, sen mukaan kumpi säilytysaika on pitempi. Jos käsittelykertoja ei kerry kolmea kertaa kolmen vuoden aikana, on dokumentaatiota säilytettävä siis pitempäänkin kuin kolme vuotta ja toisaalta, jos käsittelykertoja on kolmen vuoden aikana useampia kuin kolme, kaikki näiden dokumentoinnit on säilytettävä.

Riskien arvioinnin dokumentointi ja aikaisempien tulosten säilyttäminen antaa arvokasta tietoa siitä, miten vastaavanlaisiin riskeihin on suhtauduttu aikaisemmilla käsittelykierroksilla. Riskien arvioinnin tuloksena voi olla esimerkiksi uuden uhkatiedon käsittely, joka ei kuitenkaan johda riskiarvion muuttumiseen.

4.3 Tietoturvaroolit ja -vastuut

Määräyksen kohdan 4.1.3 mukaan teleyrityksen tulee määrittää asianmukaiset tietoturvaroolit sekä niihin liittyvät vastuut tietoturvapolitiikan ja sitä toteuttavien toimintaperiaatteiden mukaisesti.

[23] ENISA GL SO2, 5G Security Control Matrix: M07–M013, SO2-001, SO2-003–SO2-005 sekä ISO/IEC 27005:2018: 8 ja 9.

Selkeästi määritellyt ja dokumentoidut, koko henkilöstön tiedossa olevat tietoturvaroolit ja -vastuut mahdollistavat järjestelmällisen tietoturvallisuuden toteuttamisen ja tietoturvan hallinnan rakenteen, joka tukee tietoturvan toteuttamista päivittäisessä työskentelyssä. Teleyrityksen toiminnan laajuudesta ja eri tietoturvaroolien luonteesta riippuen vastuu voi olla osa henkilön muuta toimenkuvaa. Kohdan toteuttamisessa voi soveltuvin osin tukeutua ENISA:n suuntaviivojen mukaisiin toimenpiteisiin ja tietoturvakontrolleihin.[24] Erityisesti viestintäverkon keskeisten osien ja muiden merkittävien suojattavien kohteiden tietoturvasta huolehtimiseen liittyvät velvollisuudet on käytännössä perusteltua yksilöidä selkeästi.

Lisäksi teleyrityksen on määräyksen mukaisesti mahdollisuuksien mukaan estettävä tietoturvaa vaarantavien vastuu- ja tehtäväkokonaisuuksien syntyminen eriyttämällä keskenään ristiriitaiset tehtävät ja vastuualueet, kuten esimerkiksi pääsyoikeuksien pyytäminen, hyväksyminen ja myöntäminen.[25] Tällaisten vastuu- ja tehtäväkokonaisuuksien syntyminen voidaan tilapäisesti sallia, mikäli tilanteeseen liittyvät riskit on arvioitu ja asianmukaiset hallintatoimenpiteet toteutettu. Jos kuitenkin kyseessä on esimerkiksi pieni toimija, ei kaikkia ristiriitaisia tehtäviä ole kuitenkaan välttämättä käytännössä mahdollista kokonaisuudessaan eriyttää; tällöin toiminnasta aiheutuvat riskit tulisi hallita muilla keinoin, kuten esimerkiksi teknisellä valvonnalla ja toimenpiteiden lokituksella.

Yksittäisen henkilön tai yhden avainhenkilön vastuulla olevat osa-alueet olisi perusteltua dokumentoida ja käsitellä tilanteeseen liittyvät havaitut riskit.

Määräyksen kohdassa 5.1.2 määrätään henkilöstön tietoturvaosaamisesta ja koulutuksesta.

On hyvä huomata, että tietoturvaroolien keskinäisten suhteiden ja vastuuhenkilöiden tarkastelua tulee tehdä säännöllisesti osana määräyksen kohdan 4.1.1 edellyttämää tietoturvapolitiikan ja toimintaperiaatteiden ylläpitoa. Tämän toteuttamisessa on käytännössä hyvä ottaa huomioon toimintaympäristön muutokset, henkilöstövaihdokset sekä havaitut poikkeamat (ks. myös määräyksen kohdat 4.1.3, 5.1.3 ja 5.1.4).

4.4 Toimittajasuhteet

Toimittajasuhteiden hallinta on olennainen osa teleyrityksen riskienhallintaa. Esimerkiksi viestintäverkon keskeisten osien tai muiden tietoturvan kannalta merkittävien toimintojen alihankintaketjujen riittämätön riskienhallinta voi johtaa koko viestintäverkon tai -palvelun tietoturvan vaarantumiseen.

Määräyksen kohta 4.1.4 edellyttää, että teleyritys laatii tarkentavat toimintaperiaatteet ja riskienhallintaprosessit toimitusketjujen riskien hallitsemiseksi. Kohta vastaa ENISA suuntaviivojen mukaista SO4:ää, ja sen toteuttamisessa voidaan tukeutua soveltuvin osin ENISA:n määrittelemiin toimenpiteisiin ja niitä tukeviin tietoturvakontrolleihin.[26]

Määräyksen vaatimus tarkoittaa siis käytännössä sitä, että teleyrityksellä tulee olla käytössään menettelyt, joilla se varmistaa, että kolmannet osapuolet kuten laite-, ohjelmisto- ja palvelutoimittajat sekä yhteenliittämis- ja muut yhteistyökumppanit noudattavat teleyrityksen edellyttämää tietoturvan tasoa. Käytännössä teleyrityksen on hyvä määritellä kolmansien osapuolten kanssa tehtäviä sopimuksia koskevat asianmukaiset tietoturvavaatimukset. Vaatimuksilla varmistetaan teleyrityksen tietoturvapolitiikan tai

[24] ENISA GL SO3, 5G Security Control Matrix: M014–M018, SO3-001 ja ISO/IEC 27002:2022: 8.8.
[25] Vastaavasti ISO/IEC 27002:2022: 5.3.
[26] ENISA GL SO4, 5G Security Control Matrix: M019–M026, SO4-004 - SO4-014 ja SO4-016 - SO4-048.

muun ohjeistuksen toteutuminen. Teleyritys voi esimerkiksi vaatia asianmukaisten turvallisuusstandardien noudattamista toimittajan tuotteissa, palveluissa ja toiminnassa.

Toimittajasuhteita koskevissa toimintaperiaatteissa on hyvä yksilöidä menettelyt tietoturvasta huolehtimiseen toimittajasuhteissa, toimittajien valvontaan liittyvät menettelyt sekä mahdollisten sellaisten jäännösriskien hallinta, joita ei ole toimittajan omin toimenpitein saatu teleyrityksen hyväksymälle tasolle.

Toimintaperiaatteiden on hyvä kattaa toimittajien kanssa tehdyistä sopimuksista ylläpidettävä rekisteri, jonka avulla sopimukset voi tarvittaessa katselmoida säännöllisesti esimerkiksi tietoturvavaatimusten ajantasaisuuden varmistamiseksi.

Teleyrityksen on syytä määritellä toimittajasuhteita varten asianmukaiset menettelyt siirrettävän tai käsiteltävän tiedon asianmukaiseen suojaamiseen (ks. myös määräyksen kohta 6.1.4) sekä tietojen salassapitoa koskevat velvoitteet.[27]

Tietoturvavaatimusten toteutumista kolmannen osapuolen toiminnassa on myös syytä seurata. Tämä voi tapahtua esimerkiksi auditointien avulla tai vaikkapa edellyttämällä säännöllistä, riippumatonta raportointia toimittajan tietoturvan hallintakeinoista ja niiden vaikuttavuudesta.

Toimintaperiaatteiden on hyvä sisältää myös kolmansien osapuolten toiminnasta johtuvien poikkeamien seurannan ja esimerkiksi keinoja kolmannen osapuolen toimittamien ohjelmistokomponenttien aitouden ja muuttumattomuuden varmistamiseksi.[28]

Teleyrityksen tulee määräyksen kohdan 4.1.1 mukaisesti säännöllisesti tarkastella ja päivittää tarkentavia toimintaperiaatteitaan ottaen huomioon toimintaympäristön muutokset sekä toimittajien toiminnassa havaitut poikkeamat.

5. Henkilöstöturvallisuus

5.1 Henkilöstön luotettavuus

Määräyksen kohdan 5.1.1 mukaan teleyrityksen on toteutettava asianmukaiset selvitykset käyttämänsä henkilöstön luotettavuudesta varmistumiseksi soveltuvan lainsäädännön puitteissa, mikäli se on henkilön tehtävien ja vastuiden kannalta tarpeen. Kohdan vastine on ENISA:n suuntaviivojen mukainen SO5, ja sen toteuttamisessa voidaan tukeutua esimerkiksi ENISA:n määrittelemiin toimenpiteisiin ja niitä tukeviin tietoturvakontrolleihin.[29] Teleyrityksen tulee etukäteen määritellä toimintaperiaatteet ja menettelytavat henkilöiden taustatarkistuksen toteuttamiseksi, sillä teleyrityksen on dokumentoitava, miten se ottaa vaatimuksen huomioon ja laadittava tietoturvapolitiikka ja siihen liittyvät tarkemmat toimintaperiaatteet (määräyksen kohdat 3.2 ja 4.1.1).

Teleyrityksen tulee toteuttaa rekrytoinnissa valituille henkilöille asianmukainen taustatarkistus, mikäli se katsotaan henkilön työtehtävien kannalta tarpeelliseksi. Taustatarkistusten toteuttamisessa tulee huomioitavaksi soveltuva työelämän tietosuojaan ja turvallisuus- ja luotettavuusselvityksiin liittyvä lainsäädäntö, kuten turvallisuusselvityslaki (726/2014) ja luottotietolaki (527/2007).

Taustatarkastukset tulee suhteuttaa tunnistettuihin riskeihin ja käsiteltävän tiedon luokitukseen. Taustatarkistusprosessia tulee soveltaa myös vuokratyöntekijöihin ja ulkopuolisiin toimittajiin, kun se on perusteltua suhteessa tällaisen henkilöstön käyttöön liit-

[27] ISO/IEC 27002:2022: 5.20.
[28] Ks. keinoista esim. NIST, Defending Against Software Supply Chain Attacks (April 2021).
[29] ENISA GL SO5 sekä 5G Security Control Matrix: M027–M030 ja SO5-001. Ks. myös ISO/IEC 27002:2022: 6.1.

tyviin riskeihin. Mikäli taustatarkistusprosessin keinoin ei saavuteta hyväksyttävää riskitasoa, tulisi teleyrityksellä olla menettelyt jäännösriskien hallintaan. Mikäli jäännösriskejä ei saada hyväksyttävälle tasolle, henkilöä ei tulisi osoittaa kyseiseen tehtävään. Jäännösriskejä voidaan hallita esimerkiksi pääsynhallinnallisin keinoin tai toteuttamalla erillistä valvontaa.

Taustatarkistusten tekemisessä ja tarkistusten laajuuden määrittelyssä tulisi ottaa erityisesti huomioon erityisesti roolit, joissa henkilöllä on fyysinen tai looginen pääsy matkaviestinverkon tai muun keskeisen viestintäverkon kriittisiin osiin tai muihin merkittäviin suojattaviin kohteisiin.

Velvoite liittyy myös määräyksen kohdan 5.1.3 mukaiseen velvollisuuteen huolehtia henkilöstön tehtävissä tapahtuvista muutoksista aiheutuvista riskeistä. Kun henkilö siirtyy teleyrityksen sisällä tällaiseen rooliin, on teleyrityksen arvioitava aiemman taustatarkistuksen riittävyys ja tarvittaessa toteutettava roolia vastaava taustatarkistus. Taustatarkistukset olisi muutoinkin hyvä tarvittaessa toistaa säännöllisin määräajoin ottaen huomioon tarvittaessa turvallisuusselvitysten voimassaoloajat.

Teleyrityksen on tarvittaessa tarkasteltava ja päivitettävä taustatarkistuksen toteuttamiseksi laadittuja kohdennettuja toimintaperiaatteita ja menettelytapoja ottaen huomioon toimintaympäristön ja uhkien muutokset sekä havaitut turvallisuuspoikkeamat, kuten määräyksen kohta 3.1 käytännössä edellyttää.

5.2 Henkilöstön tietoturvaosaaminen ja sen kehittäminen

Määräyksen kohdan 5.1.2 mukaan teleyrityksellä tulee olla menettelyt henkilöstön riittävän tietoturvaosaamisen varmistamiseksi ja osaamisen ylläpitämiseksi. Teleyrityksen on järjestettävä henkilöstölle tietoturvakoulutusta, joka voi olla tarpeen mukaan yleistä tai tehtäväkohtaisesti kohdennettua. Koulutuksiin osallistumista on perusteltua seurata. Yleisissä tietoturvakoulutuksissa tulisi huomioida esimerkiksi haittaohjelmien leviämisen ehkäisy sekä erityisesti pyrkiä kehittämään ja ylläpitämään henkilöstön tietoisuutta ja toimintavalmiutta tietojenkalastelun torjumiseksi.[30]

Teleyrityksen henkilöstö tulee saattaa tietoiseksi tietoturvapolitiikasta ja kohdennetuista toimintaperiaatteista sekä niiden tavoitteista ja vaikutuksista omien työtehtäviensä osalta.[31]

Tietoturvakoulutusten sisältöä on käytännössä hyvä tarkastella ja päivittää säännöllisesti ottaen huomioon toimintaympäristön muutokset, arviointien tulokset sekä havaitut poikkeamat.

Henkilöstön tietoturvaosaamisen todentamiseksi teleyritys voi ottaa käyttöön menettelyjä henkilöstön tietoturvaosaamisen tason testaamiseksi. Lisäksi teleyritys voi ottaa käyttöön keinoja, joilla sen henkilöstö voi, esimerkiksi anonyymisti, ilmoittaa havaitsemistaan tietoturvauhkista, -loukkauksista, -riskeistä tai kehittämiskohteista. Näillä toimin teleyritys voi rakentaa omaa tietoturvakulttuuriaan.

5.3 Työsuhteen päättyminen ja muutokset

Määräyksen kohdan 5.1.3 mukaan teleyrityksellä tulee olla dokumentoidut menettelytavat henkilöstömuutoksista tai henkilöstön tehtävissä tapahtuvista muutoksista aiheutuvien tietoturvariskien hallitsemiseksi.[32]

[30] ENISA GL SO6 ja ISO/IEC 27002:2022: 6.2, 6.3, 6.6 ja 8.7. Ks. myös https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-epailyttavien-sivujen-tunnistamiseksi.
[31] 5G Security Control Matrix: M004 ja ISO/IEC 27002:2022: 5.1.
[32] ENISA GL SO7 ja ISO/IEC 27002:2022: 6.2, 6.5, 6.6.

Käytännössä menettelytapoihin kuuluu se, että teleyritys perehdyttää henkilöstönsä työtehtäviin ja niissä tapahtuviin muutoksiin sekä se, että teleyritys tarvittaessa poistaa viipymättä henkilöstö- ja tehtävämuutosten tapahtuessa käytöstä tarpeettomat käyttöoikeudet, kulkuluvat, henkilökortit ja laitteet.

Määräyksen kohdassa 5.1.2 määrätään henkilöstön tietoturvaosaamisesta ja siitä, että henkilöstö on tietoinen etenkin omiin työtehtäviinsä liittyvistä toimintaperiaatteista.

Teleyrityksen tulee käytännössä määräyksen kohdan 3.2 johdosta huolehtia henkilöstössä tai henkilöstön tehtävissä tapahtuviin muutoksiin liittyvien toimintaperiaatteiden ja menettelytapojen ajantasaisuudesta ottamalla huomioon toimintaympäristön muutokset sekä havaitut poikkeamat.

5.4 Henkilöstön tietoturvapolitiikan vastaiset toimet

Teleyrityksellä tulee olla dokumentoitu menettely, jonka perusteella puututaan tilanteisiin, joissa työntekijä rikkoo teleyrityksen tietoturvaa koskevia toimintaperiaatteita tai menettelyjä. Käytännössä menettelyn tulee sisältää esimerkiksi se, miten käsitellään tilanteet, joissa tietoturvaloukkaus johtuu henkilöstön tietoturvaperiaatteiden vastaisesta toiminnasta.[33] Osana menettelyä on myös hyvä arvioida mahdollisia toimenpiteitä, joilla poikkeamat voidaan välttää jatkossa.

Tietoturvaloukkauksesta tai sen uhasta on ilmoitettava soveltuvan lainsäädännön mukaisesti valvontaviranomaiselle sekä tilaajille ja käyttäjille.

6. Tietojärjestelmä- ja tietoliikenneturvallisuus sekä fyysinen turvallisuus

6.1 Pääsynhallinta

Teleyrityksen viestintäverkkoon ja tietojärjestelmiin pääsyä varten tulee olla käytössä asianmukaiset loogiset, fyysiset ja hallinnolliset pääsynhallintamekanismit, joita ylläpidetään huolellisesti koko käyttäjäidentiteetin elinkaaren ajan.[34]

Määräys edellyttää, että teleyrityksen on määriteltävä ja dokumentoitava kohdennetut toimintaperiaatteet ja menettelyt, joissa huomioidaan pääsynhallinnan tietoturvallisuutta koskevat vaatimukset ja joilla varmistetaan vain luvallinen pääsy viestintäverkon tai -palvelun komponentteihin sekä teletoiminnan yhteydessä käsiteltyihin tietoihin. Pääsynhallinnan vaatimuksista on myös viestittävä niille sidosryhmille, jotka teleyrityksen valtuuttamana osallistuvat pääsyoikeuksien hallintaan.

Käytännössä toimintaperiaatteissa kuvataan ainakin pääsynhallintaa ja identiteetinhallintaa koskevat säännöt sekä pääsy- ja käyttöoikeuksien myöntämis- ja hallintaperiaatteet.

Pääsynhallintaa koskevat säännöt toteutetaan määrittelemällä vaatimusten mukaisesti pääsyoikeuksia ja -rajoituksia. Pääsyoikeus voidaan antaa ihmiselle, tekniselle tai loogiselle kohteelle, kuten koneelle, laitteelle tai palvelulle. Pääsynhallinnan lähtökohtana tulisi aina olla vähimpien käyttöoikeuksien periaate. Lisäksi on hyvä ottaa huomioon pääsyoikeuksien hakemiseen ja myöntämiseen liittyvien tehtävien eriyttäminen (ks. myös määräyksen kohta 4.1.3).[35]

[33] ENISA GL SO7 ja ISO/IEC 27002:2022: 6.2, 6.4, 6.5, 6.6.
[34] ENISA GL SO11.
[35] ISO/IEC 27002:2022: 5.15, 5.16, 8.2.

Pääsyoikeuksien hallintaan on useita eri toteutustapoja, joilla hallintaa voidaan myös automatisoida ja helpottaa. Roolipohjaisessa pääsynhallinnassa pääsyoikeudet perustuvat käyttäjien rooleihin, jolloin on erityisen tärkeää, että keskenään ristiriitaiset tietoturvaroolit ja -vastuut on eriytetty määräyksen kohdan 4.1 luetelmakohdan 3 mukaisesti. Esimerkiksi dynaamisella pääsynhallinnalla voidaan lisäksi rajoittaa pääsyä ajallisesti tai vain tiettyyn osaan tietoa ja suojata viestintäverkon ja -palvelujen jatkuvuuden kannalta kriittisiä komponentteja.

Yksilöidyllä identiteetillä mahdollistetaan käyttäjien yksilöllinen tunnistaminen ja hallinnointi. Identiteetin hallinnassa pyritään oletusarvoisesti henkilökohtaisten identiteettien käyttöön. Mikäli tämä ei yksittäisessä järjestelmässä ole teknisesti mahdollista tai kustannuksiltaan kohtuullista, on käytännössä hyvä toteuttaa ja dokumentoida menettelytavat käyttäjien yksilöimiseksi riittävällä tavalla järjestelmän ulkopuolisin keinoin (esimerkiksi hyppykoneen avulla).

Toimintaperiaatteet on dokumentoitava määräyksen kohdan 3.2 mukaisesti.

Henkilöstömuutoksiin liittyviä vaatimuksia käsitellään myös perustelumuistion luvussa 5.3.

6.2 Verkkojen ja tietojärjestelmien eheyden suojaaminen

Määräys edellyttää, että teleyritys huolehtii verkkojensa ja palvelujensa sekä henkilöstönsä käytössä olevien päätelaitteiden ja tietojärjestelmien eheydestä ja suojaa niitä viruksilta, haitallisen koodin lisäykseltä ja muilta haittaohjelmilta, jotka voisivat päästä muuttamaan järjestelmien toimintoja.[36] Tämän velvoitteen edellyttämät toimintaperiaatteet on dokumentoitava määräyksen 3.2 kohdan mukaisesti.

Verkkojen ja palvelujen sekä niitä toteuttavien laitteiden suojaaminen, hallinnointia ja valvonta ovat tärkeitä järjestelmien ja sovellusten tietojen suojaamiseksi verkon kautta tapahtuvalta vaarantumiselta. Tämän toteuttamiseksi teleyrityksellä on hyvä olla käytössä kontrolleja, joilla voidaan varmistaa verkon tietoturvaa ja suojata verkkoon liitettyjä palveluita luvattomalta käytöltä.

Teleyrityksen henkilöstön työssään käyttämien päätelaitteiden asianmukainen hallinta, käyttö ja suojaaminen on tärkeää, koska puutteellisesti tai vastoin ohjeistusta käytettynä päätelaitteet voivat altistua haittaohjelmille ja tietojen kalastelulle, ja siten toimia pääsyreittinä teleyrityksen verkkoon tai tietoaineistoihin.[37]

Käytännössä teleyrityksen kohdennetuissa toimintaperiaatteissa ja menettelyohjeissa on hyvä määritellä tietoturvapolitiikan mukaisesti eri luokitustason ympäristöihin liittyvät tietoturvan hallintakeinot päätelaitteille sekä kuvata henkilöstön vastuut hallintakeinojen toteuttamiseksi. Henkilöstön koulutukseen liittyviä vaatimuksia käsitellään määräyksen kohdassa 5.1.2.

Haittaohjelmilta voidaan suojautua esimerkiksi rajaamalla käyttöoikeuksia vähimpien käyttöoikeuksien periaatteiden mukaisesti, koventamalla järjestelmiä, turvallisuuspäivitysten asianmukaisilla asennuskäytännöillä, henkilöstön tietoturvatietoisuuskoulutuksilla sekä haittaohjelmien havainnointi- ja korjausohjelmistoilla.[38]

Haavoittuvuuksien hallintaa tukee riittävän tarkka ja kattava sekä mahdollisuuksien mukaan automaatioon perustuva omaisuuden hallinta, joka sisältää tarpeelliset tiedot oh-

[36] ENISA GL SO12.
[37] ISO/IEC 27002:2022: 8.1.
[38] ISO/IEC 27002:2022: 8.7.

jelmistojen riippuvuussuhteista (hierarkia, järjestelmät), tiedon ohjelmiston toimittajasta, ohjelmiston nimen ja version sekä ohjelmistosta vastaavien henkilöiden tiedot.[39] Menettelyistä omaisuuden hallintaan määrätään kohdassa 7.1.3.

Matkaviestinverkon komponenttien turvallisuustoimintoja käsitellään myös määräyksen kohdassa 10.

Luottamattomuuden periaate (zero trust) on tietoturvamalli, jossa rajoitetaan järjestelmien ja käyttäjien pääsy vain välttämättömiin resursseihin sekä minimoidaan luvattomasta pääsystä aiheutuvat riskit.[40] Mallissa myös pakotetaan entiteettien välinen toistuva todentaminen ja valtuuttaminen. Mallissa oletetaan, että hyökkääjä on aina läsnä, joten mikään komponentti tai järjestelmä ei ole lähtökohtaisesti luotettava. Tätä tietoturvamallia on perusteltua soveltaa teleyrityksen verkossa tapahtuvaan liikennöintiin erityisesti, kun on kyse jatkuvuuden kannalta keskeisistä komponenteista ja malli on teknisesti soveltuva.

Tunkeutumisen laajentaminen (lateral movement) on käsite, jolla tarkoitetaan hyökkääjän liikkumista hyökkäyksen kohteena olevan verkon sisällä saatuaan jalansijan johonkin verkon järjestelmään. Tämän liikkumisen rajaamista voidaan toteuttaa esimerkiksi jakamalla verkko eri alueisiin luottamustasojen mukaisesti.[41]

Verkkojen jakamiseen erilaisiin verkkoalueisiin, vyöhykkeisiin tai segmentteihin eri luottamustasojen mukaan sekä verkkoalueiden eriyttämiseen toisistaan joko fyysisesti tai loogisesti (esimerkiksi virtuaalisilla erillisverkoilla) on hyvä laatia omat kohdennetut toimintaperiaatteet ja menettelyohjeet. Verkkoalueet on hyvä erottaa julkisesta verkosta aina, kun se on mahdollista. Erottelun yhtenä tarkoituksena on hankaloittaa hyökkääjän liikkumista verkon sisällä eri verkkoalueiden välillä, jos hyökkääjä onnistuu saamaan jalansijan yhden verkkoalueen sisäpuolelta. Edellä kuvattu luottamattomuuden periaate myös tukee tätä ajattelua.

Kriteerien, joilla verkot eriytetään eri verkkoalueisiin, on käytännössä hyvä perustua kunkin verkkoalueen turvallisuusvaatimusten arviointiin. Erottelua voidaan toteuttaa esimerkiksi siten, että käyttäjä-, ohjaus- ja hallintaliikennettä kuljettavat verkkokerrokset pyritään erottamaan toisistaan edellä mainituin keinoin. Liikenne ja pääsy verkkoalueiden välillä voidaan sallia, mutta tällöin tulisi huolehtia, että verkkoalueiden välille on järjestetty valvonta ja mahdollisuus rajoittaa liikennettä siten, että vain toiminnalle tarpeellinen ja välttämätön liikennöinti sallitaan. Liikenteen suodattamista ja valvontaa voidaan toteuttaa esimerkiksi palomuureilla, reitittimillä, sovellusyhdyskäytävillä tai erillisillä tunkeutumisenestojärjestelmillä (IPS) ja tunkeutumisenhavaitsemisjärjestelmillä (IDS).[42]

Toimintaperiaatteissa tulisi ottaa huomioon verkon loogisten ja fyysisten rajapintojen ja liitäntöjen osalta tarpeettomien palvelujen ja protokollien poistaminen käytöstä mahdollisuuksien mukaan. Loogiset ja fyysiset rajapinnat ovat yhdyskäytäviä, joiden avulla verkkolaitteet kommunikoivat ulkoisten laitteiden ja järjestelmien kanssa. Rajapinnoissa tarjottavat palvelut ja protokollat mahdollistavat erilaisia toiminnallisuuksia, ja mitä enemmän tällaisia protokollia ja palveluita on samanaikaisesti käytössä, sitä suurempi riski näiden hyödyntämiseen myös mahdollisissa hyökkäyksissä.

[39] ISO/IEC 27002:2022: 8.8.
[40] NIST - Zero Trust Architecture - SP.800-207, https://csrc.nist.gov/publications/detail/sp/800-207/final.
[41] Tietoturva Nyt! Tunnetko tunkeutumisen laajentamisen (osa 1 ja 2), https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnetko-tunkeutumisen-laajentamisen-osa-1 ja https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnetko-tunkeutumisen-laajentamisen-osa-2.
[42] ISO/IEC 27002:2022: 8.22.

6.3 Palvelunestohyökkäyksiltä suojautuminen

Määräyksen kohdan 6.3 mukaan teleyrityksen tulee suojata viestintäverkkojen ja -palvelujen kannalta keskeiset järjestelmät palvelunestohyökkäyksiä vastaan. Suojaustoimenpiteet tulee mitoittaa ajantasaisen riskiarvion mukaisesti. Riskiarvion tulee siis perustua ajantasaiseen uhkatietoon, jonka ylläpitämiseen voi kuulua esimerkiksi tiedonvaihto eri yhteistyöverkostojen kanssa sekä eri lähteiden ajantasainen seuranta asianmukaisia työkaluja hyödyntäen. Uhkatiedon ylläpitoa käsitellään määräyksen kohdassa 9.

> Palvelunestohyökkäys (Denial of Service attack) on hyökkäys, jolla pyritään estämään verkkoresurssin tai verkossa sijaitsevan palvelun käyttö. Palveluestohyökkäykset tapahtuvat yleensä joko kuormittamalla kohteena olevaa palvelua/verkkoliikennettä ylimääräisellä liikenteellä tai hyödyntämällä kohteessa olevaa haavoittuvuutta. Nykyisin iso osa palvelunestohyökkäyksistä on hajautettuja, jolla tarkoitetaan sitä, että hyökkäys tulee useammasta laitteesta samanaikaisesti. Näin mahdollistetaan esimerkiksi suuremman liikennemäärän käyttäminen kohteena olevan palvelun ylikuormittamiseen. Hajautettujen hyökkäysten taustalla on usein laitteita, jotka ovat kaapattu hyökkäyskäyttöön ilman omistajiensa tietämystä asiasta.
>
> Palvelunestohyökkäysten toteutustavat vaihtelevat. Useimmiten hyökkäyksessä kuormitetaan kohde suurella määrällä liikennettä, jolloin kohteena olevan verkkoresurssin tai palvelun taso laskee tai estyy. Esimerkki yleisesti käytetystä palvelunestohyökkäystyypistä on niin sanottu SYN-tulvahyökkäys (SYN flood), joka perustuu TCP-protokollan kolmivaiheiseen kättelyyn. Hyökkäyksessä hyökkääjä lähettää kohteeseen suuria määriä TCP SYN -paketteja, mutta ei lähetä ACK-pakettia ollenkaan, jolloin kohteena oleva palvelin tai laite täyttyy keskeneräisistä yhteyksistä, eikä pysty vastaanottamaan uusia yhteydenottopyyntöjä.
>
> Palvelunestohyökkäys voidaan kohdistaa myös sovellustasolle. Tällöin hyökkääjä kohdistaa hyökkäyksensä sovellukseen itseensä käyttäen hyväkseen haavoittuvuuksia tai yleisessä tiedossa olevia ongelmia. Tällaiset hyökkäykset eivät välttämättä vaadi suuria määriä liikennettä toimiakseen, joten niiden havaitseminen on hankalampaa. Esimerkki tällaisesta hyökkäyksestä on HTTP-tulvahyökkäys (HTTP flood), jossa hyökkääjä lähettää harkittuun kohteeseen tarvittavan määrän HTTP-pyyntöjä, jotta kohteen käyttö estyy muilta käyttäjiltä. Nämä HTTP-pyynnöt voivat olla hankalia erottaa oikeiden ihmisten lähettämistä pyynnöistä, jonka seurauksena tämänkaltaisten hyökkäysten havaitseminen voi olla haasteellista.

Uusien teknologien ja tekniikoiden myötä myös palvelunestohyökkäysten kohteet, määrä ja laatu ovat jatkuvassa muutoksessa. Esimerkiksi 5G-verkon eri rajapintoihin kohdistuvat hyökkäykset luovat uusia haasteita palveluntarjoajille. 5G-verkko mahdollistaa moninkertaisen laitetiheyden edellisiin verkkosukupolviin verrattuna, ja esimerkiksi potentiaalisten palvelunestohyökkäyksiin käytettävien IoT-laitteiden (Internet of Things, IoT) määrän odotetaan kasvavan. Laitteiden määrän kasvu ja mahdollinen vaihteleva tietoturvan taso edellyttävät riskien huomioimista ja niihin varautumista.

Tyypillisiä tapoja lieventää palvelunestohyökkäysten vaikutusta ovat esimerkiksi pakettipesurit, jotka hajauttavat verkkoliikennettä, tai käyttämällä SAV-tekniikoita (Source Address Validation), esimerkiksi ACL:iä (Access Control Lists), joilla voidaan mm. määritellä verkkoliikenteessä hylättävät IP-prefiksit.[43] Palvelunestohyökkäysten vaikutusta voidaan vähentää myös laitteistojen, kuten palomuurien ja kuormantasaajien oikeaoppisilla konfiguraatioilla. Joko erikseen toimivat tai palomuuriin sisältyvät IDS- (Intrusion Detection System) ja IPS (Intrusion Prevention System) -järjestelmät auttavat havaitsemaan ja estämään palvelunestohyökkäyksiä.

[43] NIST - Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation, s. 27–28, https://csrc.nist.gov/publications/detail/sp/800-189/final.

6.4 Salauksen ja kryptografian käyttö

Kryptografian käytöllä suojataan tiedon luottamuksellisuutta, aitoutta ja eheyttä. Asianmukaisella salauksen käytöllä estetään ja minimoidaan tietoturvahäiriöiden vaikutuksia käyttäjiin, verkkoihin ja palveluihin. Salausta koskevat määräyksen velvoitteet vastaavat osittain Ruotsin PTS:n (Post- och telestyrelsen) määräyksessä ja sen soveltamisohjeessa teleyrityksille asetettuja velvoitteita.[44]

Määräyksen mukaisesti teleyrityksen tulee luoda ja ylläpitää menettelyt salausta koskevien kohdennettujen toimintaperiaatteiden (salauspolitiikka) mukaisesti. Toimintaperiaatteiden tulee sisältää ainakin salauksen toteutustavat sekä milloin ja missä tilanteissa salausta ei mahdollisesti käytetä. Toimintaperiaatteiden tulee myös sisältää yleistä tietoa käytettävien salausmenetelmien toiminnasta, tyypistä ja vahvuudesta. Lisäksi toimintaperiaatteissa tulee olla kuvaukset tietojen vaatimasta suojaustasosta sekä siitä, mikä salausmenetelmä soveltuu käytettäväksi minkäkin tiedon salaamiseen.[45]

Erilaisiin tietotyyppeihin liittyy erilaisia riskejä, jotka vaihtelevat ympäristön uhkatason mukaan. Teleyrityksen tulisikin aina arvioida tapauskohtaisesti tietojen edellyttämä salauksen tarve, salaustaso ja asianmukaiset salausmenettelyt. Erityisesti salasanat, salausavainmateriaalit ja muut todentamiseen käytettävät salaiset tiedot tulisi aina salata, jos se on teknisesti mahdollista. Salaukseen tulisi käyttää aina tilanteeseen sopivaa, riittävän suojauksen tuottavia salausratkaisuja ja -protokollia. Salaustarpeen arvioinnissa voidaan huomioida esimerkiksi se, onko riittävää, että jokin osa liikenteestä on tietyissä tilanteissa salattu. On esimerkiksi mahdollista, että ohjausliikenteen salaamisella saavutetaan riittävä tietoturvan taso, jolloin käyttäjätason liikenteen salaamiselle ei ole erillistä tarvetta. Lisäksi riskiarviossa voidaan huomioida liikenteen siirtotavasta aiheutuvat erilaiset tietoturvariskit. Arviointiin vaikuttavat myös sellaiset seikat kuin eri tahojen pääsymahdollisuudet liikenteeseen ja kulkeeko liikenne esimerkiksi internetin yli, luotettujen kumppaneiden verkossa vai yksinomaan teleyrityksen omassa verkossa, sekä teleyrityksen kyky ja tarpeet havainnoida haitallista liikennettä.

Määräyksen mukaisesti asianmukaista salausta tulee käyttää aina, kun tietoa säilytetään tai kun sitä siirretään, mikäli se on tiedon luonteen vuoksi tarkoituksenmukaista, teknisesti mahdollista ja oikeasuhtaista. Jos tietoa salataan sitä liikuteltaessa tai säilöttäessä, on syytä valita tekniikka, joka on suojaukseltaan riittävä salattavan tiedon luokitukseen ja suorituskykyvaatimuksiin nähden. Salaustekniikan osalta on hyvä huomioida algoritmit, käyttötavat ja avainvahvuudet. Käytetyn salausmenetelmän vaatimusten tulisi olla ajantasaisia koko järjestelmän elinkaaren ajan. Mikäli salauksen toteuttaminen ei ole mahdollista, on teleyrityksen perusteltava se ylläpitämissään toimintaperiaatteissa. Mikäli salausta ei käytetä tiedon säilyttämisessä tai tiedon siirrossa, on teleyrityksen käytännössä laadittava asiasta riski- ja vaikutusarvio osana määräyksen kohdan 4.1.2 vaatimusten toteuttamista, ja kuvattava se toimintaperiaatteissa.[46]

Salausmenetelmien puutteita voi olla haastava korvata muilla suojausmenetelmillä, joten teleyrityksen tulisi kiinnittää huomiota salausratkaisujen valintaan ja turvalliseen käyttöön.[47] Erityistä huomiota tulee käyttää viestintäverkon tai -palvelun jatkuvuuden kannalta keskeisten komponenttien suojaamiseen käytettävien salausprotokollien valintaan ja käyttöön sekä sensitiivistä tietoaineistoa sisältävien tai käsittelevien komponenttien suojaamiseen.

[44] Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster, PTSFS 2022:11, 10 luku, https://www.pts.se/sv/dokument/foreskrifter/telefoni--internet/ptsfs-202211---foreskrifter-och-allmanna-rad-om-saker-het-i-nat-och-tjanster/.
[45] ENISA GL SO13, 5G Security Control Matrix: M071, M073 ja M074.
[46] ENISA GL SO13, 5G Security Control Matrix: M072.
[47] Vastaavasti Katakri 2020 - tietoturvallisuuden auditointityökalu viranomaiselle. I-12, s. 89, https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille.

Esimerkiksi tietoliikenteen salaamiseksi TLS-salausprotokollan osalta tulisi käyttää vähintään versiota 1.2 tai uudempaa. TLS-protokollan versiot 1.0 ja 1.1 ovat vanhentuneita, joten niitä ei tulisi enää käyttää.[48]

6.5 Salausavainmateriaalin ja salaisten todentamisessa käytettyjen tietojen suojaaminen ja hallinta

Määräyksen kohdassa 6.1.5 edellytetään, että teleyrityksellä tulee olla asianmukaiset toimintaperiaatteet ja menettelytavat salausavainmateriaalien ja todentamisessa käytettävien salaisten tietojen suojaamiselle ja hallinnalle. Tämä on tärkeää, koska näiden päätyminen vääriin käsiin vaarantaisi muun muassa tietoliikenneturvallisuutta ja pääsynhallintamenettelyjen tehokkuuden.

Teleyrityksen tulee siis käytännössä varmistaa, että salauksen avainaineistoa tai salaisia todennustietoja, mukaan lukien autentikoinnissa käytettyä salausavainmateriaalia, ei paljasteta ja että niitä suojataan muuttamiselta ja katoamiselta. Salausavainten tulee siis olla vain niille tarkoitettujen käyttäjien ja prosessien käytössä. Salauksen avainaineisto ja salaiset todennustiedot sekä laitteet, joilla luodaan, säilytetään ja arkistoidaan salausavaimia, on hyvä suojata tietoturvan parhaiden käytäntöjen ja standardien avulla.[49] Salausavainmateriaalin ja muiden todentamiseen käytettävien salaisten tietojen suojaamisessa on perusteltua käyttää myös salausta.

Salausavainten hallintaan liittyvät toimintaperiaatteet ja menettelyt tulee olla suunniteltu, toteutettu ja kuvattu. Teleyrityksellä tulee siis käytännössä olla käytännöt koskien salausavainten käyttöä, suojausta ja käyttöikää. Toimintaperiaatteissa on syytä myös määritellä erilaiset roolit, vastuut ja valvonta salausavainten koko elinkaaren ajan, mukaan lukien yksityisten avainten käyttö, varmuuskopiointi ja palauttaminen.[50]

6.6 Virtualisointiympäristön koventaminen

Määräyksen kohdassa 6.1.6 edellytetään, että virtualisointiympäristössä toteutetut viestintäverkon tai -palvelun komponentit toteutetaan siten, että vain niiden toiminnan kannalta välttämättömät toiminnallisuudet ja pääsyoikeudet on sallittu. Toisin sanoen määräys edellyttää virtualisointiympäristöjen niin sanottua koventamista. Teleyrityksellä tulee olla dokumentoidut toimintaperiaatteet ja menettelyt virtualisointiympäristöjen koventamiseksi (määräyksen kohta 3.2).

Virtualisoinnilla tarkoitetaan prosessia, jossa simuloidaan jotakin toiminnallisuutta luomalla sille virtuaalinen laskentaympäristö, jolla toiminnallisuus erotetaan taustalla olevasta fyysisestä resurssista.[51] *Virtualisointiympäristö* koostuu eri komponenteista ja järjestelmistä. Virtualisointiarkkitehtuurissa puhutaan pääsääntöisesti seuraavista komponenteista ja järjestelmistä: fyysiset laitteet, virtualisointitaso, virtualisoinnin hallinnointitaso, yksittäiset virtualisoidut järjestelmät sekä operatiiviset ja teletoiminnan tu-

[48] IETF RFC 8996, Deprecating TLS 1.0 and TLS 1.1, https://www.rfc-editor.org/rfc/rfc8996.
[49] ENISA GL SO14, 5G Security Control Matrix: M075.
[50] ENISA GL SO14, 5G Security Control Matrix: M076 ja M077.
[51] Virtualisointi häivyttää fyysisen resurssin muilta järjestelmiltä, sovelluksilta ja käyttäjiltä. Virtualisoinnissa sama taustalla oleva fyysinen resurssi kuten palvelin, muisti tai suoritin voi toimia useana loogisena resurssina tai jos fyysisiä resursseja on useita, voidaan ne esittää virtualisoinnin avulla yhtenä loogisena kokonaisuutena. Virtualisointia voidaan soveltaa useisiin eri osa-alueisiin, kuten palvelimiin ja laskentatehoon, verkkoon, tallennustilaan, käyttöjärjestelmään tai sovelluksiin. Virtualisointi voidaan toteuttaa eri tavoin. Ensimmäinen tapa on luoda virtuaalikone, joka on ohjelmallisesti luotu emuloimaan vierasta käyttöjärjestelmää. Yhdelle fyysiselle laitteelle voidaan luoda useampi virtuaalikone, jotka käyttävät isäntälaitteen resursseja ajaakseen ohjelmistoja ja toimintoja. Virtuaalikoneiden tapauksessa virtualisointialusta (hypervisor) luo ja ajaa virtuaalikoneita. Virtualisointialusta on vastuussa isäntälaitteen resurssien jakamisesta virtuaalikoneille. Toinen tapa toteuttaa virtualisointia on konttiteknologian (containerization) avulla. Kontit eroavat virtuaalikoneista siinä mielessä, että virtuaalikoneet virtualisoivat koko käyttöjärjestelmän, mutta kontit virtualisoivat vain kontin tarvitsemat ohjelmistot ja riippuvuudet. Konttien luominen ja ajaminen toteutetaan sille tarkoitetun ohjelmiston avulla.

kijärjestelmät. Mitä enemmän komponentteja sekä eri toimittajia on käytössä virtualisoinnin tukemiseksi, sitä todennäköisempää on, että virtualisointiympäristössä on tietoturvaa uhkaavia haavoittuvuuksia sekä järjestelmän oleellisen käytön kannalta ylimääräisiä toiminnallisuuksia, jotka voivat myös osoittautua tietoturvauhiksi. Useat eri toimittajat tuovat haasteita haavoittuvuuksien hallintaan ja seurantaan, joten on erityisen tärkeää, että tarpeettomat ominaisuudet poistetaan käytöstä.

Koventamisella taas tarkoitetaan tässä tapauksessa sitä, että viestintäverkkojen ja -palvelujen komponentit asennetaan ja ylläpidetään siten, että niissä on käytössä vain niiden toiminnan kannalta *välttämättömät toiminnallisuudet ja pääsyoikeudet*. Toiminnallisuuksia rajoittamalla kuten tarpeettomia sovelluksia ja palveluita käytöstä poistamalla vähennetään järjestelmien haavoittuvuuspinta-alaa.

Teleyritys voi määritellä itse tavat ja tekniikat, joilla se toteuttaa määräyksen vaatimukset. Alla esitetään joitakin tekijöitä, joita teleyrityksen on hyvä huomioida valitessaan omaan toimintaansa soveltuvaa toteutusta:

- Yleisesti on hyvä käyttää asianmukaisia konfiguraationhallintaan liittyviä työkaluja kovennetun asennuksen toteuttamiseksi sekä sen ylläpitämiseksi.

- Käyttöoikeuksien rajoittaminen on yksi koventamisen toteutustavoista. Tässä on hyvä noudattaa pienimmän käyttöoikeuden periaatetta eli, että oikeuksia annetaan vain sen mukaan, mikä on ehdottoman tarpeellista. On myös syytä rajata sellaisien käyttäjien määrää, joilla on järjestelmänvalvojan oikeudet. Edellä mainittujen lisäksi on usein järkevää rajoittaa arkaluonteisiin tiedostoihin, kuten vaikkapa erilaisiin asetustiedostoihin pääsyä ja muokkausoikeuksia.

- Virtualisointiympäristön tuottamiseen ja toteuttamiseen olennaisesti liittyvät komponentit ja järjestelmät, kuten esimerkiksi virtualisointialustat ja isäntäkäyttöjärjestelmät, on syytä pitää ajan tasalla säännöllisin päivityksin ja suojauskorjauksin. Tämän toteuttamiseksi virtualisointiympäristön tuottamiseen ja toteuttamiseen olennaisesti liittyviä ohjelmistoja voi esimerkiksi skannata säännöllisesti, jotta niihin liittyvät haavoittuvuudet on mahdollista havaita. Päivityksistä voidaan huolehtia säännöllisillä päivityskäytänteillä, kuten esimerkiksi kuukausittaisilla paikkaus/päivityspäivillä. Lisäksi teleyrityksellä on hyvä olla omat prosessit tilanteisiin, jossa ilmenee järjestelmiin kohdistuvia kriittisiä haavoittuvuuksia. Tällaisten haavoittuvuuksien osalta päivitykset tai korjaukset on syytä pyrkiä tekemään ensi tilassa.

- Virtualisoidut verkon funktiot ja komponentit on käytännössä hyvä luokitella ja eriyttää hallinnollisiin alueisiin sen perusteella, kuinka korkeariskisestä komponentista tai funktiosta on kyse. Hallinnolliset alueet on mahdollisuuksien mukaan hyvä myös eriyttää toisistaan tai vähintään pyrkiä huolehtimaan siitä, että niiden välistä liikennettä voidaan jollain tapaa kontrolloida. Tämä voidaan toteuttaa esimerkiksi jakamalla eri työkuormat eri segmentteihin niiden tietoturvatarpeiden ja riskiluokittelun perusteella ja liittämällä nämä segmentit eri hallinta-alueisiin. Riskiä voidaan arvioida isännän tyypin ja ominaisuuksien ja roolin mukaan. On myös syytä huomioida, että joissain kriittisissä järjestelmissä fyysinen eriyttäminen voi olla tarpeen.[52]

- Virtualisoitujen ympäristöjen hallintakerros on syytä mahdollisuuksien mukaan eriyttää heikomman luottamuksen hallinta-alueista, kuten operatiivisesta infrastruktuurista, teleyrityksen omasta sisäverkosta, internetistä, sekä käyttäjäverkoista ja muiden teleyritysten verkoista. Eriyttäminen voidaan toteuttaa joko fyysisesti tai loogisesti. Fyysinen eriyttäminen voidaan toteuttaa esimerkiksi siten, että hallinta-

[52] ENISA 5G Security Matrix: SO12-018 ja ENISA NFV security in 5G: BP-T16, https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices.

kerrokseen liittyviä funktioita ei ajeta samoilla fyysisillä alustoilla, kun muiden kerrosten funktioita. Looginen eriyttäminen taas voidaan toteuttaa esimerkiksi käyttämällä erillisiä virtuaalikoneita hallintakomponenteille ja funktioille tai verkkokerroksen eriyttämisellä käyttäen vxlaneja, vlaneja tai liikenteen salausta.

- Hallintakerrokseen pääsyä on hyvä suojata esimerkiksi käyttämällä monivaiheista tunnistautumista, joka toteutetaan luomalla toinen todentamistekijä esimerkiksi paikallisesti. Hallinnolliselle pääsylle voi myös asettaa aikarajan tai aikakatkaisun. Hallinnointiin käytettävien tunnusten on perusteltua olla henkilökohtaisia. Henkilökohtaisten tunnusten lisäksi voidaan hyödyntää hätä- tai poikkeustilanteisiin tarkoitettuja tunnuksia, kun henkilökohtaisten tunnusten käyttö on estynyt. Näiden tunnusten käyttö on syytä rajoittaa vain ennalta dokumentoituihin käyttötapauksiin. Lisäksi tunnusten käyttöä tulee riittävällä tavalla kontrolloida kohdejärjestelmän ulkopuolisin keinoin, huomioiden asiaan liittyvät riskit.

- Kolmansien osapuolien osalta hallintayhteyksien tarve ja käyttöoikeuksien myöntäminen on järkevää arvioida tapauskohtaisesti ja noudattaa oikeuksien myöntämisessä pienimmän käyttöoikeuden periaatetta. Erityisesti silloin kun pääsy järjestelmiin ja niiden osiin myönnetään etäyhteyksien avulla, tulisi huolehtia yhteyksien ja tehtyjen toimenpiteiden asianmukaisesta lokituksesta ja lisäksi harkita muitakin auditointitoimenpiteitä, joilla varmistetaan, ettei verkko- ja tietojärjestelmiin tehdä luvattomia muutoksia.

- Mikäli virtualisointiympäristössä ja verkon funktioiden toteutuksessa käytetään konttitekniikkaa, on näidenkin osalta tärkeää huolehtia riittävien tietoturvakontrollien käyttöönottamisesta. Konttien eriyttäminen toisistaan voidaan saavuttaa esimerkiksi, kun kontteja suoritetaan ajonaikaisina prosesseina määriteltyjen nimiavaruuksien (namespaces) sisällä. Lisäkontrolleina voivat toimia esimerkiksi konttien ajamisen etuoikeuksilla rajaaminen minimiin ja varmistamalla, ettei oikeuksien korottamista sallita. Etuoikeuksin ajettavilla konteilla oikeudet periytyvät tavallisesti isäntäkoneelta, jolloin laajat oikeudet saattavat mahdollistaa pääsyn arkaluonteisiin tietoihin. Ne voivat lisäksi mahdollistaa sellaisten haitallisten API-kutsujen teon, jotka voivat päästää hyökkääjän liikkumaan klustereiden sisällä eli laajentamaan tunkeutumistaan (lateral movement).

- Virtualisoiduissa ympäristöissä konteilla ja muilla komponenteilla tulisi olla yksilölliset tunnisteet, mikä edesauttaa mahdollisen tunkeutumisen laajentamisen havaitsemista ja estämistä.[53] Lisäksi erilaisilla politiikoilla ja ryhmämäärityksillä voidaan rajoittaa sitä, mitä resursseja kontit näkevät ja kuinka paljon resursseja (CPU, muisti, tallennustila, verkko) niiden sallitaan käyttävän ja miten kontteihin on mahdollista liittää uusia hakemistoja. Myös konttien sisällä olevien prosessien suorittamista root-oikeuksilla on perusteltua rajoittaa. Parhaita käytäntöjä ja keinoja yleisimpien konttiteknologioiden kuten Kubernetesin ja Dockerin tietoturvakontrolleihin on löydettävissä esimerkiksi ohjelmistojen turvallisuuden parantamiseen keskittyvän Open Web Application Security Project (OWASP) järjestön turvallisuusoppaista.[54]

6.7 Fyysinen turvallisuus

Määräyksen kohdassa 6.2 asetetaan teleyritykselle velvoite laatia asianmukaiset toimintaperiaatteet ja menettelyt tietojärjestelmien, laitteiden, tietoaineistojen ja toimitilojen fyysisestä turvallisuudesta huolehtimiselle. Teleyrityksen tulee huolehtia myös

[53] NSA - Security Guidance for 5G Cloud Infrastructures - Part I: Prevent and Detect Lateral Movement, s. 8, https://www.cisa.gov/sites/default/files/publications/Security_Guidance_For_5G_Cloud_Infrastructures_Part_I_508_Compliant.pdf.
[54] OWASP Cheat Sheet Series, https://cheatsheetseries.owasp.org/.

laitteiden ympäristöolosuhteista. Teleyrityksen tulee siis huolehtia teletoiminnassa käytettyjen tietoaineistojen, laitteiden sekä laite- ja muiden tilojen asianmukaisesta suojaamisesta fyysisiä uhkia vastaan. Uhat, joita vastaan on suojauduttava, liittyvät erityisesti oikeudettomaan pääsyyn sekä ympäristötekijöihin, kuten tulipaloihin tai vesivahinkoihin.[55]

Liikenne- ja viestintäviraston määräyksessä viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista määrätään mm. laitetilojen fyysisestä suojaamisesta ja suojaamisten dokumentoinnista (määräyksen 17 kohta). Kyseinen määräys ei kuitenkaan ole kattava fyysistä turvallisuutta koskeva määräys, joten fyysiseen turvallisuuteen liittyvät näkökohdat katetaan tarpeellisilta osin myös tässä teletoiminnan tietoturvaa koskevassa määräyksessä. Määräyksen kohdan 6.2 mukainen velvoite koskeekin myös niitä tapauksia, joissa edellä mainittu määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista ei aseta erityisiä kulunvalvonta- tai muita vaatimuksia, ja kattaa laitetilojen lisäksi myös työskentelyyn tai tietoaineistojen säilytykseen käytetyt toimitilat.[56]

Toimintaperiaatteissa ja menettelyissä tulee tarvittaessa ottaa huomioon, kuinka tärkeä suojattava kohde on kyseessä, kuten onko kyseessä viestintäverkon kriittinen osa. Muita riskiarviossakin huomioon otettavia tekijöitä ovat esimerkiksi tilojen sijainti ja ympäristön turvallisuus. Toimintaperiaatteiden ja menettelyjen laatimisen osana käsiteltäväksi tulevat käytännössä ainakin pääsynhallinta, laitteiden ja laitetilojen rakenteellinen suojaaminen, varashälyttimet sekä ympäristöolosuhteiden valvonta ja vaikkapa sammutuslaitteistojen käyttö. Pääsy tulisi sallia vain rajatulle henkilöstölle, jonka luotettavuudesta ja tietoturvaosaamisesta on huolehdittu. Erityisesti kolmansien osapuolten henkilöstön pääsyä tulee vastaavasti rajoittaa ja erityisesti valvoa.[57]

7. Tietoturvallinen operointi ja muutoshallinta

Määräyksen kohdan 7 velvoitteilla pyritään saavuttamaan mm. jäljitettävyysketju laitteistoille ja ohjelmistoille. Ohjelmistoympäristöjen kompleksisuus tekee jäljitettävyydestä erityisen tärkeää. Jotta voidaan saada varmuutta ohjelmistoympäristöjen tietoturvalliseen operointiin, on tärkeää tietää, milloin muutoksia on tehty, mitä muutoksia on tehty ja kuka muutokset on tehnyt.

7.1 Viestintäverkon ja -palvelun tietoturvallinen käyttö

Teleyrityksellä tulee määräyksen kohdan 7.1.1 mukaisesti olla toimintaperiaatteet ja menettelyt viestintäverkon tai -palvelun komponenttien käytölle eli operoinnille.[58] Toimintamenettelyjen osalta vaatimus voidaan toteuttaa esimerkiksi dokumentoimalla vastuut verkko- ja tietojärjestelmien operoinnille ja täydentämällä tätä kuvaamalla myös ne keskeisimmät käytännöt, miten järjestelmien operointia ja hallinnointia tulee suorittaa. Käytäntöjä ja vastuita on syytä tarkastella säännöllisesti ja päivittää tarvittaessa erityisesti, jos ympäristöihin on tullut muutoksia tai jokin aiempi tapahtuma on osoittanut, että käytännöissä on puutteita tai aukkoja.

[55] Kohta perustuu ENISA GL:n mukaiseen tietoturvatavoitteeseen SO9, ja sen toteuttamisessa voidaan hyödyntää ENISA:n suosittelemia toimenpiteitä.
[56] Viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista annetun määräyksen 17.3 kohta velvoittaa suojaamaan viestintäverkon tai -palvelun komponentit fyysisesti siten, että asiaankuulumattomat eivät pääse niihin helposti käsiksi.
[57] 5G Toolbox: TM06, s. 25.
[58] ENISA GL SO15.

7.2 Muutostenhallinta

Teleyrityksellä tulee määräyksen kohdan 7.1.2 mukaisesti olla muutoksenhallintamenettelyt, joilla pienennetään muutoksista johtuvien tietoturvahäiriöiden todennäköisyyttä tai tarvittaessa palautetaan muutosta edeltänyt tai muu toimiva tila, millä tarkoitetaan palautusmenettelyjä (rollback procedure). Muutoksilla tarkoitetaan tässä yhteydessä kaikkia tietoturvan kannalta olennaisia muutoksia, jotka voivat kohdistua esimerkiksi ohjelmistoihin, laitteistoihin, konfiguraatioihin ja rajapintoihin. Muutoksenhallintamenettelyt voidaan suhteuttaa muutoksesta aiheutuviin tietoturvariskeihin, joihin vaikuttavat muutoksen laatu ja laajuus.

Muutoksenhallintamenettelyjen osalta vaatimus voidaan toteuttaa dokumentoimalla ennalta määritellyt menettelyt muutoksien toteuttamiselle.[59] Dokumentoinnin on syytä sisältää kuvaus muutostarpeista, ennakkotestauksesta, tuotantotestauksesta ja muutoksen tuotantoon viennistä sekä jokaisen vaiheen hyväksymismenettelyt. Muutoksenhallintamenettelyjen osana on perusteltua erityisesti huolehtia määräyksen kohdassa 6.1.2 ja 6.1.7 tarkoitetuista toimenpiteistä, joilla kovennetaan komponentit poistamalla tarpeettomat käyttöoikeudet ja palvelut käytöstä. Testausta koskee määräyksen kohta 8.1.

Myös menettelyt epäonnistuneen muutoksen peruuttamiseksi tai muutoksen keskeyttämiseksi palaamalla toimivaksi tiedettyyn versioon tai konfiguraatioon tulisi suunnitella. Muutoksenhallintamenettelyjen tulisi kattaa järjestelmien koko kehityskaari.[60]

Muutostenhallinnasta määrätään lisäksi Liikenne- ja viestintäviraston teletoiminnan häiriötilanteista antaman määräyksen 9 §:ssä. Kyseistä velvoitetta ei ole kuitenkaan kohdistettu nimenomaan tietoturvasta huolehtimiseen.

7.3 Omaisuuden sekä konfiguraatioiden hallinta

Teleyrityksellä tulee määräyksen 7.1.3 kohdan mukaisesti olla asianmukaiset toimintaperiaatteet ja menettelyt omaisuuden sekä komponenttien konfiguraatioiden hallitsemiseksi.[61]

Omaisuuden, kuten laitteiden ja ohjelmistojen hallinta tukee muun muassa haavoittuvuuksien hallintaa sekä riippuvuussuhteiden ja riskien ennakointia. Konfiguraatioiden hallinta on tärkeää, jotta oikeat asetukset voidaan tarvittaessa palauttaa ja havaita oikeudettomat muutokset. On myös hyvä huomata, että on tärkeää pitää toimintaperiaatteet ja menettelyt ajantasaisina muutosten ja tietoturvaa uhkaavien tapahtumien jälkeen.

Menettelyjen tulisi sisältää asianmukaiset toimenpiteet oikeudettomien tai tahattomien konfiguraatiomuutosten estämiseksi ja korjaamiseksi, mikäli konfiguraatio on virheellinen. Konfiguraationhallintaa voidaan toteuttaa esimerkiksi erityisten työkalujen avulla ja pitämällä muutoksista tapahtumalokia. Omaisuuden ja konfiguraatioiden hallinta liittyykin kiinteästi määräyksen kohdassa 7.1.2 tarkoitettuihin muutoksenhallintamenettelyihin. Ennen muutosten toteuttamista on hyvä määritellä menettelyt aikaisempaan versioon palauttamiseksi (ks. myös perustelumuistion luku 7.2), ja ohjelmistojen vanhat versiot on hyvä arkistoida varotoimenpiteenä yhdessä tarvittavien tietojen kanssa, joita ovat esimerkiksi konfiguraatioiden yksityiskohdat ja käytetyt parametrit.[62]

[59] ENISA GL SO16, 5G Security Control Matrix: M84.
[60] ISO/IEC 27002:2022: 8.32.
[61] ENISA GL SO17.
[62] ISO/IEC 27002:2022: 8.19.

Määräyksen vaatimus voidaan toteuttaa konfiguraatioiden osalta esimerkiksi konfiguraatiohallintatietokannalla (Configuration Management Database, CMDB), jolla hallinnoidaan tietoja teleyrityksen laitteisto- ja ohjelmisto-omaisuudesta. CMDB:n avulla on mahdollista pitää kirjaa verkon rakennetta kuvaavista kaavioista, komponenteista ja ohjelmistoversioista sekä hallita viestintäverkon ja -palvelun komponenttien keskinäisriippuvuuksia.[63]

Lisäksi teleyrityksen ohjelmistoympäristön monimuotoisuuden kasvaessa on suunnitelmallinen ja keskitetty ohjelmistohaavoittuvuuksien seuranta ja hallinta järkevää. Haavoittuvuuksien hallinnan voi toteuttaa esimerkiksi ennakoivan ja eri tietolähteisiin perustuvan viestintäverkon komponenttien ja haavoittuvuuksien luokitteluun perustuvan ohjelmisto-omaisuuden materiaaliluettelon (Software Bill of Materials, SBOM) avulla, jolloin haavoittuvuuksien tunnistaminen ja niihin reagointi helpottuu ja nopeutuu.[64]

On hyvä huomata, että Liikenne- ja viestintäviraston määräyksessä viestintäverkon kriittisistä osista asetetaan teleyrityksille velvollisuus tunnistaa viestintäverkon kriittiset osat ja niissä käytetyt viestintäverkon ja palvelun komponentit. Lisäksi Liikenne- ja viestintäviraston määräyksessä viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista määrätään velvollisuudesta dokumentoida tiedot kaikista viestintäverkkojen ja -palvelujen tärkeysluokitelluista komponenteista.

8. Testaaminen ja tietoturvallisuuden arvioinnit

Määräyksen kohdassa 8 määrätään testaamisesta ja tietoturvallisuuden arvioinneista.

8.1 Viestintäverkon ja -palvelun tietoturvallisuuden testaus sekä turvallisuusarviointien suorittaminen

Määräyksen kohta 8.1.1 edellyttää, että teleyrityksellä on asianmukaiset ja ajantasaiset toimintaperiaatteet ja menettelyt viestintäverkkojen ja -palvelujen komponenttien tietoturvallisuuden testaamiseksi sekä riskiarvion perusteella turvallisuusarviointien suorittamiseksi. Menettelyt ovat myös tärkeä osa muutoshallintaa (määräyksen kohta 7.2), ja ne voidaan suhteuttaa muutosten luonteeseen ja laajuuteen.

Testaus tarkoittaa ensisijaisesti tietoturvaan liittyvien toimintojen testaamista. Testauksen tulisi todentaa ainakin turvallisuustoimintojen oikeellisuus sekä ohjelmistokehityksen ja konfiguraatioiden turvallisuus.[65] Testaamisessa on perusteltua hyödyntää automaattisia testaustyökaluja, joskin tästä voi olla asianmukaista poiketa esimerkiksi vähäisen tai muutoin pienimuotoisen teletoiminnan kohdalla. Erityisten turvallisuusarviointien toteuttaminen tietoturvaskannausten ja esimerkiksi tunkeutumistestauksen avulla tulee kyseeseen, kun se on riskiarvion perusteella tarpeen.

Testaaminen ja turvallisuusarvioinnit ovat tärkeitä ennen uusien komponenttien ja ohjelmistojen ottamista käyttöön ja ennen ohjelmistomuutosten tekemistä, jotta häiriöt ja tietoturva-aukkojen syntyminen voidaan välttää.[66] Lisäksi testauksella ja turvallisuusarvioinneilla on perusteltua muutoksen jälkeen varmistua siitä, ettei muutoksesta ole aiheutunut haittaa tietoturvalle. Testausta ja turvallisuusarviointeja voi olla syytä to-

[63] ENISA GL SO17, 5G Security Control Matrix: M88
[64] Ks. NIST - Guide to Enterprise Patch Management Planning.SP.800-40r4, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf, SBOM at a Glance (ntia.gov), https://ntia.gov/sites/default/files/publications/sbom_at_a_glance_apr2021_0.pdf ja Kyberturvallisuuskeskus: Haavoittuvuudet hallintaan SBOMmin-varmasti, https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-hallintaan-sbommin-varmasti.
[65] ISO/IEC 27002:2022: 8.29.
[66] ENISA GL SO25–SO26.

teuttaa koko komponenttien elinkaaren ajan, jotta mahdolliset oikeudettomat tai tahattomat konfiguraatiomuutokset samoin kuin komponenteissa olevat haavoittuvuudet havaitaan. Näin saadaan tietoa verkon ja palvelujen tietoturvan tilasta.

Testaaminen ja turvallisuusarvioinnin tekeminen ennen uusien komponenttien käyttöönottoa sekä käytön aikana on tärkeää. Etukäteisarviointi voi sisältää muun muassa tarkistuksen siitä, miten komponentti on kovennettu, onko komponentissa tunnettuja tietoturvahaavoittuvuuksia ja onko komponentti päivitetty uusimpaan tarkoituksenmukaiseen ohjelmistoversioon. Käytön aikaista testausta ja turvallisuusarviointeja voidaan toteuttaa esimerkiksi skannaamalla verkossa olevia komponentteja sellaisten laitteiden ja ohjelmistoversioiden varalle, joissa on tunnettuja haavoittuvuuksia. Tämä edellyttää kolmansien osapuolten tuottamien haavoittuvuustietokantojen käyttöä ja niihin turvallisuusarvioinnin tulosten vertaamista. Esimerkiksi CVE (Common Vulnerabilites and Exposures) -tietokanta on tällainen vaihtoehto. Turvallisuusarvioinnin tulokset on järkevää dokumentoida, jotta voidaan ylläpitää tietoutta verkon tietoturvan tilasta. Tulosten olisi hyvä sisältää tiedot siitä, mitkä olivat arvioinnin kohteena olleet komponentit, mitä on arvioitu, kuka on arvioinut, arvioinnin tulokset sekä mahdolliset jatkotoimenpiteet.[67]

8.2 Tietoturvallisuuden arvioinnit

Määräyksen kohta 8.1.2 edellyttää, että teleyrityksellä on asianmukaiset toimintaperiaatteet ja menettelyt, joilla se seuraa tietoturvapolitiikkansa ja toimintaperiaatteidensa sekä toimintaansa kohdistuvien tietoturvavaatimusten toteutumista.[68]

Säännöllinen vaatimustenmukaisuuden katselmointi tukee toiminnan turvallisuutta ja kaikkien tietoturvan osa-alueiden toteutumista, kun teleyrityksen toimenpiteitä vaatimusten toteuttamiseksi tarkastellaan säännöllisesti teleyrityksen ennalta määrittelemällä tavoilla.

Arvioinneissa tulisi tarkastella vaatimustenmukaisuuden toteutumista suhteessa paitsi teleyrityksen itselleen määrittelemiin tietoturvapolitiikkaan, toimintaperiaatteisiin ja menettelyihin myös soveltuvien tietoturvaan liittyvien lakisääteisten velvoitteiden ja määräysten toteutumiseen. Lisäksi niissä voidaan tarkastella soveltuvien standardien noudattamista. Standardeilla tarkoitetaan tässä yhteydessä sellaisia standardeja, joiden noudattaminen on teleyritykselle pakollista tai joita se on sitoutunut noudattamaan osana tietoturvallisuuden ja tietoturvariskien hallinnan menettelyjään.

Tällainen tietoturvallisuuden arviointi voi tapahtua tapauksen mukaan itsearviointina toteutettavana katselmointina tai sitten sisäisten tai ulkoisten riippumattomien tietoturva-arviointien (auditointien) avulla. Toimintaperiaatteissa ja menettelyissä olisi tarpeen määritellä käytettävät arviointitavat eli miten vaatimustenmukaisuutta arvioidaan, arviointien tiheys, korjaavien toimenpiteiden kirjaaminen ja toteuttaminen sekä katselmoinnin tai auditointien kohdentaminen. Niissä voidaan määritellä myös se, toteutetaanko arvioinnit ennalta ehkäisevänä toimina vai mahdollisesti myös vakavien tietoturvapoikkeaman tai merkittävien muutosten jälkeen.

Vähintään viimeisimmän arvioinnin tulokset tulee määräyksen mukaisesti säilyttää.

[67] ENISA GL SO26.
[68] ENISA GL SO27 koskee lakisääteisten velvoitteiden ja standardien noudattamista. Ks. myös ISO/IEC 27002:2022: 5.36, joka koskee tietoturvapolitiikan, tietoturvallisuutta koskevien toimintaperiaatteiden, sääntöjen ja standardien noudattamista.

9. Uhkatiedon ylläpito

Määräyksen kohdassa 9 edellytetään, että teleyrityksellä on asianmukaiset menettelyt viestintäverkkojen ja -palvelujen tietoturvaan liittyvien uhkatietojen keräämiseksi ja uhkien arvioimiseksi. Tämän velvoitteen tarkoituksena on, että teleyritys ylläpitää jatkuvaa, ajantasaista uhkatietoa viestintäverkon ja -palvelun komponentteihin kohdistuvista uhista. Toimintaperiaatteet ja tarkemmat menettelyt tulee sisältää strategisen tason, taktisen tason ja operatiivisen tason tarkastelun. Ajantasainen, arvioitu uhkatieto toimii merkittävänä lähtötietona tietoturvariskien käsittelyssä.

Teleyrityksen on mahdollista ennaltaehkäisevästi lieventää tai poistaa tunnistettujen sisäisten ja ulkoisten uhkien vaikutuksia tietoturvariskeihin ylläpitämällä jatkuvaa tietoisuutta ajantasaisesta uhkatilanteesta.[69] Uhkaympäristön jatkuvasti muuttuessa on oleellista, että uhkatietoa hyödynnetään tietoturvariskien jatkuvassa arvioinnissa. Lisäksi uhkatiedon muuttuessa voidaan tunnistaa kokonaan uusia viestintäverkkojen ja -palvelujen komponentteihin kohdistuvia tietoturvariskejä.

Uhkatiedon keräämiseen tulisi sisällyttää soveltuvin osin ainakin ohjelmistojen ja laitteiden toimitusketjuihin kohdistuvat uhat, palvelunestohyökkäysten vaikutukset viestintäverkon tai -palvelun komponenttien toimintaan, kiristys- ja muiden haittaohjelmien vaikutukset, komponenttien haavoittuvuudet, BGP-reititykseen liittyvien uhkien seuranta ja työntekijöihin kohdistuvan manipuloinnin uhka.[70]

Ks. myös perustelumuistion liitteen luku 7.3 (Tiedottaminen haavoittuvasta asiakaslaitteesta).

Teleyrityksiä suositellaan myös välittämään tietoa palvelunestohyökkäyksistä Liikenne- ja viestintäviraston ilmoitusrajapintaan. Ilmoitusrajapinnan hyödyntämisen tarkoituksena on kerätä tietoa palvelunestohyökkäyksistä yleisen tietoturvatason kehittämiseksi. Tämän tiedon avulla Liikenne- ja viestintävirasto voi esimerkiksi auttaa teleyrityksiä reagoimaan nopeasti palvelunestohyökkäyksiin liittyviin uhkiin ja häiriötilanteisiin. Tiedonkeruu edistää myös pidemmän aikavälin tilannekuvan tuottamista.

10. Standardien noudattaminen

Uudet matkaviestiverkkojen sukupolvet laajentavat verkon palveluja yhteiskunnan eri osa-alueille tuoden ne yhä olennaisemmaksi osaksi yhteiskunnan toimintaa sekä muuta kriittistä infrastruktuuria. Viidennen sukupolven matkaviestinverkon uusi palveluperusteinen rajapinta-arkkitehtuuri antaa mahdollisuuden verkon toimintojen avaamiseen kolmansille osapuolille ja luo uusia toiminta- ja palvelumalleja. Lisäksi samaan aikaan on käytössä vanhempia verkkosukupolvia, joista erityisesti 4G-verkko on vielä pitkään käytössä yhdessä 5G-verkon kanssa. Samaan aikaan rajapintojen hallinnointi ja avaaminen kuitenkin lisäävät monimutkaisuutta ja uhkapinta-alaa. Tällöin on erityisen tärkeää, että kaikki verkkolaitteiden turvallisuustoiminnot huomioidaan ja niitä hyödynnetään niin täysimääräisesti, kuin se teleyrityksen toiminnassa on tarpeellista.

Määräyksen kohta 10.1 edellyttää, että matkaviestinverkon teleyrityksellä on käytössä tarkoituksenmukaiset menettelyt, joilla se varmistaa, että kaikki määräyksen liitteen 1

[69] ENISA GL SO28. Ks. myös ENISA 5G Matrix: M138–M144 ja SO29-001–SO29-003, ISO/IEC 27002:2022: 5.6, 5.7 ja 8.8), 3GPP TS 33.501, cl. 5.10.1 sekä ENISA Report: Cyber Threats Outreach in Telecom, Chapter 4, https://www.enisa.europa.eu/publications/cyber-threats-outreach-in-telecom.

[70] Ks. ENISA Threat Landscape for Supply Chain Attacks, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, ENISA Threat Landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 ja ENISA Threat Landscape for 5G Networks Report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

teknisten määritysten mukaisten 4G-, 5G- ja IMS-järjestelmien tarvittavat turvallisuustoiminnot toteutuvat.

Turvallisuustoimintojen toteutumisella tarkoitetaan paitsi sitä, että käytetyt viestintäverkon ja -palvelun komponentit tukevat näiden standardien mukaisia toimintoja, myös toimintojen käyttöönottoa teleyrityksen viestintäverkossa. Menettelyillä tulee huolehtia turvallisuustoimintojen pysyvyydestä myös ohjelmistopäivitysten yhteydessä ja uusien toimintojen toteuttamisesta.

3GPP laatii tekniset eritelmänsä ja standardinsa versioiksi (release), joiden käyttöönotto voi toisinaan kestää pitkään ja edetä vaiheittain verkossa. Uudemman version määrittämiä toimintoja voidaan joskus myös toteuttaa ja ottaa käyttöön myös osittain tilanteessa, jossa viestintäverkon tai -palvelun komponentti muilta osin vielä toteuttaa aiemman version. Tämän johdosta teknisten määritysten versioista on tarkasteltava aina sellaista 3GPP:n hyväksymää versiota, joka vastaa teleyrityksen verkossa toteuttamaa toiminnallisuuden versiota.

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 (määräyksen kohta 10.2). Standardin mukaisen turvallisuustoiminnon toteuttamatta jättämisen perusteena voi olla esimerkiksi jonkin vaihtoehtoisen turvallisuustoiminnon toteuttaminen, joka lieventää riittävällä tavalla tunnistettujen uhkien aiheuttamaa riskiä. Esimerkiksi turvallisuustoiminnon puuttuminen laitteesta, ohjelmistosta tai sen osasta, laitteen looginen tai fyysinen sijainti sekä verkon hallintaan tai havainnointiin liittyvä tarve voivat olla perusteena valinnaisen turvallisuustoiminnon toteuttamatta jättämiselle joko tilapäisesti tai tarvittaessa pysyväisluonteisesti riskiarvion edellyttämällä tavalla. Riskiarviossa on huomioitava sekä teleyritykseen että viestintäpalvelun käyttäjään kohdistuvat uhat.

Määräyksen kohdan 10.3 mukaisesti teleyrityksen on ylläpidettävä kuvaus siitä, millaisin menettelyin se varmistaa standardien turvallisuusvaatimusten toteuttamisen. Lisäksi vaatimuksena on, että kunkin turvallisuustoiminnon tai -mekanismin toteuttamatta jättäminen kohdan 10.2 mukaisella perusteella dokumentoidaan erikseen. Tämän vaatimuksen tarkoituksena on mahdollistaa velvoitteen valvonta ja se, että perusteet poikkeuksen soveltamiselle voidaan todentaa jälkikäteen.

Määräys ei edellytä teleyritystä esimerkiksi omin toimin testaamaan kaikkien toimintojen toteutuksen standardinmukaisuutta, vaan tarkoituksenmukaiset menettelyt voisivat sisältää esimerkiksi laitetoimittajalle asetettavat asiaa koskevat vaatimukset, joiden toteutumista seurataan asianmukaisin toimenpitein. Teleyritys voi mahdollisuuksien mukaan myös hyödyntää osana menettelyjä komponentille tehtyä EU:n kyberturvallisuusasetuksen mukaista tietoturvasertifiointia sen tullessa saataville,[71] tai komponentille tehtyä NESAS-skeeman[72] mukaista arviointia. Tämän lisäksi menettelyillä tulee huolehtia myös turvallisuustoimintojen asianmukaisesta käyttöönotosta ja ylläpidosta osana komponenttien konfiguraationhallintaa.

[71] ENISA Securing EU's Vision on 5G: Cybersecurity Certification, https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification.
[72] GSMA Network Equipment Security Assurance Scheme (NESAS), https://www.gsma.com/security/network-equipment-security-assurance-scheme/.

11. Tietoaineistot

Jotta teletoimintaan liittyvät tärkeät tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, teleyrityksessä on oltava käytössä teletoiminnan kannalta tärkeiden tietoaineistojen luokitusjärjestelmä, luokituskriteerit ja luokitukseen liittyvä käsittelymenettely.

Tietoaineistojen luokitteluun ja käsittelyyn liittyy myös olennaisesti käyttäjien pääsynhallinta tietoaineistojen luokitusten mukaisesti.

Käyttäjien pääsynhallintaa käsitellään määräyksen kohdassa 6.1.1.

Teleyrityksen on määriteltävä omaan toimintaansa soveltuva tietoaineistojen luokittelukriteeristö. Aineistot voi esimerkiksi luokitella seuraavasti: julkinen, luottamuksellinen, salainen.

Lisäksi teleyrityksen on määriteltävä, miten se käsittelee (suojaa) eri luokkiin luokiteltuja aineistoja.

Luokitus ja siihen liittyvät käsittelymenettelyt on dokumentoitava (ks. määräyksen kohta 3.2). Luokituksen määrittelyssä ja sen dokumentoinnissa huomioitavia tekijöitä ovat esimerkiksi seuraavat asiat:

- yleiset periaatteet tietoaineiston turvaluokan ja luottamuksellisuuden arvioimiseksi ja tietoaineistojen salassa pysymiseksi
- käsittely- ja muutosoikeudet tietoaineiston lukuoikeuksien jakamisesta, muutosoikeuksista sekä näiden oikeuksien jakamisesta
- luottamuksellisuusluokan määrittäminen
- tiedon tai asiakirjan julkisuus: esimerkiksi asiasta puhuminen julkisesti
- asiakirjan ominaisuudet: paperi, leima ja muut merkinnät
- säilytys ja salaaminen
- tulostaminen ja kopiointi
- varmuuskopiointi
- vastaanottaminen, jakaminen, lähettäminen ja kuljettaminen
- tietojen ja asiakirjan käsittelyn dokumentoiminen
- asiakirjan arkistointi, käsittely tai käsittelyoikeuksien päättyminen, tietojen ja asiakirjan tuhoaminen.

12. Asiakkaan tunnistaminen tietoturvasta huolehtimiseksi

Määräyksen kohdassa 12 edellytetään, että teleyrityksellä on toimintaperiaatteet ja menettelyt tilaajan tai käyttäjän tunnistamiseksi riittävän luotettavalla tavalla ennen kuin asiakkaan palveluun tehdään olennaisia viestintäpalvelun tietoturvaan vaikuttavia muutoksia tai tilaajalle tai käyttäjälle annetaan luottamuksellisia tietoja. Tunnistamiseen käytettävä menettely voidaan suhteuttaa asioinnin riskitasoon palveluun tehtävien muutosten tai annettavien luottamuksellisten tietojen näkökulmasta. Riskitasoa arvioitaessa on asiakastapahtuman arvioinnin lisäksi huomioitava tilaajan tai käyttäjän erityispiirteet, kuten esimerkiksi mahdolliset tietojenluovutuskiellot. Toimintaperiaatteissa ja menettelyissä voitaisiin esimerkiksi määritellä riittävät tunnistusmenettelyt riskiperusteisesti erilaisten palvelumuutosten ja asiakastietojen kohdalla.

Laadittujen toimintaperiaatteiden ja menettelyjen on syytä sisältyä asiakaspalveluun osallistuvan henkilöstön koulutusohjelmaan. Määräyksen 5 kohdassa asetetaan teleyrityksille velvollisuus huolehtia henkilöstön tietoturvaosaamisesta ja järjestää säännöllistä tietoturvakoulutusta, ja henkilöstön tietoturvaosaamiseen ja sen kehittämiseen liittyviä vaatimuksia käsitellään kohdassa 5.2.

Sähköisessä asioinnissa luotettavana tapana tilaajan tai käyttäjän tunnistamiseksi voidaan pitää esimerkiksi sähköisistä tunnistus- ja luottamuspalveluista annetun lain (617/2009) mukaisen vahvan sähköisen tunnistuksen käyttöä. Vaihtoehtoinen luotettava tapa käyttäjän ja tilaajan tunnistamiseksi voi olla riskitaso huomioiden kaksivaiheisen tunnistamisen hyödyntäminen esimerkiksi mobiilisovelluksella. *Käyntiasioinnissa* luotettavana tapana voidaan pitää esimerkiksi tilaajan tai käyttäjän henkilöllisyysasiakirjan tarkastamista. Luotettavia henkilöllisyysasiakirjoja ovat esimerkiksi suomalainen passi, henkilökortti tai ajokortti sekä niihin luotettavuudeltaan rinnastuvat ulkomaiset asiakirjat, kuten toisen Euroopan talousalueen valtion myöntämä passi tai henkilökortti. Asiakirjaa ei tule hyväksyä, ellei teleyritys saa riittävää varmuutta, että asiakirja todella kuuluu sen esittävälle henkilölle, tai jos asiakirjaa on syytä epäillä väärennetyksi.[73] Myös *puhelinasioinnissa* asiakas on tunnistettava riittävän luotettavalla tavalla. Riskiarvion perusteella puhelinasioinnissa voi olla mahdollista tunnistaa asiakas riittävän luotettavasti esimerkiksi sellaisen kysymyslistan avulla, johon annettavat vastaukset eivät ole ulkopuolisten tiedossa. Lisäksi puhelinasioinnissa voidaan mahdollisuuksien mukaan hyödyntää vahvaa sähköistä tunnistusta tai mobiilisovellusta.

Olennaisiksi palveluun tehtäviksi, viestintäpalvelun tietoturvaan vaikuttaviksi muutoksiksi voidaan katsoa ainakin liittymän SIM-kortin vaihtaminen, liittymän uudelleen avaus (PUK-koodin luovuttaminen), eSIM:n lataaminen tai aktivointi sekä liittymän sulkeminen.[74] Olennaisia muutoksia ovat myös sähköpostitilin unohtuneen salasanan vaihtaminen tai lukkiutuneen käyttäjätilin avaaminen. Luottamuksellisiksi tiedoiksi katsotaan muun muassa tilaajaan tai käyttäjään liittyvät välitystiedot, kuten yksityiskohtaiseen laskuerittelyyn sisältyvät tiedot, tai sähköposti- tai pikaviestipalveluun tallentuneet tiedot. Teleyrityksen ei tule tehdä olennaisia palvelumuutoksia eikä antaa luottamuksellista tietoa, mikäli palvelun tilaajaa tai käyttäjää ei ole tunnistettu riittävä tasolla.

13. IP-osoitteiden dokumentointi

Määräyksen kohdassa 13 edellytetään, että teleyritys dokumentoi sille osoitettujen ja sen mainostamien IP-osoitteiden käytön huolellisesti kirjaamalla IP-osoitteet luovuttaneen tai muun asianmukaisen internetosoiterekisterin (IR) tietokantaan. Tämä on tärkeää, koska teleyritykset voivat käyttää näitä tietoja esimerkiksi automaattisten reittisuodatuslistojen (prefix list) luomiseen. Reittisuodatuslistoilla huolehditaan siitä, että reittejä mainostava teleyritys mainostaa vain hallinnoimiaan osoiteavaruuksia. Asianmukaisesti dokumentoidut IP-verkkoresurssit helpottavat myös merkittävästi reititystietojen ylläpitoa ja häiriötilanteiden sekä tietoturvaloukkaustilanteiden selvittelyä.

Teleyrityksen tulee ilmoittaa hallinnoimansa verkot tarkoituksenmukaisen internetosoiterekisterin (IR) WHOIS-tietokantaan. Hallinnoitavilla verkoilla tarkoitetaan määräyksen yhteydessä teleyrityksen omistamia tai sen asiakkaille toimittamia verkkoalueita. Tiedot kirjataan ja niitä ylläpidetään rekisterinpitäjän ohjeiden mukaan. Kirjattavia tietoja ovat muun muassa IP-osoiteavaruus, teleyrityksen yhteystiedot, ylläpitäjän yhteystiedot, abuse- ja irt-kontaktitiedot sekä verkon AS-numero, josta kyseiset IP-osoitteet löytyvät. Euroopassa toimivalla alueellisella internetosoiterekisterillä RIPE NCC:llä on käytössä oma tietokenttä abuse-kontaktitietojen rekisteröintiin.

Teleyrityksen on huolehdittava erityisesti omassa käytössään olevien IP-verkkojen dokumentoinnin ajantasaisuudesta. Jos teleyritys on reittimainostuksen lähteenä muiden organisaatioiden hallussa oleville PI (Provider Independent) -verkkoavaruuksille, on näiden osoiteavaruuksien tietojen asianmukaisuus tarkistettava reittimainostuksen aktivoinnin yhteydessä. Samoin, jos teleyritys ylläpitää alueellista verkkorekisteripalvelua

[73] Muun kuin Suomen viranomaisen myöntämän asiakirjan hyväksymisestä ks. KHO 2017:19, https://www.kho.fi/fi/index/paatoksia/vuosikirjapaatokset/vuosikirjapaatos/1486031131275.html.
[74] Ks. SIM-kortinvaihtopetosten torjumiseen liittyvistä menettelyistä SIM-ENISA Countering SIM-Swapping, s. 17–20, https://www.enisa.europa.eu/publications/countering-sim-swapping.

(LIR) ja luovuttaa PI-osoiteavaruutta kolmannelle osapuolelle, on osoitetietojen oikeellisuus tarkistettava verkko-osoiteavaruutta rekisteröitäessä.

Käytännössä dokumentointivaatimus tarkoittaa myös sitä, että jollei nimenomaisesti ole toisin sovittu, teleyritys ei saa mainostaa dokumentoimattomia IP-osoiteavaruuksia muille teleyrityksille.

14. Hallintaverkon ja hallintayhteyksien liikenne

Teleyrityksellä tulee olla asianmukaiset verkonhallintaa ja hallintayhteyksiä koskevat toimintaperiaatteet ja menettelyt, joilla varmistetaan riskiarvion mukaisen varmuustason toteutuminen tietoturvauhkien minimoimiseksi (määräyksen kohta 14.1). Määräyksessä edellytetään, että teleyritys suojaa viestintäverkon tai -palvelun komponenttien niin sanotun hallintaliikenteen (määräyksen kohta 14.2). Hallintaliikenne on liikennettä, jolla teleyritys valvoo ja hallinnoi verkkolaitteitaan. Hallintaliikenteen suojaamisvaatimuksella pyritään varmistamaan se, että viestintäverkon tai -palvelun komponentteihin ei pääse oikeudettomasti tekemään muutoksia.

Toimintaperiaatteiden tulee sisältää vähintään hallintaliikenteen suojaamiseen liittyvät vaatimukset, verkonhallintaan käytettäviä päätelaitteita koskevat kovennusvaatimukset sekä pääsynhallinnan periaatteet viestintäverkon ja -palvelujen komponenttien keskeisyyden mukaan.

Hallintaliikenteen suojaaminen voidaan toteuttaa käytännössä liikenteen fyysisellä erottamisella omiin johtoihinsa tai erottamalla liikenne loogisesti esimerkiksi salauksen avulla. Hallintaliikenteen salaaminen käyttötilanteeseen soveltuvalla menetelmällä tulee tarpeeseen varsinkin, jos ei muutoin voida varmistua siitä, että liikenteen seuraaminen tai kaappaaminen on estetty. Salaamaton hallintaliikenne voi paljastaa tietoja tai ominaisuuksia viestintäverkon tai -palvelun komponenteista.

Lisäksi teleyrityksellä on oltava käytössä asianmukaiset menettelyt, joilla arvioidaan verkonhallintaan käytettävistä päätelaitteesta aiheutuvat tietoturvauhat ja hallitaan niistä johtuvat riskit (määräyksen kohta 14.3). Viestintäverkon ja -palvelujen komponenttien hallintaan käytettävien päätelaitteiden suojaamiseen on kiinnitettävä erityistä huomiota, sillä jos samalla päätelaitteella voidaan käyttää esimerkiksi sähköpostia ja internetin palveluita, kohdistuu myös hallintaverkkoon näiden palvelujen kautta tietoturvauhkia.

Joissakin tilanteissa voidaan käyttää dedikoitua, kovennettua työasemaa, jolloin päätelaitteesta poistetaan mahdollisuus käyttää muita kuin verkonhallinnan kannalta välttämättömiä toimintoja. Riskien hallinnassa voidaan käyttää kokonaisarvion perusteella myös muita menettelyjä, joissa päätelaitteesta aiheutuvat riskit on muilla keinoin hallittu. Määräyksen lähtökohtana on, että verkonhallintaan käytettäviä päätelaitteita ei tule kytkeä suoraan hallintaverkon järjestelmiin, vaan hallintaverkon käyttö olisi toteutettava esimerkiksi virtuaalisesti terminoituna, tarkasti valvotun hyppykoneen välityksellä, tai etätyöpöytään perustuvan ratkaisun avulla. Pelkkää kaksivaiheista tunnistamista, virustorjuntaa tai VPN-yhteyttä ei tulisi pitää riittävänä. Välttämättömien tiedostojen siirrossa koneelta toiselle on myös huomioitava haittaohjelmien riski mm. pitämällä huolta siitä, että käytetään vain luotettavia lähteitä ja varmistetaan tietoturvallisuus (eheys) kaikilla tarpeellisilla menetelmillä.

Hallintaverkon yhteyksien pääsynhallinnassa tulee poikkeuksetta soveltaa vähimpien käyttöoikeuksien periaatetta, ja käyttäjien tunnistaminen tulee tehdä vähintään kahta todentamistekijää hyödyntäen. Todentamistekijän toimittamista tekstiviestin välityksellä ei tulisi pitää ensisijaisena keinona. Lisäksi tulee toteuttaa ja dokumentoida sovel-

tuvat menettelyt, joilla lievennetään hallintayhteyden tietoturvallisuuden varmistamiseen liittyviä jäännösriskejä. Menettelyt voivat sisältää esimerkiksi yhteyksien rajaamisen vain tiettyihin IP-osoitteisiin, hallintayhteystapahtumien sallimisen tarveperusteisesti, tapahtumien keston rajoittamisen, reaaliaikaisen valvonnan ja hallintayhteystapahtumien lokituksen.

Käyttäjien pääsynhallintaan liittyviä vaatimuksia käsitellään myös määräyksen kohdassa 6.1.

Suositus

Liikenne- ja viestintävirasto suosittelee, että teleyritys ylläpitää lokia viimeiseltä puolelta vuodelta verkkolaitteidensa asetuksiin tehdyistä muutoksista mahdollisten verkkolaitteiden oikeudettomien asetusmuutosten havaitsemiseksi ja jäljittämiseksi. Virasto myös suosittelee, että lokitettavaa tapahtumaa ja havaintoa ilmaisevissa ajankohtamerkinnöissä ilmoitetaan erikseen tapahtuman ja havainnon ajankohta. Havainnon ajankohta suositellaan lokitettavan vähintään päivämäärän tarkkuudella ja tapahtumaa ilmaiseviin järjestelmälokeihin suositellaan tallennettavan myös tarkka kellonaika, sovellettava aikavyöhyke (esimerkiksi: UTC+2) sekä mahdollisen kellovirheen suuruus ja suunta verrattuna viralliseen aikaan. Teknisten järjestelmälokien aikaleimat on suositeltavinta ilmaista ISO 8601 -yhteensopivassa formaatissa.[75]

Luku 3 Viestintäverkkojen ja -palvelujen rajapintojen erityiset vaatimukset

Tässä luvussa käsitellään määräyksen luvussa 3 asetettuja yhteenliittämis-, sovellus- ja asiakasrajapintojen tietoturvaa koskevia vaatimuksia.

15. Rajapintojen häiriöiden estäminen ja niiltä suojautuminen

15.1 Häiriöiden estäminen

Teleyrityksen verkko tai palvelu ei saa aiheuttaa häiriöitä muille viestintäverkoille tai -palveluille. Määräyksen kohdassa 15.1 asetettu velvoite kieltää toki myös tahallisen häirinnän, mutta vaatimus on silti ensisijaisesti tarkoitettu estämään tahattomien, esimerkiksi konfiguraatiovirheestä aiheutuvien häiriöiden leviäminen verkosta toiseen. Yhteenliittämisrajapinnan yli leviävät häiriöt voivat aiheuttaa verkkoon silmukoita, ohjata liikennettä väärin tai vain ruuhkauttaa jonkin verkon osan tai palvelun ylimääräisellä liikenteellä. Pahimmillaan palvelu voi kokonaan estyä.

Koska näiden häiriöiden vaikutukset voivat olla merkittäviä, teleyrityksille on katsottu tarpeelliseksi antaa velvoite estää omaa viestintäverkkoaan tai -palveluaan häiritsemästä muiden viestintäverkkojen palveluja. Näin siitä huolimatta, että teleyrityksille on annettu määräyksen kohdassa 15.2 myös velvoite suojautua näiltä häiriöiltä.

Vaatimusta ei ole kohdennettu mihinkään tiettyyn tekniikkaan tai protokollatasoon, vaan teleyrityksen tulee arvioida eri yhteenliittämisrajapinnassa käytettävien tekniikoiden ja palvelujen asettamia uhkia ja toteuttaa tämän jälkeen kaikki häiriöiden leviämisen estämisen kannalta tarpeelliset suojausmekanismit.

Tarpeellisena suojausmekanismina voidaan pitää esimerkiksi mekanismeja, joilla estetään silmukoiden muodostuminen yhteenliittämisrajapinnoissa. Esimerkiksi piirikytkentäisissä puhelinpalveluissa puhelun saa siirtää vain 5 kertaa, jonka jälkeen puhelu pu-

[75] Vastaavan sisältöinen suositus on annettu teletoiminnan häiriötilanteista annetun määräyksen 66 A/2019 M perustelumuistion k. 9.2.

retaan. Internetyhteyspalvelun yhteenliittämisessä tällä tarkoitetaan taas sitä, että teleyritys ei lähetä yhteenliittämisrajapinnassa saman loogisen rajapinnan yli liikennettä, jonka se on vastaanottanut ko. rajapinnan yli.

Vaikka määräystä sovelletaan muutoin vain yleiseen teletoimintaan, on hyvä huomata määräyksen soveltamisalassa säädetysti se, että määräyksen kohdan 15.1 mukainen velvoite häiriöiden estämisestä koskee myös viranomaisverkkoja ja viranomaisviestintään liittyvää viestintäpalvelua siltä osin, kun ne on yhteenliitetty yleiseen viestintäverkkoon tai yleisesti saatavilla olevaan viestintäpalveluun eli teleyrityksen verkkoon tai palveluun. Viranomaisverkkoa tai viranomaisviestintään liittyvää viestintäpalvelua tarjoavaa ja ylläpitävää tahoa koskee näin ollen velvoite huolehtia, että sen viestintäverkon tai -palvelun komponentit eivät aiheuta häiriöitä yleisille viestintäverkoille. Tällaisella taholla on oltava tarkoituksenmukaiset mekanismit kyseisten häiriöiden estämiseksi.

Tämän perustelumuistion liitteen luvussa 6 annetaan Ethernet-rajapintojen tietoturvaa koskevia suosituksia.

15.2 Häiriöiltä suojautuminen

Määräyksen kohdan 15.2 mukaan teleyrityksen on suojattava oma viestintäverkkonsa ja -palvelunsa yhteenliittämis-, sovellus- ja asiakasrajapinnoista tulevalta haitalliselta liikenteeltä toteuttamalla verkossaan tarvittavat suojausmekanismit.

Verrattuna viestintäverkkojen väliseen yhteenliittämisrajapintaan asiakasrajapinnan uhat ovat vielä moninaisemmat. Esimerkiksi internetyhteyspalvelun osalta teleyrityksen tulee varmistua muun muassa siitä, että asiakas ei pääse salakuuntelemaan muiden asiakkaiden liikennettä tai aiheuttamaan näihin kohdistuvia palvelunestohyökkäyksiä. Uhkien laatu, vakavuus ja tarvittavat suojaustoimenpiteet vaihtelevat tarjotusta palvelusta ja käytetystä tekniikasta riippuen.

Velvoitteessa mainittu haitallien liikenne merkitsee tässä tapauksessa pääasiassa teleyrityksen oman viestintäverkon tai -palvelun toiminnan kannalta haitallista liikennettä, joka voi pahimmassa tapauksessa vaarantaa teleyrityksen viestintäverkon tai -palvelun toiminnan.

Vaatimusta ei ole kohdennettu mihinkään tiettyyn tekniikkaan tai protokollatasoon, vaan teleyrityksen tulee arvioida eri rajapinnoissa käytettävien tekniikoiden ja palvelujen asettamia uhkia ja toteuttaa tämän jälkeen kaikki oman viestintäverkkonsa ja -palvelunsa suojaamisen kannalta tarpeelliset mekanismit. Tällaisia mekanismeja voivat olla esimerkiksi lähde- tai kohdeosoitteeseen, käytettyyn protokollaan, viestin sisältöön tai viestien määrään perustuvat suodattamistoimet.

Edellä mainitut suojausmekanismit voidaan toteuttaa myös kontrollitasolla, joten viestejä ei ole välttämätöntä suodattaa. Ainakin tiettyjä uhkia vastaan teleyrityksen verkon suojaamiseksi voi siten riittää, että teleyritys suojaa vain ko. liikennettä käsittelevien laitteiden kontrollitason ja välittää liikenteen normaaliin tapaan verkkonsa läpi. Mikäli teleyritys toteuttaa suojauksen kontrollitasolla liikenteen suodattamisen sijaan, sen on luonnollisesti toteutettava tarvittavat mekanismit kaikissa tarpeellisissa verkkoelementeissä.

Alla on esitetty muutamia esimerkkejä uhista ja niiden kannalta tarpeellisista suojausmekanismeista. On huomattava, että esimerkit eivät ole poissulkevia ja teleyrityksen on arvioitava tarvittavat toimenpiteet itse:

- Bitstream-asiakasrajapinta: Verkko-operaattorin on esimerkiksi syytä suodattaa asiakasrajapinnassa olevassa Ethernet-DSLAM:ssa (Digital Subscriber Line Access Multiplexer) tai tämän perässä olevassa reunakytkimessä asiakasporttiin tulevat

ja siitä lähtevät BPDU-viestit (Bridge Protocol Data Units) ja valmistajakohtaiset L2-tason ohjausprotokollaviestit.
- VoIP-asiakas- ja yhteenliittämisrajapinnat: Ongelmaa on käsitelty tarkemmin esimerkiksi RFC:issä 5390[76] ja 6404[77]. Mahdollisesti tarpeellisina suojaustoimenpiteinä voidaan pitää esimerkiksi lähdeosoitteisiin tai puheluyritysmääriin perustuvia rajoituksia. Edellä mainitut mekanismit on mahdollista toteuttaa esimerkiksi SBC:llä[78].

16. Tarpeettomien porttien, palvelujen ja protokollien sulkeminen

Viestintäpalvelujen ja teleyrityksen järjestelmien toiminnan kannalta tarpeettomien palvelujen ja protokollien poiskytkeminen viestintäverkon tai -palvelun komponenteista on oleellista, sillä tällöin viestintäverkon tai -palvelun komponentissa on ajossa vähemmän ohjelmistoja, joiden haavoittuvuuksia mahdollinen hyökkääjä voisi käyttää hyödyksi. Lisäksi esimerkiksi tarpeettomien reititysprotokollien tai muun ohjausliikenteen suodattaminen hallintarajapinnoissa vähentää mahdollisuutta, että rajapinnan yli tuleva liikenne pääsisi sekoittamaan teleyrityksen verkon toimintaa.

Vaatimusta sovelletaan sekä yhteenliittämis- että asiakasrajapinnoissa oleviin viestintäverkon tai -palvelun komponentteihin (eli ei asiakaspäätelaitteisiin, joita ovat esimerkiksi asiakkaan omistamat ja hallinnoimat modeemit, kytkimet, tietokoneet tms.). Vaatimusta ei ole kohdennettu mihinkään tiettyyn tekniikkaan tai protokollatasoon, vaan teleyrityksen tulee arvioida laitekohtaisesti ja mahdollisesti myös porttikohtaisesti tarpeettomat fyysiset portit, tietoliikenneportit (esim. TCP- ja UDP-protokollien portit) tai palvelut ja kytkeä ne pois päältä. Velvoite ei sen sijaan koske internetyhteyspalvelun asiakasliittymän liikenteessä käytettävissä olevia tietoliikenneportteja yleisesti.

Osassa laitteista asia on voitu huomioida jo oletusasetuksissa tai laitevalmistaja voi tarjota komentoja, joilla monet tällaiset palvelut saadaan kytkettyä pois päältä kerralla. Teleyrityksen on selvitettävä, miten kunkin laitteen kanssa on syytä toimia, sillä oletusarvoisesti tarpeettomien palvelujen ja protokollien ei voida olettaa olevan kunnossa.

Alla on esitetty muutamia esimerkkejä velvoitteen toteuttamisesta eri verkkoelementeissä. On huomattava, että esimerkit eivät ole poissulkevia ja teleyrityksen on arvioitava tarvittavat toimenpiteet itse:

- Bitstream-asiakasrajapinta (PE-reititin): Tällä tarkoitetaan esimerkiksi sitä, että asiakasrajapinnassa olevassa PE-reitittimen asiakasporteissa ei ole päällä esimerkiksi FTP-, HTTP-, NTP-, finger- tai bootp-palveluita. Vastaavasti kontrollitasolla ei tule käsitellä esimerkiksi asiakasporteista tulevia reititysprotokolla- tai proxy ARP-viestejä. Liikenne voidaan kuitenkin välittää verkon läpi.
- Sähköpostin lähetyspalvelin (MSA): Sähköpostin lähetyspalvelin on asiakasrajapinnassa oleva laite tai virtuaalipalvelin, jonka kautta lähtevät sähköpostit lähetetään eteenpäin. Tällainen palvelin ei käsittele reititys- tai muita verkkotason ohjausprotokollia. Haavoittuvuusuhkien pienentämiseksi tällaisessa verkkoelementissä ei kuitenkaan saa pitää päällä tarpeettomia palveluita, joita voivat MSA:n tapauksessa mahdollisesti olla esimerkiksi FTP- tai HTTP-palvelimet.

[76] IETF RFC 5390, Requirements for Management of Overload in the Session Initiation Protocol, https://tools.ietf.org/html/rfc5390.
[77] IETF RFC 6404, Session PEERing for Multimedia INTerconnect (SPEERMINT) Security Threats and Suggested Countermeasures, https://tools.ietf.org/html/rfc6404.
[78] IETF RFC 5853, Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments, https://tools.ietf.org/html/rfc5853.

17. IP-yhteenliittämisrajapintojen suojaaminen ja liikenteen suodattaminen

Reititysprotokollan tietoturvallisuus

Internetin runkoverkon keskeisestä reititysprotokollasta BGP:stä (Border Gateway Protocol) puuttuu oletuksena sisäänrakennettu turvallisuus, mikä altistaa sen konfiguraatiovirheille ja hyökkäyksille. BGP on yhteenliittämisprotokolla, jonka avulla organisaatiot voivat liittää oman verkkonsa muuhun internetiin lähettääkseen liikennettä oikeaan määränpäähän ja toisaalta vastaanottaakseen liikennettä, joka on tarkoitettu organisaation omissa IP-osoitteissa oleviin kohteisiin.

Edellä mainitusta syystä johtuen Liikenne- ja viestintävirasto on katsonut tarpeelliseksi asettaa velvoitteita reitityksen tietoturvan parantamiseksi. Määräyksessä asetetut velvoitteet perustuvat pääosin ENISA:n suosituksiin BGP-reititysprotokollan suojaamiseksi.[79]

Internetiin kytkeytyneiden toimijoiden verkkokokonaisuuksia kutsutaan autonomisiksi järjestelmiksi (Autonomous System, AS). Jokaisella autonomisella järjestelmällä on oma yksilöllinen numerotunnus (ASN), jolla kyseinen AS tunnetaan internetissä. Internetin numerotunnukset jakavat Internet Assigned Numbers Authority IANA ja sen alaisuudessa toimivat alueelliset internetrekisterinpitäjäorganisaatiot (Regional Internet Registry, RIR). Jokainen autonominen järjestelmä hallitsee yhtä tai useampaa tiettyä IP-osoiteryhmää ja on yhteydessä useisiin muihin AS-järjestelmiin, joille se ilmoittaa BGP-protokollan avulla hallinnoimistaan osoitesarjoista. Tätä tietoa käytetään ohjaamaan datapaketeista muodostuva verkkoliikenne oikeaan kohteeseen eli siis sille toimijalle, joka hallitsee kohteena olevia osoitteita.

BGP-protokolla on suunniteltu yli 25 vuotta sitten, jolloin sen toimintaperiaatteeksi muodostui yksinkertaisuus, käyttöönoton helppous sekä toimintavarmuus ja joustavuus, mikä on vaikuttanut siihen, että protokolla on käytössä vielä tänä päivänäkin. Internetin rooli ja koko oli tuolloin huomattavasti nykyistä pienempi ja reittejä vaihtoi keskenään vain pieni joukko toimijoita, jotka tunsivat toisensa ja heidän välillään vallitsi luottamus, jolloin turvallisuusnäkökulmia ei katsottu tarpeelliseksi painottaa. BGP perustuu ennen kaikkea siis luottamukseen vastaanotetun tiedon oikeellisuudesta. Reitittävät solmut eli reititinlaitteet julkaisevat tietoa tiedonsiirtopoluista eli reiteistä muille reitittimille ja muut reitittimet luottavat saatuun tietoon ja levittävät sitä edelleen ilman tarkistuksia. Toimijoiden määrä on internetin käytön yleistyessä ja palvelujen siirtyessä verkkoon kasvanut räjähdysmäisesti, jonka johdosta konfiguraatiovirheet ja inhimilliset erehdykset mahdollistavat laajojenkin häiriötilanteiden synnyn. Reittejä keskenään vaihtavien keskuudessa voi olla myös pahantahtoisia tahoja, jotka haluavat väärentää reittitietoa omiin käyttötarkoituksiinsa, kuten varastaakseen liikennettä ja sen sisältämää tietoa, pyrkiäkseen aiheuttamaan katkoja määrättyihin palveluihin tai ohjatakseen liikennettä väärään paikkaan huijaustarkoituksissa.[80]

Reittikaappaukset ovat yksi yleisimmistä BGP:n turvallisuuteen liittyvistä ongelmista. Reittikaappauksessa yksi reitittävä solmu alkaa mainostaa väärää tietoa reiteistä siihen suoraan kytkeytyneille naapurisolmuille tai vaihtoehtoisesti mainostaa omistavansa joitakin IP-osoitteita, jotka tosiasiassa kuuluvat jollekin toiselle taholle. BGP ei itsessään sisällä tarkistusmenettelyä mainostuksille, joten tällainen virheellinen tieto voi hyvinkin lyhyessä ajassa ehtiä levitä suureen osaan internetiä, jolloin liikenne ohjautuu väärin ja palveluihin pääsy ja niiden käyttö saattavat estyä.

[79] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP), https://www.enisa.europa.eu/publications/7-steps-to-shore-up-bgp.
[80] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP).

BGP:hen kohdistuu myös muita tietoturvauhkia reittikaappausten lisäksi. BGP-istuntojen muodostamiseen kahden tahon välillä käytetään TCP/IP-protokollaa. Hyökkääjä voi pyrkiä esimerkiksi muuttamaan aitoa BGP-vertaisviestintää syöttämällä väärennettyjä BGP-viestejä BGP-kumppanien väliseen viestintään tarkoituksenaan katkaista tai muuttaa yhteyttä internetliikenteen häiritsemiseksi, sieppaamiseksi tai uudelleenkirjoittamiseksi.

Väärät lähde-IP-osoitteet

Teleyrityksen verkkoon ja sen tilaajille suuntautuvissa IP-paketeissa voi olla virheellisesti määritelty lähdeosoite joko erehdyksessä tai tahallisesti väärennettynä. Teleyrityksen omia eli sen itsensä hallinnoimia tai yksityiseen eli ei-julkiseen/ei-reitittyvään IP-osoiteavaruuteen kuuluvia osoitteita lähdeosoitteina käyttävien IP-pakettien vastaanottaminen toiselta teleyritykseltä ilman erillistä sopimusta ei ole normaalitilanne ja sisältää merkittävän tietoturvariskin. Edellä mainittujen lisäksi on olemassa myös muita osoitteita, joiden ei tulisi koskaan esiintyä internetreitityksessä. Näitä ovat esimerkiksi verkkoalueet, joita alueelliset internetrekisterit (RIR) eivät vielä ole jakaneet käyttöön, sekä erityiskäyttöön tarkoitetut verkkoalueet.

Lähde-IP-osoitteen väärentämistä (IP spoofing) käytetään myös usein palvelunestohyökkäyksissä. Hyökkäys tapahtuu siten, että hyökkääjä väärentää oman verkko-osoitteensa niin, että hyökkäyksen kohde luulee IP-pakettien tulevan luotettavasta lähteestä. Lähdeosoitteen väärentämistä käytetään hyökkääjän sijainnin piilottamiseksi. Väärennetyllä lähettäjän osoitteella lähetettyjen IP-pakettien suodatuksen puuttuminen mahdollistaa muihin internetin käyttäjiin kohdistuvan vahingonteon ilman mahdollisuutta selvittää tekijää. Virheellisiä lähdeosoitteita koskevilla vaatimuksilla pyritään rajoittamaan merkittävästi väärennettyjä IP-lähdeosoitteita käyttävien hyökkäysten ja verkon virhetilanteiden aiheuttamia ongelmia.

17.1 Reitityspoikkeamien havainnointi

Reitityspoikkeamalla tarkoitetaan epänormaalia ja usein myös äkillistä muutosta verkon saavutettavuus- ja topologiatietoihin, jolla saattaa olla negatiivia vaikutuksia internetliikenteen välittämiseen. Reitityspoikkeaminen havainnointi on tärkeää, jotta saadaan ylläpidettyä tilannekuvaa muutoksista, jotka saattaisivat vahingoittaa teleyrityksen omaa verkkokokonaisuutta. Havainnoinnin ja sen mahdollistamanpoikkeamiin reagoinnin tärkeys korostuu eritoten siksi, että hyökkäykset BGP-protokollaa kohtaan voivat johtaa merkittäviin vaikutuksiin verkkoliikenteen kulun kannalta. Lisäksi monitorointi ja havainnointi mahdollistavat pidemmän aikavälin analyysien teon, joiden avulla voidaan suunnitella ennakoivia toimenpiteitä verkkoliikenteen turvallisuuden ylläpitämiseksi.

Määräys edellyttää, että teleyrityksellä tulee olla kyky havainnoida poikkeamia sen omien reittien näkyvyydessä. Omien reittien osalta tulisi kyetä havainnoimaan ainakin sitä, miten teleyrityksen mainostamat reitit näkyvät teleyrityksen oman ympäristön ulkopuolella (ts. maailmalla), jotta esimerkiksi olisi mahdollista havaita tilanne, jossa joku muu alkaa mainostamaan kilpailevaa reittiä kyseisiin verkkoihin vahingossa tai pahantahtoisissa tarkoituksissa. Havainnoinnin toteuttamisessa voi hyödyntää esimerkiksi julkisia reititystietopalvelimia, kuten RIPE NCC:n Routing Information Servicen[81] keräämää tietoa.

Teleyrityksen tulisi myös monitoroida ja valvoa muista verkkokokonaisuuksista saapuvaa ja teleyrityksen omasta verkkokokonaisuudesta lähtevää BGP-verkkoliikennettä, jotta teleyritys voi ylläpitää tietoutta sekä oman verkkokokonaisuutensa vakaudesta ja sietokyvystä, että tilaajiensa yksityisyydensuojasta ja tietoturvasta.

[81] RIPE NCC, https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris

17.2 BGP-istuntojen suojaaminen

Määräys edellyttää, että teleyritys suojaa sellaiset BGP-istunnot, joita käytetään reittitietojen vaihtamiseen reititysnaapurien kanssa aina kun se on mahdollista. BGP:n TCP-istuntojen suojaaminen voidaan toteuttaa esimerkiksi IETF:n määrittelyssä RFC 5925[82] kuvatuilla vaihtoehdoilla. BGP-istuntojen väärentämistä voidaan puolestaan esimerkiksi estää käyttämällä yleistä TTL-suojausmekanismia (Generalized TTL Security Mechanism, GTSM[83]). GTSM:ssä hyödynnetään joko IPv4:n paketin elinaikaa (Time to Live, TTL) tai IPv6:n hypynrajoitusta (hop limit) sen tarkistamiseen onko paketin lähettänyt yhdistetyn linkin viereinen solmu, eli se naapuri, jonka kanssa BGP-istunto on muodostettu. GTSM-ratkaisua on kuvattu IETF:n määrittelyssä RFC 5082[84].

Istuntojen suojaamista koskevalla velvoitteella pyritään mm. estämään välimieshyökkäyksien avulla tehtäviä BGP-istuntojen katkaisuja tai väärennetyn tiedon syöttämistä istuntoihin.

Edellä mainittujen suojaustoimenpiteiden käyttöönotto edellyttää konfiguraatiomuutoksia paikallisten reititinlaitteiden lisäksi myös liikenteenvaihtokumppanin reititinlaitteissa. Teleoperaattorilla voi olla liikenteenvaihtokumppanuuksia muidenkin kuin toisten teleoperaattoreiden kanssa, ja tällaisissa tapauksissa ei välttämättä ole mahdollista sopia suojauksien käyttöönotosta. Tällöin teleyrityksen tulee joka tapauksessa mahdollistaa BGP-istuntojen suojaaminen ja pyrkiä omalta osaltaan edistämään suojaustoimenpiteiden käyttöönottoa, mutta mikäli tiettyä toimenpidettä ei pystytä liikenteenvaihtokumppanin kanssa sopimaan, ei kyseistä suojausta luonnollisestikaan ole mahdollista toteuttaa.

17.3 Virheellisten lähdeosoitteiden suodatus

Määräys edellyttää teleyritystä suodattamaan viestintäverkkoonsa suuntautuvaa virheellisen IP-lähdeosoitteen sisältävää liikennettä, ellei toisin ole sovittu. Reitittimissä on suositeltavaa käyttää erityisiä suodattimia, joiden avulla voidaan vähentää verkkoon saapuvien ja sieltä lähtevien osoiteväärennettyjen IP-pakettien määrää.[85]

Vaatimus koskee vain teleyrityksen verkon kannalta merkitseviä lähdeosoitteita, eli teleyrityksen ei tarvitse tarkistaa esimerkiksi IP-pakettien hyötykuormassa VPN-tunneloinnin yhteydessä välitettäviä muita lähdeosoitteita.

Suodatustoimenpiteet on tehtävä teknisesti tarkoituksenmukaisella tarkkuudella yhteenliittämisrajapinnassa. Käytettäviä ratkaisumahdollisuuksia ja huomioonotettavia tekijöitä on kuvattu IETF:n spesifikaatioissa RFC 2827[86] ja RFC 3704[87].

Suodatettavia osoiteavaruuksia voivat olla muun muassa ns. bogon-prefixit, joilla tarkoitetaan yksityiseen käyttöön (RFC 6761[88]) tai erityisiin tarkoituksiin varattuja osoiteavaruuksia, joita ei ole tarkoitettu käytettäväksi avoimesti internetissä. Lisäksi suodatettavia osoiteavaruuksia voivat olla IANA:n tai paikallisten internetosoiterekistereiden toistaiseksi käyttöön luovuttamattomat verkot.[89]

[82] IETF RFC 5925, The TCP Authentication Option, https://tools.ietf.org/html/rfc5925
[83] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP), s. 12 (TTL Security (GTSM)
[84] IETF RFC 5082, The Generalized TTL Security Mechanism (GTSM), https://tools.ietf.org/html/rfc5082
[85] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP). Ks. myös MANRS Actions for Network Operators, Action 2. Version 2.5.2 – 17 May 2021, https://www.manrs.org/netops/network-operator-actions/.
[86] IETF RFC 2827, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, https://tools.ietf.org/html/rfc2827.
[87] IETF RFC 3704, Ingress Filtering for Multihomed Networks, https://tools.ietf.org/html/rfc3704.
[88] IETF RFC 6761, Special-Use Domain Names, https://tools.ietf.org/html/rfc6761.
[89] ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP), s. 11 (Bogon Filtering).

Bogon-suodatusta tehtäessä voidaan käyttää esimerkiksi luotettavien tahojen tarjoamaa BGP-reititystietoa, jossa osoiteavaruuksien käytössä tapahtuvat muutokset tehdään suodatustunnusmerkistöön keskitetysti. Laitteiden mukana tulevia default-bogon-listoja ei tule käyttää, koska ne ovat vanhentuneita.

Joissain poikkeuksellisissa tilanteissa teleyritys saattaa sopia toisen teleyrityksen kanssa siitä, että osaa teleyrityksen osoiteavaruudesta reititetään väliaikaisesti toisen verkosta lähtevänä. Toimenpide on suunniteltava ja toteutettava käyttäen tarkkaa harkintaa ja yhdysliikennetilanteeseen soveltuvia menetelmiä. Pääasiallisesti vastuu virheellisiä lähdeosoitteita sisältävän liikenteen välittämisen estämisessä on liikennettä välittävällä teleyrityksellä.

Virheellisen lähdeosoitteen tilanteena ei pidetä teleyritysten välisessä yhdysliikennöinnissä tilannetta, jossa teleyritys saa reittimainostuksia toiselta teleyritykseltä mutta ei mainosta niitä eteenpäin. Tällöin reittimainostukset eivät vastaa teleyrityksen reititystietoja, mutta teleyritysten välinen yhdysliikenne voidaan silti välittää.

17.4 Reittimainostusten suodatus

Määräyksen mukaan teleyrityksen on oletusarvoisesti hylättävä yhteenliittämisrajapinnoissa vastaanotettavista reittimainostuksista sellaiset reitit, jotka kuuluvat teleyrityksen omiin tai sellaisiin teleyrityksen asiakkaalle toimittamiin osoitelohkoihin, joiden ei voida olettaa mainostuvan muilta teleyrityksiltä. Määräys sallii tästä perussäännöstä poikkeamisen erikseen sopimalla.

Teleyrityksen tulee hylätä sellaiset reittimainostukset, joiden ROA-tietue (Route Origin Authorization) ei vastaa RPKI (Resource Public Key Infrastructure) -tietokantaan ilmoitettuja ROA-tietoja.

Minkään teleyrityksen ei pitäisi mainostaa toisen teleyrityksen tai tämän asiakkaan hallinnoimia verkko-osoitelohkoja tai tarkemmin näiden osalohkoja sisältäviä reittejä ilman erillistä sopimusta. Esimerkiksi tietyt moniliittymisratkaisut (multihoming) voivat edellyttää tällaista sopimusta.

Oikeudeton mainostus voi olla tahallista tai tahatonta liikenteen ohjaamista ulkopuolisen toimijan järjestelmään. Oikeudettoman mainostuksen aiheuttamalta uhalta suojautumiseksi reittimainostuksia vastaanottavan teleyrityksen on suodatettava mainostuksesta pois virheelliset mainostukset, kuten esimerkiksi jo edellä mainitut toisille teleyrityksille ja heidän asiakkailleen kuuluvat osoitelohkot, sekä osoitelohkot, joiden ei pitäisi esiintyä internetreitityksessä. Mahdollisia ratkaisuvaihtoehtoja suodattamiseen on kuvattu IETF:n määrittelyssä RFC 7454[90].

Suositus

Liikenne- ja viestintävirasto suosittelee, että teleyritys toteuttaa teknisen ja operatiivisen kyvykkyyden suodattaa BGP AS-polkuja. Polkujen suodatus on tekniikka, jolla voidaan hyväksyä tai hylätä prefiksejä, joiden alkuperä tai reitti tulee jonkin tietyn AS:n kautta. Tätä tekniikkaa voidaan käyttää esimerkiksi hylkäämään prefiksit, joiden alkuperä on yksityinen AS, ellei kyseinen AS ole teleyrityksen asiakas. Lisätietoa BGP AS-polkujen suodattamisesta löytyy IETF:n määrittelyssä RFC 7454[90].

[90] IETF RFC 7454, BGP Operations and Security: https://tools.ietf.org/html/rfc7454. Ks. myös MANRS Action 1 ja ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP).

17.5 Reittimainostusten todentaminen

Määräys edellyttää teleyritystä luomaan sen omistamille tai teleyrityksen asiakkailleen toimittamille verkkoalueille ROA-tietueet. Lisäksi tulee huolehtia, että tietueet on allekirjoitettu ja julkaistu asiaankuuluvassa internetosoiterekisterissä.

Eräs BGP:n turvallisuutta merkittävästi heikentävä tekijä on, että reittimainostusten aitoutta ei tavallisesti tarkisteta mitenkään, koska lähtökohtaisesti luotetaan siihen, että reittienvaihtokumppanina olevalta autonomiselta järjestelmältä saatu tieto reiteistä pitää paikkaansa. Tavallisesti näin onkin, mutta mainostuksissa voi myös olla tahattomasti tai tahallisesti aiheutettuja virheitä. Reititystietojen todentamista varten on kuitenkin kehitetty ratkaisuja, joista tunnetuin ja yleisimmin käytössä oleva on RPKI. RPKI:n avulla autonomisten järjestelmien on mahdollista todentaa omistamansa reittimainostukset. Teknisesti tämä tapahtuu luomalla ROA-tietueet, jotka vahvistetaan digitaalisella allekirjoituksella. ROA-tietue kertoo, mikä autonominen järjestelmä on valtuutettu luomaan ja mainostamaan reittejä tietyille IP-osoiteryhmille. Jotta reittimainostukset voidaan todentaa, tulee reititinlaitteet konfiguroida tarkistamaan reititystieto käyttämällä RPKI:ta ja tekemään toimenpiteitä reiteille, jotka eivät läpäise tarkistusta. ROA-tietueet voidaan luoda ja allekirjoittaa yksinkertaisimmin käyttämällä paikallisten internetrekisterien luottamusketjuja. Suomen osalta alueellinen internetrekisteri on RIPE NCC, jonka verkkosivuilta löytyy kattavat ohjeet niin ROA-tietueiden luomiseen, hallinnointiin ja allekirjoittamiseen kuin reittimainostusten todentamiseen reitittimillä[91].

BGP-reittimainostusten oikeellisuuden varmistamisessa BGP-reititykseen osallistuvien reitittimien validoituja RPKI-tietoja verrataan saapuviin reittimainostuksiin. Validoiduilla RPKI-tiedoilla tarkoitetaan RPKI-validoitujen (RPKI Validator) palvelimien ROA-tietoja. RPKI-validoiduille palvelimille tieto ROA-tietueiden tilasta saadaan RPKI-tietokannasta (RPKI Repository), joka on alueellisen internetosoiterekisterin hallinnoima.

Tässä varmistusprosessissa on olemassa kolme eri lopputulosta: "Valid", "Invalid", ja "NotFound".[92] Lopputulemat "Valid" ja "Invalid" tarkoittavat, että ROA-tietue on olemassa ja että se joko vastaa RPKI-validoitua ROA-tietuetta RPKI-tietokannassa, tai että nämä kriteerit eivät toteudu. "NotFound" tarkoittaa, että ROA-tietuetta ei ole joko luotu tai että sitä ei ole julkaistu RPKI-tietokantaan.

ROA-tietueisiin liittyvien vaatimusten ulkopuolelle voidaan jättää internetosoiterekisterijärjestelmän piiriin kuulumattomat verkkoalueet sekä verkkoalueet, joille on teknisesti mahdotonta luoda ROA-tietue.

Yllä mainittujen toimien lisäksi teleyritys voi hyödyntää esimerkiksi BGP-protokollan BGPsec-laajennusta reitityksen turvallisuuden parantamiseksi. IETF on kuvaillut BGPsec-laajennusta RFC 8205:ssa[93] ja RFC 8206:ssa[94]. BGPsec:llä pystytään kryptografisesti varmistamaan, että jokainen verkkoliikenteen reitin varrella ollut AS on valtuuttanut reitin mainostuksen seuraavalle AS:lle.

18. IP-liikenteen lähdeosoitteen väärentämisen estäminen asiakasrajapinnassa

Hajautetuissa palvelunestohyökkäyksissä pyritään usein vaikeuttamaan hyökkääjän löytämistä käyttämällä liikennöinnissä väärennettyjä lähdeosoitteita. Liikenteen lähteeksi voidaan väärentää esimerkiksi hyökkäykseen liittymätön ulkopuolinen verkko tai

[91] RIPE NCC, RPKI, https://www.ripe.net/manage-ips-and-asns/resource-management/rpki. Ks. myös ENISA: 7 Steps to shore up the Border Gateway Protocol (BGP), toimenpide 7.
[92] IETF RFC 6811, BGP Prefix Origin Validation, https://tools.ietf.org/html/rfc6811.
[93] IETF RFC 8205, BGPsec Protocol Specification, https://tools.ietf.org/html/rfc8205.
[94] IETF RFC 8206, BGPsec Considerations for Autonomous System (AS) Migration, https://tools.ietf.org/html/rfc8206.

satunnaisesti valittu kohdeverkon osoite. Väärennetyt lähdeosoitteet saattavat olla myös satunnaisesti valittuja osoitteita yksityiseen käyttöön tai erityisiin tarkoituksiin varatuista osoiteavaruuksista. Virheellisiä lähdeosoitteita sisältävän IP-liikenteen suodattamista koskevilla vaatimuksilla pyritään rajoittamaan väärennettyjä IP-lähdeosoitteita käyttävien hyökkäysten aiheuttamia ongelmia.

Suodattamista lievempänä toimenpiteenä asiakkaaseen voidaan myös ottaa yhteyttä tilanteen selvittämiseksi. Tämä mahdollisuus perustuu siihen, että SVPL:n mukaan teleyritys voi estää tai rajoittaa viestien välittymisen asiakkaan päätelaitteeseen estääkseen viestintäverkkoihin tai niihin liitettyihin palveluihin kohdistuvia tietoturvauhkia ja haittaa aiheuttavia häiriöitä. Liikenteen rajoitustoimenpiteitä lievempänä toimenpiteenä teleyritys voi selvittää tietoturvauhan tai häiriön aiheuttavan käyttäjän henkilöllisyyden ja olla käyttäjään tai tämän edustajaan yhteydessä uhkan tai häiriön poistamiseksi.

18.1 Suodattaminen

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

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

Esimerkiksi ADSL-yhteyden tapauksessa suodatus voidaan toteuttaa keskittimen DSLAM-verkkoelementissä, DSL-verkon yhteyksien terminointilaitteessa tai runkoverkon reitittimessä. Suodatuksen tarkoituksenmukainen toteutuspiste riippuu verkkolaitteiden tekniikasta, suodatuskyvystä ja teleyrityksen käytännöistä suodattamisen toteuttamisessa.

18.2 Käyttäjän tunnistaminen

Teleyrityksen on tietoturvasyistä pystyttävä tunnistamaan tiettyä IP-osoitetta käyttänyt asiakasliittymä tarvittaessa DHCP-lokiin tallentuneita välitystietoja käsittelemällä. Asiakasliittymän tunnistaminen on välttämätöntä tietoturvatoimenpiteiden kohdistamiseksi oikeaan asiakasliittymään, vaikka sen IP-osoite olisi vaihtunut.

Aiemman Viestintäviraston tulkinnan (dnro 387/64/2009) mukaan teleyritys saa tarvittaessa käsitellä välitystietoja sekä tilanteissa, jotka nykyisin määritellään SVPL 272 §:n 1 momentissa, että käyttäessään nykyisin pykälän 2 momentissa tarkoitettuja keinoja. Viestintäviraston tulkinnan mukaisesti teleyritys saa käsitellä välitystietoja varsinaisen 272 §:ssä tarkoitetun toimenpiteen suorittamisen lisäksi myös toimenpiteen suorittamiseksi välttämättömien valmistelevien toimenpiteiden suorittamiseksi. Tällainen valmisteleva toimenpide voi olla esimerkiksi tiettyä IP-osoitetta käyttäneen asiakkaan tunnistaminen DHCP-lokiin tallentuneita välitystietoja käsittelemällä.

19. Matkaviestinverkon rajapintojen suojaaminen

5G-verkon uudet käyttötapaukset ja niiden edellyttämät arkkitehtuuriratkaisut ovat tuoneet uusia rajapintoja teleyritysten viestintäverkkoihin, joiden kautta on mahdollista luovuttaa myös verkon kontrollia kolmansille osapuolille, esimerkiksi viestintäverkon viipaleen tai reunalaskentayksikön osittaisen hallinnan. Edellisten verkkosukupolvien signalointiprotokollat ovat yhä laajalti käytössä ylläpitäen yhteyksiä eri verkkosukupolvien välille. Kokonaisuutena tämä lisää uhkapinta-alaa, jonka hallitseminen edellyttää

teleyrityksiltä kokonaisvaltaista rajapintojen suojaamista toteuttamalla tämän määräyksen velvoitteita sekä aktiivisesti seuraamalla ja toteuttamalla eri sidosryhmien tuottamia suosituksia oman uhka- ja riskiarvionsa perusteella.

19.1 Signalointirajapinnat

Signaloinnilla matkaviestinverkoissa tarkoitetaan matkaviestinverkon eri elementtien välisen kontrolli- ja käyttäjäviestinnän ohjaamista halutulla tavalla. Verkkojen kehittyessä on signaloinnin määrä ja tarve kasvanut entisestään. Viestintäverkkoon lisätään uusia toiminnallisuuksia ja niiden välille luodaan uusia signalointirajapintoja. Vanha sanomavälitysjärjestelmä Signalling System 7 (SS7) on ollut käytössä jo 2G- ja 3G-verkoissa. Sitä on käytetty esimerkiksi puheluiden reitityksessä teleyrityksen sisällä, yritykseltä toiselle, verkkovierailutietojen vaihtamista varten tai tilaajan tiedottamiseen käytettävistä olevista ominaisuuksista. SS7:n suunnittelussa ei ole aikanaan huomioitu tietoturvan merkitystä tarpeeksi, mikä on mahdollistanut SS7:n väärinkäytön. Mahdollinen hyökkääjä voisi esimerkiksi injektoida SS7-liikennettä matkaviestinverkkoon ja vastaanottaa tietoja, joihin hyökkääjän ei pitäisi päästä käsiksi, tai valvoa verkon toimintoja luvattomasti. Hyökkäyksillä voi myös toteuttaa matkaviestinverkon kartoitusta eri skannaustekniikoilla, joita käytetään verkon sisällä. Verkon rakenteesta ja hyökkääjän sijainnista riippuen hyökkääjä voi kartoittaa esimerkiksi ydinverkon, radioliityntäverkon tai IMS:n rakennetta.[95] Kartoituksessa kerätyn tiedon avulla voidaan kohdentaa hyökkäyksen seuraava vaihe ja valita siihen toimiva menetelmä.

4G-verkoissa Diameter-protokolla korvaa 2G- ja 3G-verkoissa käytetyn SS7:n. Vastaavasti 5G-verkoissa Diameter on pääsääntöisesti korvattu HTTP/2 JSON:lla. Yhteinen piirre näille protokollille on, että mahdolliset hyökkääjät hyödyntävät ydinverkon normaalia toiminnallisuutta, esimerkiksi esiintymällä verkon HLR-/HSS-elementtinä, ja hyökkäyksellä voidaan yrittää saada selville loppukäyttäjän sijainti verkossa tai selvittää verkon rakennetta. Toinen hyökkäystapa on luoda palvelunestotilanteita verkossa hyödyntämällä tiettyjä signalointiviestejä. Tällä tavalla voidaan kuluttaa verkkoresursseja tai kohdistaa hyökkäys suoraan tiettyyn käyttäjään. Tämä olisi huomioitava erityisesti erilaisten sovellusrajapintojen suojaamisessa.

Määräyksen kohdan 19.1.1 mukaan teleyrityksen on matkaviestinverkon rajapinnoissaan valvottava signalointirajapintojen tietoturvaa sekä suunniteltava, toteutettava ja ylläpidettävä ajantasaiseen uhkatietoon ja riskiarvioon pohjautuvat signalointirajapintojen tietoturvan hallintatoimenpiteet.

Signalointiprotokollahyökkäyksiä on mahdollista estää tai lieventää esimerkiksi signalointiviestejä suodattamalla. Verkon reunalla toimivan dedikoidun signalointipalomuurin (Signalling Firewall, SigFW) avulla voi suodattaa signalointiviestejä sovelluskerroksessa jo ennen kuin ne saavuttavat kohdennetun verkkoelementin ja vaikuttavat verkkoelementin toimintaan. Myös signalointia käsittelevissä verkkoelementeissä (SS7:n Signal Transfer Point, STP; Diameter Agents, DRA, DEA; 5G:n Security Edge Protection Proxy, SEPP) voidaan tekniikasta riippuen toteuttaa eritasoista liikenteen suodatusta. Yleisesti turvallisuutta voidaan parantaa järjestelmien koventamisella eli poistamalla verkkoelementtien tarpeettomat toiminnot käytöstä.

SEPP on 3GPP:n määrittelemä pakollinen turvallisuustoiminto, joka parantaa 5G-verkkojen välisen liikenteen turvallisuutta toteuttamalla mm. todentamisen, valtuutuksen ja salauksen N32-rajapinnalla.[96] Huolehtimalla SEPP-toiminnallisuuden asianmukaisesta

[95] Rao, S. P. – Chen, H. Y. – Aura, T., Threat modeling framework for mobile communication systems. Computers and Security 125 2023, 103047, s. 1–23.
[96] Kyberturvallisuuskeskus, 5G Security Architecture, s. 33–34, https://www.kyberturvallisuuskeskus.fi/en/publications/5g-security-architecture.

suunnittelusta, toteuttamisesta ja ylläpidosta voidaan esimerkiksi piilottaa viestintäverkon arkkitehtuuri sekä suodattaa tulevaa ja lähtevää liikennettä. Lisäksi voidaan esimerkiksi pyrkiä mahdollisimman kattavaan välitettävien tietojen salaamiseen 5G-verkkojen välisen tiedonsiirron turvallisuuden varmistamiseksi.

Suositukset

SS7-protokolla on edelleen laajasti käytössä, joten on perusteltua ylläpitää ja kehittää sen turvallisuutta myös jatkossa. Liikenne- ja viestintävirasto suosittelee vuonna 2015 laaditun yhteispohjoismaisen SS7-suosituksen mahdollisimman laajaa toimeenpanoa kattavan suojaus- ja havainnointikyvykkyyden saavuttamiseksi.[97]

Diameter-protokollan turvallisuuden varmistamiseksi Liikenne- ja viestintävirasto suosittelee seuraamaan GSMA:n laatimaa ja ylläpitämää Diameter-protokollaa koskevaa suositusta, jonka toimenpiteiden toteuttaminen auttaa teleyrityksiä suojautumaan useimmilta tunnetuilta uhilta.[98]

19.2 Matkaviestinverkon viipalointi

Verkon viipaloinnilla tarkoitetaan matkaviestinverkon palvelujen loogista eriyttämistä, jonka avulla voidaan tarjota eri käyttötapauksiin optimoituja ja kohdennettua palveluja. 5G-verkon kehityksen edetessä on määritelty seuraavia käyttötapauksia:

- mobiililaajakaistapalvelut (enhanced Mobile Broadband, eMBB), ajoneuvojen viestintä (Vehicle to X, V2X)
- erittäin luotettavat lyhyen viiveen palvelut (Ultra-Reliable Low Latency Communication, URLLC)
- laajamittainen IoT-laitteiden välinen viestintä (massive Machine-Type Communication, mMTC)
- korkean välityskyvyn IoT-laitteiden viestintä (High-Performance Machine-Type Communications, HMTC).

Edellä kuvattujen viipaletyyppien suositusominaisuudet sekä palvelun laatuun liittyviä ominaisuuksia on määritelty GSMA:n julkaisussa.[99] Suositusominaisuudet ja -arvot on johdettu 3GPP:n teknisestä määrityksestä,[100] ja niiden on katsottu GSMA:n taholta täyttävän kyseisten viipaletyyppien vähimmäisvaatimukset. Kun kyse on muusta kuin edellä mainituista käyttötapauksista, voi viipaletta tarjoava teleyritys määritellä ominaisuudet vapaammin yhdessä asiakkaan kanssa (Network Slice Customer, NSC). Kyse voi olla esimerkiksi viipaleen avulla toteutetusta yksityisestä verkosta (Public Network Integrated Non-Public Network, PNI-NPN).

Hallintayhteyden suojaaminen

Määräyksessä edellytetään (kohta 19.2), että matkaviestinverkon teleyritys suojaa viipaleen hallintayhteyden siten, että oikeudeton viipaleen luonti, muuttaminen tai poistaminen on estetty, ja ettei viipaleen ominaisuuksia, eikä tilaajien tai käyttäjien tietoja luovuteta oikeudettomasti. Hallintaliittymän suojaamisella pyritään estämään hyökkääjää käyttämästä esimerkiksi veloitettavia palveluita oikeudettomasti tai luomasta verkkoviipaletta, jolla voi estää palveluita tai seurata viestintäverkon asiakkaita. Hyökkääjä voi myös pyrkiä suorittamaan esimerkiksi välimieshyökkäyksen muuttamalla viipaletta liikenteen uudelleenreitittämiseksi.

[97] Common Nordic Recommendations on SS7 Security Issues, 18.12.2015.
[98] GSMA, FS.19 - Diameter Interconnect Security.
[99] GSMA, Official Document NG.116 - Generic Network Slice Template.
[100] 3GPP TS 23.501.

Viipaleen hallintaliittymän suojaamisessa on syytä huomioida erityisesti tilanteet, joissa viipale on toteutettu palveluna (Network Slice as a Service, NSaaS) ja asiakkaalle (NSC) on myönnetty yksilöidyt pääsyoikeudet verkon toimintoihin ja tietoihin. Tällöin on hyvä tarkoin määritellä, rajata ja valvoa, että asiakkaalla on pääsy vain ennalta sovittuihin tietoihin. Tietoturvan varmistamiseksi liikenne voidaan ohjata NEF-toiminnallisuuden (Network Exposure Function) kautta, joka esimerkiksi kontrolloi 3GPP:n ydinverkon ominaisuuksiin liittyvien tietojen luovuttamista 3GPP-toimialueen ulkopuolelle sekä todentaa ja valtuuttaa kaiken ulkopuolelta tulevan viestiliikenteen.

Viipalekohtainen käyttöoikeustodennus

Määräyksessä edellytetään (kohta 19.1.3), että teleyritys toteuttaa riskiperusteisesti viipalekohtaisen käyttöoikeustodennuksen ja -valtuutuksen (Network Slice Specific Authentication and Authorization, NSSAA) viipaletta käyttäville päätelaitteille. Ensisijaisen 3GPP-todennuksen lisäksi viipalekohtaisessa käyttöoikeustodennuksessa ja -valtuutuksessa tulee käyttää muita kuin ensisijaisessa todennuksessa käytettyjä tunnistetietoja. Näin tulee toimia, jos se on tarpeen ottaen huomioon viipaleen käyttöön liittyvät tietoturvauhat ja tekniset mahdollisuudet käyttöoikeustodennuksen ja valtuutuksen toteuttamiseksi.

Viipalekohtainen käyttöoikeustodennus ja -valtuutus päätelaitteen ja AAA-palvelimen (Authentication Authorization and Accounting Server) välillä toteutetaan välityspalvelimena toimivan NSSAAF:n (NSSAA Function) avulla. NSSAAF toimittaa AAA-palvelimelle tiedon viipaleesta (Single-Network Slice Selection Assistance Information, S-NSSAI), sekä päätelaitteen tunnistamistiedot (Generic Public Subscription Identifier, GPSI). 3GPP-alueen tunnisteita ei tule toimittaa ulkopuolisiin verkkoalueisiin.

3GPP Release 17 tuo uuden toiminnon verkkoviipaleen pääsynhallintaan (Network Slice Admission Control, NSACF), joka mahdollistaa viipaleiden paremman hallinnan ja käytön. Kyseisen toiminnon avulla on mahdollista valvoa ja kontrolloida rekisteröityjen päätelaitteiden ja PDU-istuntojen (Protocol Data Unit) viipalekohtaista määrää. Turvallisuustoiminnolla voidaan lieventää riskejä erityisesti tilanteessa, jossa viipaleen hallintaoikeus on 3GPP-toimialueen ulkopuolella. Analyysiä ja jatkokäsittelyä varten viipaleen haltijalle (Application Function, AF) toimitettavat tiedot välitetään NEF-toiminnallisuuden avulla.[101]

Määräyksessä on otettu huomioon, että kaikissa käyttötapauksissa tarvetta erityiselle viipalekohtaiselle käyttöoikeustodennukselle ja valtuutukselle ei välttämättä ole, kuten jos viipaleen käyttöön ei liity tavallisesta poikkeavia tietoturvauhkia. Määräys ottaa näin huomioon myös sen, että käytetty päätelaite voi rajoittaa mahdollisuuksia toteuttaa lisätoimia, joskaan hallitsemattomia tietoturvariskejä ei saa tällaisessakaan tilanteessa syntyä.

Mikäli viipalekohtaista todennusta ei suoriteta, saattavat viipaleeseen oikeudettomat päätelaitteet käyttää sen resursseja tai oikeudettomasti saada tietoja verkon ominaisuuksista. Oikeudeton päätelaite voi olla mikä tahansa tavallinen laite, joka on saattanut suorittaa ensisijaisen todennuksen onnistuneesti 3GPP-tunnistetiedoilla mutta jolla ei ole tietyn verkkoviipaleen käyttämiseen tarvittavia käyttöoikeuksia.[102]

19.3 Reunalaskenta viestintäverkossa

Viestintäverkon ja erityisesti matkaviestinverkon uudet käyttötapaukset asettavat suorituskyky- ja luotettavuusvaatimuksia, joiden mahdollistamiseksi viestintäverkon järjestelmiä tuodaan lähemmäs loppukäyttäjää. Tällöin käyttäjän liikenne voidaan ohjata

[101] 3GPP, Network Slicing Security for 5G and 5G advanced systems, https://www.3gpp.org/technologies/slicing-security
[102] ENISA GL SO11, 5G Security Control Matrix: SO11-010.

lyhyempää reittiä palvelun resursseihin tai jopa toteuttaa palvelu paikallisesti reunalaskentayksikön piirissä. Reunalaskentaympäristö on luonteenomaisesti useiden eri toimijoiden ohjelmistoista ja laitteista koostuva ympäristö, joka mahdollistaa monipuolisten, uusien toimintatapojen kehittämisen ja palvelujen tarjoamisen käyttäjille. Tyypillisesti järjestelmien fyysiset laitteet, virtualisointialustat ja sovellukset ovat eri toimijoiden toteuttamia. Teleyrityksen verkkotoiminnot luovat yhdessä kolmansien osapuolien sovellusten sekä erilaisten virtualisointiratkaisujen kanssa epäyhtenäisen kokonaisuuden, joka on altis haavoittuvuuksille, varsinkin mikäli asiaan ei kiinnitetä erityistä huomiota. Lisäksi on huomioitavaa, että reunalaskentayksikkö voi sijaintinsa vuoksi olla alttiimpi fyysiselle vaikuttamiselle (hyökkäykselle) kuin teleyrityksen keskitetymmät verkon toiminnallisuudet.

Reunalaskentaympäristön toteuttamisessa ja ylläpidossa on syytä huomioida virtualisoinnin toteuttavien ohjelmistokomponenttien koventaminen laitavalmistajan ohjeiden mukaisesti huomioiden riskit liittyen ympäristön fyysisen järjestelmien sijaintiin. Tällöin reunalaskentayksiköiden sekä muun viestintäverkon turvallisuuden varmistamiseksi on yhteys sovellusten, NEF-toiminnon ja reunalaskentaympäristön välillä toteutettava turvallisesti toteuttamalla molemminpuolinen, toistuva todentaminen ja tunnistautuminen, sekä varmistamalla NEF-toiminnon turvallisuustoimintojen toteutus ja pysyvyys koko niiden elinkaaren aikana. Erityistä huomiota tulee kiinnittää järjestelyyn, jossa reunalaskentayksikön ohjaus toteutetaan kolmannen osapuolen toimesta 3GPP-järjestelmän ulkopuolelta. Reunalaskentayksikön turvallisuuden varmistamiseksi on hyvä toteuttaa viipalointiin ja virtualisoinnin osalta keskeiset turvallisuustoimenpiteet, kuten viipalekohtaisen pääsyn- ja todennuksenhallinta, sekä virtualisointiympäristön koventamistoimenpiteet ja haavoittuvuuksien kokonaisvaltainen hallinta.

Luku 4 Internetyhteyspalvelujen erityiset vaatimukset

20. Internetyhteyspalvelujen liikennöinnin eriyttäminen

Määräyksen kohdan 20.1 mukaan 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.

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

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

Salaamattomat WLAN-yhteydet ovat yleisesti käytössä erityisesti paikoissa, jossa on paljon liikkuvia tilaajia. WLAN-yhteyksien salaaminen on teknisesti mahdollista, mutta salauksen toteuttaminen, erityisesti salausavainten hallinta, vaikeuttaisi palvelun tarjoamista merkittävästi. Tästä syystä määräyksen kohta 20.2 sisältää erityisen poikkeuksen, joka mahdollistaa salaamattomien WLAN-yhteyksien tarjoamisen ilman radiorajapinnassa tapahtuvaa liikenteen erottamista. Mahdollisuuksien mukaan käyttäjiä tulisi

tiedottaa salaamattomien WLAN-yhteyksien käyttöön liittyvistä riskeistä. WLAN-yhteyksillä tarkoitetaan IEEE-standardin 802.11 mukaisia langattomia lähiverkkoyhteyksiä.[103]

21. Kuluttajaliittymistä lähtevän sähköpostiliikenteen ohjaus

Määräyksen kohdan 21 mukaan teleyrityksen on estettävä kuluttajaliittymistä lähtevä rajoittamaton SMTP-liikenne muuten kuin sovittujen, lähtevälle SMTP-liikenteelle tarkoitettujen palvelimien kautta. Määräys mahdollistaa kuitenkin myös rajoituksesta poikkeamisen, jolloin teleyrityksen tulee tiedottaa tilaajaa asiaan liittyvistä riskeistä, sekä omata kyvykkyys reagoida mahdollisiin asiaan liittyviin häiriötilanteisiin.

Rajoittamaton SMTP-liikenne (portti 25) liittymästä internetiin mahdollistaa haittaohjelmille roskasähköpostiviestien lähettämisen. Haittaohjelmien tuottamien roskapostiviestien lähettämistä voidaan tehokkaasti rajoittaa sallimalla lähtevä sähköpostiliikenne vain teleyrityksen lähtevälle SMTP-liikenteelle tarkoitettujen palvelimien kautta. Rajoitus ei merkittävästi vaikuta käyttäjien viestintämahdollisuuksiin, koska sähköpostia on mahdollista lähettää internetyhteyspalvelun tarjoavan teleyrityksen postipalvelimen kautta, tunnistettua sähköpostin lähetystä[104] käyttäen tai www-pohjaisten sähköpostipalvelujen käyttöliittymien kautta. Porttia 25 koskeva suodatustoimenpide kuitenkin rajoittaa sähköpostipalvelimen toteuttamista kuluttajaliittymässä.

Määräyksellä vahvistetaan IETF:n dokumentissa RFC 5068[105] kuvatut parhaat käytännöt sähköpostin lähetysmenetelmistä.

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

Joillakin kuluttaja-asiakkailla voi olla perusteltuja tarpeita suoralle SMTP-liikenteelle kuluttajaliittymästä minne tahansa teleyrityksen verkon ulkopuolelle. Tällainen tarve on esimerkiksi kuluttaja-asiakkaan hallinnoidessa SMTP-liikennettä oman palvelimensa kautta. Määräys mahdollistaa portin 25 suodatuksesta poikkeamisen esimerkiksi tällaisia tilanteita varten. Poikkeusten tekeminen jää teleyrityksen harkintaan, sillä määräys ei sisällä teleyrityksille velvollisuutta tehdä asiakaskohtaisia poikkeuksia suodatukseen. Esimerkiksi liittymätyyppikohtaiset tekniset rajoitukset voivat rajoittaa tällaisten poikkeusten tekemistä.

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

Määräyksen mukaisesti toteutetulla rajoittamattoman SMTP-liikenteen estolla ei saa olla vaikutusta muita tietoliikenneportteja käyttävään sähköpostiliikennöintiin, kuten käyttäjätunnistusta tai salausta käyttäviin sähköpostiprotokolliin. Erityisesti tulee huolehtia, että rajoitus ei koske liikennettä IETF:n dokumentissa RFC 6409[104] kuvattuun Mail Submission -palvelun käyttämään porttiin 587. Näin internetyhteyspalvelun tarjoavan teleyrityksen asiakkailla on mahdollisuus liikennöidä turvallisesti ja tunnistetusti myös toisen sähköpostipalveluntarjoajan hallinnassa olevaan sähköpostijärjestelmään.

[103] IEEE, 802.11 standard, https://standards.ieee.org/ieee/802.11/7028/.
[104] IETF RFC 6409, Message Submission for Mail, https://tools.ietf.org/html/rfc6409.
[105] IETF RFC 5068, Email Submission Operations: Access and Accountability Requirements, https://tools.ietf.org/html/rfc5068.

Määräyksen mukaan teleyritys voi poikkeuksena myös 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

Määräyksen kohdan 22 vaatimuksilla asetetaan velvoite suodattaa haitallista internetyhteyspalvelujen liikennettä sekä ylläpitää dokumentaatiota käytössä olevista suodatustoimenpiteistä.

Määräyksessä velvoitetaan teleyritys pitämään yllä teknistä valmiutta tilapäisesti suodattaa internetyhteyspalvelujen haitallista liikennettä (ks. määritelmä kohdasta 2.3). Määräyksellä pyritäänkin varmistamaan, että teleyrityksellä on valmiit ja ajantasaiset prosessit, toimintamallit ja järjestelmät haitallisen liikenteen tilapäiseen suodattamiseen mahdollisimman nopeasti. Tekninen valmius suodattaa pitää luonnollisesti sisällään kyvykkyyden ensin havaita haitallinen liikenne ja sen jälkeen tarvittaessa suodattaa sitä, mutta on hyvä huomata, että tämän kohdan vaatimus liittyy myös Liikenne- ja viestintäviraston määräykseen teletoiminnan häiriötilanteista, jonka 4 §:ssä määrätään mm. tietoturvaa häiritsevien tilanteiden havainnointikyvykkyydestä.

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

On huomattava, että SVPL 272 §:n 4 momentin mukaan suodatustoimenpiteet on toteutettava huolellisesti ja ne on mitoitettava torjuttavan häiriön vakavuuteen. Toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä toimenpiteelle asetettujen tavoitteiden turvaamiseksi. Toimenpiteet on lopetettava, jos niiden toteuttamiselle ei enää ole laissa säädettyjä edellytyksiä.

Määräyksen kohdassa 22 asetetun yleisen suodatuskyvykkyysvelvoitteen lisäksi määräyksen kohdassa 26 asetetaan nimenomaisia vaatimuksia haitallisen sähköpostiliikenteen suodattamiseen.

Teleyrityksen järjestelmien ja palvelujen suojaamista palvelunestohyökkäyksiltä käsitellään myös määräyksen kohdassa 6.3.

22.1 Tekninen valmius suodatustoimenpiteisiin

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

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

Teleyritys voi käyttää esimerkiksi verkon liikennemääriä tai poikkeuksellisia tapahtumia seuraavaa automaattista hallintajärjestelmää, jolloin ennalta määriteltyjen raja-arvojen

ylittyessä välittyy hälytys tapahtumien valvontajärjestelmään. Lisäksi verkon tietoturvatapahtumien hallinnassa voidaan käyttää esimerkiksi tunkeutumisen havaitsemis- ja estojärjestelmiä.

Viestintäverkon tai -palvelun tietoturvaa vaarantavassa tilanteessa teleyritys voi joutua ottamaan käyttöön tilapäisiä toimenpiteitä esimerkiksi tiettyyn tietoliikenneporttiin suuntautuvan liikenteen estämiseksi tai liikenteen rajoittamiseksi tiettyihin kohdeosoitteisiin. Suodatustoimenpiteet tulee keskeyttää, kun viestintäverkon tai -palvelun tietoturvaa vaarantava uhkatilanne on päättynyt.

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

22.2 Suodatussäännöstö ja sen dokumentointi

Erilaisia tietoliikenteen suodatuslistoja käytettäessä tulee kiinnittää erityistä huomiota suodatussäännöstön ajantasaisuuteen, jotta vanhentunut suodatussäännöstö ei aiheuta virheellistä ja tarpeetonta suodatusta. Suodatus ei esimerkiksi saa rajoittaa jo myönnettyjen IP-verkkoresurssien asianmukaista käyttöä.

Käytössä olevista suodatustoimenpiteistä on ylläpidettävä ajantasaista dokumentaatiota, jotta pysytään selvillä verkoissa ja palveluissa käytössä olevista suodatuksista ja pystytään seuraamaan niiden tarkoituksenmukaisuutta.

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

23. Internetyhteyspalvelun irtikytkeminen

Asiakasliittymästä lähtevän tai siitä tulevan liikenteen vaarantaessa viestintäpalvelun tietoturvaa, puututaan tilanteeseen ensisijaisesti määräyksen 22 kohdassa määrätyin toimenpitein eli suodattamalla liikennettä teleyrityksen verkossa tai muilla asiakasliittymän irtikytkentää lievemmillä toimenpiteillä, kuten ottamalla yhteyttä asiakkaaseen. Jos näillä toimilla ei saada tietoturvaa vaarantavaa, asiakasliittymään liittyvää tilannetta hallintaan, on teleyrityksellä oikeus aloittaa toimenpiteet saastuneen päätelaitteen aiheuttaman uhkan poistamiseksi.

Liikenne- ja viestintäviraston vakiintuneen tulkinnan mukaan teleyrityksen verkkoon liitetyt saastuneet päätelaitteet, jotka esimerkiksi lähettävät liittymästä suuria määriä roskapostia tai haittaliikennettä, vaarantavat aina teleyrityksen palvelujen tietoturvaa. Saastunut päätelaite voi näin ollen muodostaa perusteen irtikytkeä laite verkosta SVPL 273 §:n nojalla.

Koska liittymän irtikytkeminen estää asiakasta käyttämästä kyseistä liittymää, on irtikytkemisprosessi suunniteltava ja ohjeistettava yksityiskohtaisesti sekä toteutettava siten, että liittymän käyttökatko tai käyttörajoitukset jäävät mahdollisimman lyhyiksi.

23.1 Irtikytkemistilanteet

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

Tietoturvasta huolehdittaessa ja irtikytkemistilanteissa on syytä kiinnittää huomiota siihen, että viestinnän välitystietoja on oikeus käsitellä ainoastaan viestintäverkkoihin ja -palveluihin kohdistuvissa tietoturvauhka- tai -loukkaustilanteissa. Teleyrityksellä ei siten ole oikeutta käsitellä välitystietoja esimerkiksi estääkseen liittymän käyttämisen palvelun tietoturvaa vaarantamattoman rikoksen suorittamiseen. Poikkeuksen tähän sääntöön muodostaa kuitenkin SVPL 272 §:n 1 momentin 3 kohdassa tarkoitettu maksuvälinepetoksen valmistelu (ks. myös perustelumuistion liitteen luku 4).

23.2 Irtikytkentäprosessi

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

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

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

Kun palvelu- ja verkko-operaattorit ovat eri toimijoita, sopivat nämä 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.

Toimenpiteitä toteutettaessa voidaan ottaa huomioon liittymätyypistä johtuvat erityisolosuhteet. Esimerkiksi matkaviestinliittymien datapalveluihin liittyvissä tietoturvaongelmissa matkaviestinliittymästä voidaan estää vain datapalvelun käyttö kunnes tietoturvaongelma on selvitetty.

Mikäli asiakasliittymät ovat ns. automaattivalvonnan piirissä, asiakasliittymien tai asiakasliittymän tiettyjen palvelujen irtikytkeminen viestintäverkosta tapahtuu tyypillisesti haitalliselle liikennöinnille asetettujen raja-arvojen ylittyessä automaattisesti esimerkiksi puolen tunnin ajaksi ilman operaattorin manuaalisia toimenpiteitä. Liittymän ollessa irtikytkettynä, asiakkaan liikenne voidaan ohjata palveluun, jossa asiakkaalle kerrotaan irtikytkemisen syy sekä mahdolliset asiakkaan toimenpiteet asiakkaan laitteen korjaamiseksi. Lisäksi asiakkaalla voi olla mahdollisuus liikennöidä tarvittaville sivus-

toille esimerkiksi virustorjunnan asentamiseksi ja käyttöjärjestelmän ohjelmistopäivitysten suorittamiseksi. Tämä toimintamalli vähentää tarvetta asiakasliittymien pysyvämpään irtikytkemiseen.

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

Luku 5 Tekstiviesti- ja multimediaviestipalvelujen erityiset vaatimukset

24. Teksti- ja multimediaviestiliikenteen suodatus

Määräyksessä (kohta 24) edellytetään, että teleyrityksellä on tarkoituksenmukaiset järjestelmät ja menettelytavat haitalliseksi tunnistetun tekstiviesti- ja multimediaviestiliikenteen suodattamiseen. Tällä tarkoitetaan sekä teknisiä valmiuksia että ennalta määritettyjä prosesseja ja toimintaohjeita. Teleyrityksillä tulee olla kyky suodattaa haitallisia viestejä sekä saapuvassa että lähtevässä viestiliikenteessä. Suodatusvelvollisuutta koskevat 1 ja 2 alakohdat vastaavat muutoin sähköpostin suodattamista koskevan 26 kohdan 1 ja 2 alakohtaa, mutta SMS- ja MMS-viestien kohdalla ei ole tunnistettu erityistä tarvetta määrätä palvelun tuottamiseen liittyvien järjestelmien toiminnan varmistamiseksi tapahtuvasta suodatuksesta.

Teksti- tai multimediaviestien lähettäjä- ja muihin välitystietoihin ja viestien sisältöön perustuvalla suodatuksella voidaan puuttua erityisesti tilanteeseen, jossa teksti- tai multimediaviestien avulla pyritään toteuttamaan laajamittainen haittaohjelmien tai kalasteluviestien lähetyskampanja.

Haitallisen liikenteen tunnistaminen voi perustua esimerkiksi Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tai muiden teleyritysten jakamaan uhkatietoon, teleyrityksen omien asiakkaiden välittämiin viesteihin tai muilta tahoilta saatuun luotettavaksi arvioituun tietoon.

Viestien suodattamista lievempänä keinona määräys mahdollistaa haitalliseksi epäiltyjen viestien merkitsemisen tunnisteella (esim. sender ID:tä muuttamalla tai tekstin lisäämisellä viestin alkuun) tai viestien sisältämien linkkien toiminnan estämisen, kun tämä on teknisesti mahdollista. Edellä mainitut toimenpiteet ehkäisevät vastaanottajan erehdyttämisen estämättä kokonaan viestien toimittamista esimerkiksi tilanteessa, jossa riittävän korkeaa varmuutta viestin haitallisesta luonteesta ei toimenpidehetkellä ole. Toimenpiteiden tulee vaikuttaa mahdollisimman vähän asiallisten viestien välittämiseen.

SMS-palvelun kohdalla suodatuksen toteuttamiseen voidaan käyttää SMS-palomuuria. MMS-palvelun kohdalla yhtä vakiintuneita teknisiä ratkaisuja ei välttämättä ole helposti saatavilla. Uusien teknisten ratkaisujen kehittäminen ei välttämättä ole myöskään uhkaan suhteutettuna välttämättä perusteltua, kun otetaan huomioon palvelun suhteellisen vähäiset käyttömäärät. Tämän johdosta määräyksen kohtaan 24.3 sisältyy poikkeus, jonka mukaan MMS-palvelun osalta sisältöön ja välitystietoihin perustuva suodatus voidaan tietyin edellytyksin jättää toteuttamatta. Tällöin edellytetään, että teleyrityksen on havainnoitava muilla keinoin tietoturvan häiriötilanteita ja kyettävä reagoimaan niihin nopeasti. Havainnointi voi sisältää esimerkiksi poikkeavien viestimäärien tarkkailun, mikä voi viitata saastuneeseen päätelaitteeseen. Suodatuksen sijasta teleyritys voi tällöin reagoida muulla tietoturvahäiriön vaikutusten poistamiseen soveltuvalla mahdollisimman lievällä tavalla, mikä voi sisältää esimerkiksi MMS-viestien lähettämisen estämisen, kunnes haittaohjelma on poistettu päätelaitteelta. Toimenpiteiden tulee olla SVPL 272 §:n mukaisia.

Luku 6 Sähköpostipalvelujen erityiset vaatimukset

Tässä luvussa käsitellään määräyksen luvussa 6 asetettuja velvoitteita.

25. Sähköpostipalvelujen yhteystiedot ja osoiteresurssien hallinta

Määräyksessä edellytetään, että sähköpostipalvelun tarjoamiseen käytettävissä verkkotunnuksissa on oltava postmaster- ja abuse-osoitteet tai abuse-kontaktitiedot, johon saapuvia viestejä seurataan säännöllisesti. Vaatimuksella pyritään huolehtimaan siitä, että sähköpostipalveluissa on käytössä yhteydenottopiste mahdollisten toiminnan tai käytön häiriöiden ilmoittamiseksi palveluntarjoajalle, riippumatta ilmoittajan sijainnista.

Lisäksi määräyksessä edellytetään, että yhdeltä asiakkaalta vapautunutta sähköpostiosoitetta ei saa luovuttaa alle kuudessa kuukaudessa toiselle asiakkaalle. Sähköpostisoitteeseen tulee usein viestejä myös kyseisen osoitteen sulkemisen jälkeen. Mikäli vapautunut osoite annettaisiin välittömästi tai pian käytöstä poistumisen jälkeen toisen asiakkaan käyttöön, voisi uusi asiakas saada vanhalle asiakkaalle osoitettuja sähköpostiviestejä. Sähköpostiviestien luottamuksellisuuden ja sähköpostiosoitteiden väärinkäytön estämiseksi tulee käytöstä poistetun sähköpostiosoitteen olla karanteenissa kuusi kuukautta ennen kuin sitä on mahdollista vapauttaa uudelleen käyttöön.

25.1 Sähköpostipalvelua tarjoavan teleyrityksen yhteystiedot

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

Postmaster- ja abuse-osoitteiden levinneisyyden vuoksi ne keräävät usein asiatonta viestintää ja teleyrityksen onkin syytä järjestää osoitteen seuranta siten, että osoitteisiin tulevien asiallisten yhteydenottojen käsittely ei viivästy haitallisen sähköpostiliikenteen suuren määrän vuoksi. Mikäli teleyrityksen hallussa on suuri määrä verkkotunnuksia, teleyrityksen hallussa olevien verkkotunnusten postmaster- ja abuse-osoitteisiin tulevat viestit on syytä ohjata soveltuviin yhteydenottopisteisiin.

Teleyritys voi siirtää yhteydenottojen seurannan myös verkkotunnuksesta vastaavalle osapuolelle. Toisin sanoen, on myös mahdollista toimia siten, että verkkotunnuksesta vastaava taho seuraa postmaster- ja abuse-osoitteisiin tulevia viestejä teleyrityksen puolesta.

25.2 Asiakkaalta vapautuneen sähköpostiosoitteen uudelleenkäyttö

Sähköpostipalvelua tarjoava teleyritys ei saa luovuttaa asiakkaalta vapautunutta sähköpostiosoitetta toiselle asiakkaalle ennen kuin kuusi kuukautta on kulunut sähköpostiosoitteen vapautumisesta. Mikäli sähköpostiosoitteen entinen haltija haluaa vapautuneen sähköpostiosoitteensa takaisin käyttöönsä kuuden kuukauden sisällä osoitteen vapautumisesta, voidaan osoite luovuttaa takaisin hänen käyttöönsä. Oikeus sähköpostiosoitteen takaisinsaamiseen ei kuitenkaan itsessään velvoita palveluntarjoajaa säilyttämään sähköpostitilin sisältämiä sähköpostiviestejä tilin sulkemisen jälkeen. Tällainen velvoite voi kuitenkin johtua esimerkiksi osapuolten välisestä sopimuksesta.

26. Sähköpostipalvelujen erityinen suodatusvelvollisuus

Tässä määräyksen kohdassa käsitellään kyvykkyyttä tunnistaa haitallista sähköpostiliikennettä ja asetetaan haitallisen sähköpostiliikenteen suodattamista koskevat vaatimukset.

Merkittävä osuus sähköpostiliikenteestä on nykyään tulkittavissa haitalliseksi liikenteeksi. Mahdollisimman varhaisessa vaiheessa tunnistetut ja suodatut haitalliset sähköpostiviestit vähentävät sähköpostijärjestelmän kuormitusta ja asiallisten viestien läpimeno parantuu.

Vaatimusten tarkoituksena onkin vähentää sähköpostipalveluja tarjoavien teleyritysten palvelimien kautta kulkevan haitallisen sähköpostiliikenteen ja roskapostiliikenteen määrää, mikä vähentää sähköpostijärjestelmän kuormitusta, ehkäisee järjestelmään kohdistettuja haitallisia vaikutuksia (esimerkiksi palvelunestohyökkäystapauksissa), parantaa teleyrityksen sähköpostipalvelimien mainetta ja turvaa asiallisten viestien läpimenoa. Esimerkiksi suodattamalla haitallisia saapuvia sähköpostiviestejä estetään asiakkaan tietoturvalle ja sitä kautta myös viestintäverkoille haitallisen sisällön pääsy asiakkaan sähköpostilaatikkoon ja käsiteltäväksi. Lisäksi asiakkaan sähköpostiviestien käsittely helpottuu, kun asiallisia viestejä ei tarvitse erotella haitallisista viesteistä. Samalla asiakkaiden kokema palvelunlaatu ja käytettävyys parantuvat.

Haitallisen sähköpostiliikenteen tunnistus- ja käsittelymenetelmiä on useita erilaisia. Määräys ei edellytä käyttämään mitään tiettyjä niistä, vaan sähköpostipalvelua tarjoavalle teleyritykselle on haluttu jättää mahdollisuus valita tarjoamaansa palveluun parhaiten soveltuvat keinot.

Koska osa sähköpostipalvelun asiakkaista haluaa varmistua itse siitä, että virheellistä suodatusta ei tapahdu, on sähköpostipalveluntarjoajilla myös mahdollisuus merkitä haitalliseksi havaitsemansa saapuva liikenne sen suodattamisen sijaan. Määräys mahdollistaa myös asiakaskohtaisesti sopimisen siitä, että sähköpostipalveluntarjoaja jättää saapuvan liikenteen suodattamatta tai merkitsemättä.

26.1 Haitallisen sähköpostiliikenteen tunnistaminen

Haitallisen sähköpostiliikenteen tunnistaminen on edellytys kaikille sähköpostipalveluntarjoajan tekemille käsittelytoimenpiteille, kuten suodatus- ja merkitsemistoimenpiteille. Sähköpostipalvelua tarjoavalla teleyrityksellä onkin oltava käytössä ajantasaiset ja luotettavat mekanismit haitallisen sähköpostiliikenteen tunnistamiseksi.

Haitallisen sähköpostiliikenteen tunnistus ja edelleen tunnistuksen perusteella tehtävä suodatus tai merkitseminen voi perustua haitallisten sähköpostilähteiden tunnistusmekanismeihin, heuristisiin suodatusjärjestelmiin, lähtevän liikenteen virussuodatukseen, käyttäjän poikkeavaan lähtevän sähköpostiliikenteen määrään tai esimerkiksi viestin otsikkotietojen internetstandardien mukaisuuden tarkistamiseen. Erilaisia käytettävissä olevia tunnistusmekanismeja on esitelty tämän perustelumuistion liitteen luvussa 2.

Sähköpostiliikenteen lähteiden perusteella voidaan tunnistaa merkittävä osa tunnetuista oikeutettujen sähköpostiviestien lähteistä sekä tunnetuista haitallisen sähköpostiviestien lähteistä. Tunnistus voidaan tehdä esimerkiksi lähettäjän verkko-osoitteen, verkkotunnuksen tai lähettäjän sähköpostipalvelimen perusteella. Haitallisuuden määrittäminen perustuu ennalta saatuihin tai kerättyihin tietoihin lähteen kautta välitetyistä viesteistä tai viestin sisällön analysointiin. Oikeutettujen lähteiden tunnistamisella voidaan välttää asianmukaisen sähköpostiliikenteen suodatus johtuen virheellisestä tunnistuksesta. Tunnistamalla haitallisen sähköpostiliikenteen lähteet taas voidaan näistä lähteistä vastaanotettujen viestien toimitus sähköpostilaatikkoon estää tai sähköpostiviesti voidaan merkitä epäilyttäväksi ennen asiakkaan sähköpostilaatikkoon toimittamista.

Sähköpostipalveluntarjoaja voi kuitenkin havaita vain osan haitallisesta sähköpostiliikenteestä sähköpostin lähteiden perusteella. Siksi palvelun tarjoajalla on oltava käytössään myös muita menetelmiä haitallisen sähköpostiliikenteen havaitsemiseksi. Monet

näistä menetelmistä voivat kuitenkin aiheuttaa sähköpostipalveluntarjoajalle merkittäviä kustannuksia. Tiukempi tunnistuskriteeristö on myös herkempi virheellisille tulkinnoille. Sähköpostipalvelua tarjoava teleyritys voikin valita itse järjestelmässään käytettävät mekanismit useista eri vaihtoehdoista siten, että merkittävä osa haitallisesta sähköpostiliikenteestä tulee tunnistetuksi vaarantaen mahdollisimman vähän asiallisten viestien välitystä.

Jo yhden käytössä olevan menetelmän avulla on mahdollista tunnistaa merkittävä osa haitallisesta sähköpostiliikenteestä. Haitallisen liikenteen tunnistamisen tulokset kuitenkin yleensä paranevat käytettäessä useita toisiaan täydentäviä menetelmiä yhtäaikaisesti. Jokainen menetelmä tarjoaa omia etuja toisiin menetelmiin nähden, mutta valitettavasti kuhunkin menetelmään liittyy myös ongelmia. Sähköpostipalveluntarjoajan tulee olla tietoinen käyttämiensä menetelmien eduista ja haitoista ja arvioida näiden vaikutukset ennen menetelmien käyttöönottoa.

Kaikille asiakkaille käytössä olevien, edellä mainitut kriteerit täyttävien, perustason tunnistusmekanismien lisäksi sähköpostipalveluntarjoaja voi tarjota asiakkailleen myös edistyneempiä ja pitemmälle räätälöityjä haitallisen liikenteen tunnistus- ja käsittelymekanismeja esimerkiksi erillisellä sopimuksella.

26.2 Suositukset haitallisen sähköpostiliikenteen tunnistamisesta

Sähköpostipalvelua tarjoavia teleyrityksiä suositellaan tekemään haitallisen sähköpostiliikenteen lähteiden tunnistamista jo SMTP-yhteydenottovaiheessa. Näin suuri osa haitallisesta sähköpostiliikenteestä on mahdollista estää jo ennen sen pääsyä sähköpostijärjestelmään. Toimenpiteellä on mahdollista vähentää merkittävästi haitallisen sähköpostiliikenteen aiheuttamaa kuormitusta sähköpostipalvelimilla.

Haitallisen sähköpostiliikenteen tunnistamisessa suositellaan käytettäväksi useita menetelmiä samanaikaisesti. Näin voidaan parantaa haitallisen sähköpostiliikenteen tunnistustarkkuutta ja käyttää siten myös esimerkiksi tiukempia suodatuskriteereitä.

Pääsylistojen käyttöä suositellaan väärien tulkintojen välttämiseksi, kun sähköpostipalveluntarjoajalla on käytössään esto- ja suodatusmenetelmiä.

26.3 Saapuvan sähköpostiliikenteen käsittely

Saapuvan sähköpostiliikenteen käsittelyllä tarkoitetaan toimenpiteitä, joita voidaan toteuttaa sähköpostipalveluntarjoajan vastaanottopalvelimien (MDA) tai välityspalvelimien kautta asiakkaille saapuville sähköpostiviesteille. Näitä toimenpiteitä ovat haitallisen sähköpostiliikenteen lähteiden ja haitallisen sähköpostiliikenteen tunnistaminen, haitalliseksi tunnistetulle liikenteelle tehtävät suodatus- ja merkitsemistoimenpiteet sekä liikenteen toimittaminen asiakkaalle.

Saapuvan sähköpostiliikenteen suodatuksella tarkoitetaan asiakkaille saapuvan tunnistetun haitallisen sähköpostiliikenteen pääsyn estämistä asiakkaiden sähköpostilaatikkoon. Suodattamalla haitalliset sähköpostiviestit voidaan vähentää sähköpostipalvelimien kuormitusta ja asiakkaiden sähköpostilaatikkoon päätyvän haitallisten sähköpostiviestien määrää ja näin helpottaa asiallisten viestien läpikäymistä. Samalla ehkäistään haitallisen sähköpostiviestien vaikutuksia esimerkiksi asiakkaiden avatessa sähköpostiviestien sisältämiä liitetiedostoja tai asiakkaiden ohjautuessa viestin linkin osoittamalle haittaohjelman sisältävälle sivustolle. Sähköpostiliikenteen suodatuksella voidaan parantaa asiakkaiden kokemaa palvelun laatua ja palvelun tietoturvaa.

Määräyksen mukaan sähköpostipalveluntarjoajan on merkittävä tai suodatettava saapuvasta sähköpostiliikenteestä sellainen sähköpostiliikenne, jonka se on käytössään olevien haitallisen sähköpostiliikenteen tai sen lähteiden tunnistusmekanismien avulla

määritellyt haitalliseksi. Automaattisen haitalliseksi havaitun liikenteen suodattamisen sijasta sähköpostipalveluntarjoaja voi myös esimerkiksi ohjata osan tai kaikki haitalliksi havaitsemistaan ja merkitsemistään viesteistä erilliseen haitalliselle sähköpostille tarkoitettuun käyttäjäkohtaiseen kansioon, jossa viestejä voidaan säilyttää esimerkiksi tietty määrä tai tietty aika käyttäjän tarkastettavana. Sähköpostipalveluntarjoaja voi myös poistaa viesteistä haitalliseksi tunnistamansa sisällön ennen viestin toimittamista asiakkaalle.

Palveluntarjoaja voi erikseen sopia asiakkaan kanssa, että haitalliseksi tunnistettua liikennettä ei suodateta tai merkitä haitalliseksi. Sähköpostipalveluntarjoaja ei siis voi oletusarvoisesti toteuttaa palvelua ilman haitalliseksi tunnistetun liikenteen suodatusta tai merkintää, eikä tätä vaihtoehtoa näin ollen voi sisällyttää oletukseksi vakiosopimuksiin.

Edellä mainituista poikkeuksista huolimatta sähköpostipalveluntarjoajan on kuitenkin aina suodatettava saapuvasta liikenteestä sellainen haitalliseksi tunnistettu sähköpostiliikenne, joka vaarantaa sähköpostipalvelun tuottamiseen käytettävien järjestelmien tietoturvaa (mukaan lukien käytettävyys).

26.4 Lähtevän sähköpostiliikenteen käsittely

Lähtevän sähköpostiliikenteen käsittelyllä tarkoitetaan toimenpiteitä, jotka voidaan suorittaa lähtevän sähköpostipalvelimen (MSA) kautta välitettäville sähköpostiviesteille. Näitä toimenpiteitä ovat oikeutettujen lähettäjien tunnistaminen sekä lähtevän sähköpostipalvelimen kautta lähtevän haitalliseksi tunnistetun sähköpostiliikenteen suodattaminen.

Määräyksen mukaan sähköpostipalvelua tarjoavan teleyrityksen on suodatettava lähtevästä sähköpostiliikenteestä haitalliseksi tunnistamansa liikenne. Tämän toteuttamiseksi teleyritys voi valita järjestelmässään käytettävät mekanismit eri vaihtoehdoista (ks. esimerkiksi tämän perustelumuistion liitteen luku 2). Tavoitteena on, että merkittävä osa lähtevästä haitallisesta sähköpostiliikenteestä tulee tunnistetuksi ja suodatetuksi kuitenkin siten, että asiallisten viestien läpimeno vaarantuu mahdollisimman vähän.

Mikäli sähköpostipalveluntarjoaja havaitsee, että sen asiakkaan päätelaitetta käytetään haitallisen sähköpostiliikenteen välitykseen, tulee sähköpostipalveluntarjoajan suodattaa asiakkaalta lähtevä haitallinen sähköpostiliikenne tai estää asiakkaan sähköpostiliikenne sekä ottaa mahdollisuuksien mukaan yhteyttä asiakkaaseen.

27. Avoimet sähköpostin välityspalvelimet

Avoimia sähköpostin välityspalvelimia (ks. määritelmä kohdasta 2.2) käytetään yleisesti haitallisen sähköpostiliikenteen välittämiseen.

Tunnistamalla avoimena toimivat sähköpostin välityspalvelimet ja estämällä kolmansien osapuolien sähköpostipalvelimien käyttö sähköpostiviestien välitykseen voidaan vähentää välitettyä haitallisen sähköpostiliikenteen määrää.

Sähköpostipalvelua tarjoavan teleyrityksen on huolehdittava siitä, että sen hallinnoimat sähköpostijärjestelmät eivät toimi avoimina sähköpostin välityspalvelimina. Järjestelmien ja palvelujen käyttöönoton ja muutosten yhteydessä suoritettavat testaustoimenpiteet sekä asetusten huolellinen määrittely ovat esimerkkejä sähköpostijärjestelmien käyttöturvallisuudesta huolehtimisesta.

Teleyrityksen tulisi säännöllisesti testata kaikki hallinnoimansa sähköpostijärjestelmät varmistuakseen siitä, etteivät järjestelmät toimi avoimina sähköpostin välityspalvelimina. Mikäli yritys ei ole hankkinut omaa testausjärjestelmää, se voi käyttää testaamiseen internetissä yleisesti saatavilla olevia julkisia palveluja.

Internetyhteyspalveluliittymään kuuluvan sähköpostin lähetyspalvelimen osalta tällä velvollisuudella tarkoitetaan sitä, että sähköpostien lähettäminen on mahdollista ilman tunnistusta vain kyseisen teleyrityksen omasta verkosta.

28. Asiakkaan ja sähköpostipalvelimen välinen yhteys

Asiakkaan ja sähköpostipalvelimen välisellä yhteydellä tarkoitetaan asiakkaan (MUA) ja sähköpostilaatikon (MS) välistä yhteyttä sekä asiakkaan (MUA) ja sähköpostin lähetyspalvelimen (MSA) välistä yhteyttä.

Asiakkaan ja sähköpostipalvelimen sekä asiakkaan ja sähköpostilaatikon välisien yhteyksien suojaamisella tarkoitetaan asiakkaan tunnistamista sekä edellä mainittujen asiakkaan ja palvelun välisten yhteyksien salaamista.

Asiakkaan ja sähköpostipalvelimen välillä välitetään käyttäjätunnuksia ja salasanoja. Asiakkaan ja palvelimen välisten yhteyksien suojaamisella voidaan estää näiden tietojen päätyminen kolmannen osapuolen tietoon sekä estää palvelun väärinkäyttöä ja parantaa palvelun tietoturvaa. Lisäksi asiakkaan ja palvelimen välisen yhteyden suojaamisella voidaan varmistaa asiakkaiden viestien säilyminen luottamuksellisena asiakkaan ja palvelimen välisessä liikenteessä. Yhteyden suojaamisella voidaan lisäksi tarjota asiakkaille turvallinen tapa käyttää sähköpostipalvelua liityntäverkkoriippumattomasti ja parantaa asiakkaiden kokemaa palvelun luottamuksellisuutta.

Asiakkaita on kuitenkin syytä tiedottaa siitä, että asiakkaan ja palvelimen välisen yhteyden suojaaminen ei kuitenkaan välttämättä tarkoita, että yhteys olisi suojattu päästä päähän, lähettäjältä vastaanottajalle.

Selainpohjaisten sähköpostipalvelujen (webmail) tyypillisten käyttötapojen vuoksi on perusteltua, että yhteydet ovat aina suojattuja.

Sähköpostipalveluntarjoajan on tarjottava asiakkaille ensisijaisena vaihtoehtona suojattu yhteys asiakkaan ja sähköpostilaatikon sekä asiakkaan ja lähtevän liikenteen sähköpostipalvelimen välillä. Velvoite koskee myös muita kuin selainpohjaisia sähköpostipalveluja.

Tällä velvollisuudella tarkoitetaan sitä, että teleyrityksen on tarjottava sähköpostipalvelun käyttäjille mahdollisuus suojattujen yhteyksien käyttöön ja että suojattujen yhteyksien käyttö ohjeistetaan asiakkaille joko ensisijaisena tai ainoana vaihtoehtona asiakkaille jaettavassa ja asiakkaiden saatavilla olevassa käyttöohjeistuksessa.

Oikeutettujen käyttäjien tunnistamiseksi ja suojatun asiakasyhteyden muodostamiseksi asiakkaalta sähköpostin välityspalvelimelle suositellaan käytettäväksi SMTP-AUTH-protokollaa.[106] Asiakkaan ja sähköpostilaatikkopalvelimen välillä tähän tarkoitukseen voidaan käyttää esimerkiksi SSL/TLS-protokollalla suojattuja IMAP- tai POP-yhteyksiä.[107]

[106] IETF RFC 4954, SMTP Service Extension for Authentication, https://tools.ietf.org/html/rfc4954.
[107] IETF RFC 2595, Using TLS with IMAP, POP3 and ACAP, https://tools.ietf.org/html/rfc2595 ja IETF RFC 4616, The PLAIN Simple Authentication and Security Layer (SASL) Mechanism, https://tools.ietf.org/html/rfc4616.

Käytettäessä porttia 25 sähköpostin lähettämiseen tai välittämiseen (releointiin) voidaan yhteyden suojaamiseen käyttää STARTTLS:ää myös, kun käyttäjää ei autentikoida.[108]

Selainpohjaisten sähköpostipalvelujen asiakasyhteydet on suojattava aina. Suositeltava suojausmenetelmä kuljetuskerrokselle on TLS-protokolla.[109]

Luku 7 Voimaantulosäännökset

Tässä luvussa käsitellään määräyksen lukua 7 eli voimaantulo- ja siirtymäsäännöksiä.

29. Voimaantulo [ja siirtymäaika]

[Määräys tulee voimaan kolme kuukautta määräyksen antamisesta.]

[108] IETF RFC 3207, SMTP Service Extension for Secure SMTP over Transport Layer Security, https://tools.ietf.org/html/rfc3207 ja IETF RFC 7817, Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols, https://tools.ietf.org/html/rfc7817.
[109] HTTPS-protokollaa käytettäessä ks. IETF RFC 2818, HTTP Over TLS, https://tools.ietf.org/html/rfc2818.

LIITE Määräyksen aihepiiriin liittyvät muut asiat

Tähän osaan on kerätty erilaisia teletoiminnan tietoturvaan liittyviä suosituksia, Liikenne ja -viestintäviraston tulkintoja ja muuta määräyksen kattamaa aihekokonaisuutta taustoittavaa materiaalia.

1. Harhauttavat sähköpostiosoitteet

Harhauttavat sähköpostiosoitteet luodaan harhauttamaan toista osapuolta luulemaan osoitteen omistajaa toiseksi henkilöksi tai tahoksi. Harhauttavalla sähköpostiosoitteella tarkoitetaan esimerkiksi toisen henkilön tai yrityksen nimellä, yritystunnuksella tai yleisesti tiedossa olevalla ylläpito-osoitteella (esimerkiksi postmaster, webmaster tai asiakaspalvelu) rekisteröityä sähköpostiosoitetta.

Mikäli sähköpostipalvelua tarjoava teleyritys havaitsee tai saa tietoonsa verkkotunnukselleen rekisteröidyn harhauttavan sähköpostiosoitteen, on teleyrityksen syytä puuttua ongelmaan. Teleyrityksellä on oikeus poistaa käytöstä osoitteet, jotka on perustettu harhauttavassa tarkoituksessa.

Sähköpostiosoite voi olla myös toisen henkilön henkilötieto. Henkilötietoja koskee henkilötietolain mukainen virheettömyysvaatimus ja siihen liittyvä henkilötiedon korjaamisen velvollisuus. Toisen henkilötietojen käyttö hyötymistarkoituksessa voi olla myös rikosoikeudellisesti rangaistavaa.

Liikenne- ja viestintävirasto suosittelee, että sähköpostipalvelua tarjoava teleyritys ei myönnä asiakkailleen sen omaan verkkotunnukseen liittyviä RFC 2142:ssa[110] määriteltyjä harhauttavia sähköpostiosoitteita tai niiden suomenkielisiä vastineita.

2. Haitallisen sähköpostiliikenteen tunnistusmekanismeja

Tässä luvussa esitellään erilaisia tunnettuja ja yleisesti käytössä olevia haitallisen sähköpostiliikenteen tunnistusmekanismeja.

2.1 Estolistaus

Estolistojen (block list) avulla voidaan tunnistaa ja suodattaa tai merkitä tunnetuista oikeudettomista sähköpostilähteistä saapuvat yhteydet tai sähköpostiviestit. Estolista koostuu yleensä haitallisen sähköpostiliikenteen lähteinä toimivista verkko-osoitteista.

Estolista voi koostua myös yksittäisistä roskapostin lähetykseen käytetyistä sähköpostiosoitteista, verkkotunnuksista tai sähköpostipalvelimista. Estolista voi olla sähköpostipalveluntarjoajan itsensä ylläpitämä, kolmannen osapuolen ylläpitämä tai käyttäjän henkilökohtainen. Sähköpostijärjestelmissä käytetään tavallisesti kolmannen osapuolen ylläpitämiä keskitettyjä estolistoja.

Estolistojen käytössä ja valinnassa tulee käyttää erityistä huolellisuutta virheellisten tulkintojen välttämiseksi. Staattiset estolistat ovat usein epäluotettavia, sillä haitallisen sähköpostiliikenteen lähteet vaihtuvat tiheään ja mahdollinen staattinen väärä tieto estolistalla estää pitkäkestoisesti asiallista sähköpostiliikennettä. Tiedon poistaminen staattiselta estolistalta vaatii aina käsin tehtävää työtä. Dynaamisesti ylläpidetyt estolistat sen sijaan päivittyvät nopeasti ja virheelliset listaukset tyypillisesti poistuvat listoilta säännöllisesti.

[110] IETF RFC 2142, Mailbox names for Common Services, Roles and Functions, https://tools.ietf.org/html/rfc2142.

Oman estolistan rakentaminen ei ole yleensä järkevää listan tietosisällön jatkuvan muuttumisen vuoksi. Sähköpostipalvelun käytettävyyden turvaamiseksi estolistoja käytettäessä on syytä välttää suuria verkkoalueita yksittäisten käyttäjien toimenpiteiden perusteella listaavia estolistoja. Lisäksi sellaisia estolistoja tulee välttää, jossa listalle joutumisen perusteet ovat epäselvät, listalta poispääsyyn ei ole selkeitä menettelyjä tai listan käyttöä ei suositella suurille palveluntarjoajille.

Kolmannen osapuolen ylläpitämää estolistaa valitessa sähköpostipalveluntarjoajan tulee kiinnittää erityistä huomiota seuraaviin listan ominaisuuksiin:

- Listausperiaatteiden julkaiseminen
- Listalta poisto on yksinkertaista ja hyvin opastettua
- Listan ylläpitäjän yhteystiedot on julkaistu
- Listaus ei perustu yhteen virheelliseen viestiin
- Listaa päivitetään säännöllisesti.

Estolistoja käytettäessä on huomioitava, että listat saattavat sisältää myös virheellistä tietoa ja näin ollen listan käyttäminen saattaa estää asiallista sähköpostiliikennettä. Käytettäessä kolmannen osapuolen ylläpitämää listaa tulee listan toimintaa seurata jatkuvasti. Eri listat sisältävät yleensä eri lähteitä, joten useamman listan yhtäaikainen käyttö antaa usein parhaan tuloksen. Sähköpostin vastaanottopalvelimelle eri lähteistä tulevan haitallisen liikenteen tunnistusprosentti kasvaa, kun eri listat tunnistavat toisistaan poikkeavia haitallisia lähteitä. Estolistoja voidaan käyttää myös osana sähköpostilähteen haitallisuuden pisteytystä heuristisessa suodatuksessa. Tällöin yksittäinen virheellinen listaus ei aiheuta asiallisen viestin suodatusta.

Käyttäessään estolistoja sähköpostipalveluntarjoajalla tulee olla käytössään toimiva mekanismi tunnettujen tärkeimpien asiallisten sähköpostilähteiden tunnistamiseksi. Määräyksen julkaisuhetkenä tällä tarkoitetaan pääsylistojen käyttöä. Sähköpostipalveluntarjoajan tulee listata olennaiset yhteistyökumppaninsa ja luotettavat kotimaiset palveluntarjoajat sähköpostijärjestelmässä estolistan ohittavien osoitteiden listalle (pääsylistalle) estolistan mahdollisesti aiheuttamien häiriöiden vaikutusten pienentämiseksi.

2.2 Pääsylistaus

Pääsylistalla (allow list) merkitään viestien vastaanotto sallituksi tiettyjen verkko-osoitteiden, sähköpostipalvelimien tai sähköpostiosoitteiden kautta, jotka tiedetään yleisesti luotetuiksi asiallisten viestien lähettäjiksi. Luotettuihin lähettäjiin voivat kuulua muun muassa tunnetut sähköpostipalveluntarjoajat ja yhteistyökumppanit.

Pääsylistan käyttö on käytännössä välttämätöntä käytettäessä muita sähköpostilähteeseen perustuvia esto- tai suodatusmenetelmiä. Pääsylistan avulla voidaan varmistaa viestien läpimeno luotetuista lähteistä, mikäli viestit tulisivat muuten suodatetuiksi esimerkiksi virheellisen estolistauksen seurauksena.

Pääsylistaa käytettäessä on huomioitava, että myös luotettujen tahojen kautta voidaan välittää haitallista sähköpostiliikennettä, joten myöskään pääsylistalla oleviin lähteisiin ei voi luottaa ehdoitta. Lisäksi esimerkiksi pääsylistattuja osoitteita voidaan väärentää haitallisen sähköpostiliikenteen viesteihin edistämään haitallisen sähköpostiliikenteen läpimenoa. Ongelmien välttämiseksi myös pääsylistalla olevien lähteiden lähettämiä viestejä tulee seurata.

Pääsylista on usein hyvin staattinen lista verkko-osoitteita. Palveluntarjoajan tulee huolehtia, että listalla olevat tiedot ovat ajantasaisia, jotta vältytään vanhentuneiden tietojen aiheuttamilta ongelmilta.

2.3 Seurantalistaus

Seurantalistaus (track list, tunnetaan myös nimellä greylist) perustuu haitallista sähköpostiliikennettä lähettävien ohjelmistojen toimintaan. Tavallisesta sähköpostijärjestelmästä poiketen nämä ohjelmistot eivät yritä lähettää viestiä uudestaan, vaikka viestin toimitus olisi epäonnistunut. Harmaalistauksessa tilastoidaan automaattisesti tiettyjä parametreja (saapuvan sähköpostin lähettäjän IP-osoite, osoitteen C-luokka, SMTP-lähettäjä ja SMTP-vastaanottaja) tai näistä muodostettu hash-taulu. Tuntemattomalta lähettäjältä/tietyillä parametreilla saapuvan viestin vastaanotosta kieltäydytään. Kun lähde yrittää viiveen jälkeen uutta lähetystä, viesti vastaanotetaan. Jatkossa ko. lähteestä viestit vastaanotetaan ilman viivettä.

Harmaalistauksen ongelmana on sen aiheuttama viive asiallisille sähköpostiviesteille, jotka saapuvat ennalta tuntemattomista lähteistä. Lisäksi harmaalistauksen toiminta perustuu haitallisen sähköpostiliikenteen lähettäjien yhden lähetyskerran periaatteeseen. Mikäli haitallisen liikenteen lähettäjät alkavat harmaalistauksen kiertääkseen yrittämään viestien lähetystä uudelleen, ei harmaalistaus enää toimi. Lisäksi sähköpostiviestien uudelleenlähetykset aiheuttavat lisää sähköpostiliikennettä, mikä kuormittaa sekä verkkoja että sähköpostipalvelimia.

2.4 Mainejärjestelmät

Mainejärjestelmät perustuvat viestin lähteen aiempaan lähetyshistoriaan. Sähköpostilähteiden (esim. lähettäjän IP-osoite ja SMTP-lähettäjä) lähettämiä viestejä seurataan, tilastoidaan ja vertaillaan lähteen aiempaan viestihistoriaan. Tilastoinnissa ja vertailussa kiinnitetään huomiota siihen lähettääkö lähde asianmukaisia sähköpostiviestejä vai haitallisia sähköpostiviestejä. Sähköpostilähteitä voidaan myös tarkkailla palvelimelta lähtevien viestien määrän perusteella. Tietoja hyödynnetään määrittämään sähköpostilähteen mainetaso pisteytyksen perusteella lähettäjän aiemman lähetys- ja viestihistorian perusteella. Mainetason perusteella tehdään päätös, toimitetaanko lähteestä tuleva viesti asianmukaisesti vastaanottajalle, toimitetaanko viesti vastaanottajalle alemmalla prioriteetilla vai estetäänkö viestin toimitus vastaanottajalle.

Mainejärjestelmien etuna on se, että ne hyödyntävät pitkäaikaista lähteiden seurantaa, eikä viestien suodatusta tapahdu yksittäisten asiattomien viestien perusteella. Mainejärjestelmät tukevat hyvin muita suodatusjärjestelmiä ja osana heuristista suodatusta mainejärjestelmän käyttö vähentää muun kriteeristön tekemiä virheitä. Mainejärjestelmien käytössä on kuitenkin otettava huomioon, ettei järjestelmän pisteytys välttämättä ehdi reagoida nopeaan haitallisen liikenteen tulvaan.

Kolmansien osapuolten ylläpitämät mainejärjestelmät keräävät pisteytyksen muodostamiseen tarvittavia tietoja omilta asiakkailtaan. Laajalti saaduista tiedoista kootaan yhtenäinen tietokanta pisteytystä varten mainetason määrittämiseksi.

2.5 Heuristinen analyysi

Sähköpostipalveluntarjoaja voi toteuttaa viestien haitallisuuden määrittämisen ja suodattamisen myös sähköpostiviestin sisältöön perustuvan analyysin avulla tai käyttää näitä menetelmiä sähköpostilähteiden tunnistamiseen käytettyjen menetelmien lisänä sähköpostiviestien suodatuksessa.

Haitallisten sähköpostiviestien sisältö yleensä täyttää tietyt ennalta tunnetut kriteerit. Viestin sisältöön perustuva suodattaminen voi tapahtua esimerkiksi vertaamalla viestistä laskettua tarkistussummaa tunnettuihin haitallisista viesteistä laskettuihin tarkistussummiin tai etsimällä viestistä haitallisuuteen viittaavia elementtejä, kuten tiettyjä sanoja, muotoiluja, liitetiedostoja, kuvia tai linkkejä. Sähköpostiviestistä voidaan myös

etsiä asiallisen sähköpostiviestin piirteitä. Sisältöön perustuvaan suodattamiseen voidaan yhdistää myös esimerkiksi estolistoihin perustuvia suodatusmenetelmiä.

Useita mekanismeja yhdisteltäessä kukin käytetty menetelmä joko lisää tai vähentää viestin haitallisuuden pistetasoa. Viestin saaman loppupistemäärän perusteella tehdään ratkaisu siitä, onko viesti haitallinen vai ei. Suoritetun analyysin perusteella suodatusohjelmisto joko estää viestin välityksen, merkitsee viestin todennäköisesti haitalliseksi tai välittää viestin eteenpäin sellaisenaan.

2.6 Poikkeava liikennemäärä

Poikkeavan liikennemäärän tunnistamiseksi sähköpostipalveluntarjoajan tulisi asettaa normaalikäytön raja-arvot. Mikäli lähtevän sähköpostiliikenteen määrä ylittää normaaliksi määritellyn lähetysrajan, voi sähköpostipalveluntarjoaja estää asiakkaan sähköpostiliikenteen väliaikaisesti. Lisäksi sähköpostipalveluntarjoajan on mahdollisuuksien mukaan otettava yhteyttä asiakkaaseen, jolloin asiakas voi tehdä tarvittavat toimenpiteet tilanteen korjaamiseksi esimerkiksi puhdistamalla saastuneen koneensa.

2.7 Muita sähköpostin turvallisuutta ja luotettavuutta parantavia menetelmiä

Edellisissä luvuissa mainittujen mekanismien lisäksi sähköpostipalveluntarjoajalla on mahdollisuus valita lukuisia muita menetelmiä sähköpostin turvallisuuden ja luotettavuuden parantamiseksi.

Sähköpostin lähettäjän aitouden tarkistamisen keinoihin kuuluvat mm. Sender Policy Framework (SPF)[111] ja Domain Keys Identified Mail (DKIM),[112] joiden avulla voidaan tunnistaa, että sähköpostiviesti on lähtenyt sähköpostiosoitteen osoittamalta verkkotunnuksen sähköpostipalvelimelta. Näiden lisänä voidaan ja on suositeltavaa käyttää DMARC protokollaa, jolla pystytään seuraamaan ja määräämään se, miten verkkotunnuksen nimissä lähetettyjä viestejä käsitellään ja mitkä varmennusmenetelmät viestin tulisi läpäistä. DMARC tuo lisänä myös raportointiominaisuuden, jolla voidaan seurata, miten lähetyksiä on läpäisty ja hylätty.

SPF käyttöönotetaan nimipalvelun (DNS) avulla. Nimipalveluun julkaistaan tekstityyppinen nimitietue, johon määritellään parametreina ne auktorisoidut sähköpostipalvelimet, joiden on sallittua lähettää sähköpostia kyseisen verkkotunnuksen tai alemman tason verkkotunnuksen nimissä. Sähköpostin välityspalvelin (MTA) vahvistaa vastaanotetun viestin alkuperän sen paluusuunta (return path) -otsakekentästä DNS:ssä julkaistujen tietojen kanssa ja soveltaa viestille määriteltyä käsittelykäytäntöä, joka johtaa joko kyseessä olevan viestin hyväksymiseen, hylkäämiseen tai viestin siirtämiseen karanteeniin. SPF:n heikkous on se, että se tarkistaa ainoastaan return path -otsakekenttää eikä esimerkiksi lähettäjä (from) -otsakekenttää, jonka vuoksi haitallinen lähettäjä voi silti manipuloida viestin kirjekuorta ja yrittää näin hämätä viestin vastaanottajaa. Tämä mahdollistuu, koska peruskäyttäjä tavallisesti tarkastelee ainoastaan lähettäjäkenttää yksityiskohtaisempien otsakekenttien ollessa oletuksena piilotettuja. Tämä heikkous voidaan korjata käyttämällä SPF:n lisäksi toista sähköpostin todennusprotokollaa DMARC:ia.

DKIM tarjoaa sähköposteihin menetelmän viesteihin liittyvän digitaalisen identiteetin, joka tyypillisesti on lähettäjän toimialue, vahvistamiseksi kryptografisesti. Lisäksi menetelmällä pyritään varmistamaan, ettei viestin sisältöön ole kajottu lähettämisen jäl-

[111] IETF RFC 7208, Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, https://tools.ietf.org/html/rfc7208.
[112] IETF RFC 6376, DomainKeys Identified Mail (DKIM) Signatures, https://tools.ietf.org/html/rfc6376.

keen. DKIM-menetelmä perustuu digitaalisen allekirjoituksen ja avainparin yhdistelmään. Viestien otsakkeeseen lisätään digitaalinen allekirjoitus, joka salataan yksityisellä avaimella ja lisäksi lähettävän verkkotunnuksen DNS-tietoihin lisätään julkinen avain, jolla viestien vastaanottajien on mahdollista purkaa tiedot. DKIM-allekirjoitus ei yksinään merkittävästi lisää tai vähennä viestin kiistämättömyyttä, mutta viestiin liitetty allekirjoitus on kuitenkin tärkeä tieto sähköpostin mainearviointijärjestelmille ja erityisesti viestiä koskevalle päätöksenteolle ja siten DKIM:iä tulisikin käyttää yhdessä muiden sähköpostin luotettavuutta parantavien menetelmien kanssa.

Kuten SPF ja DKIM, perustuu myös DMARC:in käyttö DNS:ään, eli DMARC-tietueet luodaan muiden todennusprotokollien tapaan nimipalveluun. DMARC:lla voidaan määrittää pakolliseksi se, että viestin on läpäistävä SPF- ja DKIM-validoinnit. DMARC:in avulla on myös mahdollista varmistaa, että käyttäjälle näkyvässä From-kentässä oleva verkkotunnus vastaa sitä verkkotunnusta, mitä on käytetty SPF- ja DKIM-todennuksissa.

Kuten muissakin haitallisen sähköpostiliikenteen torjuntakeinoissa, myös näissä mekanismeissa on joukko heikkouksia, jotka tulee ottaa huomioon otettaessa menetelmiä käyttöön. DKIM-mekanismia koskien asiaa on kuvattu muun muassa RFC:ssä 4686[113]. Koska esimerkiksi sähköpostin välityspalvelut, verkkopostikortit ja internetyhteyspalveluntarjoajien lähetyspalvelut rikkovat näiden mekanismien toimintaa, soveltuvat mekanismit parhaiten vain lähteen positiiviseen tunnistamiseen.

Ennen uusien menetelmien käyttöönottoa sähköpostipalveluntarjoajan tulee perehtyä tarkoin menetelmän toimintaperiaatteisiin ja riskeihin virheellisten asiallisten sähköpostiviestin suodattamisen välttämiseksi. Usein yksittäisten menetelmien toimintatarkkuus on epävarmaa, mikäli menetelmän antamaan tulkintaan liikenteen haitallisuudesta luotetaan varauksettomasti. Sen sijaan käytettäessä useita menetelmiä yhtäaikaisesti osana pisteytysjärjestelmää voidaan saada hyvinkin täsmällisiä suodatustuloksia pienellä virhemarginaalilla.

3. Haittaohjelmaliikenteen estäminen haittaohjelman päivittämiseen käytettäviin verkkotunnuksiin tai IP-osoitteisiin

Silloinen Viestintävirasto sai vuonna 2009 tietoonsa useita satoja Conficker/Downadup-matotartuntaepäilyjä suomalaisista verkoista. Maailmalla matotartunnan saaneita koneita arvioitiin olevan useita miljoonia. Verkkomadon toimintaa tutkittaessa saatiin selville madon päivittämiseen käytettävä tapa: Tartunnan jälkeen mato luo päivämäärän perusteella satunnaisia verkkotunnuksia, joihin se yrittää ottaa yhteyttä päivittääkseen itsensä. Osa tartunnan saaneista päätelaitteista pystyttiin selvittämään rekisteröimällä joitakin madon käyttämiä verkkotunnuksia ja seuraamalla niihin suuntautuvaa verkkoliikennettä. Tiedot tartunnan saaneiden päätelaitteiden osoitteista toimitettiin verkkojen ylläpitäjille.

Viestintävirasto katsoi tulkinnassaan (dnro 46/64/2009), että teleyritykset voivat pienentää merkittävästi matotartuntojen aiheuttamaa tietoturvauhkaa estämällä madon liikennöinti sen päivittämiseen käytettäviin verkkotunnuksiin. Liikennöinnin estäminen tekee madon päivittämisestä ja murretun järjestelmän hyödyntämisestä merkittävästi vaikeampaa. Viestintäviraston tulkinnan mukaan liikenteen estämistä haittaohjelman päivittämisverkkotunnuksille voitiin pitää (nykyisin SVPL 272 §:ssä tarkoitettuna) välttämättömänä toimena verkkopalvelujen tai viestintäpalvelujen turvaamiseksi.

Jos teleyritys haluaa tunnistaa sen verkossa olevat saastuneet päätelaitteet, voi liikenteen estäminen tapahtua esimerkiksi antamalla muokattu vastaus saastuneen pääte-

[113] IETF RFC 4686, Analysis of Threats Motivating DomainKeys Identified Mail (DKIM), https://tools.ietf.org/html/rfc4686.

laitteen teleyrityksen resolverinimipalvelimille tekemään nimipalvelukyselyyn. Muokatun vastauksen IP-osoitteeksi voidaan valita esimerkiksi vapaa IP-osoite teleyrityksen omasta IP-osoiteavaruudesta.

Viestintäviraston tulkinnan mukaan teleyrityksillä oli oikeus tallentaa haittaohjelman päivittämiseen käytettäviin verkkotunnuksiin suuntautuvan liikenteen lähdeosoitteet ja selvittää lähdeosoitetta käyttävä tilaaja. Tilaajan selvittämiseksi teleyritys sai käsitellä myös muussa yhteydessä kertyneitä välitystietoja. Kerätyt välitystiedot oli tuhottava heti, kun niiden käsittelylle ei ole enää perustetta. Välitystietoja voitiin luovuttaa kolmansille osapuolille ainoastaan laissa yksilöidyillä perusteilla.

Vuonna 2021 Liikenne- ja viestintäviraston Kyberturvallisuuskeskus taas suositteli teleyrityksille matkapuhelimiin leviävän Flubot-haittaohjelman aktiivisten komentopalvelimien IP-osoitteiden suodattamista.[114] Tapauksessa haittaohjelma käytti salattua DNS-liikennettä, joten liikenteen estäminen käytettyihin verkkotunnuksiin ei tuossa tapauksessa ollut tehokas keino suodatukseen.

4. SMS-liikenteen suodattaminen haittaohjelman leviämisen estämiseksi

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus suositteli vuonna 2021 matkaviestinverkon teleyrityksille SMS-viestien suodattamista sisällön perusteella Flubot-haittaohjelman leviämisen estämiseksi.[115] Haittaohjelma pyrki leviämään lähettämällä tekstiviestejä, jotka sisälsivät linkkejä haittaohjelmaan, joka käyttäjä pyrittiin saamaan asentamaan puhelimeensa.[116] Tällaiseen suodatukseen liittyvä viestin sisällön käsittely oli mahdollista toteuttaa SVPL 272 §:n puitteissa.

5. Liikenteen suodattaminen maksuvälinepetosten valmistelun ehkäisemiseksi

Silloisen Viestintäviraston tietoon tuli vuonna 2009 tapauksia, joissa suomalaisten verkkopankkiasiakkaiden verkkoliikennettä oli ohjattu käyttäjän tietämättä kolmannen osapuolen ylläpitämälle www-palvelimelle. Ohjaus oli toteutettu muokkaamalla DNS-asetuksia käyttäjän päätelaitteelle asentuneella haittaohjelmalla: Muokkaamisen jälkeen päätelaite käyttää verkkotunnusten IP-osoitteiden selvittämiseen haittaohjelman ylläpitäjän määrittelemiä DNS-palvelimia. Toimenpiteeseen käytettiin todennäköisesti DNS changer -tyyppistä haittaohjelmaa (esimerkiksi Zlob).

Viestintäviraston tulkinnan (dnro 1952/64/2009) mukaan teleyritykset saattoivat nykyistä SVPL 272 §:ää vastaavan sääntelyn nojalla suodattaa tapauskohtaisesti yksilöidyille verkkoalueille suuntautuvan liikenteen viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseksi. Suodattaminen on perusteltua myös tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi.

SVPL:n mukaan välitystietoja saa käsitellä siinä määrin kuin se on tarpeen verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun toteuttamiseksi ja käyttämiseksi sekä laissa säädetyllä tavalla tietoturvasta huolehtimiseksi. Teleyrityksen verkossa olevat saastu-

[114] FICORA #1157426 Suositus internetyhteyspalveluliikenteen suodattamisesta, 8.6.2021.
[115] FICORA #1176113 Suositus tekstiviestiliikenteen suodattamisesta, 25.11.2021.
[116] Traficom, Julkaisimme vakavan varoituksen tekstiviestitse levitettävästä haittaohjelmasta, https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/julkaisimme-vakavan-varoituksen-tekstiviestitse-levitettavasta-haittaohjelmasta.

neet päätelaitteet vaarantavat teleyrityksen palvelujen tietoturvaa. Siten haittaohjelmatartunnan saaneiden päätelaitteiden selvittämistä voidaan pitää välttämättömänä palvelun toteuttamiseksi ja sen tietoturvasta huolehtimiseksi.

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

6. Ethernet-rajapintojen tietoturvaa koskevia suosituksia

Tässä luvussa käsitellään muutamia tärkeimpiä Ethernet-tekniikkaan liittyviä viestintäverkkojen ja -palvelujen toimintaan vaikuttavia tietoturvaongelmia sekä esimerkkejä niiden torjumista. Kuvatut esimerkit käsittelevät tilanteita, joissa teleyrityksen verkko on toteutettu perinteisellä kytkinratkaisulla. Esitetyt ongelmat eivät siten pääsääntöisesti koske esimerkiksi MPLS- tai pseudowiretunnelointia käyttäviä verkkoja.

Vaikka tässä määräyksessä aiheesta ei anneta yksityiskohtaisia velvoitteita, Liikenne- ja viestintävirasto suosittelee, että teleyritykset varautuvat myös tässä luvussa mainittuihin uhkiin toteuttaessaan tarvittavia suojausmekanismeja.

6.1 Lähetysmyrskyt

Lähetysmyrsky syntyy, kun yhteislähetysviestejä lähetetään liikaa verkkoon yhteenliittämisrajapinnan portista. Lähetysmyrsky voi saattaa yhteenliittämisrajapinnan käyttökelvottomaksi, mikäli yhteislähetysviestit täyttävät yhteenliitetyn verkon kapasiteetin. Tästä syystä yhdysliikennettä harjoittavien osapuolten tulee varautua lähetysmyrskyjen vaikutusten rajoittamiseen. Rajoitus voidaan toteuttaa esimerkiksi rajoittamalla levitysviestien saamaa kapasiteettia verkossa.

Liikenne- ja viestintävirasto suosittelee, että yhdysliikennerajapinnoissa käytettäisiin vain sellaisia kytkimiä, jotka tukevat niin sanottua storm control -suodatusta. Tämän suodatuksen avulla on mahdollista rajoittaa tietty osuus linjakapasiteetista yksittäislähetys- ja yleislähetysliikenteelle. Suodattimen asetukset pitää tehdä niin, että suodatuksesta ei aiheudu haittaa verkon normaalille liikenteelle.

6.2 L2-ohjausprotokollat

Spanning Tree -protokollalla (STP) operaattori voi estää silmukoiden synnyn omassa L2-verkossaan. Protokolla voi tuottaa myös merkittäviä ongelmia väärin käytettynä. Myös monet valmistajakohtaiset protokollat kuten Ciscon protokollat CDP tai VTP voivat aiheuttaa vastaavia ongelmia. Pahimmillaan asiakas voi tahallisesti tai tahattomasti kaataa tarjotun palvelun tai ohjata liikennettä oikeudettomasti oman liittymänsä kautta, mikä mahdollistaa esimerkiksi liikenteen salakuuntelun ja liikenteen muokkaamisen. STP ja valmistajakohtaiset protokollat tuleekin eristää ohjaustasolla.

6.3 VLAN hopping

Kahdella VLAN-tunnisteella (Double Tag VLAN) varustetuilla paketeilla voidaan lähettää palvelunestoliikennettä asiakasportista kytkimen runkoyhteyden kautta muiden kytkimien takana oleviin VLAN:eihin. Tämä on mahdollista, koska natiiviliitännässä kytkin ottaa tyypillisesti pois vain ulommaisen VLAN-tunnisteen, jolloin pakettiin jää jäljelle vielä toinen VLAN-tunniste. Kaksisuuntaisen yhteyden muodostaminen ei onnistu, mutta tällä tavalla on mahdollista tehdä palvelunestohyökkäys jonkin toisen palvelun tai asiakkaan porttiin.

Uhkan realisoitumisen estämiseksi verkko-operaattorin on varmistettava, että tilaajakytkimen runkoportissa sallitaan vain tilaajalla käytössä olevat VLAN:it. Yhteenliittämisrajapinnassa verkko-operaattorin tulee sallia vain palveluoperaattorin kanssa sovittu VLAN-alue. Myös kytkimien määrä reitittävien laitteiden ja asiakaslaitteiden välillä suositellaan pidettäväksi minimissä.

6.4 MAC-osoitteiden käytön hallinta ja suodatus

MAC-osoitteiden käytön hallinta ja suodatus ovat verkonsuojausmenetelmiä, jotka ovat tarpeen suojauduttaessa teleliikenteen häiritsemiseltä ja laiterikkojen aiheuttamilta vikatilanteilta. Jos asiakas saa täytettyä kytkimen MAC-taulun, kytkin levittää kaikki paketit jokaiseen kytkimen porttiin, jolloin jokainen kytkimeen kytketty laite näkee kaiken kytkimen kautta kulkevan asiakasliikenteen. Kytkimissä ja DSLAM:eissa MAC-taulun rajattu koko on siis yksi tunnetuista tietoturvauhista.

Edellä mainitun ongelman vakavuus riippuu kuitenkin käytetystä tekniikasta. Teleyritys voi esimerkiksi vähentää edellä kuvattuja ongelmia hyödyntämällä Provider Backbone Bridging -tekniikkaa (802.1ah).[117] Ongelma voidaan estää myös rajoittamalla porttikohtaisten MAC-osoitteiden määrä ja sallimalla liikenne vain opittuihin oikeisiin MAC-osoitteisiin. Vanhemmissa tai edullisimmissa kytkimissä ei ole aina mahdollista estää MAC-taulujen täyttämistä asiakasporteista.

Edellä mainittu ongelma koskee myös Ethernet-verkon mitoituksia terminointireitittimen ja asiakaspäätelaitteen välissä. Verkko- ja palveluoperaattorin tulisikin olla mahdollista hallita porttikohtaisesti (tilaajakytkin tai yhteenliittämisrajapinta) aktiivisten MAC-osoitteiden määrää.

7. Suosituksia tietoturvaan liittyvästä tiedottamisesta

7.1 Yleinen tiedottaminen tietoturvariskeistä ja asiakkaan käytettävissä olevista suojakeinoista

Huonosti ylläpidetyt päätelaitteet ja huolimaton palvelujen käyttö vaarantavat asiakkaan oman päätelaitteen tietoturvan lisäksi myös teleyrityksen tarjoamien palvelujen ja muiden käyttäjien tietoturvan.

Teleyrityksiä suositellaan tuottamaan asiakkaille etukäteistietoa siitä, miten viestintäpalvelua tai liittymää tulee käyttää tietoturvallisesti. Teleyrityksen asiakkaisiin kohdistamalla yleisellä tietoturvatiedotuksella lisätään asiakkaiden tietoisuutta verkkojen ja palvelujen yleisistä tietoturvariskeistä. Merkittävä osa raportoiduista asiakkaiden tietoturvaongelmista voidaan välttää, jos asiakas on asianmukaisesti huolehtinut päätelaitteiden perustietoturvasta ja palveluja käytetään tietoturvauhat huomioiden.

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

Teleyritys voi käyttää tiedottamiseen erilaisia tapoja. Tiedottaminen on mahdollista järjestää esimerkiksi yhteyden käyttöönoton mahdollistavalla kirjautumissivulla tai ohjaamalla asiakas tietylle verkkosivulle. Teleyritys voi oman asiakastiedotuksen lisäksi ohjata asiakkaan Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen sivustolle.

[117] IEEE Standards Association, IEEE Std. 802.1ah - Provider Backbone Bridges, https://www.ieee802.org/1/.

Tiedottamisessa tulee painottaa asiakkaan tai asiakasliittymän käyttäjän käytettävissä olevia keinoja oman päätelaitteensa tietoturvallisuudesta huolehtimiseksi. Tällaisia keinoja ovat esimerkiksi liikenteen salaaminen, käyttäjien liikenteen eriyttäminen, palomuurin käyttöönotto ennen tietokoneen liittämistä verkkoon, virustorjunnan hankkiminen ja käyttöjärjestelmän sekä muiden ohjelmistojen päivittäminen.

Tarvittaessa tiedottamisessa tulee keskittyä liittymätyyppikohtaisiin tietoturvariskeihin, joilla tarkoitetaan liittymän teknisestä toteutustavasta johtuvia erityisiä riskejä. Esimerkkinä riskistä voidaan mainita internetyhteyspalvelun tarjoaminen salaamattoman WLAN-yhteyden avulla. Tällaisissa tilanteissa teleyrityksen on tiedotettava liittymän käyttämiseen liittyvistä viestinnän luottamuksellisuuteen kohdistuvista erityisistä riskeistä. Tietoturvariskejä voi liittyä myös liittymiin, jossa käyttäjät jakavat kapasiteettia.

Asiakkaan ohjeistamista koskee myös SVPL 246.3 §. Sen mukaan tilaajan on ylläpidettävä yleiseen viestintäverkkoon liitettävää laitetta tai järjestelmää teleyrityksen antamien ohjeiden mukaisesti siten, ettei se vaaranna yleisen viestintäverkon ja -palvelun tietoturvallisuutta. Lisäksi SVPL 274.2 §:ssä säädetään teleyrityksen velvollisuudesta kertoa käytettävissä olevista suojautumistoimenpiteistä, kun teleyritys ilmoittaa tilaajalle tai käyttäjälle teleyrityksen palveluun kohdistuvasta tietoturvaloukkauksesta tai sen uhasta.

7.2 Yleinen tiedottaminen tietoturvatoimenpiteistä

Teleyrityksiä suositellaan tuottamaan asiakkaille etukäteistietoa siitä, millaisia toimia voi seurata mahdollisesta yleisen viestintäverkon tai -palvelun tietoturvaa vaarantavasta käytöstä.

Valtioneuvoston asetuksessa ennen viestintäpalvelusopimuksen tekemistä annettavista tiedoista (96/2021) säädetäänkin, että teleyrityksen on annettava kuluttajalle ennen viestintäpalvelusopimuksen tekemistä tiedot palveluntarjoajan toimista tietoturvan vaarantuessa tai tietoturvauhkien tai -haavoittuvuuksien ilmetessä (1 §:n 6 kohta). Teleyrityksen olisi kuvattava asiakkaille myös yleiset periaatteet, joilla puututaan viestintäpalvelujen tietoturvaa vaarantavaan liittymän tai palvelujen käyttöön. Tämä tarkoittaa, että asiakkaalle kerrotaan esimerkiksi siitä, että jos liittymään on kytketty saastunut päätelaite, liittymä saatetaan sulkea tilapäisesti.

7.3 Tiedottaminen haavoittuvasta asiakaslaitteesta

Viestintäpalvelujen käyttäjillä voi olla merkittävä rooli viestintäverkkoihin ja -palveluihin liittyviltä tietoturvauhilta suojautumisessa.[118]

SVPL 274 §:ssä säädetään teleyrityksen häiriöilmoituksista tilaajalle ja käyttäjälle tilanteessa, jossa teleyrityksen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus taikka muu tapahtuma, joka estää viestintäpalvelun toimivuuden tai häiritsee sitä olennaisesti. SVPL 246 §:n 3 momentissa taas säädetään, että tilaajan on ylläpidettävä yleiseen viestintäverkkoon liitettävää laitetta tai järjestelmää teleyrityksen antamien ohjeiden mukaisesti siten, ettei se vaaranna yleisen viestintäverkon ja -palvelun tietoturvallisuutta.

Haavoittuvat asiakaslaitteet muodostavat uhan sekä asiakkaan että teleyrityksen viestintäverkkojen ja -palvelujen tietoturvalle. Etenkin 5G-verkkojen laitemäärien moninkertaistuessa on hyvä varautua myös verkon kontrollien avulla signalointimyrskyihin tilanteessa, jossa suuri määrä haavoittuvia asiakaslaitteita saastuu haittaohjelman

[118] ENISA GL SO29 koskee käyttäjien tiedottamista tietoturvauhista sekä käyttäjän käytettävissä olevista toimenpiteistä niiltä suojautumiseksi.

vuoksi. Lisäksi on hyvä kiinnittää huomiota haavoittuvien laitteiden päivittämiseen tai poistamiseen viestintäverkosta.

Liikenne- ja viestintävirasto suosittelee, että teleyritys tiedottaa asiakastaan tullessaan tietoiseksi asiakkaan haavoittuvasta päätelaitteesta, jonka haavoittuvuus uhkaa asiakkaan tai teleyrityksen viestintäverkon tai -palvelun tietoturvaa, niissäkin tapauksissa, joissa velvollisuutta tähän ei olisi lain nojalla. Tietoturvaa vaarantaviin haavoittuvuuksiin voidaan tapauksen mukaan puuttua myös SVPL 272 ja 273 §:n sekä määräyksen 22 ja 23 kohdan mukaisin keinoin.

7.4 Sähköpostipalvelun suodatusperiaatteiden kuvaaminen

Asiakkaalla on oikeus saada tietoa sähköpostipalvelua tarjoavan teleyrityksen käyttämistä suodatusperiaatteista.[119]

Sähköpostiliikenteen suodatus aiheuttaa usein asiakastiedusteluja palveluntarjoajalle, mikäli asiallisia sähköpostiviestejä tulee virheellisesti suodatetuksi tai esimerkiksi asiakkaan sähköpostilaatikkoon saapuvan haitallisen sähköpostiliikenteen määrä kasvaa merkittävästi. Koska haitallisen sähköpostiliikenteen tunnistaminen ja suodattaminen tai merkitseminen on välttämätöntä sähköpostipalvelun toimivuuden ja käytettävyyden turvaamiseksi, tiedottamalla asiakkaita käytössä olevista sähköpostiliikenteen suodatuksen perusperiaatteista voidaan välttää väärinkäsityksiä ja turhia asiakasvalituksia.

Teleyrityksen on suositeltavaa kuvata asiakkaalle käyttämänsä yleiset sähköpostin suodatusperiaatteet. Kuvauksen tarkoituksena on kertoa asiakkaalle yleisellä tasolla käytettävistä suodatusmenetelmistä ja niiden vaikutuksesta asiakkaan liikennöintiin. Suodatusperiaatteiden kuvaaminen asiakkaalle ei saa kuitenkaan vaarantaa viestintäpalvelun tietoturvallisuutta. Kuvauksen ei tarvitse olla tarpeettoman yksityiskohtainen ja kertoa tarkkoja perusteita esimerkiksi siitä, miksi yksittäinen sähköpostiviesti tulkitaan sisällön perusteella haitalliseksi liikenteeksi. Esimerkiksi estolistoja käytettäessä sähköpostipalveluntarjoajan ei tarvitse luetella suodatuksessa käytettäviä estolistoja yksityiskohtaisesti, sillä käytettävät listat saattavat vaihdella tilanteesta riippuen.

7.5 Sähköpostiosoitteiden hallinnan kuvaus

Sähköpostiosoitteiden hallinnointikäytännöt vaihtelevat eri palveluntarjoajien kesken. Hallinnointikäytäntöjen määrittelyllä ja kuvaamisella asiakkaille voidaankin välttää väärinkäsityksiä ja nopeuttaa ongelmatilanteiden ratkaisua.

Sähköpostipalvelua tarjoavan teleyrityksen on suositeltavaa kuvata asiakkaille käyttämänsä sähköpostiosoitteiden hallinnointikäytännöt. Kuvauksen avulla asiakkaan tulee saada selville, kuinka hän voi saada uuden sähköpostiosoitteen käyttöönsä, muokata sähköpostipalvelun asetuksia ja poistaa sähköpostiosoitteen käytöstä.

[119] Välitystietojen käsittelystä annettavista tiedoista ks. SVPL 138.2 §. Ks. myös edellä mainitun valtioneuvoston ennen viestintäpalvelusopimuksen tekemistä annettavista tiedoista antaman asetuksen (96/2021) 1 §:n 6 kohta.