Teletoiminnan tietoturvasta annetun määräyksen (Viestintävirasto 67 A/2015 M) ajantasaistaminen: Kysely kokemuksista ja kehitysideoista

Traficom/16241/09.09/2022

Johdanto

Liikenne- ja viestintävirasto Traficom kartoittaa tällä kyselyllä näkemyksiä teletoiminnan tietoturvaa koskevan nykyisen määräyksen Viestintävirasto 67 A/2015 M velvoitteiden toimivuudesta sekä mahdollisista muutostarpeista käynnistettyä määräyshanketta varten.

Tausta

Traficom on päättänyt käynnistää määräyshankkeen, jossa ajantasaistetaan 4.3.2015 voimaan tullut Viestintäviraston määräys teletoiminnan tietoturvasta (Viestintävirasto 67 A/2015 M).

Määräystä tarkastellaan kaikkien viestintäverkkojen ja -palvelujen osalta, mutta erityisesti tarkoituksena on huomioida 5G-teknologian uudet arkkitehtuuriratkaisut, matkaviestinverkkojen uudet käyttötapaukset ja niihin liittyvät tietoturvavaatimukset. Matkaviestinverkkojen ja -palvelujen osalta mahdollisia määräyksen tarkentamistarpeita aiheuttavia viimeaikaisia kehityskulkuja ovat muun muassa verkon monimuotoistuminen, uusien rajapintojen avaaminen, virtualisointi, pilvipalvelujen käyttö sekä laitetilojen monimuotoistuminen. Lisäksi hankkeessa huomioidaan sidosryhmiltä saatu palaute sekä valvonta- ja tarkastustoiminnassa saadut muut kokemukset määräyksen päivitystarpeista.

Määräys koskee yleistä teletoimintaa ja sen tarkoituksena on:

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

Tavoitteet

Kyselyn tavoitteena on kerätä kokemuksia ja kehitysideoita nykyisen määräysversion osalta sekä pyytää näkemyksiä eräistä uusista asiakohdista, joiden tarpeellisuutta ja sisältöä tullaan erityisesti arvioimaan määräyksen päivittämisen yhteydessä.

Linkit

Määräys teletoiminnan tietoturvasta (Viestintävirasto 67 A/2015 M):
https://www.finlex.fi/data/normit/44046/M67A_2015.pdf

Määräyksen 67 perustelut ja soveltaminen:
https://www.finlex.fi/data/normit/44046/M67A_MPS_2015.pdf

Kansainvälisesti toteutetun palvelun tietoturvasta tiedottaminen:
Suositus_205_2014_S_(kansainvälisesti_toteutetun_palvelun_tietoturvasta_tiedottaminen).pdf (kyberturvallisuuskeskus.fi)

Tiettyihin tietoliikenneportteihin suuntautuvan liikenteen tietoturvaperusteinen suodattaminen teleyritysten verkoissa (Liikenne- ja viestintäviraston suositus 312/2020 S): Suositus3122020.pdf (kyberturvallisuuskeskus.fi)

Aikataulu

Vastaukset pyydetään toimittamaan Liikenne- ja viestintävirastolle lausuntopalvelu.fi-verkkosivuston kautta **viimeistään 31.8.2022.**

Vastausohjeet

Kysely noudattaa pääosin voimassaolevan määräyksen rakennetta. Vastauksissa voi tuoda esiin määräykseen liittyviä kehitys- tai muutostarpeita sekä yleisesti että yksittäisten velvoitteiden osalta. Kyselyyn sisältyy useita tarkempia kysymyksiä tiettyjen määräyksen kohtien kehittämistarpeista. Useiden määräyskohtien osalta tiedustellaan näkemyksiä eräistä mahdollisista kehittämistarpeista, mutta myös muiden kohtien osalta toivotaan vastaajien kokemuksia ja uusia kehitysideoita.

Toivomme vastauksia sekä yleisesti erilaisia viestintäverkkoja- tai palveluita koskien sekä tarkemmin tiettyjen palveluiden tai verkkoteknologioiden erityispiirteiden osalta (kuten internetyhteyspalvelu tai 5G-matkaviestinverkko).

Liikenne- ja viestintävirasto varaa teille mahdollisuuden antaa lausuntonne asiasta joko suomen tai ruotsin kielellä. Halutessanne lausunnon voi antaa myös englannin kielellä.

Lausunnot pyydetään antamaan vastaamalla lausuntopalvelu.fi:ssä julkaistuun lausuntopyyntöön. Lausuntoa ei tarvitse lähettää erikseen sähköpostitse tai postitse viraston kirjaamoon.

Lausunnon antaakseen vastaajan tulee rekisteröityä ja kirjautua lausuntopalvelu.fi:hin. Tarkemmat ohjeet palvelun käyttämiseksi löytyvät lausuntopalvelu.fi:n sivulta Ohjeet > Käyttöohjeet. Palvelun käyttöönoton tukea voi pyytää osoitteesta lausuntopalvelu.om@gov.fi.

Kaikki annetut lausunnot ovat julkisia ja ne julkaistaan lausuntopalvelu.fi:ssä. Mikäli vastauksenne sisältää tietoja, jotka yrityksenne katsoo liikesalaisuuden tai muun seikan perusteella salassa pidettäviksi, pyydetään nämä tiedot toimittamaan erillisellä asiakirjalla ja lähettämään turvasähköpostilla Liikenne- ja viestintäviraston kirjaamoon osoitteeseen kirjaamo@traficom.fi käyttäen viitteenä diaarinumeroa Traficom/16241/09.09/2022. Ohjeistuksen turvasähköpostin lähettämiseen löydätte: https://www.traficom.fi/fi/traficom/yhteystiedot/salatun-viestin-lahettaminen-traficomiin

Valmistelijat

Lisätietoja asiassa antavat:

erityisasiantuntija Esa Fredriksson, p. 029 539 0330
lakimies Marko Priiki, p. 029 539 0596

Liikenne- ja viestintäviraston sähköpostiosoitteet ovat muotoa
etunimi.sukunimi@traficom.fi

Lausuntopyyntö

Yleiset säännökset (Luku 1)

Soveltamisala (2 §)

Pitäisikö vaatimuksia asettaa eri tasoisina (erilaisille) teleyrityksille? Jos kyllä, niin miten jaottelu mielestänne tulisi toteuttaa?

Määritelmät (3 §)

Ovatko määritelmät olleet riittävän kattavia ja toimivia?

Kaikkien verkkojen ja palvelujen yleiset vaatimukset (Luku 2)

Tietoturvallisuuden huomioiminen (4 §)

Ovatko vaatimukset mielestänne liian ylätasoisia? Jos ovat, miltä osin niitä mielestänne tulisi tarkentaa?

Verkon liikenteen ja rajapintojen suojaaminen (olisiko mielestänne tarpeen edellyttää teleyrityksiltä signalointi- ja käyttäjäliikenteen suojaamista salaamalla liikenne aina kun se on teknisesti mahdollista?)

Matkaviestinverkon infrastruktuurin toteutukset pilvipalveluissa (esim. miten eri pilvipalveluratkaisut tulisi huomioida määräyksessä?)

Alihankintaturvallisuuden huomiointi (toimitusketjut, ohjelmistot, tukipalvelut.)

Verkon virtualisointi (Trust domains, VNF erottelu, hyökkäysvektoreiden minimointi, virtualisointiympäristön verkonhallinta, HMEE, alustan luotettavuuden todentaminen.)

Pääsynhallintavelvoitteiden laajentaminen ja täsmentäminen (laajentaminen ohjelmistojen/laitteiden oikeuksiin (SBA-turvallisuus), Automaattinen avaintenhallinta))

Erilaisten lokien tallentaminen ja suojaaminen.

Miten määräyksessä tulisi huomioida reunalaskentayksiköiden suojaaminen?

Käyttöoikeusrekisteri: Käyttöoikeuksien ylläpito ja dokumentointivelvoitteen laajentaminen ja täsmentäminen (sisältäen tahot (henkilöt), joilla on teleyrityksen henkilöstön lisäksi järjestelmänvalvojan oikeus käyttää laitteistoa tai ohjelmistoa).

Riskien hallinta (5 §)

Tulisiko riskienhallinnan seurantasyklit määritellä joiltain osin tai kokonaan esimerkiksi kriittisten toimintojen/järjestelmien osalta? (Nykyisin teleyritys voi itse määrittää sopivat seurantasyklit.)

Tulisiko edellyttää riskienhallinnan tulosten dokumentointia useammalta käsittelykerralta? (Nykyisin vain viimeinen käsittelykerta on dokumentoitava.)

Tietoaineistot (6 §)

Ovatko tietoaineistojen luokitusjärjestelmää ja luokitteluun liittyvää käsittelymenettelyä koskevat vaatimukset ajan tasalla? Tuovatko esimerkiksi pilviratkaisut uusia haasteita?

Onko mielestänne ollut selvää, mitä tietoaineistoja velvoite koskee?

Hallintaverkon ja hallintayhteyksien liikenne (8 §)

Mitä tarpeita yleisesti ottaen näette hallintaverkon ja hallintayhteyksien liikenteen turvallisuusvaatimuksien parantamiseksi?

Tulisiko mielestänne asetusmuutoksien lokitusta koskeva suositus muuttaa velvoittavaksi? Tulisiko suosituksen tai velvoitteen mukaista tallennusaikaa pidentää esimerkiksi yhteen vuoteen

Tulisiko hallintaverkon erottamista tai verkonhallintaan käytettävien työasemien liikennöinnin rajoittamista koskeva suositus muuttaa velvoittavaksi? Jos kyllä, mitä velvoitteiden tulisi edellyttää?

Tulisiko vaatia jatkossa keskitettyä lokienhallintaa? Jos kyllä, minkä toimintojen osalta?

Tulisiko jatkossa vaatia lokienhallintapolitiikan laatimista ja ylläpitoa?

Tulisiko mielestänne lokitusten tarkkuustaso määritellä?

Rajapintojen erityiset vaatimukset (Luku 3)

Tulisiko mielestänne teleyrityksiltä edellyttää signalointirajapintojen suojaamista (esim. SS7, Diameter & HTTP/2)? Jos kyllä, mitä toimenpiteitä tulisi edellyttää?

IP-liikenteen estäminen yhteenliittämisrajapinnoissa (11 §)

Tulisiko vaatimusta tarkentaa esimerkiksi reunareitittimillä (BGP) istuntojen suojausta koskevilla vaatimuksilla, RPKI:n käyttöönottoon velvoittamisella tai liian tarkkojen reittimainostusten, väärennettyjen reittimainostusten ja erityiseen käyttöön varattujen osoiteavaruuksien suodattamisvelvollisuudella?

Internetyhteyspalvelujen erityiset vaatimukset (Luku 4)

Internetyhteyspalvelujen liikennöinnin eriyttäminen (13 §)

Vastaavatko vaatimuksen perustelut nykytilaa? Onko olemassa uudenlaisia tapoja toteuttaa liikenteen erottelua? Pitäisikö mielestänne velvoite laajentaa palvelusta riippumattomaksi?

Viipalointi (esim. viipaleiden eriyttäminen, vertikaalien pääsynhallinta.) Miten määräyksessä tulisi mielestänne huomioida viipaloinnin turvallisuuskysymykset?

Kuluttajaliittymistä lähtevän sähköpostiliikenteen ohjaus (14 §)

Onko SMTP-liikenteen rajoittaminen määräyksen kuvaamalla tavalla mielestänne jatkossakin tarpeellista? (perustelkaa näkemyksenne)

Jos ei, miten rajoitusta tulisi mielestänne muuttaa? Tulisiko rajoitus poistaa kokonaan tai osittain?

Pidättekö perusteltuna kehittää määräystä niin, että teleyrityksen tulisi kuluttajan pyynnöstä poistaa rajoitus liittymästä?

Pidättekö perusteltuna laajentaa rajoitusta määräyksessä muihinkin kuin kuluttajaliittymiin?

Haitallisen liikenteen suodatusvelvollisuus (15 §)

Pitäisikö mielestänne velvoite laajentaa palvelusta riippumattomaksi, tai laajentaa muihinkin palveluihin (kuten SMS/MMS)?

Pidättekö tarpeellisena palvelunestohyökkäysten torjuntavelvoitteen tarkentamista? Mitä velvoite viestintäverkon suojaamiseksi palvelunestohyökkäyksiltä tulisi näkemyksenne mukaan sisältää? (havainnointi ja torjunta verkon sisältä ja ulkoa)

Onko porttisuodatusten nykytila mielestänne oikea? Tulisiko joitain suosituksessa olevia suodatuksia nostaa määräykseen? Perustelkaa näkemyksenne. (Ks. myös suositus 312/2020 S.)

Miten mielestänne suodatusvelvollisuutta pitäisi kehittää vastaamaan paremmin nykyisiä haasteita erityisesti salatun liikenteen osalta? (DNS over HTTPS ym.)

SMS/MMS-liikenteen suodatuskyvykkyysvelvoitteen lisääminen?

Internetyhteyspalveluliittymän irtikytkeminen (16 §)

Vastaavatko vaatimuksen perustelut nykytilaa?

Tulisiko irtikytkemistä lievemmistä toimenpiteistä määrätä nykyistä tarkemmin?

Tulisiko velvoitteessa (irtikytkeminen ja sitä lievemmät toimenpiteet) huomioida tilanteet, joissa haitallista liikennettä ei ole vielä havaittu, mutta asiakasliittymään on liitetty laite tai ohjelmisto, jonka haavoittuvuuden hyväksikäyttö olisi mahdollista?

Sähköpostipalvelujen erityiset vaatimukset (Luku 5)

Nykyinen määräys ei sisällä juurikaan vaatimuksia koskien sähköpostipalveluiden yleistä tietoturvallisuutta tai sähköpostin välittämiseen liittyvää luotettavuuden ja eheyden parantamista. Toimenpiteitä on kuitenkin esitetty määräyksen perustelumuistion puolella.

Mikä on näkemyksenne siitä tulisiko joitakin vaatimuksia tästä sisällyttää määräyksen uuteen versioon, esimerkiksi velvoittamalla turvallisuutta parantavien protokollien, menetelmien tai standardien, kuten DMARCin, DKIMin, SPFn, DANEn tai MTA-STSn käyttöön?

Sähköpostipalvelujen erityinen suodatusvelvollisuus (18 §)

Onko suodattamistoimenpiteistä koitunut jotain erityisiä haasteita?

Määräyksen perustelumuistiossa on esitelty kattavasti eri menetelmiä sähköpostin suodatuksen toteuttamiseksi, puuttuuko näistä jotain?

Asiakkaille tiedottaminen (Luku 6)

Yleinen tiedotusvelvollisuus tietoturvatoimenpiteistä (21 §)

Vaatiko mielestänne Viestintäviraston suositus Kansainvälisesti toteutetun palvelun tietoturvasta tiedottamisesta ajantasaistamista? (205/2014 S).

Mahdolliset muut huomionne

Tähän voitte kirjoittaa mahdolliset muut huomionne määräykseen tai sen soveltamiseen liittyen.