Sosiaali- ja terveysministeriö Perusmuistio EU/372/2025-STM-2

Laurén Andrei 25.2.2025

Perusmuistio eurooppalaisesta toimintasuunnitelmasta sairaaloiden ja terveydenhuollon tarjoajien kyberturvallisuudesta

Kokous

Eduskuntatunnus

Käsittelyvaihe ja jatkokäsittelyn aikataulu

Komissio julkaisi 15.1.2025 tiedonannon ”Eurooppalainen toimintasuunnitelma sairaaloiden ja terveydenhuollon tarjoajien kyberturvallisuudesta” (COM(2025) 10 final).

Toimintasuunnitelma koskee sairaaloiden ja terveydenhuollon tarjoajien kyberturvallisuuden kehittämistoimien edistämistä. Toimintasuunnitelmaa on käsitelty kybertyöryhmässä 27.1. ja terveystyöryhmässä 3.2. Kevään 2025 aikana asia käsitellään edelleen kybertyöryhmän puitteissa terveysattaseat mukaan kutsuen. Komissio esitteli aloitteen pysyvien edustajien komitealle 22.1. Komissio käynnistää vuoden 2025 alkupuolella jäsenmaille ja sidosryhmille konsultaation, jonka perusteella komissio voi antaa lisätoimenpiteitä vuoden 2025 lopulla.

Suomen kanta

Kyberuhkien osalta Suomi painottaa yhtenäisen lähestymistavan, tiedonvaihdon ja yhteisen tilannekuvan sekä kriisivasteen tärkeyttä Euroopalle kyberturvallisuushaasteisiin vastaamiseksi. Kriittisten sektorien, kuten terveydenhuollon, kyberturvallisuuden vahvistaminen, on tärkeä osa Suomen ja EU:n kokonaisturvallisuuden parantamista. Suomi kannattaa tavoitetta turvata entistä paremmin terveydenhuollon kyberturvallisuutta EU-tasolla ja vahvistaa terveydenhuoltojärjestelmien toimintakykyä niin normaali- kuin kriisitilanteissa. Suomi pitää tiedonannon tavoitteita oikean suuntaisina ja kannatettavina.

Suomi pitää tärkeänä vahvistaa sosiaali- ja terveyspalveluiden, sairaaloiden ja terveydenhuollon tarjoajien kyberturvallisuutta, koska ala käsittelee valtavia määriä arkaluonteisia

terveystietoja. Vakavat kyberpoikkeamat voivat vaarantaa myös potilasturvallisuutta. Suomi katsoo, että terveystietojen suojaaminen arkaluontoisina tietona on lakisääteinen velvollisuus ja myös keskeinen eettinen kysymys.

Turvalliset, luotettavat ja kriisin kestävät palvelut ovat välttämättömiä ammattilaisten työn tukemiseksi ja asiakkaiden palveluihin pääsyn turvaamiseksi. Suomi katsoo, että toimintasuunnitelma sairaaloiden ja terveydenhuollon tarjoajien kyberturvallisuudesta voi auttaa sairaalaympäristöjen häiriönsietokykyä EU-laajuisesti.

Suomi pitää tärkeänä, että painopisteet keskittyvät NIS2-direktiivin täytäntöönpanoa tukeviin toimenpiteisiin terveydenhuollossa, esimerkiksi riskitiedon jakamiseen ja ylläpitoon, haavoittuvuuksien tunnistusprosessien kehittämiseen sekä poikkeamien tehokkaaseen hallintaan ja nopeaan toipumiseen. Suomen painopisteenä on myös kehittää EU-tasolla menetelmiä, joilla kyberuhkatoimijoiden hyökkäykset voidaan estää tehokkaammin, kuten toimenpiteitä kiristyshaittaohjelmien hyökkäysten varalle. Suomi suhtautuu myönteisesti toimintasuunnitelman puitteissa kehitettävien menetelmien hyödyntämiseen myös muilla NIS2-direktiivin soveltamisalaan kuuluvilla toimialoilla soveltuvin osin. Lisäksi Suomi pitää tärkeänä ylläpitää yhteistyöverkostoja eri toimijoiden kanssa kyberturvallisuuden kehittämisessä ja toimeenpanossa.

Suomi painottaa yhtenäisen lähestymistavan, tiedonvaihdon ja yhteisen tilannekuvan sekä kriisivasteen tärkeyttä Euroopalle kyberturvallisuushaasteisiin vastaamiseksi. Suomi katsoo, että kyberpoikkeamiin liittyvän rajat ylittävän tiedonjaon ja tiedonvaihdon tulisi ensisijaisesti perustua vapaaehtoisuuteen. Suomi katsoo, että uusien tilannekuva- ja tiedonvaihtotoimintojen perustamisessa tulee välttää päällekkäisyyksiä jo olemassa olevien toimintojen kanssa.

Suomi katsoo, että Euroopan kyberturvallisuusvirasto ENISAlle osoitettavien tehtävien luonnetta ja laajuutta tulisi arvioida tarkemmin jatkotyössä sekä osana ENISAn tehtäviä määrittävän kyberturvallisuusasetuksen laajempaa määräaikaisarviointia. ENISAn tehtävien tulisi keskittyä toimenpiteisiin, joilla saadaan EU-tasolla erityistä lisäarvoa, kuten kansallisen tilannetietoisuuden täydentäminen tai jäsenvaltioiden yhteistyön ja vapaaehtoisen tiedonvaihdon tukeminen. ENISAn tehtävissä tulisi välttää päällekkäisyyksiä kansallisten viranomaisten tehtävien kanssa ja toimia olisi tärkeää koordinoida kansallisten viranomaisten kanssa. Suomi pitää tärkeänä, että ENISAn kyky hoitaa sille osoitetut tehtävät varmistetaan. Suomi pitää tärkeänä, että ennen uusien tehtävien osoittamisessa ENISAlle otetaan huomioon ENISAn toimintamenojen riittävyys.

Suomi pitää tärkeänä edistää lääkinnällisten laitteiden suojaamista ja potilasturvallisuuden varmistamista. Suomi katsoo, että toimintasuunnitelma tukee osaltaan lääkinnällisten laitteiden turvallista käyttöä. Suojauksessa on huomioitava myös lääkinnällisiä laitteita koskeva lainsäädäntö ja NIS2-direktiivin vaatimustaso.

Kyberturvallisuus sairaaloissa on tärkeässä roolissa eurooppalaisen terveystietoalueen (EHDS) asetuksen toimeenpanossa. Suomi pitää tärkeänä, että tulevilla toimilla tuetaan EHDS:n toimeenpanoa. Suomi katsoo, että erityisesti suojautuminen kyberhyökkäyksiä vastaan ja kestävän sekä turvallisen EHDS-infrastruktuurin luominen ovat välttämättömiä tavoitteiden saavuttamiseksi.

Suomi katsoo, että toimintasuunnitelma tukee osalta tekoälyn turvallista käyttöä terveyspalvelussa ja sairaalaympäristöissä. Suojauksessa on huomioitava tietosuoja-asetuksen, tekoälysäädöksen ja NIS2-direktiivin vaatimustaso.

Suomi katsoo, että terveydenhuolto on kriittistä infrastruktuuria ja toimintasuunnitelma tukee kriisinkestävyyttä myös maanpuolustuksen näkökulmasta.

Pääasiallinen sisältö

Euroopan komission puheenjohtaja Ursula von der Leyen on komission 2024–2029 poliittisissa suuntaviivoissa määritellyt yhdeksi tavoitteeksi terveydenhuollon ja sairaalaympäristön kyberturvallisuuden kehittämisen ja ennaltaehkäisevän työn. Käytännön toimena komissio julkaisi sairaaloiden ja terveydenhuollon tarjoajien kyberturvallisuuden toimintasuunnitelman 15.1.2025 tiedonannossa.

Komission antamassa tiedonannossa katsotaan, että EU:n turvallisuusympäristö on muuttunut nopeasti hybridihyökkäysten ja kyberhyökkäysten lisääntyessä. Hyökkäyksillä pyritään horjuttamaan yhteiskuntaamme ja lisäämään polarisaatiota ja hyötymään rahallisesti erilaisilla tietoverkkorikollisuuden muodoilla. Lisäksi toimintasuunnitelmassa keskitytään valtaosin tahallisesti aiheutettuihin kyberuhkiin.

Komissio tukee tiedonannolla kriittisiä terveydenhuollon toimijoita ja sairaalaympäristöjä. Toimintasuunnitelma tukee myös NIS2 -direktiiviin perustuvien velvoitteiden toimeenpanoa terveysalalla.

Tiedonannossa esitetään, että Euroopan kyberturvallisuusvirasto ENISAn yhteyteen perustettaisiin uusi kyberturvallisuuden tukikeskus, jonka tehtävänä olisi vahvistaa sairaaloiden ja terveydenhuollontarjoajien kyberturvallisuutta poikkeamien estämisessä, havaitsemissa, niihin reagoimisessa sekä niistä palautumisessa. Tiedonanto jakautuu seuraaviin kokonaisuuksiin terveysalan kyberturvallisuuden kehittämiseksi.

<u>Poikkeamien estäminen</u>

Tiedonanto korostaa koulutuksen ja osaamisen sekä harjoittelun merkitystä kyberturvallisuudessa, oman organisaation infrastruktuurin tuntemista kypsyysarvioiden kautta ja valmiutta vastata kyberhyökkäyksiin sekä varautua lääkinnällisten laitteiden toimitusketjujen riskeihin mm. koordinoiduilla turvallisuusriskiarvioinneilla. Tiedonanto korostaa myös tarvetta tehdä EU:n laajuista yhteistyötä kybertaitojen kasvattamista kyberturvallisuusakatemia-aloitteen puitteissa. Toimenpiteiden ensisijainen toteuttaminen olisi ENISAn tukikeskuksen vastuulla. Tiedonanto nostaa yhtenä mahdollisena toimenpiteenä esille myös organisaatioiden kyberturvallisuuden kehittämisen tukemisen kansallisella kyberturvallisuussetelillä. Sillä tarkoitetaan rahoitusmekanismia, jonka avulla esimerkiksi sairaaloita voidaan tukea kyberturvallisuuden vahvistamisessa. ENISAn tukikeskus tekisi jäsenvaltioiden kanssa yhteistyötä ohjelmien kehittämisessä.

<u>Poikkeamien havaitseminen</u>

Tiedonanto korostaa tiedonjaon tehostamista ja EU-tason tilannekuvan kehittämisen tärkeyttä kyberturvallisuuteen liittyvien uhkien ja haavoittuvuuksien havaitsemisessa ja ennakoimisessa. ENISAn tukikeskukselle ehdotetaan keskeistä roolia EU-tason tilannekuvan sekä sille raportoitujen terveydenhuollossa käytettävien tietojärjestelmien ja laitteiden haavoittuvuustietojen tietokannan ylläpitämisessä. ENISAn tukikeskuksen ehdotetaan myös perustavan hälytyspalvelun, joka voisi tarjota terveydenhuollon toimijoille varoituksia tunnistetuista kyberuhista. Lisäksi tiedonanto korostaa luottamukseen perustuvaa tiedonvaihtoa ja yhteistyötä yksityisen ja julkisen sektorin välillä eurooppalaisten ja kansallisten terveys-ISAC-verkostojen kautta.

<u>Poikkeamiin vastaaminen</u>

Tiedonanto ehdottaa ENISAn tukikeskuksen valmistelevan yhdessä jäsenvaltioiden ja tarvittaessa Europolin kanssa ennakkoon tehtyjä toimintasuunnitelmia, joita sairaalat ja terveyshuollon tarjoajat voivat käyttää kyberhyökkäyksien tai muihin turvallisuuspoikkeamien reagoimiseen. Kyberturvallisuusharjoitukset ovat myös keskeinen osa

toimintaa, ne parantavat valmiuksia ja auttavat tunnistamaan kehityskohteita turvallisuuden ylläpitämisessä. ENISAn tukikeskus voisi tukea näiden harjoitusten toimeenpanossa. Lisäksi tiedonannossa ehdotetaan, että kybersolidaarisuusasetuksella perustetun EU:n kyberturvallisuusreservin tulisi pystyä tarjoamaan nopean vasteen palveluita myös terveyssektorin tarpeisiin.

Poikkeamista palautuminen

Tiedonanto ehdottaa EU:n tasoista keskitettyä palvelua, jolla tuetaan kiristysohjelmahyökkäyksistä toipumista Tämä sisältää kiristyshaittaohjelmien salauksen purkuun liittyvien työkalujen ja tietotokannan ylläpitoa ja kehittämistä yhteistyössä, jotta sairaalat ja terveyshuollon tarjoajat välttyisivät maksamasta lunnaita ja saisivat palvelut takaisin käyttöönsä. Palvelupiste sijoittuisi ENISAn tukikeskukseen.

Tiedonannossa korostetaan vahvasti tarvetta kerätä tietoa kiristysohjelmahyökkäyksistä muun muassa vastatoimien kehittämisen tueksi. Tähän liittyen siinä suositellaan jäsenmaita kehottamaan NIS2-toimijoita ilmoittamaan myös mahdollisista maksetuista lunnaista. Jäsenmaita kehotetaan jakamaan nämä tiedot ENISAn tukikeskuksen kanssa.

Pidäke ja pelote

Tiedonanto painottaa EU:n politiikkatoimien merkitystä pelotteen muodostamisessa kyberuhkatekijöitä vastaan. Toimien tulisi pyrkiä heikentämään uhkatoimijoiden toiminta-edellytyksiä ja taloudellisia hyötyjä esimerkiksi vahvistamalla lainvalvontaviranomaisten yhteistyötä ja yhteistutkintoja. Tiedonanto korostaa seuraamusten merkitystä pelotteen kannalta ja kehottaa jäsenvaltioita puuttumaan täysimääräisesti kyberrikollisten toimintaan unionin lainsäädännön ja Euroopan neuvoston Budapestin yleissopimuksen puitteissa. Lisäksi olemassa olevaa kyberdiplomatian työkalupakin mukaista sanktiojärjestelmää voidaan hyödyntää vastaamaan terveydenhuoltojärjestelmiin kohdistuviin kyberuhkiin.

Lisäksi kansainvälinen yhteistyö, esimerkiksi CRI-aloitteeseen liittyen ja G7-yhteistyön osana perustetun kyberturvallisuustyöryhmän puitteissa, on komission mukaan keskeisessä roolissa kyberturvallisuusuhkien torjunnassa ja globaalin kriisinkestävyyden rakentamisessa.

Kansalliset toimenpiteet

Komissio suosittelee tiedonannossa jäsenvaltioiden toteuttavan seuraavia toimenpiteitä:

- Kyberturvallisuuden poikkeamia koskevien tietojen jakaminen eurooppalaisen kyberturvallisuuden tukikeskuksen kanssa.
- Kansallisten terveydenhuollon kyberturvallisuuden tiedonvaihtoryhmien (ISAC) kehittäminen.
- Lääkinnällisten laitteiden toimitusketjujen kyberturvallisuusriskien arviointi NIS-yhteistyöryhmässä.
- Kansalliset kyberturvallisuusharjoitukset.
- Kansallisen terveydenhuollon kyberturvallisuuden tukikeskuksen nimeäminen.
- Kansallinen terveydenhuoltoalan kyberturvallisuuden toimintasuunnitelma.
- Terveydenhuollon palveluntarjoajien keskinäisen resurssien jakamisen fasilitointi.
- Kyberturvallisuuden investointien tarkkailu ja arviointi.
- Velvoittaa NIS2-direktiivin soveltamisalaan kuuluvat organisaatiot ilmoittamaan ovatko ne maksaneet tai aikovat maksaa lunnaita kiristyshaittaohjelmahyökkäyksiä tehneille rikollisille.

Sosiaalipalvelut eivät sisälly suoraan tähän toimintasuunnitelmaan.

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

-

Käsittely Euroopan parlamentissa

-

Kansallinen valmistelu

Kirjallinen menettely 10–12.2.2025 terveysjaostossa EU-33 ja viestintäjaostossa EU-19.

Eduskuntakäsittely

-

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

-

Taloudelliset vaikutukset

Euroopan komission julkaisema toimintasuunnitelma ”sairaaloiden ja terveydenhuollon tarjoajien kyberturvallisuudesta” ei aiheuta suoria kansallisia taloudellisia vaikutuksia, koska toimenpidesuunnitelma ei sisällä uusia velvoittavia toimenpiteitä jäsenvaltioille. Niiltä osin, kun toimintasuunnitelman toimenpiteet ovat osa NIS2-direktiivin täytäntöönpanoa, taloudellisia vaikutuksia on kuvattu hallituksen esityksessä kyberturvallisuuslaiksi HE 57/2024 vp. Toimenpidesuunnitelma sisältää myös joukon jäsenvaltioille osoitettuja suositusluonteisia toimenpiteitä, joiden taloudelliset vaikutukset riippuvat niiden toteuttamistavasta.

Tiedonannossa todetaan, että komissio pyrkii varmistamaan riittävät resurssit ENISA:lle kohdistettaviin uusiin tehtäviin.

Muut asian käsittelyyn vaikuttavat tekijät

<u>NIS2 -direktiivi</u>

NIS2-direktiivin täytäntöönpanoa koskee hallituksen esitys HE 57/2024 vp, jonka käsittely eduskunnassa on kesken. Määräaika direktiivin kansalliselle täytäntöönpanolle on ollut 17.10.2024. NIS2 -direktiivin velvoitteista on kansallisesti ehdotettu säädettäväksi uudella kyberturvallisuuslailla, jota sovellettaisiin myös terveysalalla NIS2 -direktiivin soveltamisalan mukaisesti.

- Euroopan parlamentin ja neuvoston direktiivin 2011/24/EU potilaiden oikeuksien soveltamisesta rajatylittävässä terveydenhuollossa 3 artiklan g alakohdassa määritellyt terveydenhuollon tarjoajat,
- Euroopan parlamentin ja neuvoston direktiivin 2001/83/EY 1 artiklan 2 alakohdassa määriteltyjen lääkkeiden tutkimusta ja kehitystä harjoittavat toimijat, sekä
- Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/123 22 artiklassa tarkoitetut vakavan kansanterveysuhan aikana kriittisiksi katsottujen lääkinnällisten laitteiden (kansan terveysuhan aikana kriittisten lääkinnällisten laitteiden luettelo) valmistavat toimijat.

Kansallinen kyberturvallisuusstrategia

Suomen kyberturvallisuusstrategia 2024–2035, on uudistettu pääministeri Petteri Orpon hallitusohjelman mukaisesti vastaamaan muuttunutta toimintaympäristöä.

Tiedonannossa esitetään terveydenhuoltoalaa koskevien säädösten kokoamista helppokäyttöiseen palveluun, jotta relevanttien ohjeiden ja säädösten löytämiseen ei kuluisi liikaa resursseja. Suomessa sellaisen laatiminen on aloitettu STM:n johdolla jo loppukesästä 2024.

Muut huomioitavat asiat

Sosiaali- ja terveydenhuollon infrastruktuuri on keskeinen EU:n ja NATO:n siviiliresiliensin ylläpidon varmistamisessa, potilashoidossa ja terveydenhuollon tarjoamisessa.

Presidentti Sauli Niinistön raportin mukaan kyberturvallisuus on olennainen osa kokonaisturvallisuutta, ja sen avulla vahvistetaan yhteiskunnan kriisinsietokykyä.

Kyberkestävyyssäädös, (EU) 2024/2847, asettaa pakollisia kyberturvallisuusvaatimuksia digitaalisia elementtejä sisältäville tuotteille. Kyberkestävyyssäädöksen soveltamisala ei kata lääkinnällisiä laitteita.

Asiakirjat

Euroopan komission tiedonanto ”Eurooppalainen toimintasuunnitelma sairaaloiden ja terveydenhuollon tarjoajien kyberturvallisuudesta” (COM(2025) 10 final).

Laatijan ja muiden käsittelijöiden yhteystiedot

Andrei Laurén, tietoturvapäällikkö/erityisasiantuntija, STM, andrei.lauren@gov.fi, +358 295 163 083
Kaisa Lähdepuro, erityisasiantuntija, STM kaisa.lahdepuro@gov.fi, +358 295 163 419
Joni Komulainen, hallitusneuvos, STM, joni.komulainen@gov.fi, + 358 295 163 453
Emma Honkanen, erityisasiantuntija, LVM emma.hokkanne@gov.fi, +358 295342106
Veikko Vauhkonen, hallitussihteeri, LVM veikko.vauhkonen@gov.fi, +358 295 342 168
Outi Äyräs-Blumberg, neuvotteleva virkamies, STM outi.ayras-blumberg@gov.fi, +358 295 163 260
Sarita Friman, EU-erityisasiantuntija, VNEUS sarita.friman@gov.fi, +358 295 160 144

VAHVA-tunnus

EU/372/2025

Liitteet -

Viite -