Euroopan unionin neuvosto

Bryssel, 16. tammikuuta 2025
(OR. en)

5426/25

CYBER 21
SAN 15

SAATE

Lähettäjä:	Euroopan komission pääsihteeri, allekirjoittajana johtaja Martine DEPREZ
Saapunut:	15. tammikuuta 2025
Vastaanottaja:	Thérèse BLANCHET, Euroopan unionin neuvoston pääsihteeri
Kom:n asiak. nro:	COM(2025) 10 final
Asia:	KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE Sairaaloiden ja terveydenhuoltopalvelujen tarjoajien kyberturvallisuutta koskeva eurooppalainen toimintasuunnitelma

Valtuuskunnille toimitetaan oheisena asiakirja COM(2025) 10 final.

Liite: COM(2025) 10 final

EUROOPAN
KOMISSIO

Bryssel 15.1.2025
COM(2025) 10 final

KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE

Sairaaloiden ja terveydenhuoltopalvelujen tarjoajien kyberturvallisuutta koskeva eurooppalainen toimintasuunnitelma

1. Johdanto

EU:n turvallisuusympäristö on nopeassa muutoksessa. Hybridihyökkäykset ja kyberhyökkäykset lisääntyvät, ja niiden tavoitteena on horjuttaa yhteiskuntaamme ja luoda jakolinjoja ja häiriöitä, mutta myös saada voittoja kyberrikollisuudesta. Sen vuoksi Euroopan on pikaisesti vahvistettava varautumistaan ja häiriönsietokykyään tätä uutta todellisuutta vastaan kaikilla osa-alueilla ja koko yhteiskunnan ja koko hallinnon kattavan lähestymistavan mukaisesti, kuten Euroopan komission puheenjohtajan erityisneuvonantajan Sauli Niinistön raportissa kehotetaan.

Turvalliset ja häiriönsietokykyiset terveydenhuoltojärjestelmät ovat EU:n sosiaalisen mallin kulmakivi. Sairaaloihin ja terveydenhuoltojärjestelmiin kohdistuu kuitenkin kasvavia uhkia, sillä erityisesti kiristysohjelmia käyttävät rikollisryhmät kohdistavat niihin hyökkäyksiä saadakseen taloudellista hyötyä. Hyökkäysten taustalla on potilastietojen, myös sähköisten potilaskertomusten, suuri arvo. Terveysalasta onkin tullut ala, johon on kohdistunut EU:ssa eniten hyökkäyksiä neljän viime vuoden aikana, myös covid-19-pandemian aikana, jolloin terveysinfrastruktuuriin kohdistuvat kyberhyökkäykset lisääntyivät. Sairaaloihin ja terveydenhuoltopalvelujen tarjoajiin kohdistuvat kyberhyökkäykset aiheuttavat välitöntä haittaa ihmisille, viivästyttävät lääketieteellisiä toimenpiteitä, ruuhkauttavat päivystyspoliklinikat ja voivat ääritapauksissa johtaa ihmishenkien menetykseen.

Panokset ovat erityisen suuret, koska alalla on tapahtumassa elintärkeä digitaalinen muutos. Digitaalisen terveydenhuollon sekä terveystietojen käytön ja uudelleenkäytön avulla voidaan luoda ihmisten ja potilaiden tarpeisiin ja mieltymyksiin paremmin sopivia hoitomalleja ehkäisemällä sairauksien puhkeamista tai mahdollistamalla hoidon aloittaminen aikaisemmin. Digitaalisten välineiden ja ratkaisujen integrointi kliinisiin prosesseihin sekä terveystietojen käyttö ja uudelleenkäyttö voivat auttaa tekemään parempia kliinisiä päätöksiä, edistää terveydenhuollon automatisointia sekä nopeuttaa ja parantaa potilaiden hoitoa. Digitaaliset välineet, datan käyttö sekä lääkinnälliset laitteet, jotka on usein liitetty internetiin ja joissa hyödynnetään tekoälyä, ovat myös avainasemassa vastattaessa terveydenhuollon henkilöstöpulan kaltaisiin haasteisiin.

Samalla digitaaliset työkalut luovat myös lisää mahdollisia kohteita kyberrikollisille. Lisäksi tietyt valtiolliset toimijat eivät epäröi kohdistaa hyökkäyksiä terveydenhuoltolaitoksiin, kuten Venäjän Ukrainaa vastaan käymä hyökkäyssota on osoittanut. Tämä tekee terveysalasta mahdollisen kohteen osana laajempaa hybridikampanjaa suoritettaville kyberhyökkäyksille. Paitsi että kyberhyökkäykset vaarantavat potilasturvallisuuden, ne heikentävät kansalaisten luottamusta terveysinfrastruktuuriin ja aiheuttavat huomattavia hyökkäyksistä palautumisesta johtuvia kustannuksia. Sen lisäksi, että häiriönsietokykyinen ja turvallinen digitaalinen infrastruktuuri antaa suojan kyberhyökkäyksiä vastaan, se on olennaisen tärkeä myös tuettaessa eurooppalaisen terveysdata-avaruuden[1] täytäntöönpanoa ja täysimittaista käyttöönottoa.

Sen vuoksi on aika parantaa ja vahvistaa Euroopan sairaaloiden ja terveydenhuoltopalvelujen tarjoajien kyberturvallisuutta ja häiriönsietokykyä, kuten puheenjohtaja von der Leyen korosti komission poliittisissa suuntaviivoissa vuosille 2024–2029[2]. Tällä toimintasuunnitelmalla vastataan kiireelliseen

[1] https://www.consilium.europa.eu/fi/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/.
[2] https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_fi.

tarpeeseen ja terveydenhuoltoalan kohtaamiin erityisuhkiin. Terveydenhuollon kyberturvallisuushaasteisiin ei ole mitään yksinkertaista ”ihmelääkettä”. Sen sijaan toimintasuunnitelmassa kehotetaan tehostamaan ehkäisemistä ja varautumista ja soveltamaan koordinoidumpaa lähestymistapaa solidaarisuuteen sekä hyödyntämään Euroopan kyberturvallisuusteollisuuden asiantuntemusta. Toimintasuunnitelmassa otetaan huomioon turvallisuutta koskeva EU:n lähestymistapa, jota kehitetään edelleen ja joka virallistetaan tulevassa EU:n sisäisen turvallisuuden strategiassa. Strategiassa määritellään kattavat toimet kaikkien sisäisten turvallisuusuhkien torjumiseksi ja keskitytään valmiuksiin ennakoida uhkia, ehkäistä vahinkoja ja suojella ihmisiä toimimalla kaikilla tasoilla koko yhteiskunnan kattavan lähestymistavan mukaisesti.

Terveysala koostuu monista erilaisista yhteisöistä ja toimijoista, kuten sairaaloista, klinikoista, hoitokodeista, kuntoutuskeskuksista ja erilaisia terveydenhuoltopalvelujen tarjoajista sekä lääke- ja bioteknologiateollisuudesta, lääkinnällisten laitteiden valmistajista ja terveysalan tutkimuslaitoksista. Tässä toimintasuunnitelmassa keskitytään pääasiassa sairaaloiden ja terveydenhuoltopalvelujen tarjoajien kyberturvallisuuteen. Terveydenhuoltopalvelujen tarjoajalla tarkoitetaan luonnollista henkilöä tai oikeushenkilöä tai muuta kokonaisuutta, joka tarjoaa laillisesti terveydenhuoltoa jonkin jäsenvaltion alueella.[3] Sairaalat ja terveydenhuoltopalvelujen tarjoajat ovat keskinäisessä riippuvuussuhteessa muiden terveydenhuoltoalan toimijoiden kanssa ja lähimpänä kansalaisia. Sairaaloiden ja terveydenhuoltopalvelujen tarjoajien kyberturvallisuutta parantavilla toimenpiteillä olisi samalla puututtava myös laajempaan toimitusketjuun ja ekosysteemiin kohdistuviin riskeihin. Niitä aiheutuu esimerkiksi toimijoista, jotka käyttävät terveystietoja tutkimukseen ja koneoppimiseen tai jotka tuottavat lääkinnällisiä laitteita, erityisesti digitaalisia lääkinnällisiä laitteita, jotka ovat yhteydessä internetiin tai muihin laitteisiin (”esineiden internet”).

Vaikka terveydenhuoltojärjestelmien turvaaminen kuuluu ensisijaisesti kansalliseen toimivaltaan, terveys on myös toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa annetun direktiivin (NIS 2 -direktiivi)[4] mukainen kriittinen toimiala. Kyberrikolliset ja muut uhkatoimijat toimivat yli rajojen, ja myös terveydenhuollon organisaatioiden kyberturvallisuushaasteet ovat samanlaisia eri jäsenvaltioissa. Euroopan tasolla tehtävä yhteistyö on arvokasta EU:n tason ja kansallisten parhaiden käytäntöjen jakamisen ja laajentamisen kannalta. Tästä syystä toimintasuunnitelmassa ehdotetaan EU:n tason koordinointia ja toimenpiteitä ja kehotetaan myös jäsenvaltioita toteuttamaan toimia, joilla voidaan vaikuttaa terveydenhuoltoon ja laajempaan terveysalan ekosysteemiin.

Toimintasuunnitelmassa keskitytään ensisijaisesti kehittämään alan valmiuksia **ehkäistä ennalta** kyberturvallisuuspoikkeamia, koska ennalta ehkäiseminen on aina parempi vaihtoehto kuin hoito. Toiseksi toimintasuunnitelmassa esitetään toimia, joilla parannetaan kyberturvallisuustietojen jakamista ja kyberturvallisuusuhkien **havaitsemisvalmiuksia**. Tämän avulla uhkiin voidaan reagoida nopeammin. Kolmanneksi suunnitelmassa esitetään toimenpiteitä, joilla voidaan **reagoida** paremmin poikkeamiin ja

[3] Euroopan parlamentin ja neuvoston direktiivi 2011/24/EU potilaiden oikeuksien soveltamisesta rajatylittävässä terveydenhuollossa, 3 artiklan g alakohta. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex:32011L0024.
[4] Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa (NIS 2 -direktiivi), https://eur-lex.europa.eu/eli/dir/2022/2555.

palautua niistä. Lisäksi toimintasuunnitelmassa kaavaillaan keinoja **estää** kyberuhkatoimijoita toteuttamasta terveydenhuoltojärjestelmiin kohdistuvia hyökkäyksiä Euroopassa.

Toimintasuunnitelmaa toteutetaan yhdessä terveydenhuoltopalvelujen tarjoajien ja laajemman terveysalan ekosysteemin, jäsenvaltioiden ja kyberturvallisuusyhteisön kanssa. Määritettäessä ja tarkennettaessa vaikuttavimpia toimia on keskeisen tärkeää soveltaa yhteistyöhön perustuvaa lähestymistapaa, jotta kaikki Euroopan kriittiset terveydenhuoltopalvelujen tarjoajat voivat hyötyä toimista. Sen vuoksi tämän tiedonannon yhteydessä toteutetaan kattava sidosryhmien, terveysalan ja jäsenvaltioiden kuuleminen. Myös kansainvälinen yhteistyö on tärkeää kyberturvallisuuden kannalta, koska kyberuhat ovat luonteeltaan rajatylittäviä ja toisiinsa nivoutuvia. Vastaavanlaisia kyberturvallisuusuhkia esiintyy myös laajentumis- ja naapuruusmaissa sekä muissa EU:n strategisissa kumppanimaissa. Tämä voi viime kädessä vaarantaa kriittisen infrastruktuurin turvallisuuden EU:ssa. Sen vuoksi toimintasuunnitelman täytäntöönpanosta saadut kokemukset on tärkeää ottaa huomioon myös EU:n sekä laajentumismaiden että muiden kumppanimaiden kanssa tekemässä yhteistyössä ottaen huomioon niihin kuhunkin kohdistuvien uhkien tasot.

2. Sairaaloiden ja terveydenhuoltopalvelujen tarjoajien kyberturvallisuushaaste

Terveysalaan kohdistuvat kyberturvallisuusuhat

Kyberhyökkäykset lisääntyvät koko maailmassa ja EU:ssa, ja uhkaympäristö on yhä monitahoisempi ja dynaamisempi. Tekoälyn kehittyminen tarjoaa rikollisille ja pahantahtoisille toimijoille tehokkaita välineitä, jotka lisäävät niiden toimien tarkkuutta ja vaikutusta, mutta samalla se antaa kyberpuolustukselle uusia mahdollisuuksia mahdollistamalla automaattiset ja reaaliaikaiset toimet hyökkäyksiä vastaan.

Kiristysohjelmat ovat edelleen kriittinen kyberturvallisuushaaste EU:ssa ja koko maailmassa, ja eräässä raportissa arvioidaan, että vuoteen 2031 mennessä ne aiheuttavat vuosittain yli 250 miljardin euron kustannukset[5]. Kiristysohjelmia käyttävien rikollisten hyökkäyksissä rikolliset paitsi salaavat uhrien tiedot kiristääkseen lunnaita myös vuotavat yhä enemmän arkaluonteisia tietoja lisäpaineen luomiseksi. Toinen merkittävä haaste ovat ohjelmistojen ja laitteiden haavoittuvuudet: Euroopan unionin kyberturvallisuusviraston (ENISA)[6] mukaan terveydenhuolto on eniten tällaisiin haavoittuvuuksiin liittyviä turvallisuuspoikkeamia ilmoittanut sektori.[7] Muita kasvavia uhkia ovat hajautetut

[5] Cybersecurity Ventures (1.6.2024): *Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031*. Saatavilla osoitteessa https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

[6] Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (kyberturvallisuusasetus), https://eur-lex.europa.eu/eli/reg/2019/881/oj/.

[7] ENISAn Threat Landscape -raportti: Terveysala (heinäkuu 2023).

palvelunestohyökkäykset (DDoS-hyökkäykset), joissa kohteena oleva järjestelmä pyritään kaatamaan kohdistamalla siihen suuri määrä liikennettä, jolloin lailliset käyttäjät eivät voi käyttää sitä.[8]

Terveysalan kyberturvallisuusuhkien kehitys on samansuuntaista, ja kiristysohjelmahyökkäykset muodostavat niistä suuren osan. ENISAn mukaan kiristysohjelmien osuus analysoiduista terveysalan kyberturvallisuuspoikkeamista vuosina 2021–2023 oli 54 prosenttia. Kaikkiaan 83 prosentilla hyökkäyksistä oli taloudellinen motiivi, joka johtui terveydenhuoltotietojen suuresta arvosta, ja 10 prosentissa hyökkäyksistä motiivi oli ideologinen.[9] Komission vuonna 2024 julkaisemassa raportissa todettiin vastaavasti, että 71 prosenttia hyökkäyksistä, jotka vaikuttivat potilaiden hoitoon esimerkiksi viivästyttämällä hoitoa ja diagnosointia ja estämällä pääsyn hätäpalveluihin, oli kiristysohjelmahyökkäyksiä.[10] Kiristysohjelmahyökkäyksillä voi olla erityisen haitallinen vaikutus terveydenhuoltopalvelujen tarjoamiseen, mikä vaarantaa potilasturvallisuuden. Lisäksi kiristysohjelmahyökkäyksiin liittyy usein potilastietojen tietoturvaloukkauksia[11], jotka koskevat usein arkaluonteisia terveyteen liittyviä tietoja ja loukkaavat kansalaisten perusoikeutta henkilötietojen suojaan.

Terveydenhuollon digitalisaation lisääntyessä myös hyökkäyspinta-ala kasvaa. Digitaalisen vuosikymmenen tilaa vuonna 2024 koskevan kertomuksen mukaan keskimäärin 79 prosentilla EU:n kansalaisista on pääsy sähköisiin terveystietoihinsa perusterveydenhuollossa.[12] Sähköiset potilaskertomukset, kliiniset tietojärjestelmät, sairaaloiden työnkulkujärjestelmät, tietojärjestelmät hoitokulukorvausten käsittelyä varten, lääketieteelliset kuvantamisjärjestelmät ja diagnostisiin tarkoituksiin tai potilasseurantaan käytettävät lääkinnälliset laitteet ovat kaikki esimerkkejä digitaalisista välineistä, joilla voi olla merkittävä rooli terveysalan tehokkuuden ja suorituskyvyn parantamisessa mutta jotka ovat myös mahdollisia kyberturvallisuushyökkäysten kohteita. Erityisen alttiita kyberhyökkäysten riskille ovat tietyt terveydenhuollon toiminnot, kuten tehohoito ja radiologinen kuvantaminen, ja onkologian ja kardiologian kaltaiset lääketieteen alat, jotka ovat erittäin riippuvaisia digitaalisista laitteista. Lisäksi toimitusketjuun liittyvät ongelmat voivat johtaa sellaisten laitteiden hankintaan, joiden kyberturvallisuus on riittämätön, mikä lisää jo olemassa olevia yleisiä riskejä.

Esimerkiksi covid-19-pandemian aikana kiristysohjelmahyökkäys lamaannutti suuren osan Irlannin terveydenhuoltojärjestelmästä, mikä johti siihen, että sinä aamuna, jona poikkeama tapahtui, ainakin osa palveluista peruutettiin 31:ssä 54:stä akuuttisairaalasta.[13] Terveydenhuoltopalvelut joutuivat palaamaan

[8] ENISAn Threat Landscape 2024 -raportti.

[9] ENISAn Threat Landscape -raportti: Terveysala (heinäkuu 2023). Raportissa analysoitiin terveydenhuoltopalvelujen tarjoajia sekä muun tyyppisiä organisaatioita, kuten terveyteen liittyvää tutkimusta harjoittavia organisaatioita, tiettyjä terveyteen liittyviä tuotteita valmistavia toimijoita, terveysviranomaisia, sairausvakuutuslaitoksia sekä pitkäaikaista laitoshoitoa tarjoavia laitoksia ja sosiaalipalvelujen tarjoajia. Saatavilla osoitteessa https://www.enisa.europa.eu/publications/health-threat-landscape.

[10] Euroopan komissio: Yhteinen tutkimuskeskus, Reina, V. ja Griesinger, C., *Cyber security in the health and medicine sector – A study on available evidence of patient health consequences resulting from cyber incidents in healthcare settings*, Euroopan unionin julkaisutoimisto, 2024, https://data.europa.eu/doi/10.2760/693487.

[11] Terveysalaa koskevan ENISAn Threat Landscape -raportin mukaan 43 prosentissa analysoiduista kiristysohjelmapoikkeamista todettiin, että oli tapahtunut tietoturvaloukkaus tai tietoja oli varastettu.

[12] Digitaalisen vuosikymmenen tila vuonna 2024.

[13] Irish Health Service Executive (2021): *Conti cyber attack on the HSE: Independent Post Incident Review*.

paperille kirjattujen tietojen käyttöön, mikä hidasti niiden toimintaa. Hyökkäys sai alkunsa sähköpostitse lähetetystä verkkourkintaviestistä, joka sisälsi haitallisen liitteen.[14] Häiriö osoitti, että kyberhyökkäykset voivat levitä eri järjestelmiin ja että sen vuoksi on tärkeää suojata terveydenhuollon organisaatioiden koko hyökkäyspinta-ala. Se toi myös selkeästi esiin, että on tärkeää varmistaa perustason kyberhygienia ja kyberturvallisuuskulttuuri organisaatioiden kaikissa osissa.

Sairaaloiden ja terveydenhuoltopalvelujen tarjoajien kyberturvallisuuden kehitystaso

Terveydenhuoltoympäristö EU:ssa on hyvin moninainen, ja sairaaloiden ja muiden terveydenhuoltopalvelujen tarjoajien omistus, rakenne ja koko vaihtelevat suuresti eri jäsenvaltioissa. Joissakin tapauksissa terveydenhuollon hallinnointi on keskitetty kansalliselle tasolle, toisissa taas alue- ja paikallistasolle, ja terveydenhuoltopalvelujen tarjoajat voivat olla julkisessa tai yksityisessä omistuksessa. Lisäksi myös saman maan sisällä voi olla eroja, esimerkiksi jos alueiden välillä on merkittäviä sosioekonomisia ja alueellisia eroja, mikä tekee kokonaiskuvasta monimutkaisen. Covid-19-pandemian kaltaiset tartuntataudeista johtuvat merkittävät terveyskriisit, mutta myös muut, esimerkiksi ilmastonmuutokseen liittyvät terveysriskit, voivat muodostaa haasteen tälle monitahoiselle terveydenhuoltoympäristölle. Lisäksi digitalisaation ja teknologian käyttöönoton taso on terveydenhuoltopalvelujen tarjoajien keskuudessa huomattavan vaihteleva ja hajanainen. Esimerkki tästä monitahoisuudesta on se, että kyberturvallisuuspoikkeaman aiheuttama palvelun käyttökatkos voi aiheuttaa vakavaa vahinkoa ja haittaa potilaille myös pienissä terveydenhuoltolaitoksissa, kuten klinikoilla tai ensihoitopalveluissa, jotka tarjoavat keskeistä palvelua suhteellisen pienelle määrälle käyttäjiä.

ENISAn vuonna 2024 julkaiseman kyberturvallisuuden tilaa unionissa koskevan raportin[15] mukaan EU:n terveysalan kyberturvallisuuden kehitystaso on kohtalainen ja terveydenhuollon yksiköiden kyberturvallisuuden kypsyysasteessa on suuria eroja eri puolilla Eurooppaa. Puutteita on havaittavissa keskeisillä osa-alueilla, kuten henkilöresurssien riittävyydessä, organisaatioiden tietämyksessä tieto- ja viestintätekniikan toimitusketjuistaan sekä ajantasaisten tietosuojaominaisuuksien asentamisessa tuotteisiin. Alalla on vaikeuksia perustason kyberhygienian ja perustavanlaatuisten turvallisuustoimenpiteiden kanssa, mistä on osoituksena se, että lähes kaikilla tutkituilla terveysalan organisaatioilla on haasteita kyberturvallisuusriskien arviointien tekemisessä ja lähes puolet organisaatioista ei ole koskaan tehnyt riskianalyysia.[16]

Toinen merkittävä haaste sairaaloiden kyberturvallisuudelle on tietotekniikan ja operatiivisen teknologian risteämiskohta, jossa turvallisuutta koskevat erilaiset painopisteet yhtyvät luottamuksellisuuden, käytettävyyden ja toimintavarmuuden osalta ja jossa yhdellä osa-alueella tapahtuva tietoturvaloukkaus voi vaikuttaa toiseen osa-alueeseen. ENISAn vuonna 2024 julkaisemassa kertomuksessa kyberturvallisuuden tilasta unionissa korostetaan lisäksi, että terveysala ei pysty

[14] Irish Health Service Executive: *Cyber-attack and HSE response*. Saatavilla osoitteessa https://www2.hse.ie/services/cyber-attack/what-happened/.

[15] ENISAn raportti kyberturvallisuuden tilasta unionissa 2024 (Report on the State of Cybersecurity in the Union, syyskuu 2024). Saatavilla osoitteessa https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[16] ENISAn Threat Landscape -raportti: Terveysala (heinäkuu 2023). Saatavilla osoitteessa https://www.enisa.europa.eu/publications/health-threat-landscape.

riittävästi varmistamaan käyttämiensä tieto- ja viestintäteknisten tuotteiden ja prosessien turvallisuutta, koska terveysalan toimijat, laitteet ja tuotteet ovat hyvin erilaisia.

Tämä monimuotoisuus sekä sairaaloiden henkilöstön ja johdon kybertietoisuuden vaihteleva taso aiheuttaa monitahoisen haasteen terveydenhuoltojärjestelmien kyberturvallisuuden varmistamiselle. Esimerkiksi vuonna 2024 toteutetun kybertaitoja koskevan Eurobarometri-tutkimuksen mukaan vain 25 prosenttia kyselyyn vastanneista terveys-, koulutus- ja sosiaalialan yrityksistä oli järjestänyt koulutusta tai antanut valistusta kyberturvallisuudesta 12 edellisen kuukauden aikana.[17] Tarvitaan toimia, joilla edistetään kyberturvallisuustietoisuuden kulttuuria etulinjassa työskentelevien terveydenhuollon ammattilaisten keskuudessa. Muita terveydenhuoltopalvelujen tarjoajien kyberturvallisuutta heikentävien haavoittuvuuksien lähteitä ovat esimerkiksi henkilöstön vuorottelujärjestelmät, yhteisten työasemien käyttö, heikko tunnistamisen hallinta ja erillisten tallennusvälineiden käyttö.[18]

Monissa tapauksissa tietotekniikka ja operatiivinen teknologia on ainakin osittain ulkoistettu. Vuoden 2024 Eurobarometri-tutkimuksessa todettiin, että niiden yritysten osuus, jotka ulkoistavat ainakin joitakin kyberturvallisuutensa osatekijöitä, on korkein terveydenhuolto-, koulutus- ja sosiaalialalla, jolla 57 prosenttia tutkimuksen kattamista yrityksistä toimii niin.[19] Samoin on havaittavissa vahva suuntaus siirtyä käyttämään pilvipalveluja, minkä taustalla on tarve skaalautuvaan tietojen tallennukseen ja hallintaan, kustannustehokkuuteen, parempaan yhteistyöhön sekä palveluihin, jotka tukevat tekoälyn ja lääketieteellisten esineiden internetin kaltaisia kehittyneitä teknologioita. Vuonna 2022 terveysalan organisaatioista 58 prosenttia käytti pilvipohjaista digitaalista terveysalustaa.[20] Vaikka tämä siirtymä voi tuoda merkittäviä tehokkuusetuja, siihen liittyy myös riskejä, jotka edellyttävät tietoon perustuvia päätöksiä hankinnoista ja turvallisesta konfiguroinnista.

Näiden haasteiden kattavana kysymyksenä on valmiuksien kehittäminen ja rahoitus. Terveysalan kyberturvallisuuden rahoitus on ollut niukkaa, ja se on edelleen yleinen haaste kaikkialla EU:ssa.[21] Nämä rahoitushaasteiden taustalla on myös väestön ikääntyminen, jonka odotetaan aiheuttavan laajasti budjettipaineita Euroopan terveydenhuoltojärjestelmille lähivuosikymmeninä.

Vanhentuneiden välineiden ja aiempien sukupolvien järjestelmien käytön jatkaminen, rajalliset resurssit turvallisuuspoikkeamien ehkäisemiseen tai niihin reagointiin sekä puutteellinen kyberturvallisuuden kehitystaso johtuvat usein rahoitusvajeista. Sairaaloiden jatkuvana haasteena on löytää tasapaino ajantasaisen ja turvallisen digitaalisen infrastruktuurin ja potilaiden hoidon parantamiseksi tarvittavien muiden investointien, kuten lääkäreiden ja muiden terveydenhuollon ammattilaisten palkkaamisen, uusien diagnostiikka- ja hoitomenetelmien käyttöönoton ja laitehankintojen, välillä. ENISAn mukaan[22]

---

[17] Kybertaitoja koskeva Flash-eurobarometri 547 (toukokuu 2024). Saatavilla osoitteessa https://europa.eu/eurobarometer/surveys/detail/3176.

[18] Panacea – People-centric cybersecurity in healthcare (2021): *White Paper – Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres*.

[19] Kybertaitoja koskeva Flash-eurobarometri 547 (toukokuu 2024). Saatavilla osoitteessa https://europa.eu/eurobarometer/surveys/detail/3176.

[20] ENISAn verkko- ja tietoturvainvestointeja koskeva raportti 2022 (NIS Investments Report, marraskuu 2022). Saatavilla osoitteessa https://www.enisa.europa.eu/publications/nis-investments-2022.

[21] Terveyspalvelujen ja sairaanhoidon järjestäminen ja tarjoaminen kuuluu Euroopan unionin toiminnasta tehdyn sopimuksen 168 artiklan nojalla kansalliseen toimivaltaan, ja terveydenhuoltojärjestelmien rahoitus vaihtelee eri jäsenvaltioissa.

[22] ENISAn verkko- ja tietoturvainvestointeja koskeva raportti 2022 (NIS Investments Report, marraskuu 2022). Saatavilla osoitteessa https://www.enisa.europa.eu/publications/nis-investments-2022.

terveysala sijoittuu 12 tutkitusta alasta vasta seitsemänneksi mitattaessa tietoturvamenojen osuutta tietotekniikkaan käytettävistä kokonaismenoista. Mediaani terveysalalla on 8,3 prosenttia.

3. Eurooppalainen kyberturvatukikeskus sairaaloille ja terveydenhuoltopalvelujen tarjoajille

EU:n kyberturvallisuuskehys tarjoaa laajan valikoiman välineitä, joita olisi hyödynnettävä sairaaloiden ja terveydenhuoltopalvelujen tarjoajien turvallisuuden ja häiriönsietokyvyn parantamiseksi. Jotta voidaan vastata edellä esitettyihin lukuisiin haasteisiin, on kehitettävä EU:n tason yhtenäinen strateginen lähestymistapa, jossa kootaan yhteen tarvittavat resurssit, asiantuntemus ja välineet, joilla kyberuhkia torjutaan tehokkaasti. Kattava yleiskuva sekä parempi suunnittelu ja koordinointi ovat olennaisen tärkeitä, jotta terveydenhuoltopalvelujen tarjoajia kaikkialla EU:ssa voidaan auttaa vahvistamaan puolustustaan. ENISAlla on parhaat edellytykset saavuttaa tämä perustamalla organisaatioonsa erityinen **eurooppalainen kyberturvatukikeskus sairaaloille ja terveydenhuoltopalvelujen tarjoajille**[23] osana ENISAn toimeksiantoa[24] turvata EU:n kriittinen infrastruktuuri ja tukea sitä.

Tukikeskuksen olisi asteittain **kehitettävä kattava palveluluettelo, joka vastaa sairaaloiden ja terveydenhuoltopalvelujen tarjoajien tarpeita** ja jossa esitetään saatavilla olevat palvelut varautumista, ennaltaehkäisyä, havaitsemista ja reagointia varten. Tukikeskuksen olisi yhteistyössä jäsenvaltioiden viranomaisten kanssa laadittava sairaaloiden ja terveydenhuoltopalvelujen tarjoajien kokemusten pohjalta käyttäjäystävällinen ja helppokäyttöinen tietovarasto kaikista unionin, kansallisella ja alueellisella tasolla saatavilla olevista välineistä. Tukikeskuksen olisi toiminnassaan varmistettava asianmukainen koordinointi jäsenvaltioiden kanssa ja tuettava toimien priorisointia ja tarvittaessa niiden toteuttamista reaaliaikaisesti.

Yhtenä tukikeskuksen palveluluettelon kehittämisen tärkeänä osatekijänä komissio ehdottaa, että kaikkialla EU:ssa käynnistetään pilottihankkeita, joilla kehitetään kyberhygieniaa ja turvallisuusriskien arviointia koskevia parhaita käytäntöjä sekä vastataan jatkuvan kyberturvallisuuden seurannan, uhkatiedustelutietojen ja turvallisuuspoikkeamiin reagoimisen tarpeeseen uusimpien kyberturvallisuusratkaisujen avulla. Näiden Digitaalinen Eurooppa -ohjelmasta rahoitettavien ja Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen (ECCC) toteuttamien pilottihankkeiden tulokset otetaan huomioon suunniteltaessa EU:n tason lisätoimia ja tukikeskuksen työtä.

[23] Tässä asiakirjassa kyberturvatukikeskukseen viitataan myös ilmauksella ’tukikeskus’.
[24] Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15–69).

Kaavio 1: Sairaaloille ja terveydenhuoltopalvelujen tarjoajille tarkoitetun tukikeskuksen palveluluettelon osatekijät

3.1. Kyberturvallisuuspoikkeamien ennaltaehkäisy

Yksinkertaisia toimia, joilla voi olla suuri merkitys

Yksinkertaiset kyberturvallisuustoimenpiteet, kuten järjestelmien päivittämisestä huolehtinen, varmuuskopioiden hallinta ja monivaiheisen todennuksen käyttöönotto, voivat erään arvion mukaan suojata organisaatioita jopa 98 prosentilta hyökkäyksistä.[25] Monet vaikuttavimmista kyberhygienia- ja

[25] Microsoft Digital Defense Report 2022. Saatavilla osoitteessa https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

riskinhallintatoimenpiteistä ovat suhteellisen yksinkertaisia toteuttaa, ja sen vuoksi ne ovat helppoja keinoja parantaa kyberturvallisuutta. Yksi tukikeskuksen keskeisistä tehtävistä olisi sen vuoksi oltava **sellaisten selkeiden ja kohdennettujen ohjeiden laatiminen, joissa korostetaan kriittisimpiä kyberturvallisuuskäytäntöjä ja joilla autetaan terveydenhuoltopalvelujen tarjoajia ottamaan ne käyttöön**. Tätä tukea on annettava muuallakin kuin suurissa sairaaloissa, ja sen on sisällettävä räätälöityä neuvontaa pienille yksiköille, kuten paikallisille yleislääkäreiden vastaanotoille ja erikoistuneille klinikoille, joilla on harvoin resursseja perustaa erityisiä kyberturvallisuusryhmiä mutta jotka ovat yhtä alttiita hyökkäyksille. Lisäksi on otettava huomioon tiettyjen terveydenhuollon toimijoiden alueellinen merkitys potilaiden hoidon varmistamisessa esimerkiksi harvaan asutuilla alueilla. Terveysalan tutkimuslaitokset, jotka käsittelevät suuria määriä arkaluonteisia henkilötietoja, voisivat myös hyötyä niiden häiriönsietokyvyn parantamiseksi toteutettavia perustavanlaatuisia kyberturvallisuustoimenpiteitä koskevista ohjeista.

Terveydenhuollon organisaatioihin sovelletaan myös useita EU:n lainsäädännöstä[26] johtuvia kyberturvallisuuteen liittyviä velvoitteita. Nämä velvoitteet ovat ratkaisevan tärkeitä kyber- ja tietoturvallisuuden korkean yhteisen perustason varmistamiseksi, mutta on olennaista varmistaa, että sääntely-ympäristössä luoviminen ei ole tarpeettoman vaikeaa ja kuormittavaa. Voimakas keskittyminen säännösten noudattamiseen ei saisi olla ristiriidassa vahvan kyberturvallisuuskulttuurin edistämistä koskevan tavoitteen kanssa. **Helposti saatavilla oleva sääntelyn kartoitustyökalu voi auttaa vähentämään sellaisten toimijoiden hallinnollista taakkaa, joihin sovelletaan useita säädöksiä.** Ohjeiden ja välineistöjen laatimisen ohella tukikeskuksen olisi tehtävä tiivistä yhteistyötä komission ja jäsenvaltioiden kanssa, jotta tällainen työkalu kehitetään ja levitetään mahdollisimman pian. Tukikeskuksella olisi siksi tärkeä rooli, jotta kyberturvallisuussäännöistä voidaan tehdä helposti ymmärrettäviä ja täytäntöönpantavia, esimerkiksi antamalla täytäntöönpano-ohjeita[27] ja edistämällä tarvittaessa asiaankuuluvia normeja.

Tulevat **eurooppalaiset digitaalisen identiteetin lompakot** ovat toinen väline, jolla helpotetaan hyvien kyberhygieniakäytäntöjen yksinkertaista toteuttamista. Heikkojen tunnistusmekanismien, kuten salasanojen, käytön vähentäminen on olennaisen tärkeää, jotta voidaan pienentää riskiä luvattomasta

[26] Esimerkiksi NIS 2 -direktiivi; Euroopan parlamentin ja neuvoston asetus (EU) 2024/2847, annettu 23 päivänä lokakuuta 2024, digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista (kyberkestävyyssäädös), https://eur-lex.europa.eu/eli/reg/2024/2847/oj/; Euroopan parlamentin ja neuvoston asetus (EU) 2017/745, annettu 5 päivänä huhtikuuta 2017, lääkinnällisistä laitteista, https://eur-lex.europa.eu/eli/reg/2017/745/oj/; Euroopan parlamentin ja neuvoston asetus (EU) 2017/746, annettu 5 päivänä huhtikuuta 2017, in vitro -diagnostiikkaan tarkoitetuista lääkinnällisistä laitteista, https://eur-lex.europa.eu/eli/reg/2017/746/oj/; Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus), https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32016R0679; Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689, annettu 13 päivänä kesäkuuta 2024, tekoälyä koskevista yhdenmukaistetuista säännöistä (tekoälysäädös), https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32024R1689; Ehdotus Euroopan parlamentin ja neuvoston asetukseksi eurooppalaisesta terveysdata-avaruudesta, COM(2022)197 final, https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex:52022PC0197. Neuvotteluissa saavutettiin poliittinen yhteisymmärrys keväällä 2024, ja kun säädös on viimeistelty, se on määrä julkaista Euroopan unionin virallisessa lehdessä keväällä 2025.

[27] Yleisen tietosuoja-asetuksen tulkintaa koskevien ohjeiden laatiminen kuuluu Euroopan tietosuojaneuvoston vastuulle. ENISAn ohjeita laadittaessa olisi kunnioitettava täysimääräisesti Euroopan tietosuojaneuvoston oikeuksia.

pääsystä terveystietoihin. On ratkaisevan tärkeää siirtyä kohti turvallisia kirjautumisratkaisuja, jotka perustuvat luotettavaan tunnistamiseen. EU:n digitaalisen identiteetin lompakko tarjoaa terveydenhuollon ammattilaisille yhdenmukaistetun ja EU:n laajuisen sähköisen tunnistamiskeinon. Tämän luotettavan ja yhtenäisen ratkaisun on tarkoitus tulla käyttöön vuoden 2026 lopussa. Kaikkien käyttäjän vahvan todentamisen toteuttamiseksi tarvittavien terveydenhuollon sähköisen tietojärjestelmien on hyväksyttävä digitaalisen identiteetin lompakko tunnistamista varten vuoden 2027 lopusta alkaen.[28]

Varautuminen ja kohdennettu tuki

Varautumisen testaus, johon kuuluu esimerkiksi tunkeutumistestauksen kaltaisia toimia, on tehokkaan kyberturvallisuuden kulmakivi, ja komissio on jo myöntänyt ENISAlle rahoitusta varautumista koskeviin pilottialoitteisiin. Näissä aloitteissa on ilmennyt, että terveydenhuoltoala on yksi niistä aloista, joilla tarvitaan eniten testausta ja lisäarviointeja kyberturvallisuuden kehitystasossa olevien puutteiden tunnistamiseksi. Kybersolidaarisuussäädöksen voimaantulon myötä nämä toimet laajenevat merkittävästi ja Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus ottaa niissä johtoaseman. Vastatakseen tähän tarpeeseen komissio aikoo ehdottaa verkko- ja tietoturva-alan yhteistyöryhmää, EU-CyCLONe-verkostoa[29] ja ENISAa kuullen, että terveys määritellään alaksi, jolle voidaan antaa kybersolidaarisuussäädöksen nojalla tukea **varautumisen koordinoituun testaukseen**. Lisäksi tukikeskuksen olisi kehitettävä **erityisesti terveydenhuoltoalalle räätälöity kehys kyberturvallisuuden kehitystason arviointeja varten**. Tällaiset kehitystason arvioinnit antaisivat toimijoille käyttökelpoista tietoa niiden haavoittuvuuksista sekä mahdollisuuden osoittaa kyberturvallisuusvalmiutensa potilaille ja sidosryhmille, mikä lisää luottamusta niiden palveluihin. Koostetulla tasolla tukikeskuksen olisi toteutettava **vuosittain terveysalan kyberturvallisuuden kehitystason arviointi**, jossa laaditaan selkeä yleiskatsaus terveysalan kyberturvallisuudesta sekä kansallisella että EU:n tasolla.

Terveysala käyttää kyberturvallisuuspalveluissaan paljolti ulkopuolisia toimeksisaajia[30], mikä korostaa kohdennetun tuen tarvetta puolustuksen vahvistamiseksi. **Jäsenvaltioiden olisi harkittava** EU:n innovaatiosetelien kaltaisten onnistuneiden aloitteiden pohjalta **kohdennettuja toimenpiteitä, kuten mikrokokoisille, pienille ja keskisuurille sairaaloille ja terveydenhuoltopalvelujen tarjoajille tarkoitettuja kyberturvallisuusarvoseteleitä**. Tällaisilla arvoseteleillä annettaisiin taloudellista tukea erityisten kyberturvallisuustoimenpiteiden käyttöönottoon. Arvosetelien jakamisen priorisoinnissa olisi otettava huomioon varautumistestauksen ja kehitystason arviointien tulokset.

Paikallistuntemus ja paikallinen konteksti ovat ratkaisevan tärkeitä, jotta arvosetelit tai muut tukiohjelmat voidaan ottaa tehokkaasti käyttöön, sillä niiden avulla varmistetaan tukitoimien tarkoituksenmukaisuus ja saavutettavuus. EU:n rahastoista, muun muassa Euroopan aluekehitysrahastosta, tuetaan jo aktiivisesti kyberturvallisuutta ja digitaalista terveydenhuoltoa

[28] Asetuksen (EU) N:o 910/2014 5 f artiklan 1 ja 2 kohta.
[29] Euroopan kyberkriisien yhteysorganisaatioiden verkosto.
[30] Ks. ENISAn verkko- ja tietoturvainvestointeja koskeva raportti 2023 (NIS Investments Report, marraskuu 2023), jossa korostetaan ulkoisen tuen suurta merkitystä kyberturvallisuuden tarkastusten ja vaatimustenmukaisuuden kannalta. Saatavilla osoitteessa https://www.enisa.europa.eu/publications/nis-investments-2023.

koskevia aloitteita, ja ne voisivat sen vuoksi toimia välineenä, jolla kehitetään kohdennettuja kyberturvallisuusarvosetelijärjestelmiä terveydenhuoltopalvelujen tarjoajille. Tämän toimen edistämiseksi tukikeskus tekisi yhteistyötä jäsenvaltioiden ja alueellisten ohjelmaviranomaisten kanssa tukeakseen alueellisten arvosetelijärjestelmien kehittämistä. Tässä yhteydessä hyödynnettäisiin nykyisistä kansallisista hankkeista sekä Digitaalinen Eurooppa -ohjelmasta rahoitetuista toimista saatuja kokemuksia vaikuttavan täytäntöönpanon varmistamiseksi käytännön tasolla.

Lisäksi Horisontti-ohjelmista on vuodesta 2014 lähtien rahoitettu useita tutkimusaloitteita, joissa keskitytään parantamaan terveydenhuoltolaitosten, kuten sairaaloiden, kykyä sietää kyberuhkia ja lieventämään uusien teknologioiden väärinkäyttöön liittyviä riskejä. Aloitteiden tuotoksina on kehitetty erilaisia erikoistyökaluja, kehyksiä ja järjestelmiä, kuten riskinarviointivälineitä, yksityisyyden suojan takaavia tiedonjakoalustoja, salausratkaisuja, kyberturvallisuustietoisuuden koulutusohjelmia ja reaaliaikaisia uhkien havaitsemisjärjestelmiä. Nämä ratkaisut on validoitu tiukasti terveydenhuollon toimintaympäristöissä toteutettujen todellisten pilottitoteutusten avulla. Tällä tavoin on varmistettu niiden tehokkuus ja käytännön sovellettavuus kyberuhkilta suojautumisessa.

Terveydenhuollon toimitusketjujen turvaaminen

Yhtenä terveydenhuollon organisaatioiden keskeisenä haasteena on hallita monimutkaisia tieto- ja viestintätekniikan toimitusketjuja, joihin liittyy monia erilaisia tuotteita, kuten verkkoon liitettyjä lääkinnällisiä laitteita, sähköisiä potilaskertomusjärjestelmiä ja toimistolaitteita. Sairaalat ja terveydenhuoltopalvelujen tarjoajat tarvitsevat toiminnassaan luotettavia ja turvallisia tieto- ja viestintäteknisiä järjestelmiä ja palveluja. Terveysalan kyberturvallisuushaasteisiin vastaamiseksi verkko- ja tietoturva-alan yhteistyöryhmän olisi toteutettava **koordinoitu turvallisuusriskien arviointi, jossa arvioidaan lääkinnällisten laitteiden toimitusketjuihin liittyviä sekä teknisiä että strategisia riskejä ja ehdotetaan riskejä lieventäviä toimenpiteitä**.[31] Verkko- ja tietoturva-alan yhteistyöryhmän olisi tarvittaessa tehtävä yhteistyötä lääkinnällisten laitteiden koordinointiryhmän kanssa.

Kyberkestävyyssäädös on uusi, kattava kehys, jossa asetetaan tuotteiden suunnittelua ja kehittämistä sekä aktiivisesti hyödynnettyjen haavoittuvuuksien käsittelyä, korjauspäivityksiä ja raportointia koskevia kyberturvallisuusvaatimuksia lähes kaikkien laitteisto- ja ohjelmistotuotteiden osalta arvoketjun jokaisessa vaiheessa.[32] Lääkinnälliset laitteet ovat tuotetyyppi, jota käytetään yhdellä yhteiskuntamme herkimmistä osa-alueista. Näitä tuotteita koskevat kyberturvallisuusvaatimukset perustuvat jo voimassa oleviin lääkinnällisiä laitteita koskevaan asetukseen ja in vitro -diagnostiikkaan tarkoitettuja lääkinnällisiä laitteita koskevaan asetukseen.[33] Kyseisten asetusten meneillään olevassa

[31] NIS 2 -direktiivin 22 artiklan mukaisesti.

[32] Ensimmäisessä vaiheessa monien lääkinnällisiä laitteita koskevan asetuksen ja in vitro -diagnostiikkaan tarkoitettuja lääkinnällisiä laitteita koskevan asetuksen soveltamisalaan kuulumattomien radiolaiteluokkien on 1. elokuuta 2025 alkaen täytettävä radiolaitedirektiivin olennaiset kyberturvallisuuteen liittyvät vaatimukset, kun tällaisia laitteita saatetaan sisämarkkinoille. Toisessa vaiheessa kyberkestävyyssäädöstä aletaan soveltaa 11. joulukuuta 2027.

[33] Lääkinnällisten laitteiden koordinointiryhmä antoi joulukuussa 2019 lääkinnällisten laitteiden kyberturvallisuutta koskevat ohjeet, joilla tuetaan valmistajia kyseisten kahden asetuksen liitteen I vaatimusten täyttämisessä: https://ec.europa.eu/docsroom/documents/41863.

arvioinnissa tarkastellaan mahdollisuuksia lisätä näiden kehysten välistä johdonmukaisuutta ja synergiaa yksinkertaistamisen ja huipputason kyberturvallisuuden takaamiseksi.

Riskinarvioinnin tulosten pitäisi myös auttaa terveydenhuollon organisaatioita tarkistamaan toimitusketjunsa kyberturvallisuuskäytännöt NIS 2 -direktiivin edellyttämällä tavalla. Tulosten pohjalta voitaisiin myös laatia **uudet hankintaohjeet**[34]. Tällaisissa ENISAn tukikeskuksensa avulla laatimissa ohjeissa olisi otettava huomioon viimeaikaiset kehityssuuntaukset, kuten pilvipalvelujen käytön yleistyminen potilastietojen säilytyksessä, sekä tarve siirtää sähköisiä terveystietoja turvallisesti pilvipalveluympäristöihin. Uusien ohjeiden pitäisi lisäksi tarjota organisaatioille käytännön välineitä, joiden avulla ne voivat seurata toimitusketjujaan, kuten tietoturvapalveluntarjoajien (MSSP) palveluja, varmennusraportteja tai kolmansista osapuolista johtuvien riskien arviointeja.

Pilvipalvelujen osalta tarvitaan lisätoimia, jotta voidaan vastata arkaluonteisten terveydenhuoltotietojen hallintaan liittyviin ainutlaatuisiin haasteisiin, kuten tiukempaan tietoturvaan ja yksityisyyden suojaan sekä operatiivisiin riskeihin. Suojatoimien vahvistamiseksi asiantuntijat suosittelevat, että oletusarvoinen ja sisäänrakennettu turvallisuus sisällytetään pilvipalveluihin. Tässä toimintatavassa asetetaan etusijalle turvallinen infrastruktuuri, haavoittuvuuksien ennakoiva hallinta sekä julkishallinnon ja yksityissektorin pilviratkaisujen yhdistelmä. Jatkuva valvonta ja myyjäkohtaiset varmennukset, kuten turvallisuuspalvelujen tarjoajien sertifioinnit ja kansallisten ja kansainvälisten standardien noudattamista koskevat tarkastukset, ovat myös olennaisen tärkeitä luotettavien kyberturvallisuuskäytäntöjen varmistamiseksi.

Infrastruktuuripalvelun (IaaS), alustapalvelun (PaaS) ja sovelluspalvelun (SaaS) kaltaisissa palveluissa kyberturvallisuuden toteutuminen on usein asiakkaan vastuulla. Monilla terveydenhuollon organisaatioilla ei kuitenkaan ole resursseja täyttää näitä vaatimuksia yksinään. Tämän vuoksi **pilvipalvelujen tarjoajia olisi kannustettava ottamaan käyttöön perustason turvallisuustoimenpiteitä vakio-ominaisuutena**. Tällaisilla toimenpiteillä pienennettäisiin virheellisten konfigurointien riskiä, ylläpidettäisiin johdonmukaista suojausta asiakkaiden hallitsemissa ympäristöissä ja annettaisiin parempi varmuus käyttäjille. Määrittämällä oletusarvoisen turvallisuuden perustaso pyrittäisiin tasapainottamaan toisaalta vankka suojaus ja toisaalta käytännöllisyys, ja näin varmistettaisiin palvelujen käytettävyys monien erilaisten terveydenhuollon organisaatioiden kannalta. Tämä toimi edellyttää pilvipalvelujen tarjoajien ja terveysalan välistä tiivistä yhteistyötä, jossa hyödynnetään alan parhaita käytäntöjä tehokkaiden ja skaalautuvien ratkaisujen luomiseksi.

Koulutus ja taitojen kehittäminen

Tarvittavat taidot omaava työvoima on tärkeä tekijä Euroopan pitkän aikavälin kestävän kasvun ja kilpailukyvyn sekä laadukkaiden palvelujen, myös terveydenhuoltopalvelujen, kannalta. Pula pätevistä kyberturvallisuusammattilaisista on merkittävä haaste kaikkialla Euroopassa, sillä työvoimatarpeiden

[34] ENISAn helmikuussa 2020 antamien sairaaloiden kyberturvallisuutta edistävien hankintaohjeiden (Procurement Guidelines for Cybersecurity in Hospitals) pohjalta. Ohjeet ovat saatavilla osoitteessa https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

täyttämiseksi EU:sta puuttuu arviolta 299 000 ammattilaista.[35] Kybertaitoja koskevan vuoden 2024 Eurobarometri-tutkimuksen[36] mukaan 81 prosenttia yrityksistä pitää vaikeuksia kyberturvallisuudesta vastaavien työntekijöiden palkkaamisessa keskeisenä riskinä, joka saattaa mahdollistaa kyberhyökkäyksiä. Koulutus-, terveys- ja sosiaalialoilla 66 prosenttia kyberturvallisuuteen liittyvistä tehtävistä hoitavat työntekijät, jotka ovat siirtyneet tehtäväänsä muista tehtävistä, mikä korostaa tarvetta järjestää kiireellisesti uudelleen- ja täydennyskoulutusta.

Tähän haasteeseen vastaamiseksi tukikeskuksen olisi tehtävä yhteistyötä kyberturvallisuusakatemiaa koskevassa komission tiedonannossa[37] tarkoitetun tulevia kyberturvallisuustaitoja koskevan eurooppalaisen digitaalisen infrastruktuurin konsortion (EDIC) kanssa. Tällä työllä on tarkoitus helpottaa terveydenhuoltoalan kyberturvallisuusammattilaisten, kuten keskustietojärjestelmien tietoturvavastaavien, välistä vaihtoa. Yksi mahdollinen toimi olisi **eurooppalaisen terveysalan keskustietojärjestelmien tietoturvavastaavien verkoston** perustaminen aloittaen asiantuntijaryhmästä, jossa jaetaan ja kehitetään parhaita käytäntöjä, osaamisen säilyttämistä koskevia strategioita sekä ratkaisuja kyberturvallisuusammattilaisten houkuttelemiseksi terveydenhuoltoalalle. Lisäksi kyberturvallisuusakatemian puitteissa olisi kehitettävä resursseja, joilla lisätään terveysalan kyberturvallisuushenkilöstöä toimialan ja tiedeyhteisön tuella. Tältä osin alan sidosryhmiä olisi kannustettava tukemaan kyberturvallisuuskoulutuksen lisäämistä.

Inhimilliset virheet ovat edelleen merkittävä terveydenhuoltoalan kyberturvallisuuspoikkeamien osasyy, mikä korostaa kriittistä tarvetta henkilöstön kattavalle koulutukselle ja kybertietoisuudelle. Koska terveydenhuollon ammattilaiset käyttävät usein digitaalisia välineitä, heille on tärkeää antaa tietoa turvallisista käytännöistä. Kohdennetuilla koulutus- ja valistuskampanjoilla riskejä voidaan vähentää merkittävästi. Tätä varten tukikeskuksen olisi tehtävä yhteistyötä terveydenhuollon ammattilaisten ja terveydenhuoltopalvelujen tarjoajien kanssa samoin kuin koulutuksen järjestäjien, toimialan, kyberturvallisuustaitoja koskevan eurooppalaisen digitaalisen infrastruktuurin konsortion ja jäsenvaltioiden viranomaisten kanssa, jotta voidaan luoda ja levittää **kattavia ja helposti saatavilla olevia verkkokoulutusmoduuleja ja -kursseja**.

Digitaalisten taitojen ja kyberturvallisuusmoduulien sisällyttäminen opetussuunnitelmiin on ratkaisevan tärkeää vahvan kyberturvallisuusperustan luomiseksi terveydenhuollossa. Näissä moduuleissa olisi käsiteltävä alakohtaisia kysymyksiä, kuten potilastietojen suojaamista ja haavoittuvuuksia lääkinnällisten laitteiden turvallisuudessa. Tällaisten resurssien kehittämisessä olisi otettava huomioon

[35] The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study | Digital Skills and Jobs Platform.
[36] Kybertaitoja koskeva Flash-eurobarometri 547.
[37] Komission tiedonanto Euroopan parlamentille ja neuvostolle: *Kyberturvallisuuteen liittyvän osaamisvajeen pienentäminen EU:n kilpailukyvyn, kasvun ja häiriönsietokyvyn parantamiseksi (”Kyberturvallisuusakatemia”)*, COM(2023) 207 final.

aiemmat toimet, kuten Erasmus+ -ohjelmasta rahoitettu BeWell-hanke[38] ja Horisontti 2020 -ohjelmasta rahoitettu PANACEA-hanke[39].

3.2. Terveysalaan kohdistuvien kyberuhkien eurooppalaiset havaitsemisvalmiudet

Kyberuhkien tehokas havaitseminen on olennaisen tärkeää, jotta poikkeamiin voidaan reagoida nopeasti. Uhkatoimijat voivat hyödyntää tekniikoita vaikeuttaakseen tunkeutumisen havaitsemista, mikä mahdollistaa sen, että järjestelmään voidaan saada luvaton pääsy pitkäksi aikaa.[40] Siksi paremmat uhkien havaitsemisvalmiudet voivat auttaa pysäyttämään kyberhyökkäykset. Esimerkiksi suomalaista psykoterapiapalvelujen tarjoajaa Vastaamoa vastaan tehdyssä kiristysohjelmahyökkäyksessä, jonka aikana tekijä kiristi potilaita, joiden potilastiedot oli varastettu, ensimmäinen tunkeutuminen tapahtui vuonna 2018, mutta se tuli palveluntarjoajan tietoon vasta vuonna 2020.[41]

Tehokas tietojenvaihto ja yhteistyö ovat olennaisen tärkeitä uhkien havaitsemisen ja tilannetietoisuuden parantamiseksi kaikkialla EU:ssa. Tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-yksiköt) ovat keskeisessä asemassa turvallisuuspoikkeamia, läheltä piti -tilanteita ja mahdollisia uhkia koskevien ilmoitusten vastaanottamisessa, ja ne antavat ohjeita lieventämistoimenpiteistä kansallisella tasolla. **Jäsenvaltioita kehotetaan kuitenkin painokkaasti myös jakamaan kaikki sairaaloiden ja terveydenhuoltopalvelujen tarjoajien kyberturvallisuuspoikkeamia koskevat ilmoitukset ENISAn tukikeskuksen kanssa EU:n laajuisen tilannetietoisuuden mahdollistamiseksi**. Ihannetapauksessa tähän olisi liitettävä turvallisuuspoikkeaman erilaisten merkityksellisten ulottuvuuksien tarkoituksenmukainen luonnehdinta, joka kattaa muun muassa taustalla olevat tunnetut haavoittuvuudet sekä vaikutukset terveydenhuoltopalveluihin ja potilaisiin kohdistuviin haittatapahtumiin. Lisäksi lääkinnällisten laitteiden ja in vitro -diagnostiikkaan tarkoitettujen laitteiden valmistajia kannustetaan ilmoittamaan vapaaehtoisesti ENISAn kyberkestävyyssäädöksen nojalla perustaman ja hallinnoiman keskitetyn raportointialustan kautta näiden laitteiden turvallisuuteen vaikuttavista hyödynnetyistä haavoittuvuuksista tai vakavista kyberturvallisuuspoikkeamista sekä mahdollisesti muista haavoittuvuuksista, poikkeamista, läheltä piti -tilanteista tai kyberuhkista, jotka voivat vaikuttaa näiden laitteiden riskiprofiiliin.

Kun ilmoitusten sisältämät tiedot eivät enää ole arkaluonteisia, tukikeskus voisi laatia ENISAn tuella eurooppalaisten tunnettujen hyödynnettyjen haavoittuvuuksien luettelon, joka kattaa lääkinnälliset laitteet, sähköiset potilaskertomusjärjestelmät sekä terveysalan tieto- ja viestintäteknisten laitteiden ja ohjelmistojen tarjoajat. Uhkien havaitsemiseen liittyviin merkittäviin haasteisiin vastaamiseksi tukikeskuksen olisi otettava käyttöön **EU:n laajuinen terveysalan ennakkovaroitusten tilauspalvelu, joka antaa lähes reaaliaikaisia varoituksia**. Palvelussa hyödynnettäisiin CSIRT-yksiköiltä,

[38] BeWell – Blueprint alliance for a future health workforce strategy on digital and green skills. Ks. https://bewell-project.eu/.
[39] PANACEA – Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for data and people. Ks. https://cordis.europa.eu/project/id/826293.
[40] ENISAn Health Threat Landscape 2023 -raportti.
[41] Suomen tietosuojavaltuutetun päätös 1150/161/2021.

terveydenhuoltoalan toimijoilta ja valmistajilta, julkisiin lähteisiin perustuvasta tiedustelusta (OSINT) ja muilta asiaankuuluvilta toimijoilta, kuten kyberkeskuksilta, tietojen jakamisen ja analysoinnin keskuksilta (ISAC-keskuksilta) ja lainvalvontaviranomaisilta, saatuja käsiteltyjä tietoja. ENISAn ja Euroopan unionin lainvalvontayhteistyöviraston (Europol) tehostettu yhteistyö – joko voisi koskea esimerkiksi terveysalaan kohdistuvan kyberrikollisuuden malleja – lisäisi tilannetietoisuutta entisestään.

ISAC-keskukset toimivat keskeisinä resursseina uhkatiedustelutiedon hankinnassa, luovat kaksisuuntaista tiedonvaihtoa julkisen ja yksityisen sektorin välillä ja edistävät luottamuksen rakentamista. Tukikeskuksen olisi lisättävä tukea **eurooppalaiselle terveysalan ISAC-keskukselle** välineiden, tietojenvaihdon ja alakohtaisten tilannetietoisuusraporttien avulla sekä edistämällä luotettavan yhteisön luomista taktista ja strategista yhteistyötä varten. Jäsenvaltioiden olisi edistettävä kansallisten terveysalan ISAC-keskusten kehittämistä.[42] ISAC-keskuksia olisi myös kannustettava saattamaan yhteen terveydenhuoltopalvelujen tarjoajat ja valmistajat, jotta myös toimitusketjussa esiintyvistä kyberturvallisuusuhista saadaan yhteinen käsitys ja jotta helpotetaan vuoropuhelua tuotteiden turvallisesta suunnittelusta, jossa otetaan aidosti huomioon käytännön käyttöönoton realiteetit.

3.3.Nopea reagointi ja palautuminen

Koska potilaiden terveystiedot ovat hyvin arkaluonteisia ja kyberhyökkäysten vaikutukset terveydenhuoltopalveluihin voivat olla tuhoisia, nopea ja tehokas reagointi kyberturvallisuuspoikkeamiin on ratkaisevan tärkeää potilasturvallisuuden takaamiseksi. Kun sairaala tai terveydenhuoltopalvelujen tarjoaja joutuu kyberhyökkäyksen kohteeksi, ensimmäiseksi on otettava yhteyttä asianomaiseen kansalliseen CSIRT-yksikköön.[43] CSIRT-yksikkö on vastuussa siitä, että tukea annetaan viipymättä, ihannetapauksessa 24 tunnin kuluessa, merkittävien poikkeamien hallitsemiseksi. Jos poikkeama kuitenkin ylittää CSIRT-yksikön valmiudet, olisi oltava mahdollista saada EU:n tukea nopean ja tehokkaan reagoinnin varmistamiseksi.

Kybersolidaarisuussäädöksen nojalla perustettu EU:n kyberturvallisuusreservi sisältää luotettavien tietoturvapalveluntarjoajien tarjoamia poikkeamienhallintapalveluja, jotka auttavat merkittäviin tai laajamittaisiin kyberturvallisuuspoikkeamiin reagoimisessa ja alkuvaiheen palautumistoimissa. Kyberturvallisuusreservin tarkoituksena on täydentää jäsenvaltioiden CSIRT-yksiköiden toimia ja antaa niille mahdollisuus pyytää lisätukea tapauksissa, joissa on kyse terveyden kaltaisista kriittisistä aloista. Tämän järjestelmän parantamiseksi **komission ja ENISAn olisi varmistettava, että reserviin sisältyy erityisesti terveydenhuoltoalaa koskeva nopean toiminnan palvelu**. Palvelu täydentäisi muita olemassa olevia kehyksiä, ja siinä lähetettäisiin asiantuntijoita hallitsemaan terveydenhuoltoalalla ilmeneviä merkittäviä tai laajoja kyberturvallisuuspoikkeamia viipymättä, kun kansallinen tuki ei riitä.

[42] Esimerkiksi Suomessa on sosiaali- ja terveysalan kansallinen ISAC-keskus. Ks. Kyberturvallisuuskeskus: ”ISAC-tiedonvaihtoryhmät”, saatavilla osoitteessa https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat?toggle=Sosiaali-%20ja%20terveydenhuoltoala.

[43] NIS 2 -direktiivin 23 artiklan 1 kohdan mukaan keskeisten ja tärkeiden toimijoiden on ilmoitettava merkittävistä poikkeamista asianomaiselle CSIRT-yksikölle tai tapauksen mukaan toimivaltaiselle viranomaiselle.

Reagoinnin ja palautumisen parantamiseksi tukikeskuksen olisi yhteistyössä verkko- ja tietoturva-alan yhteistyöryhmän, CSIRT-verkoston ja tarvittaessa Europolin kanssa laadittava **terveydenhuoltoa varten räätälöityjä kyberpoikkeamiin reagointia koskevia toimintaohjeita**. Nämä toimintaohjeet ohjaisivat sekä CSIRT-yksiköitä että terveydenhuollon organisaatioita niiden reagoidessa tiettyihin kyberturvallisuusuhkiin, kuten kiristysohjelmiin. Koska CSIRT-yksiköiden ja lainvalvontaviranomaisten tehokas yhteistyö rikollisiin kyberturvallisuuspoikkeamiin reagoimisessa ja niiden tutkimisessa on tärkeää, toimintaohjeissa olisi muun muassa annettava selkeitä ohjeita tällaisten poikkeamien ilmoittamisesta lainvalvontaviranomaisille. Lisäksi tukikeskus voisi **helpottaa kansallisten kyberturvallisuusharjoitusten laajaa käyttöönottoa ENISAn Cyber Europe 2022 -harjoituksen kaltaisista harjoituksista saatujen kokemusten pohjalta toimintaohjeiden testaamiseksi ja turvallisuuspoikkeamiin reagoimista koskevien protokollien vahvistamiseksi**.

Toimintapolitiikan perustaksi ja kiristysohjelmahyökkäysten vastaisten toimenpiteiden tehokkuuden arvioimiseksi on kerättävä lisää tietoja. Tätä varten jäsenvaltioiden olisi pyydettävä NIS 2 -direktiivin soveltamisalaan kuuluvia toimijoita, myös terveydenhuollon organisaatioita, raportoimaan muiden merkittävistä kyberturvallisuuspoikkeamista tehtävien ilmoitusten yhteydessä toimitettavien tietojen lisäksi kaikista lunnaista, joita ne ovat maksaneet tai aikovat maksaa. Tällainen raportointi tukee kiristystapausten tehokasta tutkintaa, kuten maksujen jäljittämistä kryptovaluuttojen vaihtoalustoilla vastaanottajien tunnistamiseksi.

Palautumisen nopeus on ratkaiseva tekijä häiriönsietokyvyn ja kansalaisten luottamuksen ylläpitämisessä erityisesti terveydenhuollossa, jossa käyttökatkot voivat häiritä potilaiden hoitoa. Jotta kiristysohjelmahyökkäyksistä palautuminen olisi tehokasta, terveydenhuoltopalvelujen tarjoajilla on oltava turvalliset, ajantasaiset ja erilliset varmuuskopiot, jotka voidaan palauttaa nopeasti. Tukikeskus voisi osana palveluluetteloaan tarjota **kiristysohjelmista palautumista koskevan tilauspalvelun, joka auttaa sairaaloita ja terveydenhuoltopalvelujen tarjoajia laatimaan palautumissuunnitelmia etukäteen**. ENISAn ja Europolin olisi tehtävä yhteistyötä tunnistaakseen yleisimmät terveydenhuollon organisaatioihin kohdistuvat kiristysohjelmatyypit ja **laajentaakseen** No More Ransom -hankkeessa[44] saatavilla olevaa **salauksenpurkuvälineiden tietovarastoa**. Niiden olisi myös laadittava ja tehtävä tunnetuksi helposti saatavilla olevia ohjeita, joilla autetaan terveydenhuoltopalvelujen tarjoajia välttämään lunnaiden maksaminen salauksenpurkuvälineiden avulla.

Kansainvälinen kiristysohjelmien vastainen aloite[45] tarjoaa arvokkaan foorumin, jolla voidaan keskustella konkreettisista kiristysohjelmapoikkeamista sekä kehittää jäsenvaltioiden valmiuksia vahvistaa kyberturvallisuuskehyksiään ja suorittaa kiristysohjelmia käyttävien toimijoiden vastaisia tutkintatoimia. Komissio edistää yhteistyössä unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan kanssa jatkossakin kiristyshaittaohjelmien vastaisessa aloitteessa tehtävää yhteistyötä muun muassa terveysalaan kohdistuvien kiristysohjelmauhkien torjumiseksi. Lisäksi komissio pyrkii saamaan aikaan yhteistyötä **G7-ryhmän kyberturvallisuutta käsittelevässä työryhmässä** terveysalan kyberturvallisuuden vahvistamiseksi. Työryhmä voisi erityisesti pohtia mahdollisuuksia tukea terveysalaa kiristysohjelmien kaltaisilta uhkilta suojautumisessa esimerkiksi Yhdistyneiden

[44] https://www.nomoreransom.org/en/index.html.
[45] https://www.counter-ransomware.org/.

kansakuntien turvallisuusneuvoston kokouksen yhteydessä 8. marraskuuta 2024 terveydenhuoltolaitoksiin kohdistuvista kiristysohjelmahyökkäyksistä annetussa yhteisessä julkilausumassa[46] esitettyjen näkökohtien pohjalta.

4. Kansalliset toimet

Se, voidaanko tällä toimintasuunnitelmalla parantaa kyberturvallisuutta terveysalalla, on riippuvaista jäsenvaltioiden aktiivisesta osallistumisesta ja sitoutumisesta. Jotta toimintasuunnitelma saadaan pantua onnistuneesti täytäntöön, jäsenvaltiot voisivat nimetä **kansallisia kyberturvatukikeskuksia erityisesti sairaaloita ja terveydenhuoltopalvelujen tarjoajia varten**. Nämä keskukset toimisivat terveysalan ensisijaisina yhteyspisteinä kansallisella tasolla ja tekisivät tiivistä yhteistyötä ENISAn tukikeskuksen kanssa. Jäsenvaltioiden olisi mahdollisuuksien ja tarpeen mukaan nimettävä kansallisiksi kyberturvatukikeskuksiksi jo olemassa olevia elimiä, kuten kansallisia terveysalan CSIRT-yksiköitä tai asiaankuuluvia viranomaisia.

Jäsenvaltioita kehotetaan myös laatimaan **kansallisia toimintasuunnitelmia, joissa keskitytään terveysalan kyberturvallisuuteen**. Toimintasuunnitelmissa hahmoteltaisiin terveydenhuoltojärjestelmiin kohdistuvat erityiset kyberturvallisuusriskit ja niihin puuttumiseksi toteutettavat kansalliset toimet. Lisäksi niillä varmistettaisiin, että unionin tason resursseja ja käytäntöjä hyödynnetään tehokkaasti. ENISAn tukikeskus voi auttaa näiden suunnitelmien laatimisessa ottamalla huomioon jo olemassa olevat kansalliset suunnitelmat ja koordinoimalla toimia sen varmistamiseksi, että yksittäisten jäsenvaltioiden resurssit ja strategiat täydentävät toisiaan.

Toisena jäsenvaltioiden keskeisenä painopisteenä on helpottaa terveydenhuoltopalvelujen tarjoajien resurssien jakamista, mikä voitaisiin saavuttaa kansallisella, alueellisella tai jopa unionin tasolla tehtävillä **yhteishankinnoilla tai resurssien yhdistämisellä**. Tällä tavoin vähennettäisiin yksittäisten toimijoiden taloudellista rasitetta ja lisättäisiin samalla niiden neuvotteluvoimaa suhteessa kyberturvallisuuspalvelujen tarjoajiin.

Esimerkiksi Ranskan CaRE-ohjelmassa[47] on otettu käyttöön useita kansallisen ja alueellisen tason toimenpiteitä, joilla vastataan resurssoinnin haasteisiin: ohjelman kyberluettelo sisältää yleiskatsauksen kyberratkaisuista ja -paketeista, jotka asetetaan sairaaloiden käyttöön kansallisen kyberturvallisuusviraston, digitaalisen terveydenhuollon viraston, alueellisten virastojen, kansallisten hankintaorganisaatioiden sekä kaupallisten ratkaisujen kautta. Tätä täydennetään lisärahoituksella, jonka avulla alueelliset virastot voivat tarjota yhteisiä resursseja.

[46] https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/.
[47] Ranskan digitaalisen terveydenhuollon virasto: Cybersécurité acceleration et Résilience des Établissements (CaRE). Ks. https://esante.gouv.fr/strategie-nationale/cybersecurite.

Jäsenvaltioiden olisi myös puututtava siihen, että terveysalalla ei investoida riittävästi kyberturvallisuuteen. Riittävän rahoituksen varmistamiseksi niiden olisi asetettava **ei-sitovia viitearvoja ja seurattava erityisesti kyberturvallisuuteen tähtääviä rahoitustavoitteita** ja varmistettava samalla, että nämä investoinnit eivät heikennä potilaiden oleellista hoitoa. Näillä rahoitustavoitteilla olisi myös pyrittävä sisällyttämään turvallisuusnäkökohdat kaikkiin alalla tehtäviin digitaalisiin investointeihin. Jäsenvaltiot voivat vaihtaa rahoitustavoitteita koskevia parhaita käytäntöjä ja neuvoja sähköisten terveyspalvelujen verkoston[48] kaltaisten alustojen kautta.

5. Julkisen ja yksityisen sektorin yhteistyö

Julkisen ja yksityisen sektorin yhteistyö sekä terveydenhuoltopalvelujen tarjoajien, muiden terveysalan toimijoiden ja asiaankuuluvien kyberturvallisuusalan toimijoiden kuuleminen ovat olennaisen tärkeitä seikkoja toimintasuunnitelman onnistuneen täytäntöönpanon kannalta. **Komissio perustaa ENISAn tuella yhteisen terveysalan kyberturvallisuuden neuvoa-antavan lautakunnan**, johon kuuluu korkean tason edustajia sekä terveydenhuollon että kyberturvallisuuden aloilta ja jonka pohdinnat otetaan huomioon tukikeskuksen työssä. Lautakunta voi antaa komissiolle ja tukikeskukselle neuvontaa vaikuttavista toimista, ja siinä voidaan keskustella julkisen ja yksityisen sektorin kumppanuuksien kehittämisestä tällä alalla. Lautakunnan työ perustuu julkisen ja yksityisen sektorin kumppanuuksia koskeviin nykyisiin toimiin, kuten eurooppalaiseen terveysalan ISAC-keskukseen.

Lisäksi komissio aikoo osoittaa kyberturvallisuusyrityksille, säätiöille, oppilaitoksille ja alan sidosryhmille **toimintakehotuksen sitoutua toimiin, joilla vastataan alan haasteisiin**. Kyberturvallisuusakatemiasta saatujen kokemusten pohjalta tällaiset sitoumukset voisivat olla esimerkiksi kyberturvallisuusakatemian puitteissa tehtyjä sitoumuksia tarjota kyberturvallisuusalan ammattilaisille koulutuskursseja ja -materiaaleja, joissa keskitytään terveysalaan.[49] Muut sitoumukset voisivat koskea muun muassa tietoisuuden lisäämistä koskevia toimia tai tietoturvapalvelujen tarjoamista ilmaiseksi tai alennettuun hintaan erityisesti haavoittuvassa asemassa oleville toimijoille niiden varautumisen ja kyberuhkien sietokyvyn parantamiseksi. Sitoumukset voisivat koskea myös uhkatiedustelutiedon jakamista ENISAn tukikeskuksen kanssa. Tukikeskuksen olisi seurattava toimintakehotuksen perusteella annettuja sitoumuksia niiden johdonmukaisuuden ja täydentävyyden varmistamiseksi.

6. Kyberuhkatoimijoiden torjuminen

EU:n sisäisillä ja ulkoisilla kyberturvallisuutta koskevilla toimintapolitiikoilla olisi tuettava tavoitetta estää kyberuhkatoimijoita hyökkäämästä eurooppalaisiin terveydenhuoltojärjestelmiin. Terveydenhuollon organisaatioihin kohdistuvat kyberhyökkäykset ovat haitallisten kybertoimien tyyppi, jota on erityisen mahdoton hyväksyä, koska ne voivat uhata potilasturvallisuutta ja ihmishenkiä. Sen vuoksi EU:lla kyberturvallisuuden ja lainvalvonnan alalla olevia torjuntavalmiuksia olisi käytettävä

[48] Sähköisten terveyspalvelujen verkosto on direktiivin 2011/24/EU 14 artiklan nojalla perustettu jäsenvaltioiden nimeämien sähköisistä terveyspalveluista vastaavien kansallisten viranomaisten vapaaehtoinen verkosto.
[49] Cyber Skills Academy: Get Involved | Digital Skills and Jobs Platform.

niiden koko voimalla, jotta horjutetaan hyökkäyksiä terveysalaan kohdistavien uhkatoimijoiden yleistä toimintamallia ja estetään niitä saamasta helppoja voittoja. Tähän sisältyisi rajatylittävien tutkintatoimien edistäminen lisäämällä vaarantumisindikaattorien ja muiden merkityksellisten tietojen jakamista ja keskittymällä voimakkaammin arvokkaisiin kohteisiin ja keskeisiin rikollisuutta helpottaviin tekijöihin, kuten lainvalvontaviranomaisten pyynnöistä ja kehotuksista piittaamattomiin niin kutsuttuihin ”bulletproof hosting” -palveluihin ja kryptovaluuttasekoittimiin.

Kyberdiplomatian välineistö tarjoaa kehyksen EU:hun, jäsenvaltioihin ja kumppaneihin kohdistuvien kyberhyökkäysten ehkäisemiseksi, estämiseksi ja niihin vastaamiseksi. Ulkoasioiden ja turvallisuuspolitiikan korkea edustaja hyödyntää myös jatkossa nykyistä kyberpakotejärjestelmää terveydenhuoltojärjestelmiin kohdistuviin uhkiin vastaamiseksi.

Rikollisten toimijoiden saattaminen vastuuseen teoistaan on merkittävä pelote. Sen vuoksi jäsenvaltioiden olisi varmistettava, että lainvalvonta sisällytetään kaikilta osin niiden kansallisiin toimintasuunnitelmiin. Niiden olisi etenkin hyödynnettävä täysimääräisesti tietojärjestelmiin kohdistuvia hyökkäyksiä koskevan direktiivin[50] säännöksiä ja tietoverkkorikollisuutta koskevan Euroopan neuvoston Budapestin yleissopimuksen[51] määräyksiä hyökkäysten estämiseksi, rikollisten saattamiseksi oikeuden eteen ja hyökkäyksiä helpottavien rikollisten infrastruktuurien purkamiseksi. Näiden välineiden onnistuneella täytäntöönpanolla olisi varmistettava, että terveydenhuoltoon kohdistuvista rikollisista ja pahantahtoisista toimista seuraa rangaistus.

7. Toimintasuunnitelman täytäntöönpano ja seuranta

Tässä toimintasuunnitelmassa on kaavailtu useita tehtäviä ENISAan perustettavalle tukikeskukselle. Näin varmistetaan toimintasuunnitelman kokonaisvaltainen ja johdonmukainen täytäntöönpano ja vältetään uusien toimijoiden luominen, mikä voisi aiheuttaa päällekkäisyyksiä ja yleiskustannuksia. Komissio aikoo varmistaa, että tukikeskukselle myönnetään riittävät resurssit.

Kun tukikeskus on toiminnassa, ENISAn olisi komissiota kuullen esitettävä säännöllisesti tilannekatsauksia tukikeskuksen työstä ENISAn johtokunnalle sekä jäsenvaltioiden asiaankuuluville verkostoille, erityisesti verkko- ja tietoturva-alan yhteistyöryhmälle, CSIRT-verkostolle, sähköisten terveyspalvelujen verkostolle ja tarvittaessa eurooppalaisen terveysdata-avaruuden neuvostolle. Lisäksi ENISAn olisi jatkuvasti keskusteltava terveysalan kyberturvallisuutta käsittelevän julkisen ja yksityisen sektorin yhteisen neuvoa-antavan lautakunnan kanssa tukikeskuksen tarjoamien toimien täytäntöönpanosta.

ENISAn säännöllisiä kertomuksia, kuten kyberturvallisuuden tilaa unionissa koskevaa kertomusta, jossa esitetään kokonaisarvio kyberturvallisuusvalmiuksien ja -resurssien kehitystasosta eri puolilla EU:ta, myös terveysalalla, olisi hyödynnettävä mahdollisuutena julkaista asiaankuuluvia tietoja

[50] Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU, annettu 12 päivänä elokuuta 2013, tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta: https://eur-lex.europa.eu/eli/dir/2013/40/oj/.

[51] Tietoverkkorikollisuutta koskeva yleissopimus (Budapestin yleissopimus, ETS nro 185) ja sen pöytäkirjat: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

toimintasuunnitelman seurannan tueksi. Lisäksi ENISAn EU:n kyberturvallisuusindeksi[52] voi antaa määrällistä ja laadullista tietoa, jota voidaan käyttää tietopohjana terveysalan kriittisyyden ja kehitystason arvioinnissa.

8. Seuraavat vaiheet

Tässä tiedonannossa esitetään kunnianhimoinen toimintasuunnitelma, jolla parannetaan terveysalan kyberturvallisuutta EU:ssa. Toimintasuunnitelmassa ehdotettu ENISAn yhteyteen perustettava kyberturvatukikeskus sairaaloita ja terveydenhuoltopalvelujen tarjoajia varten tarjoaa keinon luoda johdonmukainen ja yhteinen eurooppalainen lähestymistapa alan kyberturvallisuuden muodostamaan haasteeseen.

Tätä tiedonantoa olisi pidettävä alkuna prosessille, jolla parannetaan kyberturvallisuutta terveysalalla. Sen vuoksi toimintasuunnitelman hyväksymisen yhteydessä käynnistetään kattava sidosryhmien kuuleminen ja jatketaan keskusteluja jäsenvaltioiden ja asiaankuuluvien verkostojen kanssa tietojen keräämiseksi. Kuulemisten tulosten perusteella komissio aikoo antaa vuoden 2025 viimeisellä neljänneksellä suosituksia toimintasuunnitelman tarkentamiseksi edelleen.

Komissio kehottaa jäsenvaltioita ja kaikkia sidosryhmiä tekemään yhteistyötä toimintasuunnitelman tavoitteiden saavuttamiseksi.

[52] ENISA, EU Cybersecurity Index, Framework and Methodological Note (2024). Saatavilla osoitteessa https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

LIITE – Yhteenveto ehdotetuista toimista

Komissio:

ENISAn kyberturvatukikeskus sairaaloille ja terveydenhuoltopalvelujen tarjoajille	
Varmistetaan kyberturvatukikeskuksen riittävät resurssit. Käynnistetään yhteistyössä Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen kanssa pilottihankkeita, joilla laaditaan kyberhygieniaa ja turvallisuusriskien arviointia koskevia parhaita käytäntöjä ja vastataan jatkuvan kyberturvallisuuden seurannan, uhkatiedustelutietojen ja poikkeamiin reagoimisen tarpeeseen käyttämällä huipputason kyberturvallisuusratkaisuja, eurooppalaisen kyberturvatukikeskuksen palveluluettelon kehittämiseksi.	2025
Kyberturvallisuuspoikkeamien ennaltaehkäisy	
Tutkitaan verkko- ja tietoturva-alan yhteistyöryhmää, EU-CyCLONe-verkostoa ja ENISAa kuullen mahdollisuutta määritellä terveys alaksi, jolle voidaan antaa kybersolidaarisuussäädöksen nojalla tukea varautumisen koordinoituun testaukseen.	Vuoden 2025 ensimmäinen neljännes
Nopea reagointi ja palautuminen	
Varmistetaan yhdessä ENISAn kanssa, että EU:n kyberturvallisuusreserviin sisältyy erityisesti terveysalaa koskeva nopean toiminnan palvelu.	Vuoden 2025 viimeinen neljännes
Julkisen ja yksityisen sektorin yhteistyö	
Perustetaan ENISAn tukema yhteinen terveysalan kyberturvallisuuden neuvoa-antava lautakunta.	Vuoden 2025 ensimmäinen neljännes
Esitetään kyberturvallisuusyrityksille, säätiöille, oppilaitoksille ja alan sidosryhmille toimintakehotus sitoutua toimiin, joilla vastataan terveysalan haasteisiin.	Vuoden 2025 toinen neljännes
Kyberuhkatoimijoiden torjuminen	
Tutkitaan yhdessä korkean edustajan kanssa kyberdiplomatian välineistön käyttöä terveydenhuoltojärjestelmiin kohdistuvien haitallisten	2025

toimien ehkäisemiseksi, hillitsemiseksi ja estämiseksi sekä niihin reagoimiseksi.	
Edistetään yhteistyössä korkean edustajan kanssa erityisesti kansainvälisessä kiristysohjelmien vastaisessa aloitteessa tehtävää kansainvälistä yhteistyötä kiristysohjelmia käyttäviä toimijoita vastaan.	2025–2026
Pyritään saamaan aikaan yhteistyötä G7-ryhmän kyberturvallisuutta käsittelevässä työryhmässä terveysalan kyberturvallisuuden vahvistamiseksi.	2025–2026
Seuraavat vaiheet	
Käynnistetään kattavia sidosryhmien kuulemisia.	Vuoden 2025 ensimmäinen neljännes
Annetaan suosituksia toimintasuunnitelman tarkentamiseksi.	Vuoden 2025 viimeinen neljännes

ENISA:

EU:n kyberturvatukikeskus sairaaloille ja terveydenhuollon tarjoajille	
Aloitetaan työ eurooppalaisen kyberturvatukikeskuksen perustamiseksi sairaaloille ja terveydenhuoltopalvelujen tarjoajille.	Vuoden 2025 toinen neljännes
Laaditaan kattava luettelo kyberturvatukikeskuksen tarjoamista palveluista.	Vuoden 2025 viimeisestä neljänneksestä alkaen
Kyberturvallisuuspoikkeamien ennaltaehkäisy	
Annetaan ohjeita, joissa korostetaan kriittisimpiä kyberturvallisuuskäytäntöjä ja joilla autetaan terveydenhuoltopalvelujen tarjoajia näiden käytäntöjen toteuttamisessa.	Vuoden 2025 kolmas neljännes
Kehitetään tiiviissä yhteistyössä komission ja jäsenvaltioiden kanssa sääntelyn kartoitustyökalu.	Vuoden 2025 ensimmäinen neljännes
Kehitetään nimenomaan terveydenhuoltoa koskeva kyberturvallisuuden kehitystason arviointikehys.	Vuoden 2025 kolmas neljännes
Suoritetaan vuosittain terveysalan kyberturvallisuuden kehitystason arviointi.	2025–2026
Tehdään yhteistyötä jäsenvaltioiden ja alueellisten ohjelmaviranomaisten kanssa	2025–2026

kyberturvallisuusarvoseteleitä koskevien malliohjelmien luomiseksi.	
Laaditaan uudet sairaaloiden ja terveydenhuoltopalvelujen tarjoajien kyberturvallisuutta edistävät hankintaohjeet.	Vuoden 2025 kolmas neljännes
Luodaan eurooppalainen terveysalan keskustietojärjestelmien tietoturvavastaavien (CISO) verkosto.	Vuoden 2026 ensimmäinen neljännes
Suunnitellaan ja edistetään terveydenhuollon ammattilaisille tarkoitettuja kyberturvallisuusmoduuleja ja -kursseja.	Vuoden 2026 ensimmäinen neljännes
Terveysalaan kohdistuvien kyberuhkien eurooppalaiset havaitsemisvalmiudet	
Kootaan eurooppalainen tunnettujen hyödynnettyjen haavoittuvuuksien luettelo, joka kattaa lääkinnälliset laitteet, sähköiset potilaskertomusjärjestelmät sekä terveysalan tieto- ja viestintäteknisten laitteiden ja ohjelmistojen tarjoajat.	Vuoden 2025 viimeinen neljännes
Otetaan käyttöön EU:n laajuinen terveysalan ennakkovaroitusten tilauspalvelu.	Vuodesta 2026 alkaen
Tuetaan eurooppalaista terveysalan ISAC-keskusta välineillä ja tietojenvaihdolla.	2025–2026
Nopea reagointi ja palautuminen	
Varmistetaan yhdessä komission kanssa, että EU:n kyberturvallisuusreserviin sisältyy erityisesti terveysalaa koskeva nopean toiminnan palvelu.	Vuoden 2025 viimeinen neljännes
Laaditaan yhteistyössä CSIRT-verkoston kanssa terveydenhuollon tarpeisiin räätälöityjä kyberturvallisuuspoikkeamiin reagointia koskevia toimintaohjeita.	Vuoden 2025 kolmas neljännes
Edistetään kansallisten kyberturvallisuusharjoitusten laajaa käyttöönottoa toimintaohjeiden testaamiseksi ja turvallisuuspoikkeamiin reagoimista koskevien protokollien vahvistamiseksi.	Vuoden 2025 viimeisestä neljänneksestä alkaen
Tarjotaan kiristysohjelmista palautumista koskeva tilauspalvelu.	Vuodesta 2026 alkaen
Tunnistetaan yhteistyössä Europolin kanssa yleisimmät terveydenhuollon organisaatioihin kohdistuvat kiristysohjelmatyypit ja laajennetaan No	Vuoden 2025 viimeinen neljännes

More Ransom -hankkeessa saatavilla olevaa salauksenpurkuvälineiden tietovarastoa.	
Laaditaan yhteistyössä Europolin kanssa helposti saatavilla olevia ohjeita, joilla autetaan terveydenhuollon tarjoajia välttämään lunnaiden maksaminen.	Vuoden 2025 kolmas neljännes
Kansalliset toimet	
Avustetaan jäsenvaltioita kansallisten toimintasuunnitelmien laatimisessa.	2025
Koordinoidaan toimia sen varmistamiseksi, että yksittäisten jäsenvaltioiden resurssit ja strategiat täydentävät toisiaan.	2025–2026
Toimintasuunnitelman täytäntöönpano ja seuranta	
Esitetään komissiota kuullen säännöllisesti tilannekatsauksia kyberturvatukikeskuksen työstä jäsenvaltioiden asiaankuuluville verkostoille.	2025–2026
Pidetään jatkuvasti yhteyttä terveysalan kyberturvallisuuden neuvoa-antavaan lautakuntaan.	2025–2026

Jäsenvaltiot:

terveysalaan kohdistuvien kyberuhkien eurooppalaiset havaitsemisvalmiudet	
Jaetaan NIS 2 -direktiivin soveltamisalaan kuuluvien sairaaloiden ja terveydenhuollon tarjoajien poikkeamailmoitukset eurooppalaisen kyberturvatukikeskuksen kanssa.	Vuoden 2025 viimeisestä neljänneksestä alkaen
Kannustetaan kansallisten terveysalan ISAC-keskusten kehittämistä.	2025–2026
Kyberturvallisuuspoikkeamien ennaltaehkäisy	
Toteutetaan verkko- ja tietoturva-alan yhteistyöryhmässä koordinoitu turvallisuusriskien arviointi, jossa arvioidaan lääkinnällisten laitteiden toimitusketjuihin liittyviä sekä teknisiä että strategisia riskejä.	Vuoden 2025 viimeinen neljännes
Nopea reagointi ja palautuminen	

Otetaan käyttöön kansalliset kyberturvallisuusharjoitukset toimintaohjeiden testaamiseksi ja turvallisuuspoikkeamiin reagoimista koskevien protokollien vahvistamiseksi.	Vuodesta 2026 alkaen
Kansalliset toimet	
Nimetään kansallisia kyberturvatukikeskuksia sairaaloille ja terveydenhuollon tarjoajille.	Vuoden 2025 toinen neljännes
Laaditaan terveysalan kyberturvallisuuteen keskittyviä kansallisia toimintasuunnitelmia.	Vuoden 2025 viimeinen neljännes
Helpotetaan resurssien jakamista terveydenhuoltopalvelujen tarjoajien kesken.	2025–2026
Asetetaan ei-sitovia viitearvoja ja seurataan erityisesti kyberturvallisuuteen tähtääviä rahoitustavoitteita.	Vuoden 2025 viimeinen neljännes
Pyydetään terveydenhuollon organisaatioita ja muita NIS 2 -direktiivin soveltamisalaan kuuluvia toimijoita ilmoittamaan aikeistaan maksaa lunnaita.	Vuoden 2025 viimeinen neljännes