Euroopa Liidu
Nõukogu

Brüssel, 16. jaanuar 2025
(OR. en)

5426/25

CYBER 21
SAN 15

SAATEMÄRKUSED

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Martine DEPREZ, direktor
Kättesaamise kuupäev:	15. jaanuar 2025
Saaja:	Thérèse BLANCHET, Euroopa Liidu Nõukogu peasekretär
Komisjoni dok nr:	COM(2025) 10 final
Teema:	KOMISJONI TEATIS EUROOPA PARLAMENDILE, NÕUKOGULE, EUROOPA MAJANDUS- JA SOTSIAALKOMITEELE NING REGIOONIDE KOMITEELE Euroopa haiglate ja tervishoiuteenuse osutajate küberturvalisuse tegevuskava

Käesolevaga edastatakse delegatsioonidele dokument COM(2025) 10 final.

Lisatud: COM(2025) 10 final

EUROOPA
KOMISJON

Brüssel, 15.1.2025
COM(2025) 10 final

KOMISJONI TEATIS EUROOPA PARLAMENDILE, NÕUKOGULE, EUROOPA MAJANDUS- JA SOTSIAALKOMITEELE NING REGIOONIDE KOMITEELE

Euroopa haiglate ja tervishoiuteenuse osutajate küberturvalisuse tegevuskava

1. Sissejuhatus

ELi julgeolekukeskkond muutub kiiresti – meie ühiskonna destabiliseerimiseks tehakse üha rohkem hübriidrünnakuid ja küberründeid, mille eesmärk on tekitada konflikte ja korratust, aga ka küberkuritegevusest rahalist kasu saada. Sellise uue reaalsusega toime tulemiseks peab Euroopa seega kiiremas korras suurendama oma valmisolekut ja kerksust kõigis sektorites, järgides kogu ühiskonda ja kogu valitsemissektorit hõlmavat lähenemisviisi, nagu mainiti Euroopa Komisjoni presidendi erinõuniku Sauli Niinistö aruandes.

Turvalised ja kerksed tervishoiusüsteemid on ELi sotsiaalse mudeli alustala. Samas ähvardavad haiglaid ja tervishoiusüsteeme üha suuremad ohud – eeskätt püüavad neid rünnata lunavararündeid korraldavad grupeeringud, kes on huvitatud rahalisest kasust ja kelle tegevuse ajendiks on patsiendiandmete, sealhulgas elektrooniliste terviseandmete suur väärtus. Viimase nelja aasta jooksul on tervishoiusektorist saanud ELi kõige rohkem rünnatud tööstusharu; see ajavahemik hõlmab ka COVID-19 pandeemiat, mille jooksul sagenesid küberründed tervisetaristu vastu. Haiglate ja tervishoiuteenuse osutajate vastu suunatud küberründed põhjustavad inimestele otsest kahju, need tekitavad raviprotseduurides viivitusi ja kiirabivastuvõtus ülekoormust ning võivad äärmuslikel juhtudel tuua kaasa inimohvreid.

Sektoris toimuv eluliselt tähtis digipööre tähendab, et olukord muutub üha pingelisemaks. E-tervis ning terviseandmete kasutamine ja taaskasutamine võivad aidata pakkuda inimeste ja patsientide vajaduste ja eelistustega paremini sobivaid ravivõimalusi, hoides ära haiguste avaldumist ja võimaldades varasemat ravi. Digivahendite ja -lahenduste integreerimine kliinilistesse protsessidesse ning terviseandmete kasutamine ja taaskasutamine võib anda teavet, mille põhjal teha paremaid kliinilisi otsuseid, ning aidata tervishoiulahendusi automatiseerida ja patsientide ravi kiiremaks ja paremaks muuta. Digivahendid, andmekasutus ja meditsiiniseadmed (mis on sageli internetiga ühendatud ja kasutavad tehisintellekti võimalusi) on olulised ka selleks, et tulla toime selliste probleemidega nagu tervishoiutöötajate nappus.

Samal ajal laiendavad digivahendid ka küberkurjategijate võimalike sihtmärkide ringi. Veelgi enam, nagu näitab Venemaa jätkuv agressioonisõda Ukraina vastu, ei ole tervishoiuasutuste sihikule võtmine teatavate riikide jaoks tabu. See tähendab, et kõnealune sektor on suuremate hübriidkampaaniate raames küberrünnete sihtmärk. Küberründed seavad ohtu patsientide turvalisuse, kuid lisaks sellele vähendavad need üldsuse usaldust tervishoiutaristu vastu ja on taaste mõttes äärmiselt kulukad. Peale selle, et kerkne ja turvaline digitaristu pakub kaitset küberrünnete vastu, on see ülioluline ka selleks, et toetada Euroopa terviseandmeruumi[1] rakendamist ja täielikku kasutuselevõttu.

Seega on aeg tõsta ja tugevdada Euroopa haiglate ja tervishoiuteenuse osutajate küberturvalisuse ja kerksuse taset, nagu president von der Leyen 2024.–2029. aasta komisjoni poliitilistes suunistes[2] märkis. Käesolevas tegevuskavas käsitletakse olukorra pakilisust ja tervishoiusektorit ähvardavaid ainulaadseid ohte. Tervishoiuvaldkonna küberturvalisusega seotud probleemide lahendamiseks ei ole olemas lihtsat imerohtu. Selle asemel sisaldab tegevuskava üleskutset tugevdada ennetustööd ja valmisolekut ning läheneda solidaarsusele koordineeritumalt, kasutades ühtlasi Euroopa küberturvalisussektori eksperditeadmisi. Sellisel kujul peegeldab tegevuskava ELi lähenemisviisi julgeolekule. Selle

[1] https://www.consilium.europa.eu/et/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_et

lähenemisviisi arendamisega tegeletakse veel ja see sõnastatakse tulevases Euroopa Liidu sisejulgeoleku strateegias, milles määratakse kindlaks kõigile sisejulgeoleku ohtudele reageerimiseks mõeldud kõikehõlmavad meetmed ning keskendutakse ohtude ennetamise suutlikkusele, et hoida ära kahju tekkimist ja kaitsta inimesi, tegutsedes kõigil tasanditel kogu ühiskonda hõlmava lähenemisviisi põhjal.

Tervishoiusektorisse kuulub arvukalt üksusi ja tegijaid: haiglad, kliinikud, hooldekodud, taastusravikeskused ja mitmesugused tervishoiuteenuse osutajad, aga ka ravimi-, meditsiini- ja biotehnoloogiatööstus, meditsiiniseadmete tootjad ja tervisealaste teadusuuringutega tegelevad asutused. Valdavalt keskendub tegevuskava haiglate ja tervishoiuteenuse osutajate küberturvalisusele, kusjuures haigla ja tervishoiuteenuse osutaja all mõeldakse mis tahes füüsilist või juriidilist isikut või muud üksust, kes osutab liikmesriigi territooriumil seaduslikult tervishoiuteenuseid[3]. Haiglad ja tervishoiuteenuse osutajad on muude tervishoiuüksustega seotud, kuid nemad on inimestele kõige lähemal. Samas peaksid haiglate ja tervishoiuteenuse osutajate küberturvalisuse parandamise meetmed võtma arvesse ka riske, mis mõjutavad laiemat tarneahelat ja ökosüsteemi ning mille põhjustajaks on näiteks üksused, kes kasutavad terviseandmeid teadustöö või masinõppe jaoks või toodavad meditsiiniseadmeid, eeskätt digifunktsioonidega meditsiiniseadmeid, mida saab ühendada interneti või muude seadmetega („esemevõrk“).

Kuigi tervishoiusüsteemide turvalisuse tagamine on esmajoones liikmesriikide pädevuses, on kogu liidus küberturvalisuse ühtlaselt kõrge taseme tagamise meetmeid käsitlevas direktiivis (küberturvalisuse 2. direktiiv)[4] tervishoidu nimetatud kriitilise tähtsusega sektorina. Küberkurjategijad ja muud ohusubjektid tegutsevad piiriüleselt ning ka tervishoiuorganisatsioonide küberturvalisuse probleemid on eri liikmesriikides sarnased. Euroopa tasandi koostöö on ELi ja riikide tasandi parimate tavade jagamiseks ja levitamiseks väga tähtis. Seepärast tehakse tegevuskavas ettepanek ELi tasandi koordineerimise ja meetmete kohta ning esitatakse ühtlasi liikmesriikidele üleskutse tegutseda tervishoiu ja laiemalt tervise ökosüsteemi arengu huvides.

Tegevuskavas on olulisimal kohal sektori suutlikkuse suurendamine, et küberintsidente **ära hoida**, sest ennetamine on alati parem kui ravi. Teiseks kirjeldatakse tegevuskavas meetmeid, millega parandada küberturvalisuse alase teabe jagamist ja küberohtude **avastamise** suutlikkust, et seeläbi kiiremini reageerida. Kolmandaks sisaldab tegevuskava meetmeid, mis võimaldavad intsidentidele paremini **reageerida** ja neist **taastuda**. Ja lõpuks on tegevuskavas visandatud võimalused, kuidas **heidutada** küberohusubjekte Euroopa tervishoiusüsteeme ründamast.

Tegevuskava hakatakse rakendama koos tervishoiuteenuse osutajate ja laiema terviseökosüsteemi, liikmesriikide ja küberturvalisuse kogukonnaga. Kõige mõjusamate meetmete kindlaksmääramisel ja viimistlemisel on otsustava tähtsusega koostööpõhine lähenemisviis, et neist meetmetest oleks kasu kõigile Euroopa kriitilise tähtsusega tervishoiuteenuse osutajatele. Seepärast kuulutatakse käesoleva teatisega samal ajal välja põhjalik konsultatsioon sidusrühmade, tööstuse ja liikmesriikidega. Küberohud

[3] Euroopa Parlamendi ja nõukogu direktiivi 2011/24/EL (patsiendiõiguste kohaldamise kohta piiriüleses tervishoius) artikli 3 punkt g, https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex:32011L0024.

[4] Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus (küberturvalisuse 2. direktiiv), https://eur-lex.europa.eu/eli/dir/2022/2555.

on oma olemuselt piirideta ja omavahel seotud ning see muudab rahvusvahelise koostöö küberturvalisuse jaoks eriti oluliseks. Võrreldavad küberohud esinevad ka laienemisprotsessi riikides, Euroopa naabruses asuvates riikides ja muudes ELi strateegilistes partnerriikides. Varem või hiljem võib see seada ohtu ka ELi elutähtsa taristu turvalisuse. Pidades silmas seda, milliste ohutasemetega puutuvad kokku laienemisprotsessis osalevad riigid ja muud partnerriigid, on oluline, et EL võtaks ka nendega tehtavas koostöös arvesse tegevuskava rakendamisel saadud õppetunde.

2. Haiglate ja tervishoiuteenuse osutajate küberturvalisuse tagamise keerukus

Tervishoiusektorit ähvardavad küberohud

Küberründeid tuleb ette üha rohkem nii kogu maailmas kui ka ELis ning ohtude maastik muutub üha keerukamaks ja dünaamilisemaks. Tehisintellekti valdkonna areng annab kurjategijatele ja kuritahtlikele isikutele võimsad tööriistad, millega nad saavad oma tegevust täpsemaks ja mõjusamaks muuta, kuid samas kujundab see areng ümber ka küberkaitse võimalused, sest võimaldab rünnetele reageerida automaatselt ja reaalajas.

Ikka veel on ELis ja kogu maailmas oluliseks küberturvalisuse probleemiks lunavararünded, millega seotud ülemaailmsete kulude suuruseks aastal 2031 prognoositi ühes aruandes enam kui 250 miljardit eurot[5]. Kui kurjategijad teevad lunavararünde, siis nad mitte ainult ei krüpteeri ohvri andmeid, vaid üha sagedamini lekitavad nad täiendava surve avaldamiseks tundlikku teavet. Tähelepanu vääriv probleem on ka tark- ja riistvara nõrkused: Euroopa Liidu Küberturvalisuse Ameti (ENISA)[6] andmetel on tervishoiusektor teatanud kõige arvukamatest selliste nõrkustega seotud turvaintsidentidest[7]. Kasvab ka näiteks hajusate teenusetõkestusrünnete ehk DDoS rünnete arv, mille käigus ujutatakse rünnatav süsteem andmeliiklusega üle ja muudetakse see õiguspärase kasutaja jaoks kättesaamatuks[8].

Tervishoiusektorit ähvardavate ohtude suundumused on samalaadsed, kusjuures eriti olulisel kohal on lunavararünded. ENISA andmetel moodustasid lunavararünded kõigist tervishoiusektori analüüsitud küberintsidentidest 2021.–2023. aastal 54 %. 83 % juhtudel olid ründe eesmärgid rahalised ja tulenesid tervishoiuandmete suurest väärtusest ning 10 % juhtudel olid ründe põhjused ideoloogilised[9]. Komisjoni

[5] Cybersecurity Ventures (1. juuni 2024): „Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031“. Kättesaadav aadressil: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

[6] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist (küberturvalisuse määrus), https://eur-lex.europa.eu/eli/reg/2019/881/oj/est.

[7] ENISA ohtude kaardistamise aruanne: tervishoiusektor (juuli 2023).

[8] ENISA ohtude kaardistamise aruanne 2024.

[9] ENISA ohtude kaardistamise aruanne: tervishoiusektor (juuli 2023). Aruandes analüüsiti tervishoiuteenuse osutajaid, aga ka muid organisatsioone, kaasa arvatud tervisealaste teadusuuringutega tegelevaid organisatsioone, teatavaid tervisega seotud tooteid valmistavaid üksuseid, tervishoiuasutusi, tervisekindlustusorganisatsioone ning statsionaarse ravi asutusi ja sotsiaalteenuste osutajaid. Aruandega saab tutvuda aadressil https://www.enisa.europa.eu/publications/health-threat-landscape

2024. aasta aruandes tõdeti samamoodi, et näiteks ravi või diagnoosi viibimise või kiirabiteenuste piiratud kättesaadavuse tõttu patsientide ravi mõjutanud rünnetest 71 % olid lunavararünded[10]. Lunavararünded võivad avaldada tervishoiuteenuste osutamisele eriti häirivat mõju ning ohustada patsiente. Lisaks kaasneb lunavararünnetega sageli patsiendiandmete leke,[11] mis puudutab pahatihti delikaatseid terviseandmeid ja rikub inimeste põhiõigust isikuandmete kaitsele.

Samal ajal kaasneb tervishoiu üha suureneva digitaliseerimisega ründepinna kasv. 2024. aasta aruandes digikümnendi olukorra kohta märgiti, et 79 % ELi kodanikest on internetis juurdepääs oma esmatasandi tervishoiu elektroonilistele terviseandmetele[12]. Tervishoiusektori tõhususe ja tulemuslikkuse suurendamisel võib mitmesugustel digivahenditel – digitaalsed terviselood, haiglate töövoosüsteemid, ravikulude hüvitamise IT-süsteemid, piltdiagnostika süsteemid ja diagnostikas või patsientide jälgimises kasutatavad meditsiiniseadmed – olla oluline roll, kuid need võivad olla ka küberründe võimalikud sihtmärgid. Küberründe risk ähvardab eeskätt spetsiifilisi tervishoiutoiminguid, nagu intensiivravi ja radioloogiline piltdiagnostika, ja meditsiinivaldkondi, nagu onkoloogia ja kardioloogia, mis sõltuvad väga suuresti digiseadmetest. Lisaks võivad tarneahelaga seotud probleemid viia selliste seadmete hankimiseni, mille küberturvalisus ei ole piisav, ning see omakorda võimendab olemasolevaid üldisi riske.

Näiteks COVID-19 pandeemia ajal halvas lunavararünne suure osa Iirimaa tervishoiusüsteemist ning põhjustas intsidendi toimumise hommikul vähemalt mõnede teenuste tühistamise 31 aktiivravihaiglas 54st[13]. Tervishoiuteenustes tuli minna tagasi paberdokumentide kasutamisele, mis aeglustas tegevust ja vähendas selle tõhusust. Rünne sai alguse andmepüügi e-kirjast, mis sisaldas kahjurvaraga manust[14]. See intsident näitas, kuidas küberründed võivad eri süsteemides levida ja kui oluline on seega kaitsta kogu tervishoiuorganisatsiooni ründepinda. Samuti tõi see intsident esile, kui oluline on tagada organisatsioonides küberhügieeni ja küberturvalisuse kultuuri baastase.

Haiglate ja tervishoiuteenuse osutajate küberturvalisuse küpsus

ELi tervishoiumaastik on väga mitmekesine ning haiglad ja muud tervishoiuteenuse osutajad on liikmesriigiti väga erinevad nii omandisuhete, struktuuri kui ka suuruse poolest. Mõningatel juhtudel võib tervishoiu juhtimine põhineda riigi tasandil tsentraliseeritud lähenemisviisil, teistes aga võib see toimuda piirkondlikul või kohalikul tasandil; tervishoiuteenuse osutajad võivad olla riigi- või eraomandis. Peale selle võib erinevusi olla ka ühe riigi piires, näiteks võib olukorra muuta keerukaks see, kui eri piirkonnad on sotsiaal-majanduslikult või territoriaalselt väga erinevad. Nakkushaiguste

[10] Euroopa Komisjon: Teadusuuringute Ühiskeskus, 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“, Euroopa Liidu Väljaannete Talitus, 2024, https://data.europa.eu/doi/10.2760/693487

[11] ENISA tervishoiusektori ohtude kaardistamise aruandest selgub, et andmete leke või vargus leidis kinnitust 43 % analüüsitud lunavararünde juhtumite puhul.

[12] Aruanne digikümnendi olukorra kohta, 2024.

[13] Iirimaa tervishoiuteenistus, 2021, „Conti cyber attack on the HSE: Independent Post Incident Review“.

[14] Iirimaa tervishoiuteenistus, „Cyber-attack and HSE response“. Materjalidega saab tutvuda aadressil https://www2.hse.ie/services/cyber-attack/what-happened/.

põhjustatud suured tervisekriisid, nagu COVID-19 pandeemia, aga ka muud terviseriskid, mis on seotud näiteks kliimamuutustega, võivad sellisel keerukal tervishoiumaastikul probleeme tekitada. Lisaks kõigele muule on väga suuri erinevusi ja killustatust ka tervishoiuteenuse osutajate digitaliseerituse ja tehnoloogia kasutuselevõtu tasemes. Sellisest keerukusest annab aimu asjaolu, et kui teenust ei saa küberintsidendi tõttu kasutada, võib see põhjustada patsientidele tõsist kahju ka väikestes tervishoiuasutustes, kaasa arvatud kliinikutes või erakorralise meditsiini keskustes, mis pakuvad olulist teenust suhteliselt väikesele arvule kasutajatele.

ENISA 2024. aasta aruandes, mis käsitleb liidu küberturvalisuse olukorda,[15] on öeldud, et ELi tervishoiusektori küberturvalisuse küpsus on mõõdukas ning Euroopa eri paigus on küberturvalisuse küpsuse tasemes suuri erinevusi. Puudujääke on olulistes valdkondades, nagu piisav personal, organisatsioonide teadmised oma info- ja kommunikatsioonitehnoloogia (IKT) tarneahelate kohta ja toodete ajakohaste turbevahendite paigaldamine. Sektoris on raskusi küberhügieeni baastaseme ja põhiliste turbemeetmetega, mida näitab ka asjaolu, et peaaegu kõigil vaadeldud tervishoiuorganisatsioonidel on probleeme küberriski hindamisega ning peaaegu pooled ei ole kunagi riskianalüüsi teinud[16].

Veel üks haiglate küberturvalisusega seotud oluline probleem on infotehnoloogia (IT) ja käidutehnoloogia (OT) kokkupuutepunktid, kus põrkuvad konfidentsiaalsuse, käideldavuse ja usaldusväärsuse mõttes erinevad turvaprioriteedid ning kus ühes valdkonnas toimuv rikkumine võib mõjutada ka teist valdkonda. ENISA 2024. aasta aruandes, mis käsitleb liidu küberturvalisuse olukorda, rõhutatakse sedagi, et tervishoiusektori tegevus enda kasutatavate IKT-toodete ja -protsesside turvalisuse tagamisel ei ole piisav, sest tervishoiuüksused, -seadmed ja -tooted on väga erinevad.

Selline mitmekesisus koos haiglatöötajate ja juhtkonna küberteadlikkuse kõikuva tasemega tähendab, et tervishoiusüsteemi küberturvalisuse tagamine on keerukas probleem. Näiteks ilmnes küberoskusi käsitlevast 2024. aasta Eurobaromeetri kiiruuringust, et vaid 25 % vaatlusalustest tervishoiu-, haridus- ja sotsiaalhoolekandesektori ettevõtetest oli pakkunud eelmise 12 kuu jooksul küberturvalisuse alast koolitust või teadlikkuse suurendamist[17]. Küberteadlikkuse kultuuri edendamiseks eesliini tervishoiutöötajate seas tuleb tegutseda. Tervishoiuteenuse osutajate küberturvalisuse alast haavatavust suurendavad veel näiteks töötajate roteerumine, ühiste tööjaamade kasutamine, kehv autentimise haldamine ja irdkandjate kasutamine[18].

Paljudel juhtudel on nii IT kui ka OT vähemalt osaliselt allhanke korras sisseostetud. 2024. aasta Eurobaromeetri uuringu kohaselt on ettevõtteid, kes ostavad vähemalt mõne oma küberturvalisuse aspekti sisse, kõige rohkem tervishoiu-, haridus- ja sotsiaalhoolekandesektoris ning sellist võimalust

[15] ENISA: „2024 Report on the State of Cybersecurity in the Union“, september 2024. Aruandega saab tutvuda aadressil https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[16] ENISA ohtude kaardistamise aruanne: tervishoiusektor (juuli 2023). Aruandega saab tutvuda aadressil https://www.enisa.europa.eu/publications/health-threat-landscape

[17] Eurobaromeetri kiiruuring nr 547 küberoskuste kohta, mai 2024. Uuringuga saab tutvuda aadressil https://europa.eu/eurobarometer/surveys/detail/3176

[18] „Panacea – People-centric cybersecurity in healthcare“, 2021: Valge raamat „Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres“.

kasutab 57 % vaatlusalustest ettevõtetest[19]. Tulenevalt vajadusest mastabeeritava andmesalvestuse ja -halduse, kulutõhususe, parema koostöö ja kõrgtehnoloogia, näiteks tehisintellekti ja tervishoiu esemevõrgu toetuse järele, valitseb tugev suundumus minna üle pilvandmetöötlusele. 2022. aastal kasutas 58 % tervishoiuorganisatsioonidest pilvepõhist e-tervise platvormi[20]. Kuigi selline muutus võib aidata märkimisväärselt tõhusust suurendada, kaasnevad sellega ka riskid, mille leevendamiseks on vaja teha hankeid ja turvalist konfiguratsiooni käsitlevaid läbimõeldud otsuseid.

Kõiki neid probleeme mõjutavad aga suutlikkuse arendamise ja rahastamise küsimused. Tervishoiusektori küberturvalisuse rahastamine on olnud piiratud ning tegemist on kogu ELis üldise probleemiga[21]. Kõnealuste rahastamisprobleemide taustaks on rahvastiku vananemine, mis hakkab eelduste kohaselt saabuvatel aastakümnetel Euroopa tervisesüsteemide eelarvele laialdast mõju avaldama.

Vananenud vahendite ja pärandsüsteemide jätkuv kasutamine, intsidentide ennetamise või neile reageerimise ressursside piiratus ning lüngad küberturvalisuse küpsuses tulenevad sageli puudulikust rahastamisest. Haiglad peavad pidevalt tegelema keerulise probleemiga: kuidas leida tasakaal ajakohase turvalise ja digitaalse taristu ning investeeringute vahel, mida on vaja patsientide ravi parandamiseks, näiteks arstide ja muude tervishoiutöötajate palkamiseks, uute diagnostika- ja ravimeetodite kasutuselevõtmiseks ja seadmete soetamiseks. Kui vaadata, kui suure osa kõigist IT-le tehtavatest kulutustest moodustavad kulutused infoturbele, on tervishoiusektor ENISA andmetel[22] 12 uuritud sektori seas alles 7. kohal: selle näitaja mediaanväärtus tervishoiusektoris on 8,3 %.

3. Haiglatele ja tervishoiuteenuse osutajatele mõeldud Euroopa küberturvalisuse tugikeskus

ELi küberturvalisuse raamistik pakub mitmesuguseid töövahendeid, mida tuleks kasutada haiglate ja tervishoiuteenuse osutajate turvalisuse ja kerksuse parandamiseks. Kõigi eespool kirjeldatud probleemide lahendamiseks on vaja töötada ELi tasandil välja ühtne strateegiline lähenemisviis, mis aitaks koondada vajalikud ressursid, teadmised ja töövahendid, millega tulemuslikult küberohte maandada. Selleks, et aidata tervishoiuteenuse osutajatel kogu ELis ennast jõulisemalt kaitsta, on oluline omada olukorrast põhjalikku ülevaadet ning paremini tegevust kavandada ja koordineerida. Selle saavutamiseks on kõige paremad võimalused ENISA-l, et luua oma mandaadi[23] – kaitsta ja toetada ELi elutähtsat taristut – raames oma organisatsiooni sees spetsiaalne **haiglatele ja tervishoiuteenuse osutajatele mõeldud Euroopa küberturvalisuse tugikeskus**[24].

---

[19] Eurobaromeetri kiiruuring nr 547 küberoskuste kohta, mai 2024. Uuringuga saab tutvuda aadressil https://europa.eu/eurobarometer/surveys/detail/3176

[20] ENISA: võrgu- ja infoturbe investeeringute aruanne 2022, november 2022. Aruandega saab tutvuda aadressil https://www.enisa.europa.eu/publications/nis-investments-2022

[21] Terviseteenuste ja ravi korraldamine ja pakkumine kuulub vastavalt ELi toimimise lepingu artiklile 168 liikmesriikide pädevusse ning tervishoiusüsteemide rahastamine on liikmesriigiti erinev.

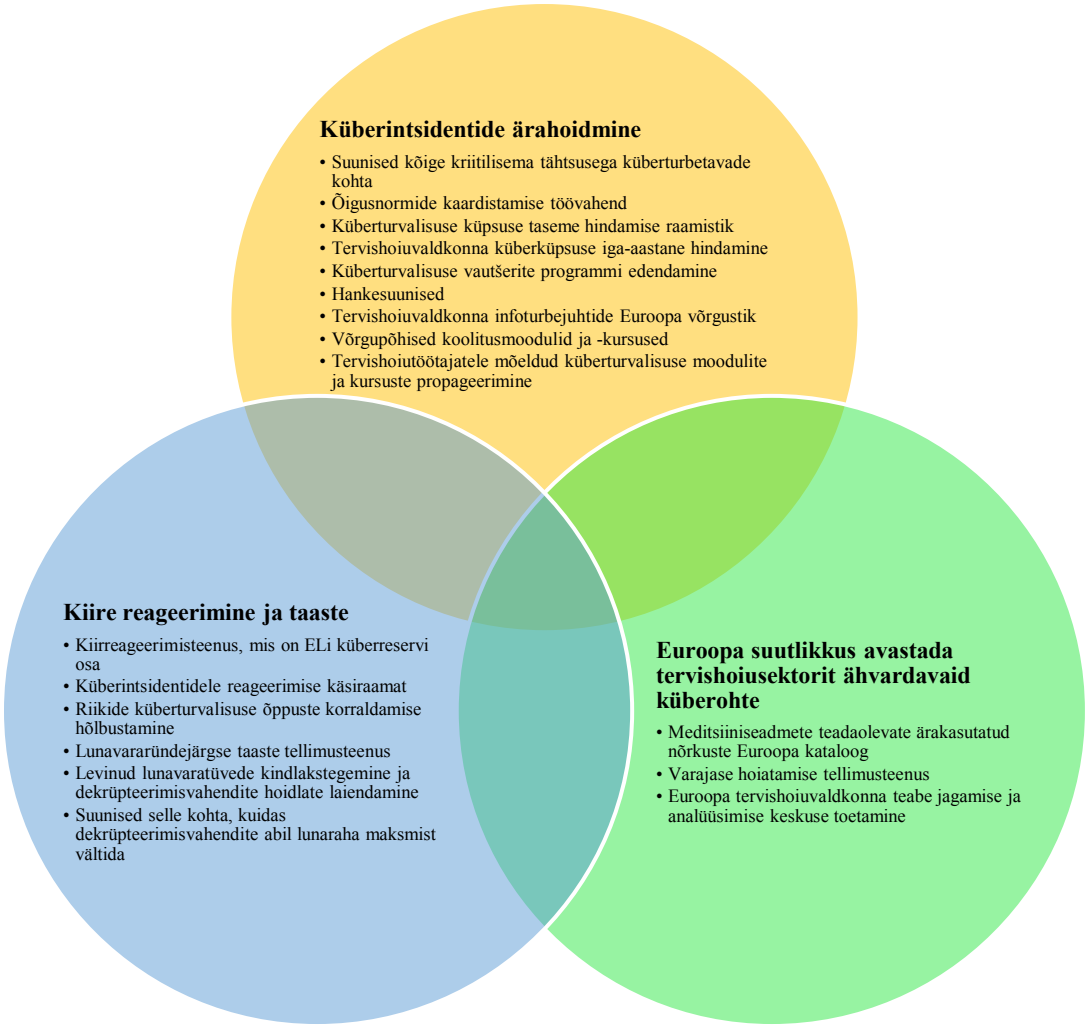
[22] ENISA: võrgu- ja infoturbe investeeringute aruanne 2022, november 2022. Aruandega saab tutvuda aadressil https://www.enisa.europa.eu/publications/nis-investments-2022.

[23] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15–69).

[24] Käesolevas dokumendis kasutatakse selle kohta ka nimetust „tugikeskus“.

Tugikeskus peaks järk-järgult **välja töötama põhjaliku teenuste kataloogi, mis vastaks haiglate ja tervishoiuteenuse osutajate vajadustele** ja annaks ülevaate valmisoleku, ennetuse, avastamise ja reageerimise vallas kättesaadavatest teenustest. Tuginedes haiglate ja tervishoiuteenuse osutajate kogemustele peaks tugikeskus koostöös liikmesriikide ametiasutustega töötama välja kasutajasõbraliku ja kergesti juurdepääsetava hoidla, mis sisaldaks kõiki Euroopa, riikide ja piirkondade tasandil kättesaadavaid vahendeid. Tugikeskus peaks tagama oma tegevuses nõuetekohase koordineerimise liikmesriikidega ning toetama vastavalt vajadustele meetmete prioriseerimist ja elluviimist reaalajas.

Tugikeskuse teenuste kataloogi väljatöötamise olulise komponendina teeb komisjon ettepaneku käivitada kogu ELis pilootprojektid, et arendada küberhügieeni ja turvariskide hindamise parimaid tavasid ning rahuldada vajadus pideva küberturvalisuse seire, ohuteadmuse ja intsidentidele reageerimise järele, kasutades selleks tipptasemel küberturbelahendusi. Neid pilootprojekte hakatakse rahastama programmist „Digitaalne Euroopa“, need viib ellu Euroopa küberturvalisuse pädevuskeskus (ECCC) ning nende tulemustest saab sisend edasistele ELi tasandi meetmetele, kaasa arvatud tugikeskuse tööle.



Joonis 1. Tugikeskuse haiglatele ja tervishoiuteenuse osutajatele mõeldud teenustekataloogi ideed

3.1. Küberintsidentide ärahoidmine

Lihtsad tegevused, millega olukorda parandada

Küberturvalisuse põhimeetmed (nt süsteemide ajakohastamine, varukoopiate haldamine ja mitmikautentimise kasutamine) võivad ühe hinnangu kohaselt kaitsta organisatsioone 98 % küberrünnete eest[25]. Paljude kõige suurema mõjuga küberhügieeni ja riskihalduse meetmete kasutuselevõtmine on suhteliselt lihtne ning need võimaldavad küberturvalisust vähese vaevaga parandada. Seega peaks tugikeskuse üks peamisi ülesandeid olema **töötada välja selged ja sihipärased suunised, mis juhiksid tähelepanu kõige suurema tähtsusega küberturbe tavadele ja aitaksid tervishoiuteenuse osutajatel neid rakendada**. Selline toetus peab lisaks suurtele haiglatele hõlmama ka kohandatud nõuandeid väiksematele üksustele, näiteks perearstidele ja erialakliinikutele, sest neil ei ole pahatihti ressursse eraldi küberturvalisuse meeskonna jaoks, kuigi neid on rünnetega sama lihtne haavata. Samuti on oluline võtta arvesse konkreetsete tervishoiuasutuste piirkondlikku olulisust patsientide ravi tagamisel, seda eriti hõredalt asustatud piirkondades. Terviseuuringute instituudid käitlevad ohtralt tundlikke isikuandmeid ja seega võiks ka neil olla oma kerksuse parandamiseks kasu küberturvalisuse põhimeetmete alastest suunistest.

Tervishoiuorganisatsioonide suhtes kohaldatakse mitmesuguseid ELi õigusaktidest[26] tulenevaid küberturvalisusega seotud kohustusi. Ühest küljest on äärmiselt tähtis, et kohustustega tagatakse küberturbe ja andmete turbe ühtlaselt kõrge baastase, kuid teisalt on oluline tagada, et regulatiivses keskkonnas ei oleks tarbetult keeruline ja koormav orienteeruda. Jõuline keskendumine õigusnormide järgmisele ei tohiks minna vastuollu eesmärgiga edendada tugevat küberturvalisuse kultuuri. **Lihtsalt**

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

[26] Näiteks küberturvalisuse 2. direktiiv; Euroopa Parlamendi ja nõukogu 23. oktoobri 2024. aasta määrus (EL) 2024/2847, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid (küberkerksuse määrus), https://eur-lex.europa.eu/eli/reg/2024/2847/oj/esthttps://eur-lex.europa.eu/eli/reg/2024/2847/oj/est; Euroopa Parlamendi ja nõukogu määrus (EL) 2017/745, 5. aprill 2017, milles käsitletakse meditsiiniseadmeid, https://eur-lex.europa.eu/eli/reg/2017/745/oj/esthttps://eur-lex.europa.eu/eli/reg/2017/745/oj/est (meditsiiniseadmete määrus), https://eur-lex.europa.eu/eli/reg/2017/745/oj/est, meditsiiniseadmete määrus; Euroopa Parlamendi ja nõukogu 5. aprilli 2017. aasta määrus (EL) 2017/746 *in vitro* diagnostikameditsiiniseadmete kohta („*in vitro* diagnostikameditsiiniseadmete määrus), https://eur-lex.europa.eu/eli/reg/2017/746/oj/enghttps://eur-lex.europa.eu/eli/reg/2017/746/oj/eng; Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus), https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32016R0679https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32016R0679; Euroopa Parlamendi ja nõukogu 13. juuni 2024. aasta määrus (EL) 2024/1689, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellektimäärus), https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32024R1689; Ettepanek: Euroopa Parlamendi ja nõukogu määrus, mis käsitleb Euroopa terviseandmeruumi, COM(2022)197 final, https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex:52022PC0197. Läbirääkimised lõppesid 2024. aasta kevadel poliitilise kokkuleppega ja eeldatavasti avaldatakse tekst pärast teksti vormistamist Euroopa Liidu Teatajas 2025. aasta kevadel.

juurdepääsetav õigusnormide kaardistamise töövahend võib aidata vähendada selliste üksuste halduskoormust, kelle suhtes kehtib mitu õigusakti. Lisaks suuniste ja töövahendite väljatöötamisele peaks tugikeskus tegema tihedat koostööd komisjoni ja liikmesriikidega, et selline vahend võimalikult kiiresti välja töötada ja seda levitada. Seega oleks tugikeskusel oluline roll küberturvalisuse alaste õigusnormide lihtsalt mõistetavaks ja rakendatavaks muutmisel; muu hulgas võib selleks koostada rakendamisjuhiseid[27] ja vajaduse korral propageerida asjaomaseid standardeid.

Veel üks vahend, mis hõlbustab heade küberhügieenitavade lihtsat rakendamist, on tulevased **Euroopa digiidentiteedikukrud**. Selleks, et leevendada terviseandmetele loata juurdepääsu riski, on oluline vähendada sõltuvust nõrkadest identimismehhanismidest, nagu paroolid. Üleminek usaldusväärsel identimisel põhinevatele turvalistele sisselogimislahendustele on äärmiselt tähtis. ELi digiidentiteedikukkur pakub tervishoiutöötajatele ühtlustatud ja kogu ELi hõlmavat lähenemisviisi e-identimisele ning toob alates 2026. aasta lõpust kaasa töökindla ja ühtse lahenduse. Kõik võrgupõhised terviseinfosüsteemid, milles tuleb rakendada kasutajate tugevat autentimist, on alates 2027. aasta lõpust kohustatud aktsepteerima identifitseerimisel digiidentiteedikukrut[28].

Valmisolek ja sihtotstarbeline toetus

Valmisoleku testimine, mis hõlmab selliseid toiminguid nagu läbistustestimine, on tegeliku küberturvalisuse nurgakivi ning komisjon on juba eraldanud ENISA-le rahalised vahendid valmiduse katsealgatuste jaoks, millest ilmnes, et tervishoiusektor on üks küberturvalisuse küpsuse lünkade kindlakstegemiseks tehtavate testimiste ja täiendavate hindamiste jaoks kõige nõutumaid valdkondi. Kui kübersolidaarsuse määrus jõustub, laieneb selline tegevus märkimisväärselt ning seda asub juhtima ECCC. Selle vajaduse rahuldamiseks teeb komisjon pärast võrgu- ja infoturbe koostöörühma, EU-CyCLONe[29] ja ENISAga konsulteerimist ettepaneku nimetada tervishoiusektor sektoriks, mille **valmisoleku koordineeritud testimist** võib toetada kübersolidaarsuse määruse alusel. Lisaks peaks tugikeskus töötama välja **spetsiaalselt tervishoiusektorile kohandatud küberturvalisuse küpsuse taseme hindamise raamistiku**. Selline küpsustaseme hindamine annab üksustele reageerimist võimaldava ülevaate nende nõrkustest ning võimaldab neil demonstreerida patsientidele ja sidusrühmadele oma küberturvalisuse alast valmisolekut, suurendades sedasi usaldust oma teenuste vastu. Tugikeskus peaks tegema koondtasandil **tervishoiuvaldkonna küberküpsuse taseme iga-aastase hindamise**, mis annaks selge ülevaate tervishoiusektori küberturvalisusest nii riigi kui ka ELi tasandil.

Tervishoiusektor sõltub küberturbeteenuste osas suuresti välistöövõtjatest[30] ning see juhib tähelepanu asjaolule, et kaitse tugevdamiseks on vaja sihipärast toetust. Tuginedes sellistele edukatele algatustele nagu ELi innovatsiooniosakud, peaksid **liikmesriigid kaaluma näiteks selliste sihipäraste meetmete**

[27] Isikuandmete kaitse üldmääruse (GDPR) tõlgendamist käsitlevate suuniste väljatöötamise eest vastutab Euroopa Andmekaitsenõukogu. ENISA peaks suuniste väljatöötamisel igati austama Euroopa Andmekaitsenõukogu õigusi.
[28] Määruse (EL) nr 910/2014 artikli 5f lõiked 1–2.
[29] Euroopa küberkriisiga tegelevate kontaktasutuste võrgustik.
[30] Vt ENISA võrgu- ja infoturbe investeeringute 2023. aasta aruanne (november 2023), milles rõhutati välistoetuse olulisust küberturvalisuse auditeerimisel ja nõuete täitmisel. Aruandega saab tutvuda aadressil https://www.enisa.europa.eu/publications/nis-investments-2023

nagu küberturvalisuse vautšerite kasutuselevõtmist mikro-, väikeste ja keskmise suurusega haiglate ja tervishoiuteenuse osutajate jaoks. Selliste vautšeritega saaks pakkuda finantsabi konkreetsete küberturvalisuse meetmete kehtestamiseks. Vautšerite jaotamise prioriteetide seadmisel tuleks aluseks võtta valmisoleku testimise ja küberturvalisuse küpsustaseme hindamise tulemusi.

Vautšerite või muude toetusprogrammide tulemusliku kasutuselevõtu jaoks on oluline arvestada kohalike teadmiste ja kontekstiga, et tagada asjakohasus ja juurdepääsetavus. ELi fondid, näiteks Euroopa Regionaalarengu Fond, toetavad juba nüüd aktiivselt küberturvalisuse ja e-tervise algatusi ning seega võiks neid kasutada tervishoiuteenuse osutajatele suunatud küberturvalisuse vautšerite süsteemi arendamiseks. Selliste püüdluste edendamiseks teeb tugikeskus koostööd liikmesriikide ja piirkondlike programmiasutustega, et toetada selliste piirkondlike vautšerisüsteemide väljatöötamist, tuginedes sellele, mida on õpitud olemasolevatest riiklikest projektidest ja programmist „Digitaalne Euroopa“ rahastatud meetmetest, et tagada praktiline ja mõjus rakendamine.

Alates 2014. aastast on „Horisondi“ programmid olnud olulised rahastamisallikad mitmesuguste teadusalgatuste jaoks, mis on keskendunud tervishoiuasutuste, näiteks haiglate küberohtudele vastupidavuse suurendamisele ja kujunemisjärgus tehnoloogia väärkasutamisega seotud riskide leevendamisele. Selle tulemuseks on muu hulgas kogum spetsiifilisi töövahendeid, raamistikke ja süsteeme, näiteks riskihindamise töövahendid, privaatsust säilitavad andmejagamisplatvormid, krüptograafilised lahendused, küberturvalisuse alase teadlikkuse koolitusprogrammid ja ohtude reaalajas avastamise süsteemid. Eeskätt on need lahendused rangelt valideeritud tervishoiuvaldkonnas reaalsetes tingimustes toimunud pilootprojektide käigus, mis tagab nende mõjususe ja praktilise kasutatavuse küberohtude eest kaitsmisel.

Tervishoiusektori tarneahelate turvalisuse kindlustamine

Tervishoiuorganisatsioonide jaoks on üks peamisi probleeme mitmesuguseid tooteid, näiteks ühendatud meditsiiniseadmeid, tervise infosüsteeme ja kontoririistvara hõlmavate keerukate IKT tarneahelate haldamine. Haiglad ja tervishoiuteenuse osutajad vajavad oma tegevuseks usaldusväärseid ja turvalisi IKT-süsteeme ja -teenuseid. Selleks et aidata tervishoiusektoris esinevaid küberturvalisuse probleeme lahendada, peaks võrgu- ja infoturbe koostöörühm tegema **turvariskide koordineeritud hindamise, mille käigus hinnatakse meditsiiniseadmete tarneahelatega seotud tehnilisi ja strateegilisi riske ning tehakse ettepanekuid leevendusmeetmete kohta**[31]. Vastavalt vajadusele peaks võrgu- ja infoturbe koostöörühm tegema koostööd meditsiiniseadmete koordineerimisrühmaga.

Küberkerksuse määruse näol on tegemist uue tervikliku raamistikuga, milles on sätestatud küberturvalisuse nõuded kavandamise, projekteerimise ja arendamise ning aktiivselt ärakasutatavate nõrkuste käsitlemise, paikamise ja teatamise kohta peaaegu kõigi riist- ja tarkvaratoodete puhul väärtusahela igas etapis[32]. Meditsiiniseadmed on tooted, mida kasutatakse meie ühiskonna ühes kõige

[31] Vastavalt küberturvalisuse 2. direktiivi artiklile 22.

[32] Esimese sammuna peavad mitmesuguste kategooriate raadioseadmed, mis ei kuulu meditsiiniseadmete määruse ega *in vitro* diagnostikameditsiiniseadmete määruse kohaldamisalasse, vastama ühtsele turule laskmise korral alates 1. augustist

tundlikumas valdkonnas. Nende toodete küberturvalisuse nõuded tulenevad varasemast meditsiiniseadmete määrusest ja *in vitro* diagnostikameditsiiniseadmete määrusest[33]. Nende määruste praegu toimuva hindamise käigus analüüsitakse nende raamistike vahel suurema sidususe ja koostoime saavutamise potentsiaali, et tagada lihtsustamine ja tipptasemel küberturvalisus.

Riskihindamise tulemused peaksid toetama tervishoiuorganisatsioone nende tarneahela küberturvalisuse tavade läbivaatamisel, mida on nõutud küberturvalisuse 2. direktiivis, ning need võiks võtta aluseks uute **hankesuuniste**[34] väljatöötamisel. ENISA on need suunised välja töötanud oma tugikeskuse kaudu ning need peaksid kajastama hiljutisi suundumusi, nagu patsiendiandmete hoidmine pilves, kaasa arvatud vajadus viia elektroonilised terviseandmed turvaliselt üle pilvkeskkonda. Lisaks tuleks uute suunistega pakkuda organisatsioonidele nende tarneahelate jälgimise praktilisi vahendeid, mille hulka kuuluvad hallatud turbeteenuse osutajad, hindamisaruanded ja kolmandate isikute riskihindamised.

Pilvandmetöötluse puhul on vaja täiendavaid meetmeid tundlike tervishoiuandmete haldamise ainulaadsete probleemide (nt rangem turvalisus, privaatsus, käitamisriskid) lahendamiseks. Eksperdid soovitavad kaitsemeetmete tugevdamiseks integreerida pilvteenustesse vaiketurbe ja sisseprojekteeritud turbe. Selline lähenemisviis seab esikohale turvalise taristu, proaktiivse nõrkusehalduse ning riiklike ja erasektori pilvlahenduste kombinatsiooni. Pidev seire ja müüjapõhised kinnitused, näiteks turbeteenuse osutaja sertifitseerimine ja riiklikele ja rahvusvahelistele standarditele vastavuse auditid, on usaldusväärsete turbetavade tagamiseks samuti olulised.

Selliste teenuste puhul nagu taristu teenusena, platvorm teenusena ja tarkvara teenusena jääb turvalisuse rakendamine sageli kliendi ülesandeks. Samas ei ole paljudel tervishoiuorganisatsioonidel piisavalt ressursse, et neid nõudeid iseseisvalt täita. Selle probleemi lahendamiseks **tuleks julgustada pilvteenuse osutajaid turvalisuse baastaseme meetmeid alaliselt rakendama**. Sellised meetmed vähendaksid väära konfigureerimise ohtu, säilitaksid järjepideva kaitse kliendi hallatavates keskkondades ja annaksid kasutajatele suurema kindlustunde. Vaiketurbe etaloni kehtestamine aitaks leida tasakaalu töökindla kaitse ja praktilisuse vahel, tagades kasutatavuse väga erinevate tervishoiuorganisatsioonide jaoks. Selline püüdlus eeldaks tihedat koostööd pilvteenuste osutajate ja tervishoiusektori vahel ning tööstuse parimate tavade kasutamist toimivate ja mastabeeritavate lahenduste loomiseks.

Koolitamine ja oskuste arendamine

Nõudlusele vastavate oskustega tööjõud on oluline nii Euroopa pikaajalise kestliku majanduskasvu ja konkurentsivõime kui ka kvaliteetsete teenuste, sealhulgas tervishoiuteenuste jaoks. Kvalifitseeritud küberturvalisuse spetsialistide nappus on kogu Euroopas suur probleem ning eelduste kohaselt on ELis

2025 raadioseadmete direktiivi olulistele nõuetele, mis puudutavad küberturvalisust. Teises etapis hakatakse alates 11. detsembrist 2027 kohaldama küberkerksuse määrust.

[33]Detsembris 2019 andis meditsiiniseadmete koostöörühm välja suunised meditsiiniseadmete küberturvalisuse kohta, et toetada seadmete valmistajaid nende kahe määruse I lisa nõuete täitmisel: https://ec.europa.eu/docsroom/documents/41863.

[34] Tuginedes ENISA 2020. aasta hankesuunistele haiglate küberturvalisuse tagamiseks, veebruar 2020. Dokumendiga saab tutvuda aadressil https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

tööjõuvajaduste täitmiseks puudu 299 000 spetsialisti[35]. 2024. aasta küberoskusi käsitleva Eurobaromeetri uuringu[36] kohaselt peab 81 % ettevõtetest küberturvalisusega tegelevate töötajate värbamise keerukust võimalike küberrünnete seisukohast peamiseks riskiks. Haridus-, tervishoiu- ja sotsiaaltöösektoris on 66 % küberturvalisusega seotud töökohtadest täidetud töötajatega, kes on sinna üle läinud küberturvalisusevälistelt ametikohtadelt, ning see toob esile tungiva vajaduse ümber- ja täiendõppe järele.

Selle probleemi lahendamiseks peaks tugikeskus tegema koostööd komisjoni küberturbeoskuste akadeemia teatises[37] kirjeldatud tulevase küberturbeoskuste Euroopa digitaristu konsortsiumiga (EDIC). Tehtav töö peaks hõlbustama teabevahetust tervishoiusektori küberturvalisuse spetsialistide, näiteks infoturbejuhtide vahel. Üks võimalik meede oleks luua **tervishoiuvaldkonna infoturbejuhtide Euroopa võrgustik**, alustades ekspertide reserviga, et jagada ja arendada parimaid tavasid, talentide säilitamise strateegiaid ja lahendusi, mis võimaldaksid meelitada küberturvalisuse spetsialiste tööle tervishoiusektorisse. Lisaks tuleks küberturbeoskuste akadeemia egiidi all töötada välja vahendid, mis aitaksid tervishoiusektori küberturvalisustööjõudu tööstuse ja akadeemiliste ringkondade toel arendada. Seoses sellega tuleks julgustada tööstusharu sidusrühmi pakkuma toetust küberturvalisuse alase koolituse parendamiseks.

Üks suur küberintsidentide põhjustaja tervishoius on endiselt inimlikud eksimused, mis näitab, kui oluline on personali põhjalik koolitamine ja küberteadlikkus. Arvestades seda, kui sageli kasutavad tervishoiutöötajad digivahendeid, on eluliselt tähtis, et nad teaksid, kuidas turvaliselt tegutseda. Sihipärase koolitamise ja teadlikkuse suurendamise kampaaniate abil on võimalik riske tunduvalt vähendada. Seda silmas pidades peaks tugikeskus tegema koostööd tervishoiutöötajate ja tervishoiuteenuse osutajatega ning haridus- ja koolitusteenuse osutajatega, küberturbeoskuste EDIC-iga ja liikmesriikide ametiasutustega, et luua ja levitada **laiahaardelisi ja lihtsalt juurdepääsetavaid võrgupõhiseid koolitusmooduleid ja kursusi**.

Digipädevuse ja küberturvalisuse moodulite lisamine õppekavadesse on tervishoiu küberturvalisuse tugeva baasi loomiseks äärmiselt tähtis. Need moodulid peaksid tegelema selliste sektorispetsiifiliste küsimustega nagu patsiendiandmete kaitse ja meditsiiniseadmete turvalisuse nõrkused. Nende ressursside arendamisel tuleks arvesse võtta varasemaid meetmeid, näiteks programmist „Erasmus+“ rahastatavat projekti BeWell[38] ja projektist „Horisont 2020“ rahastatavat projekti PANACEA[39].

[35] Küberturvalisuse maastik aastal 2024:ISC2 küberturvalisusega tegelevate töötajate uuringust saadud teadmised | Digioskuste ja töökohtade platvorm

[36] Eurobaromeetri kiiruuring nr 547 küberoskuste kohta.

[37] Komisjoni teatis Euroopa Parlamendile ja nõukogule: „Korvata küberturvalisuse valdkonna talendinappus edendamaks ELi konkurentsivõimet, majanduskasvu ja kerksust („Küberturbeoskuste akadeemia“)“. COM(2023) 207 final.

[38] BeWell – tervishoiusektori töötajate digi- ja roheoskuste tulevase strateegia tegevuskava. Projektiga saab tutvuda aadressil https://bewell-project.eu/.

[39] PANACEA – haiglate ja tervishoiutaristute kaitsmine ja privaatsus andmete ja inimeste kaitseks mõeldud aruka küberturvalisuse ja küberohtude töövahendikomplekti abil. Materjalidega saab tutvuda aadressil https://cordis.europa.eu/project/id/826293.

3.2.Euroopa suutlikkus avastada tervishoiusektorit ähvardavaid küberohte

Selleks, et intsidentidele kiirelt reageerida, on vaja küberohud tulemuslikult avastada. Ohusubjektid võivad kasutada mitmesuguseid meetodeid, et raskendada sissetungide avastamist, mis võimaldaks neile pikaajalist loata juurdepääsu süsteemile[40]. Seega aitab parem ohtude avastamise suutlikkus küberründe peatada. Võtkem näiteks Soome psühhoteraapiateenuse osutaja Vastaamo vastu korraldatud lunavararünne, mille käigus tegeleti väljapressimisega patsientidelt, kelle konfidentsiaalsed patsiendiandmed olid varastatud, – esialgne sissetung toimus 2018. aastal, kuid teenuseosutaja sai sellest teada alles 2020. aastal[41].

Kogu ELis on ohtude avastamise ja olukorrateadlikkuse parandamise seisukohast oluline tõhus teabe jagamine ja koostöö. Küberintsidentidele reageerimise üksustel (CSIRTidel) on elutähtis roll võtta riigi tasandil vastu teateid intsidentide, ohuolukordade ja võimalike ohtude kohta ning pakkuda suuniseid leevendusmeetmete kohta. Samas **julgustatakse liikmesriike tungivalt jagama kõiki haiglatelt ja tervishoiuteenuse osutajatelt küberintsidentide kohta laekunud teateid ka ENISA tugikeskusega, et kujundada ELi olukorrateadlikkust**. Ideaaljuhul peaks sellega kaasnema sisuline ülevaade intsidendi mitmesugustest asjakohastest aspektidest, sealhulgas teadaolevatest juurnõrkustest, mõjust tervishoiuteenusele ja patsiente mõjutanud kahjulikest sündmustest. Peale selle julgustatakse meditsiiniseadmete ja *in vitro* diagnostikaseadmete tootjaid vabatahtlikult teada andma aktiivselt ärakasutatavatest nõrkustest ja tõsistest küberintsidentidest, mis mõjutavad kõnealuste seadmete turvalisust, aga ka võimalikest muudest nõrkustest, intsidentidest, ohuolukordadest ja küberohtudest, mis võivad mõjutada kõnealuste seadmete riskiprofiili, ning kasutama selleks ühtset teatamisplatvormi, mille ENISA loob ja mida hakkab haldama küberkerksuse määruse raames.

Kui aruannetes sisalduv teave ei ole enam tundlik, võiks tugikeskus koostada ENISA toetatava Euroopa kataloogi meditsiiniseadmete, tervise infosüsteemide ja tervisealaste IKT seadmete ja tarkvara pakkujate teadaolevate ärakasutatavate nõrkuste kohta. Ohtude avastamisega seotud oluliste probleemide lahendamiseks peaks tugikeskus looma **tervishoiusektori jaoks kogu ELi hõlmava varajase hoiatamise tellimusteenuse, mis annab hoiatusi peaaegu reaalajas**. Selles teenuses kasutataks töödeldud andmeid, mida saadakse CSIRTidelt, tervishoiuvaldkonna üksustelt ja tootjatelt, avalikest allikatest pärinevast teabest ja muudelt asjaomastelt tegijatelt, nagu küberkeskused, teabe jagamise ja analüüsimise keskused ja õiguskaitseasutused. Olukorrateadlikkust aitaks veelgi parandada ENISA ja Euroopa Liidu Õiguskaitsekoostöö Ameti (Europol) tõhusam koostöö näiteks tervishoiusektori vastu suunatud küberkuritegevuse mustreid puudutavates küsimustes.

Teabe jagamise ja analüüsimise keskused on küberohuteadmuse kesksed vahendid, mis edendavad teabe kahesuunalist jagamist avaliku ja erasektori vahel ning usalduse loomist. Tugikeskus peaks pakkuma **Euroopa tervisevaldkonna teabe jagamise ja analüüsimise keskusele** suuremat toetust töövahendite,

[40] ENISA tervishoiusektori ohtude kaardistamise aruanne 2023.
[41] Soome andmekaitseombudsmani otsus 1150/161/2021.

teabevahetuse ja valdkondlike olukorrateadlikkuse aruannete näol, aga ka taktikalise ja strateegilise koostöö jaoks usaldusväärse kogukonna edendamise kaudu. Liikmesriigid peaksid aitama kaasa tervisevaldkonna teabe jagamise ja analüüsimise riiklike keskuste arendamisele[42]. Ühtlasi tuleks kutsuda teabe jagamise ja analüüsimise keskusi üles tervishoiuteenuse osutajaid ja tootjaid omavahel kokku viima, et tekiks ühine arusaam küberohtudest, muu hulgas tarneahelas, ning et hõlbustada toodete turvalise disaini teemalist dialoogi, võttes tõeliselt arvesse kasutuselevõtu tegelikke olusid.

3.3.Kiire reageerimine ja taaste

Arvestades seda, kui tundlikud on patsientide terviseandmed ja kui kohutav mõju võib olla küberrünnetel tervishoiuteenustele, on kiire ja tulemuslik reageerimine küberintsidentidele patsientide ohutuse tagamiseks ülioluline. Kui haigla või tervishoiuteenuse osutaja peab toime tulema küberründega, on tema esimene kontaktpunkt asjaomase riigi CSIRT[43]. CSIRTi ülesanne on pakkuda oluliste intsidentidega toime tulemiseks õigeaegset toetust, ideaaljuhul 24 tunni jooksul. Kui intsident ületab CSIRTi suutlikkust, peaks kiire ja tulemusliku reageerimise kindlustamiseks olema kättesaadav ELi toetus.

Kübersolidaarsuse määruse alusel loodud ELi küberreserv pakub usaldusväärsete hallatud turbeteenuse osutajate intsidentidele reageerimise teenuseid, et abistada oluliste või ulatuslike küberintsidentide puhul ja esialgsetel taastetöödel. Selle reservi eesmärk on täiendada liikmesriikide CSIRTide püüdlusi ja võimaldada neil taotleda täiendavat toetust juhtudel, mis puudutavad elutähtsaid sektoreid, nagu tervishoid. Selle süsteemi tõhustamiseks **peaksid komisjon ja ENISA tagama, et reserv hõlmab kiirreageerimisteenust, mis on mõeldud spetsiaalselt tervishoiusektori jaoks**. Muid olemasolevaid raamistikke täiendades lähetataks selle teenuse raames eksperte tegelema viivitamata tervishoiusektori oluliste või ulatuslike küberintsidentidega, kui riiklik toetus ei ole piisav.

Reageerimise ja taaste parandamiseks peaks tugikeskus koostöös võrgu- ja infoturbe koostöörühma, CSIRTide võrgustiku ja, kui see on asjakohane, Europoliga **töötama välja küberintsidentidele reageerimise käsiraamatud, mis on kohandatud just tervishoiusektori jaoks**. Need käsiraamatud pakuksid nii CSIRTidele kui ka tervishoiuorganisatsioonidele juhiseid konkreetsetele küberohtudele, kaasa arvatud lunavaranõuetele, reageerimiseks. Arvestades, kui oluline on kuritegelikele küberintsidentidele reageerimisel ja nende uurimisel CSIRTide ja õiguskaitseasutuste tulemuslik koostöö, peaksid käsiraamatud muu hulgas sisaldama selgeid juhiseid selle kohta, kuidas sellistest intsidentidest õiguskaitseasutustele teatada. Lisaks võiks tugikeskus **hõlbustada riiklike küberturvalisuse õppuste ulatuslikku korraldamist, toetudes muudel õppustel, näiteks ENISA**

[42] Näiteks Soomes on olemas riiklik teabe jagamise ja analüüsimise keskus sotsiaalhoolekande- ja tervishoiusektori jaoks. Vt Soome riiklik küberturvalisuse keskus: „ISAC information sharing groups“ aadressil https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

[43] Küberturvalisuse 2. direktiivi artikli 23 lõikes 1 on sätestatud nõue, et elutähtsad ja olulised üksused teavitavad olulistest intsidentidest oma CSIRTi või, kui see on kohaldatav, oma pädevat asutust.

õppusel Cyber Europe 2022 saadud kogemustele, et käsiraamatuid katsetada ja intsidentidele reageerimise protokolle tõhusamaks muuta.

Poliitika kujundamiseks ja lunavararünnete vastu võetud meetmete mõjususe hindamiseks on vaja koguda täiendavaid andmeid. Selleks peaksid liikmesriigid nõudma, et üksused, kelle suhtes kohaldatakse küberturvalisuse 2. direktiivi, kaasa arvatud tervishoiuorganisatsioonid, peaksid olulistest küberintsidentidest teada andes esitama lisaks muule teabele andmed kõigi tehtud lunarahamaksete kohta ja lunarahamaksete kohta, mille nad kavatsevad teha. Selline teatamine toetab lunavaraintsidentide tulemuslikku uurimist, kaasa arvatud maksete jälgimist krüptoraha vahetusplatvormidel, et nende saajad kindlaks teha.

Taaste kiirus on kerksuse ja üldsuse usalduse säilitamisel oluline tegur, seda eriti tervishoiusüsteemis, kus rikkeaeg võib häirida patsientide ravi. Et lunavararünnetest reaalselt taastuda, peavad tervishoiuteenuse osutajatel olema turvalised, ajakohased ja eraldatud varukoopiad, mida saab kiiresti taastada. Tugikeskus võiks oma teenuste kataloogi osana pakkuda **lunavararünnete järgse taaste tellimusteenust, mis aitaks haiglatel ja tervishoiuteenuse osutajatel taastekavasid ennetavalt ette valmistada**. ENISA ja Europol peaksid tegema koostööd, et teha kindlaks kõige levinumad lunavaratüved, millega tervishoiuorganisatsioone rünnatakse ja **laiendama dekrüpteerimisvahendite hoidlat**, mida pakutakse projekti „No More Ransom“[44] kaudu. Samuti peaksid nad välja töötama ja edendama kergesti mõistetavaid suuniseid, et aidata tervishoiuteenuse osutajatel pääseda lunaraha maksmisest tänu dekrüpteerimisvahendite kasutamisele.

Rahvusvahelise lunavaravastase algatusega[45] on loodud väärtuslik ruum, kus vahetada teavet konkreetsete lunavaraintsidentide kohta ning ühtlasi suurendada liikmesriikide suutlikkust tugevdada oma küberturvalisuse raamistikke ja tõhusamalt uurida lunavarasubjekte. Komisjon jätkab koos kõrge esindajaga lunavaravastase algatuse raames koostöö edendamist muu hulgas tervishoiusektorit ähvardavate lunavaraohtude vastu võitlemisel. Lisaks püüab komisjon teha tervishoiusektori küberturvalisuse tugevdamiseks koostööd **G7 küberturvalisuse töörühmas**. Eeskätt võiks töörühm kaaluda võimalusi toetada tervishoiusektorit selliste ohtude maandamisel nagu lunavara, tuginedes sellistele mõtteavaldustele nagu ÜRO Julgeolekunõukogus esitatud 8. novembri 2024. aasta ühisavaldus tervishoiuasutuste vastu suunatud lunavararünnete kohta[46].

4. Riiklikud meetmed

See, kuivõrd käesoleva tegevuskavaga on võimalik parandada tervishoiusektori küberturvalisust, oleneb suuresti liikmesriikide aktiivsest osalemisest ja pühendumisest. Tegevuskava edukaks rakendamiseks

[44] https://www.nomoreransom.org/en/index.html.
[45] https://www.counter-ransomware.org/
[46] https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/

võiksid liikmesriigid määrata **spetsiaalselt haiglate ja tervishoiuteenuse osutajate jaoks riiklikud küberturvalisuse tugikeskused**. Need keskused oleksid riigi tasandil tervishoiusektori esmased kontaktpunktid, mis teevad tihedat koostööd ENISA tugikeskusega. Kus võimalik ja vajalik, peaksid liikmesriigid riiklikuks küberturvalisuse tugikeskuseks määrama olemasoleva asutuse, näiteks riikliku tervishoiuvaldkonna CSIRTi või muu asjaomase asutuse.

Samuti julgustatakse liikmesriike koostama **riiklikke tegevuskavasid, mis keskenduvad tervishoiusektori küberturvalisusele**. Sellistes kavades võiks kirjeldada tervishoiusüsteemi ohustavaid spetsiifilisi küberriske ja riiklikke meetmeid, mida nendega toime tulemiseks võetakse, tagades samas, et tulemuslikult kasutatakse ka Euroopa tasandi ressursse ja tavasid. ENISA tugikeskus võib aidata neid kavasid välja töötada, võttes arvesse juba olemasolevaid riiklikke kavasid ja koordineerides tegevust, et tagada eri liikmesriikide ressursside ja strateegiate vastastikune täiendavus.

Teine oluline aspekt, millele liikmesriigid peaksid keskenduma, on ressursside jagamise hõlbustamine tervishoiuteenuse osutajate seas, milleni peaks olema võimalik jõuda riigi, piirkonna või isegi Euroopa tasandi **ühishangete või ressursside koondamise kaudu**. Selline lähenemisviis vähendaks üksikute üksuste finantskoormust ja parandaks samas nende positsiooni läbirääkimistel küberturvalisuse teenuste osutajatega.

Näiteks Prantsusmaa CaRE programmiga[47] on riiklikul ja piirkondlikul tasandil võetud mitmeid meetmeid ressursse puudutavate probleemide lahendamiseks: küberkataloog annab ülevaate küberlahendustest ja -pakettidest, mis on haiglatele kättesaadavad riikliku küberturvalisuse ameti, e-tervise ameti, piirkondlike ametite, riigihankeorganisatsioonide ja kommertslahenduste kaudu. Seda täiendavad piirkondlikele ametitele jagatud ressursside pakkumiseks mõeldud täiendavad rahalised vahendid.

Liikmesriigid peaksid tegelema ka küberturvalisusse tehtavate investeeringute ebapiisavusega tervishoiusektoris. Piisava rahastuse tagamiseks peaksid nad kehtestama **mittesiduvad sihttasemed ja jälgima konkreetselt küberturvalisuse jaoks mõeldud rahastamiseesmärke**, tagades samas, et need investeeringud ei vähenda patsientide hädavajalikku ravi. Nende rahastamiseesmärkide kaudu tuleks püüda integreerida turvalisuskaalutlused kõigisse sektori digiinvesteeringutesse. Liikmesriigid võivad vahetada parimaid tavasid ja nõuandeid nende eesmärkide kohta selliste platvormide kaudu nagu e-tervise võrgustik[48].

5. Avaliku ja erasektori koostöö

Tegevuskava edukaks rakendamiseks on oluline avaliku ja erasektori koostöö ja konsulteerimine tervishoiuteenuse osutajatega, muude tervishoiusektori üksustega ja küberturvalisuse tööstuse

[47] Prantsuse e-tervise amet: Cybersécurité acceleration et Résilience des Établissements (CaRE). Rohkem infot saab aadressil https://esante.gouv.fr/strategie-nationale/cybersecurite.

[48] E-tervise võrgustik on liikmesriikide määratud e-tervise eest vastutavate riiklike asutuste vabatahtlik võrgustik, mis on loodud direktiivi 2011/24/EL artikli 14 alusel.

asjaomaste isikutega. Tugikeskuse töösse veelgi suurema panuse andmiseks **loob komisjon ENISA toel tervishoiuvaldkonna küberturvalisuse ühise nõuandekogu**, kuhu hakkavad kuuluma mõlema valdkonna, st tervishoiu ja küberturvalisuse kõrgetasemelised esindajad, kes saavad komisjonile ja tugikeskusele mõjusate meetmete kohta nõu anda ja arutada avaliku ja erasektori partnerluste edasiarendamist selles valdkonnas. Nõuandekogu võtab aluseks avaliku ja erasektori partnerluste, sealhulgas Euroopa tervisevaldkonna teabe jagamise ja analüüsimise keskuse arendamisel seni tehtud tööd.

Lisaks esitab komisjon **üleskutse**, et küberturvalisuse ettevõtjad, sihtasutused, haridusasutused ja tööstuse sidusrühmad **võtaksid kohustusi selle sektori probleemide lahendamiseks**. Küberturbeoskuste akadeemia kogemustele toetudes võiksid sellised kohustused olla näiteks küberturbeoskuste akadeemia raames võetavad kohustused, mis puudutavad tervishoiusektorile keskendunud koolituste ja materjalide pakkumist küberturvalisuse spetsialistidele[49]. Muud kohustused võiksid olla seotud näiteks teadlikkuse suurendamise meetmetega või hallatud turbeteenuste osutamisega eriliselt haavatavatele üksustele tasuta või väiksema tasu eest, et suurendada nende valmisolekut ja küberkerksust. Samuti võiksid võetavad kohustused seisneda küberohuteadmuse jagamises ENISA tugikeskusega. Tugikeskusel peaks olema pidev ülevaade üleskutse raames võetud kohustustest, et tagada nende sidusus ja vastastikune täiendavus.

6. Küberohusubjektide heidutamine

ELi küberturvalisuse alane sise- ja välispoliitika peaks toetama eesmärki heidutada küberohusubjekte Euroopa tervishoiusüsteeme ründamast. Tervishoiuorganisatsioonide vastu suunatud küberründed on küberkuritegevuse eriti vastuvõetamatu liik, sest sellega võidakse seada ohtu patsientide ohutus ja inimeste elud. Seepärast tuleks ELi küberturvalisuse ja õiguskaitse alast heidutusvõimet rakendada täie jõuga, et kahjustada tervishoiusektori sihikule võtnud ohusubjektide üldist ärimudelit ja jätta nad ilma lihtsast kasumist. See hõlmaks piiriüleste uurimiste edendamist rikkumisindikaatorite ja muude asjaomaste andmete tõhusama jagamise kaudu ja suurema tähelepanu pööramist suure väärtusega sihtmärkidele ja peamistele kuritegevust soodustavatele teguritele, nagu nn kuulikindel veebimajutus või krüptorahamikseri teenused.

Küberdiplomaatia meetmete kogum pakub raamistikku, mis aitab ELi, liikmesriikide ja partnerite vastu suunatud küberründe ära hoida, heidutada ja neile reageerida. Kõrge esindaja kasutab ka edaspidi olemasolevat kübersanktsioonide raamistikku, et reageerida tervishoiusüsteemide vastu suunatud ohtudele.

Kurjategijate vastutusele võtmine nende tegevuse eest on oluline heidutustegur. Seepärast peaksid liikmesriigid tagama õiguskaitse igakülgse integreerimise oma riiklikesse tegevuskavadesse. Eeskätt peaksid nad rünnete ärahoidmiseks, kurjategijate kohtu ette toomiseks ja ründeid hõlbustavate kuritegelike infrastruktuuride lammutamiseks kasutama täies mahus ära infosüsteemide vastu suunatud

[49] Küberoskuste akadeemia: Löö kaasa! | Digioskuste ja töökohtade platvorm

ründeid käsitleva direktiivi[50] ja Euroopa Nõukogu Budapesti küberkuritegevuse konventsiooni[51] sätteid. Nende vahendite edukas rakendamine peaks tagama, et tervishoiu vastu suunatud kuritegelikud ja kuritahtlikud ettevõtmised saavad karistatud.

7. Tegevuskava rakendamine ja järelevalve

Käesolevas tegevuskavas on ENISA raames loodavale tugikeskusele nähtud ette mitmesuguseid ülesandeid. See tagab tegevuskava tervikliku ja sidusa rakendamise ja aitab hoiduda uute üksuste loomisest, mis võiks kaasa tuua dubleerimist ja üldkulusid. Komisjon kavatseb tagada tugikeskuse asjakohase rahastamise.

Kui tugikeskus on tööle asunud, peaks ENISA esitama komisjoniga konsulteerides ENISA haldusnõukogule ja liikmesriikide asjaomastele võrgustikele, eeskätt võrgu- ja infoturbe koostöörühmale, CSIRTide võrgustikule, e-tervise võrgustikule ja vajaduse korral ka Euroopa ühtse terviseandmeruumi nõukogule korrapäraselt ajakohast teavet tugikeskuse töö kohta. Lisaks peaks ENISA vahetama avalikku ja erasektorit ühendava tervishoiuvaldkonna küberturvalisuse ühise nõuandekoguga pidevalt teavet tugikeskuse pakutud meetmete rakendamise kohta.

ENISA korralised aruanded peaksid andma võimaluse avaldada asjakohaseid andmeid, et toetada tegevuskava järelevalvet; üks selline korraline aruanne on näiteks aruanne küberturvalisuse olukorra kohta liidus, milles antakse koondhinnang küberturvalisuse suutlikkuse ja ressursside küpsuse tasemele kõikjal ELis, kaasa arvatud tervishoiusektoris. Lisaks võib ENISA avaldatav ELi küberturvalisuse indeks[52] anda kvantitatiivseid ja kvalitatiivseid andmeid, mida kasutada tervishoiusektori kriitilisuse ja küpsuse hindamisel tõendusbaasina.

8. Edasised sammud

Käesolevas teatises on esitatud ambitsioonikas tegevuskava ELi tervishoiusektori küberturvalisemaks muutmiseks. Tegevuskavas esitatud ettepanekuga arendada ENISA osana välja haiglatele ja tervishoiuteenuse osutajatele mõeldud küberturvalisuse tugikeskus avatakse perspektiiv luua sidus ja ühine Euroopa lähenemisviis kõnealuse sektori küberturvalisuse probleemidele.

Käesolevat teatist tuleks pidada esimeseks sammuks tervishoiu küberturvalisuse suurendamise protsessis. Seepärast kuulutatakse tegevuskava vastuvõtmisega koos välja põhjalikud konsultatsioonid sidusrühmadega ning seisukohtade kogumiseks jätkub teabevahetus liikmesriikide ja asjaomaste

[50] Euroopa Parlamendi ja nõukogu 12. augusti 2013. aasta direktiiv 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK: https://eur-lex.europa.eu/eli/dir/2013/40/oj/est

[51] Küberkuritegevuse konventsioon (Budapesti konventsioon, ETS nr 185) ja selle protokollid: https://www.coe.int/en/web/cybercrime/the-budapest-convention

[52] ENISA, „EU Cybersecurity Index, Framework and Methodological Note“, 2024. Available at https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

võrgustikega. Komisjon kavatseb konsultatsioonide tulemuste põhjal esitada 2025. aasta neljandas kvartalis soovitused tegevuskava edasiseks täiustamiseks.

Komisjon kutsub liikmesriike ja kõiki sidusrühmi üles tegutsema koos tegevuskava eesmärkide saavutamise nimel.

LISA. Kavandatud meetmete ülevaade

Komisjon:

Haiglatele ja tervishoiuteenuse osutajatele mõeldud ENISA küberturvalisuse tugikeskus	
Tagab küberturvalisuse tugikeskusele asjakohased ressursid Teeb Euroopa küberturvalisuse tugikeskuse teenuste kataloogi arendamisel Euroopa küberturvalisuse pädevuskeskusega koostööd katseprojektide käivitamiseks, et arendada küberhügieeni ja turvariskide hindamise parimaid tavasid ning võtta käsile pideva küberturvalisuse seire, ohuteadmuse ja intsidentidele reageerimise vajadus, kasutades selleks tipptasemel küberturbelahendusi	2025
Küberintsidentide ärahoidmine	
Uurib võrgu- ja infoturbe koostöörühma, EU-CyCLONe ja ENISAga konsulteerides võimalust nimetada tervishoiusektor sektoriks, mille valmisoleku koordineeritud testimist võib toetada kübersolidaarsuse määruse alusel	2025. aasta esimene kvartal
Kiire reageerimine ja taaste	
Tagab koos ENISAga, et ELi küberreserv hõlmab kiirreageerimisteenust, mis on mõeldud spetsiaalselt tervishoiusektori jaoks	2025. aasta neljas kvartal
Avaliku ja erasektori koostöö	
Asutab ENISA toel tervishoiuvaldkonna küberturvalisuse ühise nõuandekogu	2025. aasta esimene kvartal
Kuulutab välja projektikonkursi, et küberturvalisuse ettevõtjad, sihtasutused, haridusasutused ja tööstuse sidusrühmad võtaksid kohustusi tervishoiusektori probleemide lahendamiseks	2025. aasta teine kvartal
Küberohusubjektide heidutamine	
Uurib koos kõrge esindajaga küberdiplomaatia meetmete kogumi kasutamist, et tervishoiusüsteemide vastu suunatud kuritahtlikku tegevust ennetada, ära hoida ja heidutada ning sellisele tegevusele reageerida	2025

Edendab koostöös kõrge esindajaga rahvusvahelist koostööd lunavara kasutajate vastu, eelkõige rahvusvahelise lunavaravastase algatuse raames	2025–2026
Otsib G7 küberturvalisuse töörühmas koostöövõimalusi, et tugevdada tervishoiusektori küberturvalisust	2025–2026
Edasised sammud	
Alustab põhjalikke konsultatsioone sidusrühmadega	2025. aasta esimene kvartal
Võtab vastu soovitused, et tegevuskava veelgi täiustada	2025. aasta neljas kvartal

ENISA:

haiglatele ja tervishoiuteenuse osutajatele mõeldud ELi küberturvalisuse tugikeskus	
Alustab tööd haiglatele ja tervishoiuteenuse osutajatele mõeldud Euroopa küberturvalisuse tugikeskuse loomiseks	2025. aasta teine kvartal
Töötab välja põhjaliku teenuste kataloogi, mida küberturvalisuse tugikeskus pakkuma hakkab	Alates 2025. aasta neljandast kvartalist
Küberintsidentide ärahoidmine	
Annab välja suunised, mis juhivad tähelepanu kõige suurema tähtsusega küberturbe tavadele, ja aitab tervishoiuteenuse osutajatel neid rakendada	2025. aasta kolmas kvartal
Töötab tihedas koostöös komisjoni ja liikmesriikidega välja õigusnormide kaardistamise töövahendi	2025. aasta esimene kvartal
Töötab välja spetsiaalselt tervishoiusektorile mõeldud küberturvalisuse küpsuse taseme hindamise raamistiku	2025. aasta kolmas kvartal
Teeb tervishoiuvaldkonna küberküpsuse taseme iga-aastase hindamise	2025–2026
Teeb liikmesriikide ja piirkondlike programmiasutustega koostööd, et luua küberturvalisuse vautšerite näidisprogrammid	2025–2026
Töötab välja uued hankesuunised haiglate ja tervishoiuteenuse osutajate küberturvalisuse jaoks	2025. aasta kolmas kvartal

Loob tervishoiuvaldkonna infoturbejuhtide Euroopa võrgustiku	2026. aasta esimene kvartal
Töötab välja tervishoiutöötajatele mõeldud küberturvalisuse moodulid ja kursused ja propageerib neid	2026. aasta esimene kvartal
Euroopa suutlikkus avastada tervishoiusektorit ähvardavaid küberohte	
Koostab meditsiiniseadmete, tervise infosüsteemide ja tervisealaste IKT seadmete ja tarkvara pakkujate teadaolevate ärakasutatavate nõrkuste Euroopa kataloogi	2025. aasta neljas kvartal
Loob tervishoiusektori jaoks kogu ELi hõlmava varajase hoiatamise tellimusteenuse	Alates 2026. aastast
Toetab Euroopa tervisevaldkonna teabe jagamise ja analüüsimise keskust töövahendite ja teabevahetusega	2025–2026
Kiire reageerimine ja taaste	
Tagab koos komisjoniga, et ELi küberreserv hõlmab kiirreageerimisteenust, mis on mõeldud spetsiaalselt tervishoiusektori jaoks	2025. aasta neljas kvartal
Töötab koostöös CSIRTide võrgustikuga välja küberintsidentidele reageerimise käsiraamatud, mis on kohandatud just tervishoiusektori jaoks	2025. aasta kolmas kvartal
Hõlbustab riiklike küberturvalisuse õppuste ulatuslikku korraldamist, et käsiraamatuid katsetada ja intsidentidele reageerimise protokolle tõhusamaks muuta	Alates 2025. aasta neljandast kvartalist
Pakub lunavarareündejärgse taaste tellimusteenust	Alates 2026. aastast
Teeb koos Europoliga kindlaks kõige levinumad lunavaratüved, millega tervishoiuorganisatsioone rünnatakse, ja laiendab dekrüpteerimisvahendite hoidlat projekti „No More Ransom“ kaudu	2025. aasta neljas kvartal
Töötab koos Europoliga välja kättesaadavad suunised, et aidata tervishoiuteenuse osutajatel pääseda lunaraha maksmisest	2025. aasta kolmas kvartal
Riiklikud meetmed	
Abistab liikmesriike riiklike tegevuskavade väljatöötamisel	2025

Koordineerib tegevust, et tagada eri liikmesriikide ressursside ja strateegiate vastastikune täiendavus	2025–2026
Tegevuskava rakendamine ja järelevalve	
Esitab liikmesriikide asjakohastele võrgustikele pärast komisjoniga konsulteerimist korrapäraselt ajakohast teavet küberturvalisuse tugikeskuse töö kohta	2025–2026
Vahetab pidevalt teavet tervishoiuvaldkonna küberturvalisuse nõuandekoguga	2025–2026

Liikmesriigid:

Euroopa suutlikkus avastada tervishoiusektorit ähvardavaid küberohte	
Jagavad küberturvalisuse 2. direktiivi kohaselt haiglatelt ja tervishoiuteenuse osutajatelt küberintsidentide kohta laekunud teateid Euroopa küberturvalisuse tugikeskusega	Alates 2025. aasta neljandast kvartalist
Julgustavad riiklike tervisevaldkonna teabe jagamise ja analüüsimise keskuste arendamist	2025–2026
Küberintsidentide ärahoidmine	
Teevad võrgu- ja infoturbe koostöörühmas turvariskide koordineeritud hindamise, mille käigus hinnatakse meditsiiniseadmete tarneahelatega seotud tehnilisi ja strateegilisi riske	2025. aasta neljas kvartal
Kiire reageerimine ja taaste	
Korraldavad riiklikke küberturvalisuse õppusi, et käsiraamatuid katsetada ja intsidentidele reageerimise protokolle tõhusamaks muuta	Alates 2026. aastast
Riiklikud meetmed	
Määravad haiglatele ja tervishoiuteenuse osutajatele mõeldud riiklikud küberturvalisuse tugikeskused	2025. aasta teine kvartal
Koostavad riiklikud tegevuskavad, mis keskenduvad tervishoiusektori küberturvalisusele	2025. aasta neljas kvartal
Hõlbustavad ressursside jagamist tervishoiuteenuse osutajate vahel	2025–2026

Kehtestavad mittesiduvad sihttasemed ja jälgivad konkreetselt küberturvalisuse jaoks mõeldud rahastamiseesmärke	2025. aasta neljas kvartal
Nõuavad, et tervishoiuorganisatsioonid ja muud üksused, kelle suhtes kohaldatakse küberturvalisuse 2. direktiivi, teataksid oma kavatsusest maksta lunaraha	2025. aasta neljas kvartal