Eiropas Savienības
Padome

Briselē, 2025. gada 16. janvārī
(OR. en)

5426/25

CYBER 21
SAN 15

PAVADVĒSTULE

Sūtītājs:	Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ*
Saņemšanas datums:	2025. gada 15. janvāris
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretāre *Thérèse BLANCHET*
K-jas dok. Nr.:	COM(2025) 10 final
Temats:	KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM, PADOMEI, EIROPAS EKONOMIKAS UN SOCIĀLO LIETU KOMITEJAI UN REĢIONU KOMITEJAI Eiropas rīcības plāns attiecībā uz slimnīcu un veselības aprūpes sniedzēju kiberdrošību

Pielikumā ir pievienots dokuments COM(2025) 10 final.

Pielikumā: COM(2025) 10 final

EIROPAS
KOMISIJA

Briselē, 15.1.2025.
COM(2025) 10 final

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM, PADOMEI, EIROPAS EKONOMIKAS UN SOCIĀLO LIETU KOMITEJAI UN REĢIONU KOMITEJAI

Eiropas rīcības plāns attiecībā uz slimnīcu un veselības aprūpes sniedzēju kiberdrošību

1. Ievads

ES drošības vide strauji mainās, saasinoties hibrīduzbrukumiem un kiberuzbrukumiem, kuru mērķis ir destabilizēt mūsu sabiedrību, cenšoties izraisīt šķelšanos un traucējumus, kā arī gūt peļņu no kibernoziedzības. Tāpēc Eiropai ir steidzami jāstiprina gatavība šai jaunajai realitātei un noturība pret to visās nozarēs un saskaņā ar "visas sabiedrības" un "visas valdības" pieeju, kā aicināts Eiropas Komisijas priekšsēdētājas īpašā padomnieka Sauli Nīnistes (*Sauli Niinistö*) ziņojumā.

Drošas un noturīgas veselības aprūpes sistēmas ir ES sociālā modeļa stūrakmens. Tomēr slimnīcas un veselības aprūpes sistēmas saskaras ar aizvien lielāku apdraudējumu, it sevišķi no izspiedējprogrammatūru grupējumiem, kuru mērķis ir gūt finansiālu labumu, pamatojoties uz pacientu datu, to skaitā e-veselības pacienta karšu datu, lielo vērtību. Pēdējo četru gadu laikā veselības aprūpes joma patiešām ir kļuvusi par ES nozari, kurai uzbrukts visvairāk, tai skaitā Covid-19 pandēmijas laikā, kad pret veselības aprūpes infrastruktūru arvien biežāk tika vērsti kiberuzbrukumi. Kiberuzbrukumi slimnīcām un veselības aprūpes sniedzējiem nodara tiešu kaitējumu cilvēkiem, jo aizkavē medicīniskās procedūras, rada "sastrēgumus" neatliekamās medicīniskās palīdzības nodaļās un ārkārtējos gadījumos var izraisīt cilvēku bojāeju.

Tā kā nozarē tiek īstenota būtiska digitālā pārveide, risks ir vēl lielāks. Digitālās veselības risinājumi un veselības datu izmantošana un atkalizmantošana var nodrošināt tādus aprūpes modeļus, kas labāk atbilst cilvēku un pacientu vajadzībām un vēlmēm, jo palīdz novērst slimības vai nodrošināt agrāku ārstēšanas uzsākšanu. Digitālo rīku un risinājumu integrēšana klīniskajos procesos, kā arī veselības datu izmantošana un atkalizmantošana var palīdzēt pieņemt labākus klīniskos lēmumus, veicināt veselības nozares automatizāciju, kā arī nodrošināt ātrāku un labāku pacientu aprūpi. Digitālajiem rīkiem, datu izmantošanas procesiem un medicīniskajām ierīcēm – kuras bieži ir savienotas ar internetu un kuru darbībā izmanto mākslīgo intelektu (MI) – ir liela nozīme arī tādu problēmu risināšanā kā veselības aprūpes speciālistu trūkums.

Tajā pašā laikā digitālie rīki arī palielina iespēju kļūt par kibernoziedznieku uzbrukumu mērķi. Turklāt dažas valstis nevilcinās uzbrukt arī veselības aprūpes infrastruktūrai, kā to apliecina Krievijas īstenotais agresijas karš pret Ukrainu. Tas padara šo nozari par potenciālu kiberuzbrukumu mērķi plašākas hibrīdkampaņas ietvaros. Kiberuzbrukumi ne tikai apdraud pacientu drošību, bet arī mazina sabiedrības uzticēšanos veselības aprūpes infrastruktūrai un rada ievērojamas atgūšanās izmaksas. Noturīga un droša digitālā infrastruktūra ne tikai nodrošina aizsardzību pret kiberuzbrukumiem, bet ir arī būtisks atbalsts Eiropas veselības datu telpas (EVDT)[1] īstenošanā un pilnīgā izvēršanā.

Tāpēc ir pienācis laiks pastiprināt Eiropas slimnīcu un veselības aprūpes sniedzēju kiberdrošību un noturību, paceļot to nākamajā līmenī, kā Politikas pamatnostādnēs 2024.–2029. gada Komisijai[2] uzsvēra priekšsēdētāja Urzula fon der Leiena. Šis rīcības plāns ir sagatavots, reaģējot uz steidzamo situāciju un specifisko apdraudējumu, ar ko saskaras šī nozare. Kiberdrošības problēmām veselības aprūpes jomā nav vienkārša risinājuma. Tāpēc rīcības plānā ir aicināts stiprināt preventīvos pasākumus un gatavību, kā arī nodrošināt labāk koordinētu pieeju attiecībā uz solidaritāti, vienlaikus izmantojot Eiropas

[1] https://www.consilium.europa.eu/lv/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_lv.

kiberdrošības nozares speciālās zināšanas. Tādējādi rīcības plāns atspoguļo ES drošības pieeju, kas tiks sīkāk izstrādāta un formalizēta gaidāmajā Eiropas iekšējās drošības stratēģijā, nosakot visaptverošus atbildes pasākumus, ar kuriem novērst visus iekšējās drošības apdraudējumus, un galveno uzsvaru liekot uz spēju paredzēt apdraudējumu, novērst kaitējumu un aizsargāt cilvēkus, īstenojot rīcību visos līmeņos ar visu sabiedrību aptverošu pieeju.

Veselības nozari veido daudzas struktūras un dalībnieki, tai skaitā slimnīcas, klīnikas, aprūpes nami, rehabilitācijas centri un dažādi veselības aprūpes sniedzēji, kā arī farmācijas, medicīnas un biotehnoloģijas nozares pārstāvji, medicīnisko ierīču ražotāji un veselības jomas pētniecības iestādes. Šajā rīcības plānā galvenā uzmanība ir pievērsta slimnīcu un veselības aprūpes sniedzēju kiberdrošībai. Ar veselības aprūpes sniedzēju saprot jebkuru fizisku vai juridisku personu vai citu organizāciju, kas dalībvalsts teritorijā likumīgi sniedz veselības aprūpi[3]. Slimnīcas un veselības aprūpes sniedzēji ir (savstarpēji) atkarīgi no citām veselības aprūpes struktūrām, un tām/tiem ir visciešākā saskarsme ar cilvēkiem. Papildus tam slimnīcu un veselības aprūpes sniedzēju kiberdrošības uzlabošanas pasākumiem būtu jānovērš arī riski, kas ietekmē plašāku piegādes ķēdi un ekosistēmu un ko rada, piemēram, struktūras, kuras izmanto veselības datus pētniecības un mašīnu mācīšanās vajadzībām vai kuras ražo medicīniskās ierīces, it īpaši digitāli iespējotas medicīniskās ierīces, kas savienojas ar internetu vai citām ierīcēm ("lietu internets").

Lai gan veselības aprūpes sistēmu drošība galvenokārt ir valstu kompetencē, veselības joma ir arī kritiski svarīga nozare saskaņā ar Direktīvu par pasākumiem nolūkā panākt vienādi augstu kiberdrošības līmeni visā ES (TID 2 direktīva)[4]. Kibernoziedznieki un citi apdraudētāji darbojas pāri robežām, un arī kiberdrošības problēmas, ar kurām saskaras veselības aprūpes organizācijas, ir līdzīgas visās dalībvalstīs. Sadarbība Eiropas līmenī ir ļoti vērtīga, jo nodrošina apmaiņu ar labāko ES līmeņa un valstu praksi un tās izvēršanu. Tāpēc rīcības plānā ir ierosināta ES līmeņa koordinācija un pasākumi, vienlaikus aicinot arī dalībvalstis rīkoties, lai panāktu pārmaiņas veselības aprūpē un plašākā veselības ekosistēmā.

Rīcības plānā galvenā uzmanība ir pievērsta nozares spēju veidošanai, lai, pirmkārt, **novērstu** kiberdrošības incidentus, jo profilakse vienmēr ir labāka nekā ārstēšana. Otrkārt, rīcības plānā ir sīki izklāstītas darbības, kuru mērķis ir uzlabot kiberdrošības informācijas apmaiņu un spēju **atklāt** kiberdraudus, tādējādi ļaujot ātrāk reaģēt uz tiem. Treškārt, tajā ir paredzēti pasākumi, kas nodrošina labāku **reaģēšanu** uz incidentiem un **atgūšanos** no tiem. Visbeidzot, rīcības plānā ir paredzēti veidi, kā **atturēt** kiberapdraudētājus no uzbrukumu veikšanas veselības aprūpes sistēmām Eiropā.

Rīcības plāns tiks īstenots kopā ar veselības aprūpes sniedzējiem un plašākas veselības ekosistēmas dalībniekiem, dalībvalstīm un kiberdrošības kopienu. Ir būtiski izmantot sadarbībā balstītu pieeju, lai sīkāk definētu un pilnveidotu tādus iedarbīgākos pasākumus, kas sniegtu labumu visiem Eiropas kritiski svarīgajiem veselības aprūpes sniedzējiem. Tāpēc līdztekus šim paziņojumam tiks uzsākta visaptveroša apspriešanās ar ieinteresētajām personām, nozares pārstāvjiem un dalībvalstīm. Svarīgs kiberdrošības elements ir starptautiskā sadarbība, jo kiberdraudus neietekmē robežas un tie ir savstarpēji saistīti.

[3] 3. panta g) punkts Eiropas Parlamenta un Padomes Direktīvā 2011/24/ES par pacientu tiesību piemērošanu pārrobežu veselības aprūpē, https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=celex:32011L0024.

[4] Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris), ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā (TID 2 direktīva), https://eur-lex.europa.eu/eli/dir/2022/2555.

Līdzīgi kiberdrošības apdraudējumi pastāv arī paplašināšanās procesā iesaistītajās valstīs un kaimiņvalstīs, kā arī citās ES stratēģiskajās partnervalstīs. Tas galu galā var apdraudēt kritiskās infrastruktūras drošību ES. Tāpēc būs svarīgi rīcības plāna īstenošanā gūto pieredzi atspoguļot arī ES sadarbībā ar paplašināšanās procesā iesaistītajām valstīm, kā arī citām partnervalstīm, ņemot vērā attiecīgos apdraudējuma līmeņus, kuriem tās ir pakļautas.

2. Slimnīcu un veselības aprūpes sniedzēju kiberdrošības problēmas

Kiberdraudi veselības nozarē

Visā pasaulē un ES pieaug kiberuzbrukumu skaits, un apdraudējuma aina kļūst arvien sarežģītāka un dinamiskāka. Sasniegumi MI jomā nodrošina noziedzīgiem un ļaunprātīgiem darboņiem spēcīgus instrumentus, ar kuriem palielināt viņu īstenoto darbību precizitāti un ietekmi, tomēr MI vienlaikus pārveido arī kiberaizsardzības iespējas, jo tas ļauj automatizēti un reāllaikā cīnīties pret uzbrukumiem.

Izspiedējprogrammatūru izmantošana joprojām ir būtiska kiberdrošības problēma ES un pasaulē, un kādā ziņojumā tiek lēsts, ka līdz 2031. gadam ar to saistītās gada izmaksas pasaulē pārsniegs 250 miljardus EUR[5]. Noziedznieki, kas uzbrukumā izmanto izspiedējprogrammatūru, ne tikai šifrē cietušo datus, lai pieprasītu izpirkuma maksu, bet arī arvien biežāk noplūdina sensitīvu informāciju, lai izdarītu papildu spiedienu. Vēl viena būtiska problēma ir programmatūras un aparatūras vājās vietas – saskaņā ar Eiropas Savienības Kiberdrošības aģentūras (*ENISA*)[6] sniegto informāciju veselības aprūpe ir nozare, kurā visbiežāk ziņots par drošības incidentiem saistībā ar šādām vājām vietām[7]. Pieaug arī citi apdraudējumi, piemēram, izkliedētās pakalpojumatteices (*DDoS*) uzbrukumi, kuru mērķis ir pārslogot nolūkoto sistēmu ar milzīgu datplūsmu, padarot to nepieejamu likumīgiem lietotājiem[8].

Veselības nozare saskaras ar līdzīgām kiberdrošības apdraudējuma tendencēm, un īpaši izplatīti ir izspiedējprogrammatūras uzbrukumi. Saskaņā ar *ENISA* datiem 2021.–2023. gadā izspiedējprogrammatūras izmantotas 54 % no analizētajiem kiberdrošības incidentiem veselības nozarē. Tā kā veselības aprūpes dati ir ļoti vērtīgi, 83 % uzbrukumu pamatā bija finansiāla motivācija, savukārt 10 % uzbrukumu bija ideoloģiska motivācija[9]. Līdzīgi arī Komisijas 2024. gada ziņojumā konstatēts, ka 71 % no uzbrukumiem, kas ietekmē pacientu aprūpi, piemēram, aizkavēta ārstēšana un diagnostika, kā

[5] *Cybersecurity Ventures* (2024. gada 1. jūnijs), "Global Ransomware Damage Costs Predicted To Exceed $ 265 Billion By 2031". Pieejams šeit: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

[6] Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju (Kiberdrošības akts), https://eur-lex.europa.eu/eli/reg/2019/881/oj/.

[7] *ENISA Threat Landscape: Health Sector* (2023. gada jūlijs).

[8] *ENISA Threat Landscape 2024*.

[9] *ENISA Threat Landscape: Health Sector* (2023. gada jūlijs). Ziņojumā analizēti veselības aprūpes sniedzēji, kā arī cita veida organizācijas, to skaitā organizācijas, kas veic ar veselību saistītu pētniecību, struktūras, kas ražo konkrētus ar veselību saistītus produktus, veselības iestādes, veselības apdrošināšanas organizācijas, stacionārās rehabilitācijas iestādes un sociālo pakalpojumu sniedzēji. Pieejams šeit: https://www.enisa.europa.eu/publications/health-threat-landscape.

arī apgrūtināta piekļuve neatliekamās palīdzības dienestiem, bija balstīts uz kādu izspiedējprogrammatūru[10]. Izspiedējprogrammatūras uzbrukumiem var būt īpaši graujoša ietekme uz veselības aprūpes pakalpojumu sniegšanu, jo tie apdraud pacientu drošību. Turklāt izspiedējprogrammatūras uzbrukumi bieži vien ietver arī pacientu datu – nereti arī sensitīvu veselības datu – aizsardzības pārkāpumus[11], ar kuriem tiek pārkāptas cilvēku pamattiesības uz personas datu aizsardzību.

Vienlaikus, pieaugot veselības aprūpes digitalizācijai, palielinās arī uzbrukumu tvērums. Saskaņā ar 2024. gada ziņojumu par stāvokli digitālajā desmitgadē vidēji 79 % ES iedzīvotāju ir tiešsaistes piekļuve savai e-veselības pacienta kartei primārās veselības aprūpes ietvaros[12]. E-veselības pacienta kartes, klīniskās informācijas sistēmas, slimnīcu darbplūsmas sistēmas, IT sistēmas ārstēšanas izdevumu atlīdzināšanai, medicīniskās attēlveidošanas sistēmas un medicīniskās ierīces, ko izmanto diagnostikai vai pacientu monitorēšanai – šie visi ir digitālie rīki, kuriem var būt būtiska nozīme veselības nozares efektivitātes un veiktspējas uzlabošanā, taču tie ir arī kiberdrošības pārkāpumu potenciālie mērķi. Īpaši augstam kiberuzbrukumu riskam ir pakļautas tādas specifiskas veselības aprūpes darbības kā intensīvā terapija un radioloģiskā attēlveidošana un tādas medicīnas jomas kā onkoloģija un kardioloģija, kas ļoti lielā mērā paļaujas uz digitāli iespējotām ierīcēm. Turklāt piegādes ķēdes problēmu dēļ var tikt iepirktas ierīces ar nepietiekamu kiberdrošības līmeni, tādējādi pastiprinot jau pastāvošos vispārējos riskus.

Piemēram, Covid-19 pandēmijas laikā izspiedējprogrammatūras uzbrukums paralizēja lielu daļu Īrijas veselības aprūpes sistēmas, kā rezultātā incidenta rītā 31 no 54 akūtās aprūpes slimnīcām tika atcelti vismaz daži pakalpojumi[13]. Veselības aprūpes dienestiem nācās atgriezties pie papīra formāta dokumentu izmantošanas, tādējādi palēninot darba tempu. Uzbrukums tika veikts, izmantojot pikšķerēšanas e-pasta vēstuli, kas saturēja ļaunprātīgu pielikumu[14]. Incidents parādīja, ka kiberuzbrukums var aptvert dažādas sistēmas, un tādējādi apliecināja, cik svarīgi ir nodrošināt aizsardzību visā veselības aprūpes organizācijas (potenciālo) uzbrukumu tvērumā. Tas arī parādīja, cik būtiski ir nodrošināt kiberhigiēnas pamatpraksi un kiberdrošības kultūru visā organizāciju struktūrā.

Slimnīcu un veselības aprūpes sniedzēju kiberdrošības gatavības līmenis

Veselības aprūpes aina ES ir ļoti dažāda, un slimnīcas un citi veselības aprūpes sniedzēji dalībvalstīs ievērojami atšķiras īpašumtiesību, organizatoriskās struktūras un lieluma ziņā. Dažos gadījumos veselības aprūpes pārvaldības pamatā var būt centralizēta pieeja valsts līmenī, citos – reģionālā un vietējā līmenī; veselības aprūpes sniedzēji var būt valsts vai privātā īpašumā. Turklāt atšķirības var būt arī vienas valsts robežās, piemēram, ja starp reģioniem pastāv ievērojamas sociālekonomiskās un teritoriālās

[10] Eiropas Komisija: Kopīgais pētniecības centrs, Reina, V. un Griesinger, C., *Cyber security in the health and medicine sector – A study on available evidence of the patients health effects from cyber incidents in health in the health*, ES Publikāciju birojs, 2024, https://data.europa.eu/doi/10.2760/693487.
[11] Saskaņā ar *ENISA* ziņojumu par veselības nozares apdraudējuma ainavu (*Threat Landscape*: *Health Sector*) 43 % analizēto izspiedējprogrammatūras incidentu tika apstiprināts, ka noticis ar datu aizsardzību vai zādzību saistīts pārkāpums.
[12] 2024. gada ziņojums par stāvokli digitālajā desmitgadē.
[13] *Irish Health Service Executive* (2021): "Conti cyber attack on the HSE: Independent Post Incident Review".
[14] *Irish Health Service Executive*: "Cyber-attack and HSE response". Pieejams šeit: https://www2.hse.ie/services/cyber-attack/what-happened/.

atšķirības, tādējādi radot sarežģītu kopainu. Šo sarežģīto veselības aprūpes ainu var apdraudēt nopietnas veselības aprūpes krīzes, ko izraisa pārnēsājamas slimības (piemēram, Covid-19 pandēmija), kā arī citi veselības riski, piemēram, saistībā ar klimata pārmaiņām. Visbeidzot, digitalizācijas un tehnoloģiju ieviešanas līmenis veselības aprūpes sniedzēju vidū ir ļoti atšķirīgs un sadrumstalots. Piemēram, šādas sarežģītības rezultātā kiberdrošības incidenta izraisīta pakalpojumu nepieejamība var radīt nopietnas problēmas un kaitējumu pacientiem pat mazākās veselības aprūpes iestādēs, to vidū klīnikās vai neatliekamās medicīniskās palīdzības dienestos, kas sniedz pamatpakalpojumus samērā nelielam skaitam lietotāju.

Saskaņā ar *ENISA* 2024. gada ziņojumu par kiberdrošības stāvokli Savienībā[15] ES veselības nozares kiberdrošības gatavības līmenis ir vidējs un dažādu Eiropas veselības aprūpes struktūru starpā tas ir ļoti atšķirīgs. Trūkumi ir vērojami tādās svarīgās jomās kā pietiekamu cilvēkresursu nodrošināšana, organizāciju zināšanas par to informācijas un komunikācijas tehnoloģiju (IKT) piegādes ķēdēm un jaunāko aizsardzības elementu instalēšana izstrādājumos. Kiberhigiēnas pamatprakses un drošības pamatpasākumu īstenošana nozarei sagādā grūtības, par ko liecina tas, ka gandrīz visas aptaujātās veselības organizācijas saskaras ar problēmām kiberdrošības riska novērtējumu veikšanā, savukārt gandrīz puse nekad nav veikusi riska analīzi[16].

Cita būtiska problēma saistībā ar slimnīcu kiberdrošību ir informācijas tehnoloģiju (IT) un operatīvo tehnoloģiju (OT) "saskares punkti", kur satiekas atšķirīgas drošības prioritātes attiecībā uz konfidencialitāti, pieejamību un uzticamību un kur ielaušanās vienā jomā var ietekmēt otru jomu. *ENISA* 2024. gada ziņojumā par kiberdrošības stāvokli Savienībā ir arī uzsvērts – tā kā veselības aprūpes struktūras, ierīces un produkti ir ļoti daudzveidīgi(-as), veselības nozare pienācīgi nenodrošina tās izmantoto IKT produktu un procesu drošību.

Šī daudzveidība apvienojumā ar slimnīcu personāla un vadības atšķirīgo informētības līmeni kiberdrošības jautājumos padara veselības aprūpes sistēmu kiberdrošības nodrošināšanu par ļoti sarežģītu uzdevumu. Piemēram, saskaņā ar 2024. gada Eirobarometra aptauju par kiberprasmēm tikai 25 % aptaujāto veselības, izglītības un sociālās aprūpes nozares uzņēmumu iepriekšējos 12 mēnešos bija īstenojuši apmācību vai izpratnes veidošanas pasākumus kiberdrošības jomā[17]. Ir jārīkojas, lai veicinātu kiberdrošības izpratnes kultūru pirmās līnijas veselības aprūpes speciālistu vidū. Papildu neaizsargātības avoti, kas ietekmē veselības aprūpes sniedzēju kiberdrošību, ir piemēram, darbinieku rotācija, koplietošanas darbstaciju izmantošana, slikta autentifikācijas pārvaldība un ārējo datu nesēju izmantošana[18].

Daudzos gadījumos IT un OT vismaz daļēji ir nodotas ārpakalpojumu sniedzēju atbildībā. 2024. gada Eirobarometra aptaujā tika konstatēts, ka to uzņēmumu īpatsvars, kuri vismaz dažus kiberdrošības

---

[15] *ENISA*: *2024 Report on the State of Cybersecurity in the Union* (2024. gada septembris). Pieejams šeit: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[16] *ENISA Threat Landscape: Health Sector* (2023. gada jūlijs). Pieejams šeit: https://www.enisa.europa.eu/publications/health-threat-landscape.

[17] Eirobarometra zibensaptauja Nr. 547 par kiberprasmēm (2024. gada maijs). Pieejama šeit: 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*.

aspektus uztic ārpakalpojumu sniedzējiem, visaugstākais ir veselības, izglītības un sociālās aprūpes nozarē, kur to dara 57 % aptaujāto uzņēmumu[19]. Tāpat vērojama spēcīga tendence migrēt datus ar mākoņdatošanu, ko nosaka vajadzība nodrošināt pielāgojamu datu glabāšanu un pārvaldību, izmaksu efektivitāti un labāku sadarbību, kā arī izvēlēties progresīvo tehnoloģiju, piemēram, MI un medicīnisko lietu interneta, atbalstu. 2022. gadā 58 % veselības organizāciju izmantoja mākoņdatošanā balstītu digitālo veselības platformu[20]. Tomēr, lai gan šī pāreja var nodrošināt ievērojamus efektivitātes uzlabojumus, tā ietver arī riskus, kuru novēršana prasa pamatotu lēmumu pieņemšanu attiecībā uz iepirkumiem un drošu konfigurāciju.

Visu šo problēmu vienojošais elements ir jautājums par spēju veidošanu un finansējumu. Finansējums kiberdrošībai veselības nozarē ir bijis ierobežots, un tā joprojām ir vispārēja problēma visā ES[21]. Turklāt šīs finansējuma problēmas aktualizējas šā brīža apstākļos, kad sabiedrība noveco, kas, paredzams, nākamajās desmitgadēs radīs plaša mēroga spiedienu uz Eiropas veselības aprūpes sistēmu budžetu.

Novecojušu rīku un vēsturisku sistēmu tālāka izmantošana, ierobežoti resursi incidentu novēršanai vai reaģēšanai uz tiem, kā arī kiberdrošības gatavības līmeņa nepilnības bieži vien rodas tieši finansējuma trūkuma dēļ. Slimnīcas pastāvīgi saskaras ar grūtībām līdzsvarot mūsdienīgas un drošas digitālās infrastruktūras nodrošināšanu ar citiem pacientu aprūpes uzlabošanai nepieciešamajiem ieguldījumiem, piemēram, ārstu un citu veselības aprūpes speciālistu algošanai, jaunu diagnostikas un ārstēšanas metožu ieviešanai un ierīču iegādei. Saskaņā ar *ENISA*[22] sniegtajiem datiem attiecībā uz informācijas drošības izdevumu īpatsvaru kopējos IT izdevumos veselības nozare ierindojas tikai 7. vietā no 12 pētījumā aplūkotajām nozarēm (mediāna veselības nozarē – 8,3 %).

3. Eiropas Kiberdrošības atbalsta centrs slimnīcām un veselības aprūpes sniedzējiem

ES kiberdrošības satvarā ir piedāvāts plašs klāsts rīku, kas būtu jāizmanto, lai uzlabotu slimnīcu un veselības aprūpes sniedzēju drošību un noturību. Lai risinātu daudzās iepriekšminētās problēmas, ir jāizstrādā vienota un stratēģiska ES līmeņa pieeja, apvienojot nepieciešamos resursus, speciālās zināšanas un rīkus efektīvai kiberapdraudējuma novēršanai. Lai palīdzētu veselības aprūpes sniedzējiem visā ES stiprināt savu aizsardzību, ir būtiski apzināt visplašāko kopainu, kā arī nodrošināt labāku plānošanu un koordināciju. *ENISA* ir vispiemērotākā organizācija šā mērķa sasniegšanai – īstenojot savas pilnvaras[23] aizsargāt un atbalstīt ES kritisko infrastruktūru, tā savā struktūrā izveidos īpašu **Eiropas Kiberdrošības atbalsta centru slimnīcām un veselības aprūpes sniedzējiem**[24].

---

[19] *Eirobarometra zibensaptauja Nr. 547 par kiberprasmēm* (2024. gada maijs). Pieejama šeit: https://europa.eu/eurobarometer/surveys/detail/3176.

[20] *ENISA: NIS Investments Report 2022* (2022. gada novembris). Pieejams šeit: https://www.enisa.europa.eu/publications/nis-investments-2022.

[21] Saskaņā ar Līguma par Eiropas Savienības darbību 168. pantu veselības aprūpes pakalpojumu un medicīniskās aprūpes organizēšana un sniegšana ir valstu kompetencē, un veselības aprūpes sistēmu finansēšana dažādās dalībvalstīs atšķiras.

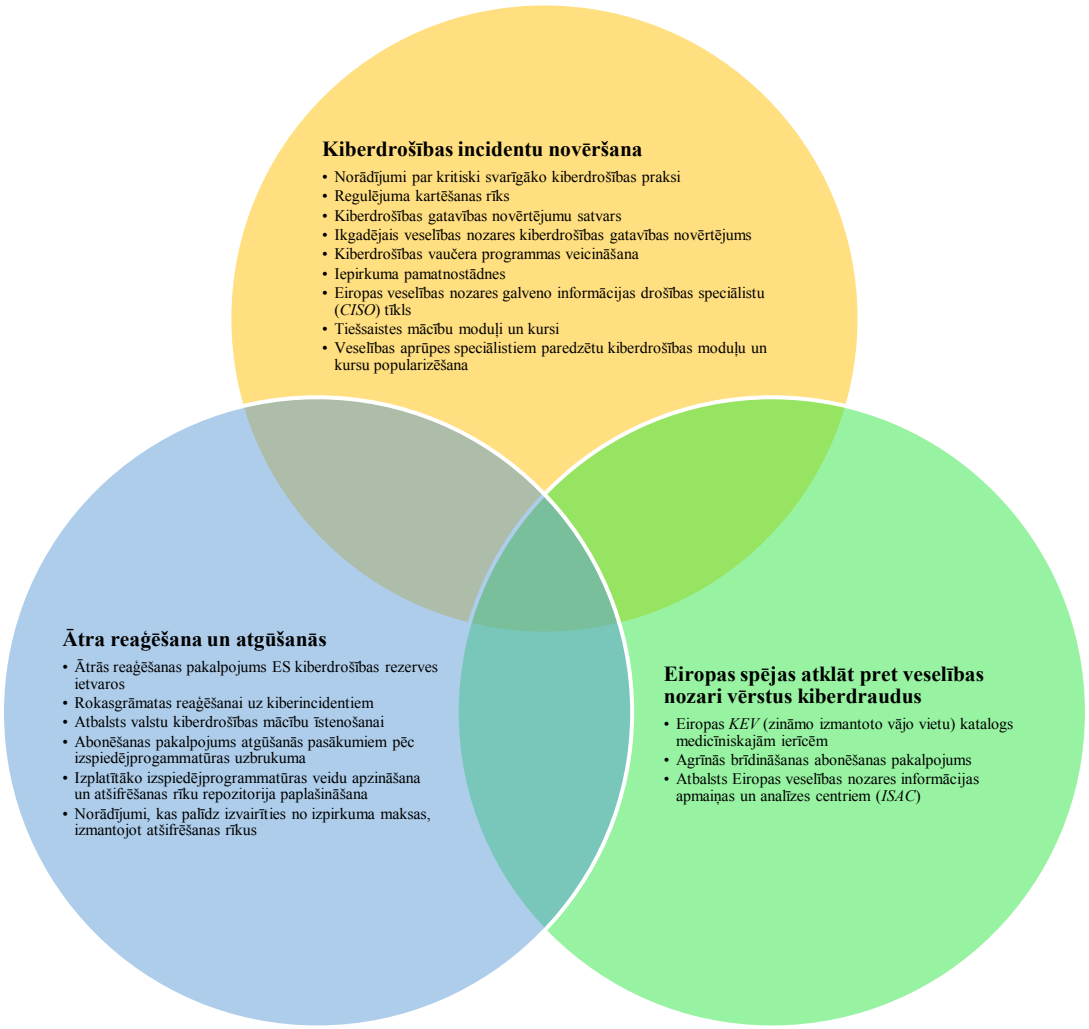
[22] *ENISA: NIS Investments Report 2022* (2022. gada novembris). Pieejams šeit: https://www.enisa.europa.eu/publications/nis-investments-2022.

[23] Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (OV L 151, 7.6.2019., 15.–69. lpp.).

[24] Šajā dokumentā tiek lietots arī apzīmējums "atbalsta centrs".

Atbalsta centram būtu pakāpeniski **jāizstrādā visaptverošs pakalpojumu katalogs, kurā ņemtas vērā slimnīcu un veselības aprūpes sniedzēju vajadzības** un kurā izklāstīts to pakalpojumu klāsts, kas pieejami gatavības, profilakses, atklāšanas un reaģēšanas nodrošināšanai. Sadarbojoties ar dalībvalstu iestādēm un balstoties uz slimnīcu un veselības aprūpes sniedzēju pieredzi, atbalsta centram būtu jāizstrādā lietotājiem ērts un viegli pieejams visu Eiropas, valstu un reģionālā līmenī pieejamo instrumentu repozitorijs. Savu darbību veikšanā tam būtu jānodrošina pienācīga koordinācija ar dalībvalstīm un jāveicina tas, ka prioritātes tiek noteiktas un darbības tiek īstenotas tad, kad tās ir nepieciešamas reāllaikā.

Kā svarīgu elementu atbalsta centra pakalpojumu kataloga izstrādē Komisija ierosinās sākt izmēģinājuma projektus visā ES, lai izstrādātu kiberhigiēnas un drošības riska novērtēšanas paraugpraksi, vienlaikus pievēršoties vajadzību nodrošināšanai saistībā ar nepārtrauktu kiberdrošības uzraudzību, draudu izlūkdatu vākšanu un reaģēšanu uz incidentiem, izmantojot mūsdienīgus kiberdrošības risinājumus. Šo programmas "Digitālā Eiropa" finansēto un Eiropas Kiberdrošības kompetence centra (*ECCC*) īstenoto izmēģinājuma projektu rezultāti tiks izmantoti turpmākajās ES līmeņa darbībās, t. sk. atbalsta centra darbā.



1. attēls. Slimnīcām un veselības aprūpes sniedzējiem paredzētā atbalsta centra pakalpojumu kataloga koncepcijas

3.1. Kiberdrošības incidentu novēršana

Vienkāršas darbības, kas mazina uzbrukumu iespējamību

Saskaņā ar vienu no aplēsēm kiberdrošības pamatpasākumi, piemēram, sistēmu atjaunināšanas nodrošināšana, dublējumkopiju pārvaldība un daudzfaktoru autentifikācijas izmantošana, var aizsargāt organizācijas no uzbrukumiem līdz pat 98 % gadījumu[25]. Daudzus no iedarbīgākajiem kiberhigiēnas un riska pārvaldības pasākumiem ir salīdzinoši vienkārši pārņemt, tāpēc tie ir viegli īstenojami kiberdrošības uzlabošanas nolūkā. Tādējādi vienam no atbalsta centra galvenajiem uzdevumiem vajadzētu būt **izstrādāt skaidrus un mērķtiecīgus norādījumus, kuros uzsvars likts uz kritiski svarīgāko kiberdrošības praksi un kuri palīdz veselības aprūpes sniedzējiem to īstenot**. Šis atbalsts ne tikai ir jāsniedz lielajām slimnīcām, bet tajā ir jāietver arī pielāgoti padomi mazākām struktūrām, piemēram, vietējām ģimenes ārstu praksēm un specializētām klīnikām, kurām bieži trūkst resursu īpašu kiberdrošības komandu izveidei, taču kuras ir tikpat neaizsargātas pret uzbrukumiem. Turklāt ir jāņem vērā konkrētu veselības aprūpes struktūru reģionālā nozīme pacientu aprūpes nodrošināšanā, piemēram, mazapdzīvotos apgabalos. Arī veselības jomas pētniecības iestādēm, kas apstrādā lielu daudzumu sensitīvu personas datu, varētu palīdzēt norādījumi par kiberdrošības pamatpasākumiem, kas uzlabotu to noturību.

Uz veselības aprūpes organizācijām attiecas arī virkne ar kiberdrošību saistītu pienākumu, kas izriet no ES tiesību aktiem[26]. Lai gan šie pienākumi ir ļoti svarīgi, lai garantētu augstu kopējo kiberdrošības un datu drošības pamatlīmeni, ir būtiski nodrošināt, ka regulatīvā vide nav nevajadzīgi sarežģīta un tajā nav grūti orientēties. Liela koncentrēšanās uz atbilstības nodrošināšanu nedrīkstētu traucēt mērķim veicināt

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

[26] Piemēram, TID 2 direktīva; Eiropas Parlamenta un Padomes Regula (ES) 2024/2847 (2024. gada 23. oktobris) par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem (Kibernoturības akts), https://eur-lex.europa.eu/eli/reg/2024/2847/oj; Eiropas Parlamenta un Padomes Regula (ES) 2017/745 (2017. gada 5. aprīlis), kas attiecas uz medicīniskām ierīcēm (Medicīnisko ierīču regula), https://eur-lex.europa.eu/eli/reg/2017/745/oj; Eiropas Parlamenta un Padomes Regula (ES) 2017/746 (2017. gada 5. aprīlis) par *in vitro* diagnostikas medicīniskām ierīcēm (*In vitro* diagnostikas medicīnisko ierīču regula), https://eur-lex.europa.eu/eli/reg/2017/746/oj; Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (Vispārīgā datu aizsardzības regula), https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:32016R0679; Eiropas Parlamenta un Padomes Regula (ES) 2024/1689 (2024. gada 13. jūnijs), ar ko nosaka saskaņotas normas mākslīgā intelekta jomā (Mākslīgā intelekta akts), https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:32024R1689; Priekšlikums – Eiropas Parlamenta un Padomes Regula par Eiropas veselības datu telpu, COM(2022) 197 final, https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=celex:52022PC0197. Sarunas noslēdzās ar politisku vienošanos 2024. gada pavasarī, un paredzams, ka pēc galīgās redakcijas sagatavošanas tā tiks publicēta *Oficiālajā Vēstnesī* 2025. gada pavasarī.

spēcīgu kiberdrošības kultūru. **Viegli pieejams regulējuma kartēšanas rīks var palīdzēt samazināt administratīvo slogu struktūrām, uz kurām attiecas vairāki regulatīvie instrumenti**. Papildus norādījumu un rīkkopu izstrādei atbalsta centram būtu cieši jāsadarbojas ar Komisiju un dalībvalstīm, lai pēc iespējas drīzāk izstrādātu un izplatītu minēto rīku. Tāpēc atbalsta centram būtu svarīgs uzdevums padarīt kiberdrošības noteikumus viegli saprotamus un īstenojamus, piemēram, tas varētu sniegt īstenošanas norādījumus[27] un vajadzības gadījumā popularizēt attiecīgos standartus.

Gaidāmie **Eiropas digitālās identitātes maki** ir vēl viens instruments, kas atvieglos labas kiberhigiēnas prakses vienkāršu īstenošanu. Lai mazinātu risku, ka var notikt neatļauta piekļuve veselības datiem, ir būtiski samazināt vāju identifikācijas mehānismu, piemēram, paroļu, izmantošanu. Izšķiroša nozīme ir pārejai uz drošiem pierakstīšanās risinājumiem, kuru pamatā ir uzticama identifikācija. ES digitālās identitātes maks, kas sākot no 2026. gada beigām nodrošinās stabilu un vienotu risinājumu, veselības aprūpes speciālistiem piedāvā saskaņotu ES mēroga pieeju elektroniskajai identifikācijai. Visām tiešsaistes veselības informācijas sistēmām, kurām ir noteikta prasība īstenot drošu lietotāju autentifikāciju, no 2027. gada beigām būs pienākums identificēšanas vajadzībām pieņemt digitālās identitātes makus[28].

Gatavība un mērķtiecīgs atbalsts

Efektīvas kiberdrošības stūrakmens ir gatavības testēšana, kas ietver tādas darbības kā ielaušanās testēšana, un Komisija jau ir piešķīrusi finansējumu *ENISA* gatavības testēšanas izmēģinājuma iniciatīvām, kas atklāja, ka veselības nozare ir viena no jomām, kurā visvairāk tiek pieprasīts veikt testēšanu un turpmākus novērtējumus, lai apzinātu kiberdrošības gatavības nepilnības. Pēc Kibersolidaritātes akta stāšanās spēkā šie centieni ievērojami paplašināsies, un *ECCC* uzņemsies vadību. Lai nodrošinātu minētās vajadzības, Komisija, apspriežoties ar TID sadarbības grupu, *EU-CyCLONe*[29] un *ENISA*, ierosinās noteikt veselības jomu par nozari, kurai saskaņā ar Kibersolidaritātes aktu var sniegt atbalstu **koordinētai gatavības testēšanai**. Turklāt atbalsta centram būtu jāizstrādā **pielāgots satvars kiberdrošības gatavības novērtējumiem, kas paredzēti tieši veselības aprūpei**. Šādi gatavības novērtējumi sniegtu struktūrām noderīgu ieskatu to vājajās vietās, vienlaikus ļaujot tām pierādīt savu kiberdrošības gatavību pacientu un ieinteresēto personu acīs, tādējādi palielinot uzticēšanos to sniegtajiem pakalpojumiem. Kopējā līmenī atbalsta centram būtu jāveic **ikgadējs veselības nozares kiberdrošības gatavības novērtējums**, kas sniegtu skaidru pārskatu par veselības nozares kiberdrošību gan valstu, gan ES līmenī.

Veselības nozare lielā mērā paļaujas uz ārējo darbuzņēmēju sniegtajiem kiberdrošības pakalpojumiem[30], kas nozīmē, ka nepieciešams mērķtiecīgs atbalsts aizsardzības stiprināšanai. Pamatojoties uz sekmīgajām iniciatīvām, piemēram, ES inovācijas vaučeriem, **dalībvalstīm būtu jāapsver mērķtiecīgi**

[27] Pamatnostādņu izstrāde attiecībā uz Vispārīgās datu aizsardzības regulas (VDAR) interpretāciju ir Eiropas Datu aizsardzības kolēģijas (EDAK) kompetencē. Ja norādījumus izstrādā *ENISA*, tai būtu pilnībā jāievēro EDAK prerogatīvas.
[28] Regulas (ES) Nr. 910/2014 5.f panta 1. un 2. punkts.
[29] Eiropas Kiberkrīžu sadarbības organizāciju tīkls (*EU-CyCLONe*).
[30] Sk. *ENISA* 2023. gada ziņojumu par TID investīcijām (2023. gada novembris), kurā parādīta ārējā atbalsta dominējošā loma kiberdrošības revīziju un atbilstības nodrošināšanā. Pieejams šeit: https://www.enisa.europa.eu/publications/nis-investments-2023.

pasākumi, piemēram, kiberdrošības vaučeri mikroslimnīcām, mazām un vidējām slimnīcām un veselības aprūpes sniedzējiem. Šie vaučeri sniegtu finansiālu palīdzību konkrētu kiberdrošības pasākumu ieviešanai. Nosakot vaučeru piešķiršanas prioritātes, būtu jāņem vērā gatavības testēšanas un gatavības novērtējumu konstatējumi.

Vietējām zināšanām un apstākļiem ir izšķiroša nozīme vaučeru vai citu atbalsta programmu efektīvā īstenošanā, nodrošinot to atbilstību un pieejamību. ES fondi, piemēram, Eiropas Reģionālās attīstības fonds, jau tagad sniedz aktīvu atbalstu kiberdrošības un digitālās veselības iniciatīvām, un tāpēc tos varētu izmantot, lai izstrādātu mērķtiecīgas kiberdrošības vaučeru shēmas veselības aprūpes sniedzējiem. Šo centienu virzības nolūkā atbalsta centrs sadarbosies ar dalībvalstīm un reģionālo programmu iestādēm, lai atbalstītu šādu reģionālu vaučeru shēmu izveidi, izmantojot pieredzi, kas gūta esošajos valstu projektos, kā arī programmas "Digitālā Eiropa" ietvaros finansētajās darbībās, ar mērķi nodrošināt praktisku un iedarbīgu to īstenošanu.

Turklāt kopš 2014. gada programmas "Apvārsnis" ir palīdzējušas finansēt virkni dažādu pētniecības iniciatīvu, kuru galvenais mērķis bija uzlabot veselības aprūpes iestāžu, piemēram, slimnīcu, noturību pret kiberdraudiem un mazināt riskus, kas saistīti ar jauno tehnoloģiju ļaunprātīgu izmantošanu. Iegūtie nodevumi ietver specializētu rīku, satvaru un sistēmu kopumu, piemēram, riska novērtēšanas rīkus, privātumu aizsargājošas datu kopīgošanas platformas, kriptogrāfiskus risinājumus, apmācības programmas kiberdrošības izpratnes veicināšanai un draudu atklāšanas reāllaika sistēmas. Būtiski ir tas, ka šie risinājumi ir rūpīgi validēti, izmēģinājumu veidā reāli ieviešot tos veselības aprūpes vidē, tādējādi nodrošinot to efektivitāti un praktisku piemērojamību aizsardzībā pret kiberdraudiem.

Veselības aprūpes piegādes ķēžu drošība

Viens no galvenajiem veselības aprūpes organizāciju izaicinājumiem ir pārvaldīt sarežģītās IKT piegādes ķēdes, kas ietver virkni produktu, piemēram, viedās medicīniskās ierīces, e-veselības pacienta karšu sistēmas un biroja tehniku. Slimnīcām un veselības aprūpes sniedzējiem to darbības nodrošināšanai ir vajadzīgas uzticamas un drošas IKT sistēmas un pakalpojumi. Lai palīdzētu risināt kiberdrošības problēmas veselības nozarē, TID sadarbības grupai būtu jāveic **koordinēta drošības riska novērtēšana, vērtējot gan tehnisko, gan stratēģisko risku, kas saistīts ar medicīnisko ierīču piegādes ķēdēm, un ierosinot riska mazināšanas pasākumus**[31]. Attiecīgā gadījumā TID sadarbības grupai būtu jāsadarbojas ar Medicīnisko ierīču koordinācijas grupu.

Kibernoturības akts ir jauns, visaptverošs satvars, kas nosaka kiberdrošības prasības attiecībā uz gandrīz visiem aparatūras un programmatūras produktiem katrā vērtību ķēdes posmā saistībā ar to plānošanu, projektēšanu, izstrādi, kā arī aktīvi [ļaunprātīgi] izmantoto vājo vietu novēršanu, labošanu un ziņošanu par tām[32]. Medicīniskās ierīces ir produkti, ko izmanto vienā no sabiedrības visjutīgākajām jomām.

[31] Saskaņā ar TID 2 direktīvas 22. pantu.

[32] Pirmajā posmā, t. i., no 2025. gada 1. augusta, plašām radioiekārtu kategorijām, kas neietilpst Medicīnisko ierīču regulas un *In vitro* diagnostikas medicīnisko ierīču regulas darbības jomā, brīdī, kad tās tiek laistas vienotajā tirgū, būs jāatbilst Radioiekārtu direktīvas pamatprasībām, kas attiecas uz kiberdrošību. Otrajā posmā, t. i., no 2027. gada 11. decembra, sāks piemērot Kibernoturības aktu.

Kiberdrošības prasības šiem produktiem izriet no iepriekš spēkā esošās Medicīnisko ierīču regulas un *In vitro* diagnostikas medicīnisko ierīču regulas[33]. Minēto regulu pašreiz notiekošajā izvērtēšanā tiek aplūkotas iespējas, kā panākt lielāku saskaņotību un sinerģiju starp šiem satvariem ar mērķi nodrošināt vienkāršošanu un mūsdienīgu kiberdrošību.

Turklāt riska novērtēšanā iegūtajiem konstatējumiem būtu jāpalīdz veselības aprūpes organizācijām pārskatīt savu kiberdrošības praksi attiecībā uz piegādes ķēdi, kā prasīts TID 2 direktīvā, un tos varētu izmantot jaunu **iepirkuma pamatnostādņu** izstrādē[34]. Šajās pamatnostādnēs, ko *ENISA* izstrādās ar sava atbalsta centra starpniecību, būtu jāatspoguļo jaunākās tendences, piemēram, pacientu datu mākoņglabāšana, ieskaitot vajadzību droši migrēt e-veselības datus uz mākoņdatošanas vidi. Turklāt jaunajās pamatnostādnēs būtu jāpiedāvā praktiski rīki organizācijām, lai tās varētu sekot līdzi savām piegādes ķēdēm, tai skaitā pārvaldītu drošības pakalpojumu sniedzējiem (*MSSP*), atestācijas ziņojumiem vai trešo personu riska novērtējumiem.

Attiecībā uz mākoņdatošanu ir vajadzīga turpmāka rīcība to specifisko problēmu risināšanai, kas saistītas ar sensitīvu veselības aprūpes datu pārvaldību, t. sk. pastiprinātu drošību, privātumu un operatīvajiem riskiem. Lai stiprinātu aizsardzības pasākumus, eksperti iesaka mākoņpakalpojumos izmantot pieeju "drošība pēc noklusējuma un integrētā drošība". Saskaņā ar šādu pieeju kā prioritāte tiek izvirzīta droša infrastruktūra, proaktīva vājo vietu pārvaldība un valdības un privātā sektora mākoņdatošanas risinājumu kombinācija. Stabilas drošības prakses nodrošināšanā būtiska nozīme ir arī nepārtrauktai uzraudzībai un konkrētu piegādātāju atestācijai, piemēram, drošības pakalpojumu sniedzēju sertifikācijai un atbilstības revīzijām saskaņā ar valsts un starptautiskajiem standartiem.

Attiecībā uz tādiem pakalpojumiem kā infrastruktūra kā pakalpojums (*IaaS*), platforma kā pakalpojums (*PaaS*) un programmatūra kā pakalpojums (*SaaS*) drošības pasākumu īstenošana bieži ir klienta ziņā. Tomēr daudzām veselības aprūpes organizācijām trūkst resursu, lai tās spētu pašas izpildīt šīs prasības. Lai to risinātu, **mākoņpakalpojumu sniedzēji būtu jāmudina kā standarta funkciju nodrošināt drošības pamatpasākumu īstenošanu**. Šie pasākumi samazinātu nepareizas konfigurācijas risku, saglabātu konsekventu aizsardzības līmeni visā klientu pārvaldītajā vidē un sniegtu lietotājiem lielāku pārliecību. Nosakot standarta drošības pamatpasākumus, mērķis būtu līdzsvarot stabilu aizsardzību ar praktiskajiem aspektiem, nodrošinot, ka tos var izmantot plašs veselības aprūpes organizāciju loks. Šie centieni ietvertu ciešu sadarbību starp mākoņpakalpojumu sniedzējiem un veselības nozari, kurā tiek izmantota nozares paraugprakse, lai radītu efektīvus un pielāgojamus risinājumus.

Apmācība un prasmju pilnveide

Lai nodrošinātu ilgtspējīgu ilgtermiņa izaugsmi un konkurētspēju Eiropā, kā arī augstas kvalitātes pakalpojumus, to skaitā veselības aprūpes pakalpojumus, noteikti ir nepieciešams darbaspēks ar

[33] 2019. gada decembrī Medicīnisko ierīču sadarbības grupa izdeva norādījumus par medicīnisko ierīču kiberdrošību, tādējādi sniedzot atbalstu ražotājiem abu regulu I pielikuma prasību izpildē, sk. https://ec.europa.eu/docsroom/documents/41863.

[34] Pamatojoties uz *ENISA* 2020. gada iepirkuma pamatnostādnēm attiecībā uz kiberdrošību slimnīcās (2020. gada februāris). Pieejamas šeit: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

pieprasītām prasmēm. Kvalificētu kiberdrošības speciālistu trūkums ir būtiska problēma visā Eiropā, un tiek lēsts, ka darbaspēka vajadzību apmierināšanai ES trūkst 299 000 speciālistu[35]. Saskaņā ar 2024. gada Eirobarometra aptauju par kiberprasmēm[36] 81 % uzņēmumu uzskata, ka grūtības noalgot kiberdrošības jomas darbiniekus rada būtisku potenciālo kiberuzbrukumu risku. Izglītības, veselības un sociālā darba nozarē 66 % no kiberdrošības pienākumiem pilda darbinieki, kuri iepriekš ir pildījuši amatus, kas nav saistīti ar kiberdrošību, un tas nozīmē, ka ir steidzami nepieciešami pārkvalifikācijas un kvalifikācijas celšanas pasākumi.

Šīs problēmas risināšanā atbalsta centram būtu jāsadarbojas ar gaidāmo kiberdrošības prasmju Eiropas digitālās infrastruktūras konsorciju (*EDIC*), kura izveidošana paredzēta Komisijas paziņojumā par Kiberdrošības prasmju akadēmiju[37]. Šim darbam būtu jāveicina informācijas apmaiņa starp kiberdrošības speciālistiem veselības nozarē, piemēram, galvenajiem informācijas drošības speciālistiem (*CISO*). Viens no iespējamiem pasākumiem būtu izveidot **Eiropas veselības nozares *CISO* tīklu**, sākot ar ekspertu grupu informācijas apmaiņai par paraugpraksi un tās izstrādei, talantīgo speciālistu noturēšanas stratēģijām un risinājumiem kiberdrošības speciālistu piesaistīšanai veselības nozarē. Turklāt Kiberdrošības prasmju akadēmijas paspārnē būtu jāattīsta resursi, kas ar nozares un akadēmisko aprindu pārstāvju atbalstu uzlabotu kiberdrošības jomas darbaspēka pieejamību veselības nozarē. Šajā sakarā būtu jāmudina nozares ieinteresētās personas apņemties nodrošināt atbalstu kiberdrošības apmācības uzlabošanai.

Cilvēciskas kļūdas joprojām būtiski veicina kiberdrošības incidentus veselības aprūpē, un tas liecina, ka ir ārkārtīgi nepieciešama visaptveroša personāla apmācība un izpratne par kiberdrošību. Ņemot vērā, ka veselības aprūpes speciālisti bieži izmanto digitālos rīkus, ir svarīgi nodrošināt viņiem zināšanas par drošu praksi. Mērķtiecīga apmācība un izpratnes veidošanas kampaņas var ievērojami samazināt riskus. Šo jautājumu risināšanā atbalsta centram būtu jāstrādā kopā ar veselības aprūpes speciālistiem un pakalpojumu sniedzējiem un jāsadarbojas ar izglītības un apmācības sniedzējiem, nozares pārstāvjiem, kiberdrošības prasmju *EDIC*, kā arī dalībvalstu iestādēm, lai izveidotu un izplatītu **visaptverošus, viegli pieejamus tiešsaistes mācību moduļus un kursus**.

Digitālās kompetences un kiberdrošības moduļu iekļaušana izglītības programmās ir būtiska, lai izveidotu spēcīgu kiberdrošības pamatu veselības aprūpē. Šajos moduļos būtu jāaplūko nozarei specifiski jautājumi, piemēram, pacientu datu aizsardzība un vājās vietas medicīnisko ierīču drošības jomā. Šo resursu izstrādē būtu jāņem vērā iepriekšējie pasākumi, piemēram, *BeWell* projekts[38], kas tika finansēts

[35] *The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study* | Digitālo prasmju un darba vietu platforma.
[36] Eirobarometra zibensaptauja Nr. 547 par kiberprasmēm.
[37] Komisijas paziņojums Eiropas Parlamentam un Padomei: Kiberdrošības talantu deficīta pārvarēšana ES konkurētspējas, izaugsmes un noturības vairošanai ("Kiberdrošības prasmju akadēmija"), COM(2023) 207 final.
[38] *BeWell* – Plāna alianse nākotnes veselības nozares darbaspēka stratēģijai par digitālām un zaļām prasmēm. Pieejams tīmekļa vietnē https://bewell-project.eu/.

no programmas "*Erasmus+*", un *PANACEA* projekts[39], kas tika finansēts pamatprogrammas "Apvārsnis 2020" ietvaros.

3.2.Eiropas spējas atklāt pret veselības nozari vērstus kiberdraudus

Efektīva kiberdraudu atklāšana ir būtisks nosacījums, lai ātri reaģētu uz incidentiem. Apdraudētāji var izmantot paņēmienus, kas apgrūtina ielaušanās atklāšanu, tādējādi ļaujot ilgāku laiku neatļauti piekļūt sistēmai[40]. Tāpēc labākas draudu atklāšanas spējas var palīdzēt nekavējoties apturēt kiberuzbrukumus. Piemēram, izspiedējprogrammatūras uzbrukumā Somijas psihoterapijas pakalpojumu sniedzējam *Vastaamo,* kur noziedznieks izspieda naudu no pacientiem, kuru konfidenciālās pacienta medicīniskās kartes tika nozagtas, sākotnējā ielaušanās notika 2018. gadā, taču pakalpojumu sniedzējs par to uzzināja tikai 2020. gadā[41].

Efektīva informācijas apmaiņa un sadarbība ir būtisks nosacījums, lai uzlabotu draudu atklāšanu un situācijas apzināšanos visā ES. Nozīmīga loma ir datordrošības incidentu reaģēšanas vienībām (*CSIRT*) – tās saņem ziņojumus par incidentiem, gandrīz notikušiem incidentiem un iespējamiem apdraudējumiem, kā arī piedāvā norādījumus par seku mazināšanas pasākumiem valsts līmenī. Tomēr papildus tam **dalībvalstis tiek īpaši mudinātas ziņot *ENISA* atbalsta centram par visiem paziņojumiem par kiberdrošības incidentiem, kas saņemti no slimnīcām un veselības aprūpes sniedzējiem, lai palīdzētu nodrošināt ES līmeņa situācijas apzināšanos**. Ideālā gadījumā informācija būtu jāpapildina ar dažādu būtisku incidentu aspektu jēgpilnu raksturojumu, ietverot zināmās pamata vājās vietas un ietekmi uz veselības aprūpes pakalpojumiem, kā arī nevēlamās sekas, kas ietekmē pacientus. Turklāt medicīnisko un *in vitro* diagnostikas ierīču ražotāji tiek mudināti, izmantojot vienoto ziņošanas platformu, kas *ENISA* jāizveido un jāpārvalda saskaņā ar Kibernoturības aktu, brīvprātīgi ziņot par aktīvi izmantotām vājajām vietām vai nopietniem kiberincidentiem, kas ietekmē šo ierīču drošību, kā arī par citām potenciālām vājajām vietām, incidentiem, gandrīz notikušiem incidentiem vai kiberdraudiem, kuri var ietekmēt šo ierīču riska profilu.

Par gadījumiem, kuros ziņojumos iekļautā informācija vairs nav sensitīva, atbalsta centrs varētu veidot *ENISA* finansētu Eiropas zināmo izmantoto vājo vietu (*KEV*) katalogu attiecībā uz medicīniskām ierīcēm, e-veselības pacienta karšu sistēmām un IKT aprīkojuma un programmatūras nodrošinātājiem veselības jomā. Lai risinātu būtiskas problēmas draudu atklāšanā, atbalsta centram būtu jāievieš **ES mēroga agrīnās brīdināšanas abonēšanas pakalpojums veselības nozarei, kas nodrošinātu reāllaikam tuvus brīdinājumus**. Šis pakalpojums balstītos uz apstrādātiem datiem, kas iegūti no *CSIRT*, veselības aprūpes struktūrām un ražotājiem, publiskos avotos pieejamiem izlūkdatiem (*OSINT*), kā arī citiem attiecīgiem dalībniekiem, piemēram, kibercentriem, informācijas apmaiņas un analīzes centriem (*ISAC*) un tiesībaizsardzības iestādēm. Situācijas apzināšanos vēl vairāk uzlabotu ciešāka

[39] *PANACEA – Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people*. Pieejams šeit: https://cordis.europa.eu/project/id/826293.
[40] *ENISA Health Threat Landscape 2023*.
[41] Somijas Datu aizsardzības ombuda Lēmums 1150/161/2021.

sadarbība starp *ENISA* un Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (Eiropolu), piemēram, saistībā ar kibernoziedzības modeļiem, kas vērsti pret veselības nozari.

ISAC ir galvenais avots kiberdraudu izlūkdatu ieguvei, tādējādi veicinot divvirzienu informācijas apmaiņu starp publisko un privāto sektoru un sekmējot uzticēšanos. Atbalsta centram būtu jāpalielina atbalsts **Eiropas veselības nozares *ISAC***, nodrošinot rīkus un informācijas apmaiņu, nozares situācijas apzināšanās ziņojumus, kā arī veicinot uzticamas kopienas izveidi taktiskai un stratēģiskai sadarbībai. Dalībvalstīm būtu jāveicina valsts veselības nozares *ISAC*[42] izveide. Būtu arī jāmudina *ISAC* pulcēt kopā veselības aprūpes sniedzējus un ražotājus, lai veidotu kopīgu izpratni par kiberdrošības apdraudējumiem, tai skaitā apdraudējumiem piegādes ķēdē, un lai veicinātu dialogu par drošu produktu izstrādi, kurā patiesi tiktu ņemti vērā to izmantošanas reālie apstākļi praksē.

3.3.Ātra reaģēšana un atgūšanās

Ņemot vērā, ka pacientu veselības dati ir ļoti sensitīva informācija un pret veselības aprūpes pakalpojumiem vērstiem kiberuzbrukumiem ir potenciāli postoša ietekme, ātra un efektīva reaģēšana uz kiberdrošības incidentiem ir būtisks nosacījums pacientu drošības aizsardzībai. Ja slimnīca vai veselības aprūpes sniedzējs saskaras ar kiberuzbrukumu, pirmais kontaktpunkts, pie kā jāvēršas, ir attiecīgā valsts *CSIRT*[43]. *CSIRT* atbild par laicīgu atbalstu, ideālā gadījumā 24 stundu laikā, lai palīdzētu tikt galā ar būtiskiem incidentiem. Tomēr, ja incidenta novēršanai *CSIRT* spēju nepietiek, jābūt pieejamam ES atbalstam, kas nodrošina ātru un efektīvu reaģēšanu.

ES kiberdrošības rezerve, kas izveidota saskaņā ar Kibersolidaritātes aktu, nodrošina uzticamu pārvaldīto drošības pakalpojumu sniedzēju pakalpojumus reaģēšanai uz incidentiem, lai palīdzētu būtisku vai plaša mēroga kiberdrošības incidentu gadījumā un sākotnējos atgūšanās pasākumos. Šī rezerve ir paredzēta kā papildinošs pasākums dalībvalstu *CSIRT* īstenotajiem centieniem, nodrošinot tām iespēju pieprasīt papildu atbalstu gadījumos, kad ir iesaistītas kritiskas nozares, piemēram, veselības nozare. Lai uzlabotu šo sistēmu, **Komisijai un *ENISA* būtu jānodrošina, ka rezervē ir iekļauts ātrās reaģēšanas pakalpojums, kas paredzēts tieši veselības nozarei**. Papildus citām jau izveidotajām sistēmām šā pakalpojuma ietvaros bez kavēšanās tiktu norīkoti eksperti būtisku vai plaša mēroga kiberdrošības incidentu pārvarēšanai veselības aprūpē, ja valsts atbalsts nebūtu pietiekams.

Lai uzlabotu reaģēšanu un atgūšanos, atbalsta centram sadarbībā ar TID sadarbības grupu, *CSIRT* tīklu un attiecīgā gadījumā Eiropolu būtu jāizstrādā **veselības aprūpes nozarei pielāgotas rokasgrāmatas reaģēšanai uz kiberincidentiem**. Šīs rokasgrāmatas palīdzētu gan *CSIRT*, gan veselības aprūpes organizācijām reaģēt uz konkrētiem kiberdrošības apdraudējumiem, tai skaitā izspiedējprogrammatūrām. Ņemot vērā, cik svarīga ir efektīva sadarbība starp *CSIRT* un

[42] Piemēram, Somijā ir valsts *ISAC* sociālās labklājības un veselības aprūpes nozarē. Sk. Somijas Nacionālais kiberdrošības centrs – *ISAC* informācijas apmaiņas grupas, informācija pieejama šeit: https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

[43] TID 2 direktīvas 23. panta 1. punktā ir noteikta prasība būtiskajām un svarīgajām vienībām [struktūrām] paziņot par incidentiem, kuriem ir būtiska ietekme, attiecīgajai *CSIRT* vai attiecīgā gadījumā kompetentajai iestādei.

tiesībaizsardzības iestādēm reaģēšanā uz noziedzīgiem kiberdrošības incidentiem un to izmeklēšanā, rokasgrāmatās cita starpā būtu jāsniedz skaidri norādījumi, kā par tādiem incidentiem ziņot tiesībaizsardzības iestādēm. Papildus tam atbalsta centrs varētu **veicināt valstu kiberdrošības mācību plašu īstenošanu, pamatojoties uz pieredzi, kas gūta tādās mācībās kā *ENISA* 2022. gada mācības "Kibereiropa", ar mērķi testēt rokasgrāmatas un nostiprināt protokolus reaģēšanai uz incidentiem**.

Lai nodrošinātu informāciju politikas veidošanai un novērtētu to pasākumu efektivitāti, kas veikti pret izspiedējprogrammatūras uzbrukumiem, ir jāvāc papildu dati. Šajā nolūkā dalībvalstīm būtu jāpieprasa struktūrām, uz kurām attiecas TID 2 direktīva, t. sk. veselības aprūpes organizācijām, ziņot par visiem veiktajiem izpirkuma maksas maksājumiem un par izpirkuma maksas maksājumiem, ko tās plāno veikt, kā arī par citu informāciju, ko tās sniedz, ziņojot par būtiskiem kiberdrošības incidentiem. Šāda ziņošana palīdz efektīvi izmeklēt izspiedējprogrammatūras incidentus, tai skaitā izsekot maksājumus kriptovalūtu maiņas platformās, lai identificētu saņēmējus.

Ātra atgūšanās ir būtisks faktors, lai saglabātu noturību un sabiedrības uzticēšanos, it īpaši veselības aprūpes nozarē, kur darbības pārtraukums var kavēt pacientu aprūpi. Lai atgūšanās no izspiedējprogrammatūras uzbrukumiem būtu efektīva, veselības aprūpes sniedzēju rīcībā jābūt drošām, atjauninātām un savrupi turētām dublējumkopijām, kuras var ātri atjaunot. Atbalsta centrs sava pakalpojumu kataloga ietvaros varētu piedāvāt **abonēšanas pakalpojumu atgūšanās pasākumiem pēc izspiedējprogammatūras uzbrukuma, tādējādi palīdzot slimnīcām un veselības aprūpes sniedzējiem laikus sagatavot atgūšanās plānus**. *ENISA* un Eiropolam būtu jāsadarbojas, lai apzinātu izplatītākos izspiedējprogrammatūru veidus, kas vērsti pret veselības aprūpes organizācijām, un **jāpaplašina atšifrēšanas rīku repozitorijs**, kas pieejams ar projekta "No More Ransom" starpniecību[44]. Tiem būtu arī jāizstrādā un jāpopularizē pieejami norādījumi, kas palīdzētu veselības aprūpes sniedzējiem izvairīties no izpirkuma maksas, izmantojot atšifrēšanas rīkus.

Starptautiskā iniciatīva izspiedējprogrammatūru apkarošanai[45] nodrošina nozīmīgu darbības lauku informācijas apmaiņai par konkrētiem izspiedējprogrammatūras incidentiem, kā arī dalībvalstu spēju veidošanai nolūkā stiprināt to kiberdrošības sistēmas un izmeklēšanas spējas cīņā pret izspiedējprogrammatūru darboņiem. Komisija kopā ar Augsto pārstāvi turpinās veicināt sadarbību, kas tiek īstenota saskaņā ar iniciatīvu izspiedējprogrammatūru apkarošanai, arī cīņā pret izspiedējprogrammatūru apdraudējumiem, kuri vērsti pret veselības nozari. Turklāt nolūkā stiprināt veselības nozares kiberdrošību Komisija meklēs sadarbības iespējas **G7 kiberdrošības darba grupā**. Konkrētāk, darba grupa varētu apsvērt iespējas atbalstīt veselības nozari cīņā pret tādiem apdraudējumiem kā izspiedējprogrammatūras, pamatojoties uz atziņām, kas iekļautas, piemēram, 2024. gada 8. novembra kopīgajā paziņojumā par izspiedējprogrammatūru uzbrukumiem veselības aprūpes iestādēm, kurš tika sniegts ANO Drošības padomes kontekstā[46].

[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/.

4. Rīcība valstu līmenī

Šā rīcības plāna spēja uzlabot kiberdrošību veselības nozarē ir atkarīga no dalībvalstu aktīvas iesaistīšanās un apņemšanās. Lai rīcības plānu sekmīgi īstenotu, dalībvalstis varētu izraudzīties **valsts kiberdrošības atbalsta centrus, kas īpaši paredzēti slimnīcām un veselības aprūpes sniedzējiem**. Šie centri, cieši sadarbojoties ar *ENISA* atbalsta centru, darbotos kā primārie valsts līmeņa kontaktpunkti veselības aprūpes nozarei. Gadījumos, kad tas ir iespējams un lietderīgi, dalībvalstīm par valsts kiberdrošības atbalsta centriem būtu jāizraugās esošās struktūras, piemēram, valsts veselības nozares *CSIRT* vai saistītās iestādes.

Dalībvalstis tiek mudinātas arī izstrādāt **valsts rīcības plānus, kas vērsti uz kiberdrošību veselības nozarē**. Šajos plānos būtu izklāstīti konkrēti kiberdrošības riski, ar kuriem saskaras veselības aprūpes sistēmas, un valsts darbības, kas tiek veiktas, lai tos novērstu, vienlaikus nodrošinot arī to, ka tiek efektīvi izmantoti Eiropas līmeņa resursi un prakse. *ENISA* atbalsta centrs var palīdzēt izstrādāt šos plānus, pamatojoties uz jau esošajiem valstu plāniem un koordinējot centienus, lai nodrošinātu, ka dalībvalstu individuālie resursi un stratēģijas ir savstarpēji papildinoši.

Papildus tam dalībvalstīm ir ļoti svarīgi veicināt resursu koplietošanu veselības aprūpes sniedzēju vidū, ko varētu panākt, veicot **kopīgus iepirkumus vai apvienojot resursus** valstu, reģionu vai pat Eiropas līmenī. Šāda pieeja samazinātu struktūru individuālo finansiālo slogu, vienlaikus palielinot to spēju aizstāvēt savas intereses sarunās ar kiberdrošības pakalpojumu sniedzējiem.

Piemēram, risinot ar resursiem saistītās problēmas, Francijas programmas *CaRE*[47] ietvaros ir ieviesti vairāki valsts un reģionālā līmeņa pasākumi – kiberkatalogs sniedz pārskatu par kiberrisinājumiem un pakotnēm, kas slimnīcām darītas pieejamas ar valsts kiberdrošības aģentūras, digitālās veselības aģentūras, reģionālo aģentūru, valsts iepirkuma organizāciju, kā arī komerciālu risinājumu starpniecību. Papildus tam tiek nodrošināts papildu finansējums reģionālajām aģentūrām, kas paredzēts koplietojumu resursu piedāvāšanai.

Dalībvalstīm būtu arī jārisina jautājums par nepietiekamām kiberdrošības investīcijām veselības nozarē. Lai nodrošinātu pienācīgu finansējumu, tām būtu jānosaka **nesaistoši kritēriji un jāuzrauga finansēšanas mērķi, kas īpaši vērsti uz kiberdrošību**, vienlaikus nodrošinot, ka šīs investīcijas nemazina pacientu pamataprūpei paredzētos līdzekļus. Šiem finansēšanas mērķiem vajadzētu būt vērstiem arī uz to, lai visās nozarē veiktajās digitālajās investīcijās tiktu integrēti drošības apsvērumi.

[47] Francijas Digitālās veselības aģentūra: *Cybersécurité acceleration et Résilience des Établissements* (*CaRE*). Informācija pieejama šeit: https://esante.gouv.fr/strategie-nationale/cybersecurite.

Dalībvalstis var apmainīties ar paraugpraksi un sniegt konsultācijas par šiem mērķiem, izmantojot tādas platformas kā e-veselības tīkls[48].

5. Publiskā un privātā sektora sadarbība

Lai sekmīgi īstenotu rīcības plānu, ir būtiski nodrošināt publiskā un privātā sektora sadarbību un apspriešanos ar veselības aprūpes sniedzējiem, citām veselības nozares struktūrām, kā arī attiecīgajiem kiberdrošības nozares dalībniekiem. Lai sniegtu turpmāku ieguldījumu atbalsta centra darbā, **Komisija ar *ENISA* atbalstu izveidos kopīgu Veselības nozares kiberdrošības konsultatīvo padomi** ar augsta līmeņa pārstāvjiem abās jomās – veselības aprūpē un kiberdrošībā –, kuri var konsultēt Komisiju un atbalsta centru par iedarbīgiem pasākumiem un apspriest publiskā un privātā sektora partnerību turpmāko attīstību šajā jomā. Padome balstīsies uz pašreizējiem centieniem, kas tiek īstenoti attiecībā uz publiskā un privātā sektora partnerībām, ieskaitot Eiropas veselības nozares *ISAC*.

Turklāt Komisija izsludinās kiberdrošības uzņēmumiem, nodibinājumiem, izglītības iestādēm un nozares ieinteresētajām personām adresētu **aicinājumu rīkoties**, lai tie **apņemtos veikt darbības nozares problēmu risināšanai**. Pamatojoties uz Kiberdrošības prasmju akadēmijas pieredzi, šādas apņemšanās varētu būt, piemēram, Kiberdrošības prasmju akadēmijas ietvaros nodrošināt uz veselības nozari vērstus mācību kursus un materiālus kiberdrošības speciālistiem[49]. Citas apņemšanās varētu ietvert arī izpratnes veicināšanas pasākumus vai pārvaldītu drošības pakalpojumu sniegšanu par brīvu vai par pazeminātu cenu struktūrām ar īpaši augstu ievainojamības līmeni, tādējādi palielinot to gatavību un kiberdrošības noturību. Turklāt tie/tās varētu apņemties kopīgot kiberdraudu izlūkdatus ar *ENISA* atbalsta centru. Atbalsta centram būtu jāpārrauga šīs apņemšanās, kas izteiktas, atsaucoties uz aicinājumu rīkoties, lai nodrošinātu to saskaņotību un papildināmību.

6. Kiberapdraudētāju atturēšana

ES iekšējā un ārējā kiberdrošības politika būtu jāveido tā, lai atbalstītu mērķi atturēt kiberapdraudētājus no uzbrukumiem Eiropas veselības aprūpes sistēmām. Kiberuzbrukumi veselības aprūpes organizācijām ir īpaši nepieņemams ļaunprātīgas kiberdarbības veids, jo tie var apdraudēt pacientu drošību un cilvēku dzīvību. Tāpēc būtu ar pilnu spēku jāizmanto ES atturēšanas spējas kiberdrošības un tiesībaizsardzības jomā, lai vājinātu to apdraudētāju vispārējo darbības modeli, kuri vēršas pret veselības nozari, un atņemtu tiem iespēju gūt vieglu peļņu. Tas ietvertu pārrobežu izmeklēšanas veicināšanu, ko panāktu, uzlabojot apmaiņu ar aizskāruma rādītājiem un citiem saistītiem datiem, un pastiprinātas uzmanības pievēršanu augstas vērtības mērķiem [noziedzīgām personām] un galvenajiem noziedzības veicinātājiem, piemēram, necauršaujamai mitināšanai vai kriptovalūtas jaukšanas pakalpojumiem.

[48] E-veselības tīkls ir brīvprātīgs tīkls, kas apvieno dalībvalstu nozīmētās par e-veselību atbildīgās valsts iestādes, kuras izveidotas, pamatojoties uz Direktīvas 2011/24/ES 14. pantu.

[49] Kiberprasmju akadēmija: Iesaistieties! | Digitālo prasmju un darba vietu platforma.

Kiberdiplomātijas rīkkopa piedāvā satvaru pret ES, dalībvalstīm un partneriem vērstu kiberuzbrukumu novēršanai, atturēšanai no tiem un reaģēšanai uz tiem. Augstais pārstāvis turpinās izmantot spēkā esošo kibersankciju regulējumu, lai reaģētu uz draudiem, kuru mērķis ir veselības nozares sistēmas.

Noziedzīgo aktoru saukšana pie atbildības par viņu īstenotajām darbībām ir svarīgs atturošs faktors. Tāpēc dalībvalstīm būtu jānodrošina, ka to valsts rīcības plānos tiek pilnībā integrēta tiesībaizsardzības dimensija. Konkrētāk, tām būtu pilnā mērā jāizmanto noteikumi, kas paredzēti Direktīvā par uzbrukumiem informācijas sistēmām[50] un Eiropas Padomes Budapeštas Konvencijā par kibernoziegumiem[51], lai atturētu noziedzniekus no uzbrukumiem, sauktu tos pie atbildības un likvidētu noziedzīgās infrastruktūras, kas atvieglo uzbrukumus. Šo instrumentu sekmīgai īstenošanai būtu jānodrošina tas, ka noziedzīgās un ļaunprātīgas darbības pret veselības aprūpi tiek sodītas.

7. Rīcības plāna īstenošana un uzraudzība

Šajā rīcības plānā ir paredzēti vairāki uzdevumi atbalsta centram, kas jāizveido *ENISA* ietvaros. Tas nodrošina rīcības plāna vienotu un saskaņotu īstenošanu, vienlaikus izvairoties no jaunu struktūru izveides, kas varētu radīt pārklāšanos un pieskaitāmās izmaksas. Komisija plāno atbalsta centram nodrošināt pienācīgus resursus.

Kad atbalsta centrs būs sācis darboties, *ENISA*, apspriežoties ar Komisiju, būtu regulāri jāsniedz jaunākā informācija par atbalsta centra darbu *ENISA* Administratīvajai padomei, kā arī attiecīgajiem dalībvalstu tīkliem, proti, TID sadarbības grupai, *CSIRT* tīklam, e-veselības tīklam un attiecīgā gadījumā – Eiropas Veselības datu telpas padomei. Turklāt *ENISA* būtu pastāvīgi jāapmainās ar informāciju par atbalsta centra nodrošināto darbību īstenošanu ar publiskā un privātā sektora Veselības nozares kiberdrošības konsultatīvo padomi.

ENISA regulārie ziņojumi, piemēram, ziņojums par kiberdrošības stāvokli Savienībā, kurā sniegts kopējs novērtējums par kiberdrošības spēju un resursu gatavības līmeni visā ES, tai skaitā veselības nozarē, būtu jāizmanto, lai publicētu attiecīgos datus, tādējādi atbalstot rīcības plāna uzraudzību. Papildus tam *ENISA* ES kiberdrošības indekss[52] var sniegt kvantitatīvus un kvalitatīvus datus, kas kalpotu par pierādījumu bāzi veselības nozares kritiskuma un gatavības novērtēšanai.

8. Turpmākie pasākumi

Šajā paziņojumā ir izklāstīta vērienīga programma, kuras mērķis ir ES veselības nozarē panākt lielāku kiberdrošību. Rīcības plānā ir izklāstīts, kā izveidot saskaņotu un kopīgu Eiropas pieeju kiberdrošības

[50] Eiropas Parlamenta un Padomes Direktīva 2013/40/ES (2013. gada 12. augusts) par uzbrukumiem informācijas sistēmām, un ar kuru aizstāj Padomes Pamatlēmumu 2005/222/TI, https://eur-lex.europa.eu/eli/dir/2013/40/oj.
[51] Konvencija par kibernoziegumiem (Budapeštas konvencija, ETS Nr. 185) un tās protokoli, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

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

problēmām attiecīgajā nozarē, ierosinot *ENISA* ietvaros izveidot Kiberdrošības atbalsta centru slimnīcām un veselības aprūpes sniedzējiem.

Šis paziņojums ir uzskatāms par sākumu kiberdrošības uzlabošanas procesam veselības nozarē. Tādējādi papildus rīcības plāna pieņemšanai tiks uzsākta visaptveroša apspriešanās ar ieinteresētajām personām un turpināta informācijas apmaiņa ar dalībvalstīm un attiecīgajiem tīkliem nolūkā apkopot viedokļus. Pamatojoties uz apspriešanās rezultātiem, Komisija plāno 2025. gada 4. ceturksnī nākt klajā ar ieteikumiem rīcības plāna turpmākai pilnveidošanai.

Komisija aicina dalībvalstis un visas ieinteresētās personas sadarboties, lai sasniegtu rīcības plāna vērienīgos mērķus.

PIELIKUMS. Ierosināto darbību pārskats

Komisija:

***ENISA* Kiberdrošības atbalsta centrs slimnīcām un veselības aprūpes sniedzējiem**	
Nodrošināt pienācīgus resursus Kiberdrošības atbalsta centram Sadarboties ar *ECCC*, lai sāktu izmēģinājuma projektus, kuru mērķis ir izstrādāt kiberhigiēnas un drošības riska novērtēšanas paraugpraksi, un lai pievērstos vajadzību nodrošināšanai saistībā ar nepārtrauktu kiberdrošības uzraudzību, draudu izlūkdatu vākšanu un reaģēšanu uz incidentiem, izmantojot mūsdienīgus kiberdrošības risinājumus, nolūkā izstrādāt Eiropas Kiberdrošības atbalsta centra pakalpojumu katalogu	2025. gads
Kiberdrošības incidentu novēršana	
Apspriežoties ar TID sadarbības grupu, *EU-CyCLONe* un *ENISA*, aplūkot iespēju noteikt veselības jomu par nozari, kurai saskaņā ar Kibersolidaritātes aktu var sniegt atbalstu koordinētai gatavības testēšanai	2025. gada 1. cet.
Ātra reaģēšana un atgūšanās	
Kopā ar *ENISA* nodrošināt, ka ES kiberdrošības rezervē ir iekļauts ātrās reaģēšanas pakalpojums, kas paredzēts tieši veselības nozarei	2025. gada 4. cet.
Publiskā un privātā sektora sadarbība	
Ar *ENISA* atbalstu izveidot kopīgu Veselības nozares kiberdrošības konsultatīvo padomi	2025. gada 1. cet.
Izsludināt kiberdrošības uzņēmumiem, nodibinājumiem, izglītības iestādēm un nozares ieinteresētajām personām adresētu aicinājumu rīkoties, lai tie apņemtos veikt darbības nozares problēmu risināšanai	2025. gada 2. cet.
Kiberapdraudētāju atturēšana	
Kopā ar Augsto pārstāvi aplūkot iespēju izmantot Kiberdiplomātijas rīkkopas pasākumus, lai novērstu ļaunprātīgas darbības, kas vērstas pret veselības sistēmām, atturētu no tām un reaģētu uz tām	2025. gads

Sadarbībā ar Augsto pārstāvi veicināt starptautisko sadarbību cīņā pret izspiedējprogrammatūru aktoriem, it īpaši starptautiskās iniciatīvas izspiedējprogrammatūru apkarošanai ietvaros	2025.–2026. gads
Meklēt sadarbības iespējas G7 kiberdrošības darba grupā nolūkā stiprināt veselības nozares kiberdrošību	2025.–2026. gads
Turpmākie pasākumi	
Sākt visaptverošu apspriešanos ar ieinteresētajām personām	2025. gada 1. cet.
Pieņemt ieteikumus rīcības plāna turpmākai pilnveidošanai	2025. gada 4. cet.

***ENISA*:**

ES Kiberdrošības atbalsta centrs slimnīcām un veselības aprūpes sniedzējiem	
Sākt darbu, lai izveidotu Eiropas Kiberdrošības atbalsta centru slimnīcām un veselības aprūpes sniedzējiem	2025. gada 2. cet.
Izstrādāt visaptverošu katalogu ar pakalpojumiem, ko nodrošinās Kiberdrošības atbalsta centrs	no 2025. gada 4. cet.
Kiberdrošības incidentu novēršana	
Izdot norādījumus, kuros uzsvērta kritiski svarīgākā kiberdrošības prakse, un palīdzēt veselības aprūpes sniedzējiem to īstenot	2025. gada 3. cet.
Ciešā sadarbībā ar Komisiju un dalībvalstīm izstrādāt regulējuma kartēšanas rīku	2025. gada 1. cet.
Izstrādāt satvaru kiberdrošības gatavības novērtējumiem, kas paredzēti tieši veselības aprūpes nozarei	2025. gada 3. cet.
Veikt ikgadēju veselības nozares kiberdrošības gatavības novērtējumu	2025.–2026. gads
Sadarboties ar dalībvalstīm un reģionālajām programmu iestādēm, lai izveidotu kiberdrošības vaučeru paraugprogrammas	2025.–2026. gads

Izstrādāt jaunas iepirkuma pamatnostādnes slimnīcu un veselības aprūpes sniedzēju kiberdrošībai	2025. gada 3. cet.
Izveidot Eiropas veselības nozares *CISO* tīklu	2026. gada 1. cet.
Izstrādāt un popularizēt veselības aprūpes speciālistiem paredzētus mācību moduļus un kursus	2026. gada 1. cet.
Eiropas spējas atklāt pret veselības nozari vērstus kiberdraudus	
Izveidot Eiropas *KEV* katalogu attiecībā uz medicīniskām ierīcēm, e-veselības pacienta karšu sistēmām un IKT aprīkojuma un programmatūras nodrošinātājiem veselības nozarē	2025. gada 4. cet.
Ieviest ES mēroga agrīnās brīdināšanas abonēšanas pakalpojumu veselības nozarei	No 2026. gada
Atbalstīt Eiropas veselības nozares *ISAC* ar rīkiem un informācijas apmaiņu	2025.–2026. gads
Ātra reaģēšana un atgūšanās	
Kopā ar Komisiju nodrošināt, ka ES kiberdrošības rezervē ir iekļauts ātrās reaģēšanas pakalpojums, kas paredzēts tieši veselības nozarei	2025. gada 4. cet.
Sadarbībā ar *CSIRT* tīklu izstrādāt veselības aprūpes nozarei pielāgotas rokasgrāmatas reaģēšanai uz kiberincidentiem	2025. gada 3. cet.
Veicināt valstu kiberdrošības mācību plašu īstenošanu ar mērķi testēt rokasgrāmatas un nostiprināt protokolus reaģēšanai uz incidentiem	No 2025. gada 4. cet.
Nodrošināt abonēšanas pakalpojumu atgūšanās pasākumiem pēc izspiedējprogammatūras uzbrukuma	No 2026. gada
Kopā ar Eiropolu apzināt izplatītākos izspiedējprogrammatūras veidus, kas vērsti pret veselības aprūpes organizācijām, un paplašināt atšifrēšanas rīku repozitoriju, izmantojot projektu “No More Ransom”.	2025. gada 4. cet.
Kopā ar Eiropolu izstrādāt pieejamus norādījumus, kas palīdzētu veselības aprūpes sniedzējiem izvairīties no izpirkuma maksas	2025. gada 3. cet.
Valstu līmeņa rīcība	

Palīdzēt dalībvalstīm izstrādāt valsts rīcības plānu	2025. gads
Koordinēt centienus, lai nodrošinātu, ka dalībvalstu individuālie resursi un stratēģijas ir savstarpēji papildinoši	2025.–2026. gads
Rīcības plāna īstenošana un uzraudzība	
Apspriežoties ar Komisiju, regulāri sniegt jaunāko informāciju par Kiberdrošības atbalsta centra darbu attiecīgajiem dalībvalstu tīkliem	2025.–2026. gads
Nodrošināt pastāvīgu informācijas apmaiņu ar Veselības nozares kiberdrošības konsultatīvo padomi	2025.–2026. gads

Dalībvalstis:

Eiropas spējas atklāt pret veselības nozari vērstus kiberdraudus	
Ziņot Eiropas Kiberdrošības atbalsta centram par slimnīcu un veselības aprūpes sniedzēju sniegtajiem paziņojumiem par incidentiem saskaņā ar TID 2	No 2025. gada 4. cet.
Veicināt valstu veselības nozares *ISAC* izveidi	2025.–2026. gads
Kiberdrošības incidentu novēršana	
TID sadarbības grupā veikt koordinētu drošības riska novērtēšanu, novērtējot gan tehniskos, gan stratēģiskos riskus, kas saistīti ar medicīnisko ierīču piegādes ķēdēm	2025. gada 4. cet.
Ātra reaģēšana un atgūšanās	
Īstenot valstu kiberdrošības mācības ar mērķi testēt rokasgrāmatas un nostiprināt protokolus reaģēšanai uz incidentiem	No 2026. gada
Valsts līmeņa rīcība	
Izraudzīties valsts kiberdrošības atbalsta centrus slimnīcām un veselības aprūpes sniedzējiem	2025. gada 2. cet.
Izstrādāt valsts rīcības plānus, kas vērsti uz kiberdrošību veselības nozarē	2025. gada 4. cet.
Veicināt resursu koplietošanu veselības aprūpes sniedzēju vidū	2025.–2026. gads

Noteikt nesaistošus kritērijus un uzraudzīt finansēšanas mērķus, kas īpaši vērsti uz kiberdrošību	2025. gada 4. cet.
Pieprasīt veselības aprūpes organizācijām un citām struktūrām, uz kurām attiecas TID 2 direktīva, ziņot par saviem nodomiem maksāt izpirkuma maksu	2025. gada 4. cet.