Europos Sąjungos Taryba

Briuselis, 2025 m. sausio 16 d.
(OR. en)

5426/25

CYBER 21
SAN 15

PRIDEDAMAS PRANEŠIMAS

nuo:	Europos Komisijos generalinės sekretorės, kurios vardu pasirašo direktorė Martine DEPREZ
gavimo data:	2025 m. sausio 15 d.
kam:	Europos Sąjungos Tarybos generalinei sekretorei Thérèse BLANCHET
Komisijos dok. Nr.:	COM(2025) 10 final
Dalykas:	KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI Europos ligoninių ir sveikatos priežiūros paslaugų teikėjų kibernetinio saugumo veiksmų planas

Delegacijoms pridedamas dokumentas COM(2025) 10 final.

Pridedama: COM(2025) 10 final

EUROPOS
KOMISIJA

Briuselis, 2025 01 15
COM(2025) 10 final

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI

Europos ligoninių ir sveikatos priežiūros paslaugų teikėjų kibernetinio saugumo veiksmų planas

1. Įvadas

ES saugumo aplinka sparčiai kinta: daugėja hibridinių ir kibernetinių išpuolių, kuriais siekiama destabilizuoti mūsų visuomenę sėjant nesantaiką ir keliant suirutę, o kartu pasipelnyti iš kibernetinių nusikaltimų. Todėl Europa turi skubiai geriau pasirengti šiai naujai situacijai ir tapti jai atsparesne visuose sektoriuose, mobilizuodama visą visuomenę ir visas valdžios grandis, kaip raginama Europos Komisijos Pirmininko specialiojo patarėjo Saulio Niinistö pranešime.

Saugios ir atsparios sveikatos priežiūros sistemos yra ES socialinio modelio kertinis akmuo. Tačiau ligoninės ir sveikatos priežiūros sistemos susiduria su vis didesnėmis grėsmėmis, visų pirma į jas dėl finansinės naudos taikosi išpirkos reikalavimo programinę įrangą naudojančios gaujos, kurias masina didelė pacientų duomenų, įskaitant elektroninius sveikatos įrašus, vertė. Per pastaruosius ketverius metus sveikatos sektorius faktiškai tapo labiausiai puolamu ES sektoriumi, be kita ko, į sveikatos infrastruktūrą kibernetiniais išpuoliais vis dažniau taikytasi per COVID-19 pandemiją. Kibernetiniai išpuoliai prieš ligonines ir sveikatos priežiūros paslaugų teikėjus daro realią tiesioginę žalą žmonėms, nes tenka atidėti medicinines procedūras, stoja darbas skubiosios pagalbos skyriuose, o kartais net galėtų būti prarasta žmogaus gyvybė.

Problema dar aštresnė dėl to, kad šiame sektoriuje vyksta gyvybiškai svarbi skaitmeninė transformacija. Skaitmeninė sveikata ir sveikatos duomenų naudojimas bei pakartotinis naudojimas gali padėti išvengti ligos ar sudaryti sąlygas paankstinti terapiją ir taip sukurti priežiūros modelius, kurie geriau atitinka visuomenės ir pacientų poreikius bei pageidavimus. Skaitmeninių priemonių ir sprendinių integravimas į klinikinius procesus, taip pat sveikatos duomenų naudojimas ir pakartotinis naudojimas gali padėti priimti geresnius klinikinius sprendimus, prisidėti prie sveikatos sektoriaus automatizavimo, taip pat pagreitinti ir pagerinti pacientų priežiūrą. Skaitmeninės priemonės, duomenų naudojimas ir medicinos priemonės, kurios dažnai prijungtos prie interneto ir palaikomos dirbtinio intelekto (DI), labai padeda spręsti tokias problemas kaip sveikatos priežiūros specialistų trūkumas.

Kita vertus, gausėjant skaitmeninių priemonių, kibernetiniams nusikaltėliams atsiranda daugiau galimų taikinių. Be to, taikytis į sveikatos priežiūros įstaigas nesibodi kai kurie valstybiniai subjektai, kaip matyti iš tebesitęsiančio Rusijos agresijos karo prieš Ukrainą. Todėl per platesnę hibridinę kampaniją šis sektorius tampa potencialiu kibernetinių išpuolių taikiniu. Kibernetiniai išpuoliai ne tik kelia pavojų pacientų saugai, bet ir griauna visuomenės pasitikėjimą sveikatos infrastruktūra, be to, atkurti veiklą po jų brangiai kainuoja. Atspari ir saugi skaitmeninė infrastruktūra ne tik saugo nuo kibernetinių išpuolių, bet ir labai svariai prisideda prie Europos sveikatos duomenų erdvės[1] (ESDE) įgyvendinimo ir sukūrimo.

Todėl atėjo laikas padidinti ir sustiprinti Europos ligoninių ir sveikatos priežiūros paslaugų teikėjų kibernetinį saugumą ir atsparumą, kaip 2024–2029 m. Komisijos politinėse gairėse[2] pabrėžė Pirmininkė U. von der Leyen. Šis veiksmų planas priimamas reaguojant į reikalo skubumą ir ypatingas sektoriui kylančias grėsmes. Kibernetinio saugumo problemos sveikatos priežiūros srityje nebus išspręstos mostelėjus burtų lazdele. Vietoj to veiksmų plane raginama stiprinti prevenciją, gerinti pasirengimą ir labiau koordinuotai būti solidariems pasinaudojant Europos kibernetinio saugumo sektoriaus

[1] https://www.consilium.europa.eu/en/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_lt

ekspertinėmis žiniomis. Kaip būdinga veiksmų planams, čia išdėstytas ES požiūris į saugumą, kuris bus plėtojamas toliau ir įformintas rengiamoje Europos vidaus saugumo strategijoje, kurioje bus apibrėžtas visapusiškas atsakas į visas vidaus saugumo grėsmes ir orientuojamasi į gebėjimą numatyti grėsmes, užkirsti kelią žalai ir apsaugoti žmones, veikiant visais lygmenimis ir mobilizavus visą visuomenę.

Sveikatos sektoriuje veikia daug subjektų ir dalyvių: ligoninės, klinikos, slaugos namai, reabilitacijos centrai ir įvairūs sveikatos priežiūros paslaugų teikėjai, taip pat farmacijos, medicinos ir biotechnologijų pramonė, medicinos priemonių gamintojai ir sveikatos mokslinių tyrimų įstaigos. Šiame veiksmų plane daugiausia dėmesio skiriama ligoninių ir sveikatos priežiūros paslaugų teikėjų, suprantamų kaip bet kuris fizinis ar juridinis asmuo (arba bet kuris kitas subjektas), teisėtai teikiantis sveikatos priežiūros paslaugas valstybės narės teritorijoje[3], kibernetiniam saugumui. Ligoninės ir sveikatos priežiūros paslaugų teikėjai yra susiję su kitais sveikatos priežiūros subjektais ir yra arčiausiai žmonių. Be to, ligoninių ir sveikatos priežiūros paslaugų teikėjų kibernetinį saugumą didinančiomis priemonėmis taip pat turėtų būti mažinama platesnę tiekimo grandinę ir ekosistemą paveikianti rizika, keliama, pvz., subjektų, kurie naudoja sveikatos duomenis moksliniams tyrimams vykdyti ir mašinoms mokyti arba gamina medicinos priemones, visų pirma skaitmenizuotas medicinos priemones, jungiamas prie interneto ar kitų priemonių (daiktų internetas).

Nors sveikatos sistemų apsauga visų pirma yra nacionalinė kompetencija, sveikatos apsauga yra ir itin svarbus sektorius pagal Direktyvą dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje ES užtikrinti (TIS2)[4]. Kibernetiniai nusikaltėliai ir kiti grėsmę keliantys subjektai veikia tarpvalstybiniu mastu, o kibernetinio saugumo iššūkiai, su kuriais susiduria sveikatos priežiūros organizacijos, taip pat yra panašūs visose valstybėse narėse. Bendradarbiavimas Europos lygmeniu padeda dalytis informacija apie geriausią ES ir nacionalinę praktiką ir plėsti jos taikymo mastą. Todėl veiksmų plane siūlomas ES lygmens koordinavimas ir priemonės, o kartu valstybės narės raginamos imtis veiksmų, kad sveikatos priežiūros srityje ir platesnėje sveikatos ekosistemoje būtų pasiekta pokyčių.

Veiksmų plane daugiausia dėmesio skiriama pirmiausia sektoriaus pajėgumų **užkirsti kelią** kibernetinio saugumo incidentams stiprinimui, nes prevencija visada geriau nei atitaisymas. Antra, veiksmų plane detaliai išdėstyti veiksmai, kuriais siekiama gerinti dalijimąsi kibernetinio saugumo informacija ir gebėjimą **aptikti** kibernetines grėsmes ir taip gerinti galimybę greičiau sureaguoti. Trečia, jame numatytos priemonės, kuriomis naudodamiesi galėsime geriau **reaguoti** į incidentus ir po jų **atsigauti**. Galiausiai veiksmų plane numatyti būdai, kaip **atgrasyti** kibernetines grėsmes keliančius subjektus nuo išpuolių prieš sveikatos priežiūros sistemas Europoje.

Veiksmų planas bus įgyvendinamas bendradarbiaujant su sveikatos priežiūros paslaugų teikėjais ir platesne sveikatos ekosistema, valstybėmis narėmis ir kibernetinio saugumo bendruomene. Norint labiau sukonkretinti ir patikslinti didžiausią poveikį turinčius veiksmus, labai svarbu bendradarbiauti, kad tie veiksmai atneštų naudos visiems svarbiausiems sveikatos priežiūros paslaugų teikėjams Europoje. Todėl

[3] 2011 m. kovo 9 d. Europos Parlamento ir Tarybos direktyvos 2011/24/ES dėl pacientų teisių į tarpvalstybines sveikatos priežiūros paslaugas įgyvendinimo 3 straipsnio g punktas, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32011L0024

[4] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (TIS 2 direktyva), https://eur-lex.europa.eu/eli/dir/2022/2555.

skelbiant šį komunikatą bus pradėtos išsamios konsultacijos su suinteresuotaisiais subjektais, pramonės atstovais ir valstybėmis narėmis.Kadangi sienos kibernetinių pavojų nesulaiko ir jie yra susipynę, tai siekiant užtikrinti kibernetinį saugumą svarbu bendradarbiauti tarptautiniu mastu. Panašių grėsmių kibernetiniam saugumui kyla ir plėtros bei kaimyninėse šalyse, taip pat kitose šalyse ES strateginėse partnerėse. Jos galiausiai gali kelti pavojų ypatingos svarbos infrastruktūros saugumui ES. Todėl Europos Sąjungai bus svarbu apmąstyti patirtį, įgytą įgyvendinant veiksmų planą ir bendradarbiaujant su plėtros šalimis ir su kitomis šalimis partnerėmis, atsižvelgiant į joms kylančios grėsmės lygį.

2. Ligoninių ir sveikatos priežiūros paslaugų teikėjų kibernetinio saugumo problema

Kibernetinės grėsmės sveikatos sektoriui

Kibernetinių išpuolių daugėja visame pasaulyje ir ES viduje, o grėsmių panorama tampa vis sudėtingesnė ir dinamiškesnė. Tobulėjant dirbtiniam intelektui nusikaltėliai ir piktavaliai subjektai įgyja galingų priemonių savo operacijų tikslumui ir poveikiui gerinti, o kartu keičiasi kibernetinės gynybos galimybės, nes tampa įmanoma automatiškai imtis tikralaikių veiksmų prieš išpuolius.

Itin opi kibernetinio saugumo problema ES ir visame pasaulyje tebėra išpirkos reikalavimo programinė įranga: vienoje ataskaitoje apskaičiuota, kad dėl jos pasaulyje išlaidos iki 2031 m. kasmet sieks daugiau kaip 250 mlrd. EUR[5]. Kai nusikaltėliai smogia naudojami išpirkos reikalavimo programinę įrangą, jie ne tik užšifruoja aukų duomenis ir reikalauja išpirkos, bet ir vis dažniau išviešina neskelbtiną informaciją, kad atsirastų papildomas spaudimas. Kita opi problema – programinės ir aparatinės įrangos pažeidžiamumas: Europos Sąjungos kibernetinio saugumo agentūros (ENISA) duomenimis[6], sveikatos priežiūra yra tas sektorius, kuriame skelbta apie didžiausius su tokiu pažeidžiamumu susijusius saugumo incidentus[7]. Tarp kitų didėjančių grėsmių yra paskirstytojo paslaugos trikdymo (DDoS) atakos, kurių tikslas – puolamą sistemą užtvindyti duomenimis, kad ji taptų neprieinama teisėtiems naudotojams[8].

Sveikatos sektorius susiduria su panašiomis grėsmių kibernetiniam saugumui tendencijomis ir jame labai dažnai per išpuolius naudojama išpirkos reikalavimo programinė įranga. ENISA duomenimis, 2021–2023 m. ši įranga buvo susijusi su 54 proc. išanalizuotų sveikatos sektoriaus kibernetinio saugumo incidentų. 83 proc. išpuolių buvo finansiškai motyvuoti dėl didelės sveikatos priežiūros duomenų vertės, o 10 proc. išpuolių motyvacija buvo ideologinė[9]. 2024 m. Komisijos ataskaitoje taip pat nustatyta, kad

[5] Cybersecurity Ventures (2024 m. birželio 1 d.): *Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031*. Skelbiama adresu https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

[6] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013, (Kibernetinio saugumo aktas), https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

[7] ENISA Threat Landscape: Health Sector (2023 m. liepos mėn.).

[8] ENISA Threat Landscape 2024.

[9] ENISA Threat Landscape: Health Sector (2023 m. liepos mėn.). Ataskaitoje analizuoti sveikatos priežiūros paslaugų teikėjai, taip pat kitų rūšių organizacijos, įskaitant vykdančias su sveikata susijusius mokslinius tyrimus, tam tikrus su sveikata

71 proc. išpuolių, nuo kurių nukentėjo pacientų priežiūra, pavyzdžiui, vėlavo gydymas ar diagnostika ir sutrikdytos skubios pagalbos iškvietimo paslaugos, buvo susiję su išpirkos reikalavimo programine įranga[10]. Išpuoliai naudojant išpirkos reikalavimo programinę įrangą gali ypač sutrikdyti sveikatos priežiūros paslaugų teikimą ir kelti pavojų pacientų saugai. Be to, tokie išpuoliai dažnai siejami su pacientų duomenų, dažnai ir neskelbtinų su sveikata susijusių duomenų, apsaugos pažeidimais[11], dėl kurių nukenčia pagrindinė teisė į asmens duomenų apsaugą.

Tuo pačiu metu išpuolių mastas sveikatos priežiūrai vis labiau skaitmenėjant auga. Remiantis 2024 m. skaitmeninio dešimtmečio pažangos ataskaita, internetinę prieigą prie savo elektroninių pirminės sveikatos priežiūros įrašų turi vidutiniškai 79 proc. ES piliečių[12]. Elektroniniai sveikatos įrašai, klinikinės informacinės sistemos, ligoninių darbo srauto sistemos, gydymo išlaidų kompensavimo IT sistemos, medicininio vizualizavimo sistemos ir diagnostikos arba pacientų stebėsenos tikslais naudojamos medicinos priemonės – tai pavyzdžiai skaitmeninių priemonių, kurios gali atlikti svarbų vaidmenį didinant sveikatos sektoriaus veiksmingumą ir gerinti jo veiklos rezultatus, tačiau ir tapti kibernetinio išpuolio taikiniais. Kibernetinių išpuolių rizika ypač kyla specifinei sveikatos priežiūros veiklai, pavyzdžiui, intensyviajai priežiūrai ir radiologinei vizualizacijai, arba tokiose medicinos srityse kaip onkologija ir kardiologija, kurios ypač priklauso nuo skaitmenizuotų prietaisų. Be to, dėl tiekimo grandinės problemų gali būti perkami įrenginiai, kurių kibernetinis saugumas yra nepakankamas, o tai gali padidinti esamą bendrą riziką.

Pavyzdžiui, per COVID-19 pandemijos išpuolį, įvykdytą naudojant išpirkos reikalavimo programinę įrangą, buvo paralyžiuota didelė Airijos sveikatos priežiūros sistemos dalis, todėl incidento rytą atšaukta bent dalis paslaugų trisdešimt vienoje iš 54 ūminių ligų gydymo ligoninių[13]. Sveikatos priežiūros tarnybos turėjo grįžti prie popierinių įrašų, todėl veikla sulėtėjo ir buvo ne tokia efektyvi. Išpuolis prasidėjo atidarius duomenims išvilioti atsiųstą e. laišką, prie kurio buvo prisegtas kenkėjiškas priedas[14]. Incidentas parodė, kokią žalą gali padaryti iš vienos sistemos į kitą plintantys kibernetiniai išpuoliai, todėl svarbu nuo jų apsaugoti visą sveikatos priežiūros organizacijos perimetrą. Kita jo pamoka – visose organizacijose svarbu užtikrinti bazinę kibernetinę higieną ir kibernetinio saugumo kultūrą.

Ligoninių ir sveikatos priežiūros paslaugų teikėjų kibernetinio saugumo branda

Sveikatos priežiūros aplinka ES labai įvairi: ligoninės ir kiti sveikatos priežiūros paslaugų teikėjai valstybėse narėse smarkiai skiriasi nuosavybės ryšiais, struktūra ir dydžiu. Kai kuriais atvejais sveikatos

susijusius produktus gaminančius subjektus, už sveikatos priežiūrą atsakingas valdžios institucijas, sveikatos draudimo organizacijas, stacionarinio gydymo įstaigas ir socialinių paslaugų teikėjus. Skelbiama adresu https://www.enisa.europa.eu/publications/health-threat-landscape.

[10] European Commission: Joint Research Centre, Reina, V. and 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“, Publications Office of the EU, 2024, https://data.europa.eu/doi/10.2760/693487

[11] Remiantis ENISA grėsmių sveikatos sektoriui apžvalga, 43 proc. analizuotų incidentų, susijusių su išpirkos reikalavimo programine įranga, atveju pasitvirtino duomenų saugumo pažeidimas arba vagystė.

[12] 2024 m. Skaitmeninio dešimtmečio pažangos ataskaita

[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“. Skelbiama adresu https://www2.hse.ie/services/cyber-attack/what-happened/.

priežiūra gali būti valdoma centralizuotai nacionaliniu lygmeniu, kitais atvejais – regionų ir vietos lygmenimis, o sveikatos priežiūros paslaugų teikėjai gali priklausyti valstybei arba būti privatūs. Be to, skirtumų gali būti ir toje pačioje šalyje, pavyzdžiui, kai regionai labai skiriasi socialiniais, ekonominiais ir teritoriniais aspektais ir tai lemia sudėtingą mozaiką. Iššūkį šioje sudėtingoje sveikatos priežiūros aplinkoje gali kelti ne tik didelės sveikatos krizės, susijusios su užkrečiamosiomis ligomis, tokios kaip COVID-19 pandemija, bet ir kita rizika sveikatai, susijusi, pvz., su klimato kaita. Galiausiai labai skiriasi sveikatos priežiūros paslaugų teikėjų skaitmenizacijos lygis ir jie labai nevienodai diegia technologijas. Tokio sudėtingumo pavyzdys – paslaugoms tapus neprieinamoms dėl kibernetinio saugumo incidento gali būti patirta didelių nuostolių ir nukentėti pacientai net mažose sveikatos priežiūros įstaigose, įskaitant klinikas ar skubios medicinos pagalbos tarnybas, kurios teikia pagrindines paslaugas palyginti nedideliam klientų skaičiui.

2024 m. ENISA ataskaitos dėl kibernetinio saugumo padėties Sąjungoje[15] duomenimis, ES sveikatos sektoriaus kibernetinio saugumo branda yra vidutinė ir visoje Europoje sveikatos priežiūros subjektų kibernetinio saugumo brandos lygis smarkiai skiriasi. Trūkumų galima pastebėti tokiose svarbiose srityse kaip žmogiškųjų išteklių pakankamumas, organizacijų žinios apie savo informacinių ir ryšių technologijų (IRT) tiekimo grandines ir naujausių saugumo priemonių diegimas produktuose. Sektoriui sunkiai sekasi laikytis bazinės kibernetinės higienos ir taikyti pagrindines saugumo priemones, kaip matyti iš to, kad beveik visoms apklaustoms sveikatos organizacijom kyla iššūkių atliekant kibernetinio saugumo rizikos vertinimus, o beveik pusė jų niekada nėra atlikusios rizikos analizės[16].

Kitas svarbus iššūkis, susijęs su ligoninių kibernetiniu saugumu, yra informacinių technologijų (IT) ir operacinių technologijų (OT) sąveika, kai kertasi skirtingi su konfidencialumu, prieinamumu ir patikimumu susiję saugumo prioritetai, o pažeidimas vienoje srityje gali turėti įtakos kitai. 2024 m. ENISA ataskaitoje dėl kibernetinio saugumo padėties Sąjungoje taip pat pabrėžiama, kad dėl didelės subjektų, prietaisų ir produktų įvairovės sveikatos sektorius nepakankamai gerai užtikrina naudojamų IRT produktų ir procesų saugumą.

Dėl šios įvairovės ir nevienodo ligoninių darbuotojų ir vadovybės kibernetinio saugumo sąmoningumo užtikrinti sveikatos priežiūros sistemų kibernetinį saugumą yra kompleksiškas uždavinys. Pvz., remiantis 2024 m. „Eurobarometro“ apklausa dėl kibernetinių įgūdžių, per pastaruosius 12 mėnesių tik 25 proc. apklaustų sveikatos, švietimo ir socialinės rūpybos sektoriaus įmonių surengė mokymus arba ugdė kibernetinio saugumo sąmoningumą[17]. Reikia imtis veiksmų pirminės grandies sveikatos priežiūros specialistų kibernetinio sąmoningumo kultūrai puoselėti. Papildomi pažeidžiamumo veiksniai, nuo kurių nukenčia sveikatos priežiūros paslaugų teikėjų kibernetinis saugumas, yra, pvz., darbuotojų rotacija,

[15] ENISA: 2024 Report on the State of Cybersecurity in the Union (2024 m. rugsėjo mėn.). Skelbiama adresu https://www.enisa.europa.eu/publications/health-threat-landscape

[16] ENISA Threat Landscape: Health Sector (2023 m. liepos mėn.). Skelbiama adresu https://www.enisa.europa.eu/publications/health-threat-landscape.

[17] Greitoji „Eurobarometro“ apklausa Nr. 547 dėl kibernetinių įgūdžių (2024 m. gegužės mėn.). Skelbiama adresu https://europa.eu/eurobarometer/surveys/detail/3176.

bendrų darbo vietų naudojimas, prastas tapatumo nustatymo valdymas ir išimamų laikmenų naudojimas[18].

Daugeliu atvejų informacinės technologijos ir operacinės technologijos bent iš dalies perkamos iš išorės tiekėjų. 2024 m. „Eurobarometro“ apklausoje nustatyta, kad sveikatos, švietimo ir socialinės rūpybos sektoriuje bent kai kuriuos savo kibernetinio saugumo elementus iš išorės tiekėjų įsigyja 57 proc. apklaustų įmonių – daugiau nei bet kuriame kitame sektoriuje[19]. Be to, pastebima stipri tendencija pereiti prie debesijos kompiuterijos, skatinama poreikio keisti duomenų saugojimo ir valdymo mastą, efektyvinti išlaidas, geriau bendradarbiauti ir remtis pažangiomis technologijomis, pvz., DI ir medicininių daiktų internetu. 2022 m. 58 proc. sveikatos organizacijų naudojosi debesija grindžiama skaitmeninės sveikatos platforma[20]. Nors šis poslinkis gali labai padidinti efektyvumą, jis taip pat kelia riziką, dėl kurios reikia priimti informacija argumentuotus viešųjų pirkimų ir saugios konfigūracijos sprendimus.

Visi šie iššūkiai susiję su gebėjimų stiprinimu ir finansavimu. Kibernetinio saugumo finansavimas sveikatos sektoriuje buvo ribotas ir lieka universalia problema visoje ES[21]. Be to, šie finansavimo sunkumai sutampa su visuomenės senėjimu, dėl kurio ateinantiems dešimtmečiams numatomas spaudimas daugelio Europos sveikatos priežiūros sistemų biudžetui.

Dažnai dėl finansavimo trūkumo toliau naudojamos pasenusios priemonės ir senos sistemos, incidentų prevencijos arba reagavimo į juos ištekliai yra riboti, o kibernetinio saugumo branda turi spragų. Ligoninės nuolat yra priverstos rinktis tarp naujausios saugios skaitmeninės infrastruktūros ir pacientų priežiūrą gerinančių kitų būtinų investicijų, pavyzdžiui, į gydytojų ir kitų sveikatos priežiūros specialistų samdymą, naujoviškų diagnostikos ir gydymo metodų diegimą ir prietaisų įsigijimą. ENISA duomenimis[22], pagal informacijos saugumui skiriamą visų IT išlaidų dalį sveikatos sektorius užima tik septintą vietą iš dvylikos tirtų sektorių, o jo mediana yra 8,3 proc.

3. Europos kibernetinio saugumo pagalbos ligoninėms ir sveikatos priežiūros paslaugų teikėjams centras

ES kibernetinio saugumo sistemoje esama įvairių priemonių, kurias reikėtų panaudoti ligoninių ir sveikatos priežiūros paslaugų teikėjų saugumui ir atsparumui didinti. Siekiant spręsti daugelį išvardytųjų uždavinių, būtina suformuoti vieningą strateginį ES lygmens požiūrį, aprėpiantį išteklius, ekspertines žinias ir priemones, būtinas veiksmingai kovai su kibernetinėmis grėsmėmis. Kad sveikatos priežiūros

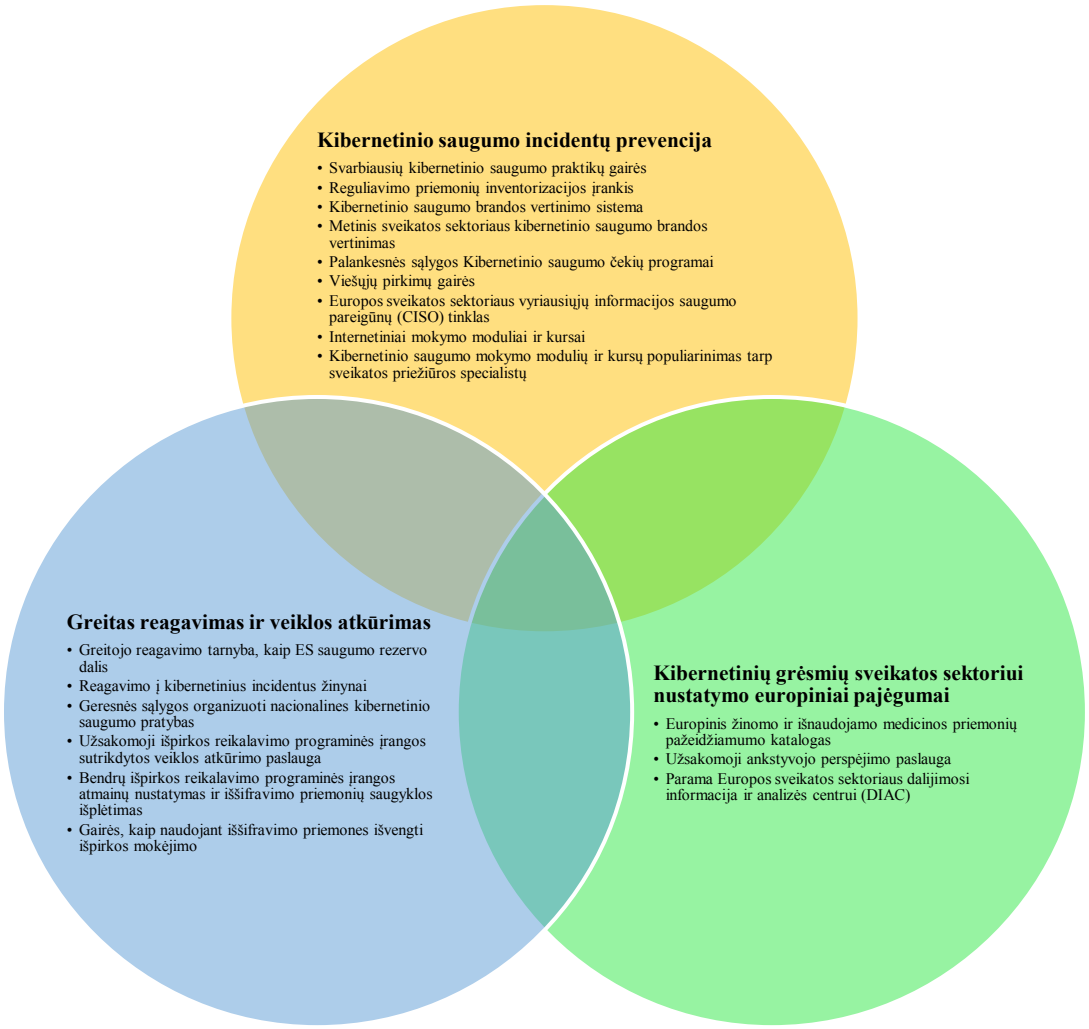
[18] Panacea – People-centric cybersecurity in healthcare (2021): White Paper – Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres.
[19] Greitoji „Eurobarometro“ apklausa Nr. 547 dėl kibernetinių įgūdžių (2024 m. gegužės mėn.). Skelbiama adresu https://europa.eu/eurobarometer/surveys/detail/3176.
[20] ENISA: NIS Investments Report 2022 (2022 m. lapkričio mėn.). Skelbiama adresu https://www.enisa.europa.eu/publications/nis-investments-2022.
[21] Pagal Sutarties dėl Europos Sąjungos veikimo 168 straipsnį, sveikatos paslaugų ir sveikatos priežiūros organizavimas ir teikimas priklauso nacionalinei kompetencijai, o sveikatos priežiūros sistemų finansavimas valstybėse narėse skiriasi.
[22] ENISA: NIS Investments Report 2022 (2022 m. lapkričio mėn.). Skelbiama adresu https://www.enisa.europa.eu/publications/nis-investments-2022.

paslaugų teikėjams visoje ES būtų lengviau stiprinti savo gynybą, labai svarbu matyti visapusį vaizdą, taip pat geriau planuoti ir koordinuoti. Tam labiausiai tiktų, kad ENISA, kuri įgaliota[23] apsaugoti ir remti ES ypatingos svarbos infrastruktūrą, savo struktūroje įsteigtų specialų **Europos kibernetinio saugumo pagalbos ligoninėms ir sveikatos priežiūros paslaugų teikėjams centrą**[24].

Pagalbos centras turėtų palaipsniui **parengti išsamų ligoninių ir sveikatos priežiūros paslaugų teikėjų poreikius atitinkančių paslaugų katalogą**, kuriame būtų aprašytos įvairios ir prieinamos parengties, prevencijos, aptikimo ir reagavimo paslaugos. Bendradarbiaudamas su valstybių narių valdžios institucijomis ir remdamasis ligoninių bei sveikatos priežiūros paslaugų teikėjų patirtimi, pagalbos centras turėtų sudaryti patogią naudoti ir lengvai pasiekiamą visų Europos, nacionaliniu ir regioniniu lygmenimis prieinamų priemonių bazę. Jis turėtų užtikrinti tinkamą savo darbų koordinavimą su valstybėmis narėmis ir padėti nustatyti veiksmų prioritetus ir juos įgyvendinti pagal poreikius realiuoju laiku.

Kaip svarbų pagalbos centro paslaugų katalogo kūrimo elementą, Komisija pasiūlys visoje ES imtis bandomųjų projektų, kad būtų plėtojama geriausia kibernetinės higienos ir saugumo rizikos vertinimo praktika, ir, atsižvelgdama į poreikį nuolat stebėti kibernetinį saugumą, rinkti žvalgybinę informaciją apie grėsmes ir reaguoti į incidentus naudojant pažangiausius kibernetinio saugumo sprendinius. Šių bandomųjų projektų, finansuojamų pagal Skaitmeninės Europos programą ir vykdomų Europos kibernetinio saugumo kompetencijos centro (ECCC), rezultatai bus panaudoti tolesniems ES lygmens veiksmams, taip pat ir pagalbos centro darbe.

[23] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013, (Kibernetinio saugumo aktas), OL L 151, 2019 6 7, p. 15–69.
[24] Šiame dokumente vadinamas ir tiesiog pagalbos centru.



1 diagrama. Pagalbos centro paslaugų katalogo ligoninėms ir sveikatos priežiūros paslaugų teikėjams koncepcijos

3.1. Kibernetinio saugumo incidentų prevencija

Paprasti veiksmai, kurie gali pakeisti situaciją

Baziniai kibernetinio saugumo žingsniai, pavyzdžiui, nuolat naujovinti sistemas, pasirūpinti atsarginėmis kopijomis ir įvesti daugiaveiksnį tapatumo nustatymą, gali, kaip rodo vienas apskaičiavimas, neutralizuoti iki 98 proc. išpuolių prieš organizaciją[25]. Daugelį paveikiausių

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

kibernetinės higienos ir rizikos valdymo priemonių įdiegti gana paprasta, todėl jomis galima lengvai padidinti kibernetinį saugumą. Todėl vienas iš pagrindinių pagalbos centro vaidmenų turėtų būti **parengti aiškias tikslines gaires, kuriose būtų aiškiai nurodytos svarbiausios kibernetinio saugumo praktikos ir kurios padėtų sveikatos priežiūros paslaugų teikėjams jas įgyvendinti**. Ši pagalba turi būti skirta ne vien didelėms ligoninėms, bet ir apimti specialiai pritaikytas konsultacijas mažesniems subjektams, pavyzdžiui, vietos bendrosios praktikos gydytojų kabinetams ir specializuotoms klinikoms, kurios dažnai neturi pakankamai išteklių specialioms kibernetinio saugumo komandoms, nors yra tokios pat pažeidžiamos išpuolių atveju. Be to, būtina atsižvelgti į regioninę specifinių sveikatos priežiūros įstaigų reikšmę užtikrinant pacientų priežiūrą, pavyzdžiui, retai apgyvendintose vietovėse. Sveikatos mokslinių tyrimų institutams, tvarkantiems didelį neskelbtinų asmens duomenų kiekį, taip pat galėtų būti naudinga gauti gaires apie bazines kibernetinio saugumo priemones, kuriomis jie galėtų didinti savo atsparumą.

Sveikatos priežiūros organizacijoms taip pat keliami įvairūs su kibernetiniu saugumu susiję ES teisės aktuose[26] nustatyti įpareigojimai. Nors įpareigojimai labai padeda užtikrinti aukštą bendrą kibernetinio ir duomenų saugumo lygį, labai svarbu užtikrinti, kad reglamentavimo aplinka nebūtų be reikalo sudėtinga ir paini. Labai susitelkus į reikalavimų laikymąsi nereikėtų išleisti iš akių uždavinio puoselėti tvirtą kibernetinio saugumo kultūrą. **Kiek įmanoma sumažinti administracinę naštą subjektams, kuriems taikomos įvairios reguliavimo priemonės, gali padėti lengvai pasiekiamas reguliavimo priemonių inventorizacijos įrankis**. Kad tokia priemonė būtų kuo greičiau sukurta ir išplatinta, pagalbos centras turėtų, be gairių ir priemonių rinkinių parengimo, aktyviai dirbti su Komisija ir valstybėmis narėmis. Taigi jis svariai prisidėtų prie to, kad kibernetinio saugumo taisyklės būtų lengvai suprantamos ir įgyvendinamos, pvz., teiktų įgyvendinimo gaires[27], o prireikus skatintų taikyti atitinkamus standartus.

Dar viena priemonė, padėsianti lengvai ir paprastai įdiegti gerąsias kibernetinės higienos praktikas, yra būsimos **europinės skaitmeninės tapatybės dėklės**. Siekiant sumažinti neteisėtos prieigos prie

[26] Tai, pavyzdžiui, TIS 2 direktyva; 2024 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847 dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, (Kibernetinio atsparumo aktas), https://eur-lex.europa.eu/eli/reg/2024/2847/oj/enghttps://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng; 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/745 dėl medicinos priemonių, https://eur-lex.europa.eu/eli/reg/2017/745/oj/enghttps://eur-lex.europa.eu/eli/reg/2017/745/oj/eng (Medicinos priemonių reglamentas), https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng; 2017 m. balandžio 5 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/746 dėl *in vitro* diagnostikos medicinos priemonių (*In vitro* diagnostikos medicinos priemonių reglamentas), https://eur-lex.europa.eu/eli/reg/2017/746/oj/enghttps://eur-lex.europa.eu/eli/reg/2017/746/oj/eng; 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas), https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32016R0679https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32016R0679; 2024 m. birželio 13 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/1689, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės, (Dirbtinio intelekto aktas), https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32024R1689; pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl Europos bendros sveikatos duomenų erdvės, COM(2022)197 *final*, https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex:52022PC0197, kuriam skirtos derybos baigtos 2024 m. pavasarį pasiekus politinį susitarimą, ir tikimasi, kad po baigiamųjų darbų teisės aktas 2025 m. pavasarį bus paskelbtas Oficialiajame leidinyje.

[27] Už Bendrojo duomenų apsaugos reglamento (BDAR) aiškinimo gairių rengimą atsakinga Europos duomenų apsaugos valdyba (EDAV). Rengdama gaires ENISA turėtų visapusiškai atsižvelgti į EDAV prerogatyvas.

sveikatos duomenų riziką, labai svarbu sumažinti priklausomybę nuo silpnų identifikavimo mechanizmų, tokių kaip slaptažodžiai. Labai svarbu pereiti prie saugių, patikimu identifikavimu grindžiamų prisijungimo sprendinių. ES skaitmeninės tapatybės dėklė užtikrina suderintą ES masto sveikatos priežiūros specialistų elektroninės atpažinties koncepciją ir kaip patikimas unifikuotas sprendinys veiks nuo 2026 m. pabaigos. Visos internetinės sveikatos informacinės sistemos, kuriose privaloma įdiegti saugesnį naudotojo tapatumo nustatymą, nuo 2027 m. pabaigos turės leisti naudoti dėklę tapatybei nustatyti[28].

Parengtis ir tikslinė parama

Veiksmingas kibernetinis saugumas neįmanomas be parengties testavimo, kuris apima tokius veiksmus kaip skverbties testavimas. Komisija jau skyrė lėšų ENISA bandomosioms parengties iniciatyvoms ir jos atskleidė, kad sveikatos sektorius yra viena sričių, kuriose testavimas ir tolesnis vertinimas ieškant kibernetinės brandos spragų yra patys paklausiausi. Įsigaliojus Kibernetinio solidarumo aktui, šių pastangų mastas bus gerokai išplėstas, o iniciatyvos imsis ECCC. Reaguodama į šį poreikį, Komisija, pasikonsultavusi su TIS bendradarbiavimo grupe, EU-CyCLONe[29] ir ENISA, pasiūlys nustatyti, kad sveikatos sektorius yra toks sektorius, kurio **koordinuotą parengties testavimą** galima remti pagal Kibernetinio solidarumo aktą. Be to, pagalbos centras turėtų parengti **specialiai sveikatos priežiūrai pritaikytą kibernetinio saugumo brandos vertinimų sistemą**. Tokie brandos vertinimai suteiktų subjektams praktinių įžvalgų apie jų pažeidžiamumą, o kartu progą parodyti pacientams ir suinteresuotiesiems subjektams savo kibernetinio saugumo parengtį ir taip didinti pasitikėjimą jų paslaugomis. Pagalbos centras turėtų atlikti metinį suvestinį **sveikatos sektoriaus kibernetinio saugumo brandos vertinimą**, kuriame būtų aiškiai apžvelgtas sveikatos sektoriaus kibernetinis saugumas tiek nacionaliniu, tiek ES lygmenimis.

Sveikatos sektorius labai priklauso nuo kibernetinio saugumo paslaugas teikiančių išorės rangovų[30] ir tai rodo, kad apsaugai stiprinti reikia tikslinės paramos. Remdamosi sėkmingomis iniciatyvomis, tokiomis kaip ES inovacijų čekiai, **valstybės narės turėtų apsvarstyti tikslines priemones, pavyzdžiui, kibernetinio saugumo čekius labai mažoms, mažoms ir vidutinio dydžio ligoninėms ir sveikatos priežiūros paslaugų teikėjams**. Šiais čekiais būtų teikiama finansinė parama konkrečioms kibernetinio saugumo priemonėms įgyvendinti. Čekių paskirstymo prioritetai turėtų būti nustatomi atsižvelgiant į parengties testavimo ir brandos vertinimų išvadas.

Siekiant veiksmingai diegti čekius ar kitas paramos programas, labai svarbios vietos žinios ir aplinkybės, nes nuo jų priklauso tinkamumas ir prieinamumas. ES fondai, pavyzdžiui, Europos regioninės plėtros fondas, jau aktyviai remia kibernetinio saugumo ir skaitmeninės sveikatos iniciatyvas, todėl galėtų būti naudojami kaip įrankis sveikatos priežiūros paslaugų teikėjams skirtoms tikslinėms kibernetinio saugumo čekių sistemoms kurti. Skatindamas šias pastangas, pagalbos centras bendradarbiautų su valstybėmis narėmis ir už programas atsakingomis regioninėmis institucijomis, kad tokių regioninių

[28] Reglamento (ES) 910/2014 5 straipsnio f dalies 1–2 punktai.
[29] Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas
[30] Žr. 2023 m. ENISA ataskaitą *NIS Investments Report 2023* (2023 m. lapkričio mėn.), kurioje pabrėžiama, kokia svarbi išorės parama atliekant kibernetinio saugumo auditą ir užtikrinant jo atitiktį. Skelbiama adresu https://www.enisa.europa.eu/publications/nis-investments-2023.

čekių sistemų kūrimas būtų remiamas naudojantis patirtimi, įgyta realiuose nacionaliniuose projektuose ir vykdant Skaitmeninės Europos programos lėšomis finansuojamus veiksmus, ir taip būtų užtikrintas vaisingas praktinis įgyvendinimas.

Be to, nuo 2014 m. „Horizonto“ programos padėjo finansuoti įvairias mokslinių tyrimų iniciatyvas, kuriomis siekiama didinti sveikatos priežiūros įstaigų, pvz., ligoninių, atsparumą kibernetinėms grėsmėms ir mažinti riziką, susijusią su netinkamu naujų technologijų naudojimu. Jas vykdant sukurta nemažai specializuotų priemonių, programų ir sistemų, pavyzdžiui, rizikos vertinimo priemonės, privatumą saugančios dalijimosi duomenimis platformos, kriptografiniai sprendiniai, kibernetinio sąmoningumo ugdymo programos ir tikralaikio grėsmių nustatymo sistemos. Beje, šie sprendiniai buvo rūpestingai patvirtinti realiomis sąlygomis įgyvendinant bandomuosius projektus sveikatos priežiūros aplinkoje, todėl saugantis nuo kibernetinių grėsmių jie tikrai veiksmingi ir praktiškai pritaikomi.

Sveikatos priežiūros tiekimo grandinių apsauga

Svarbus sveikatos priežiūros organizacijų iššūkis – valdyti sudėtingas IRT tiekimo grandines, apimančias įvairiausius produktus, pavyzdžiui, susietuosius medicinos prietaisus, elektroninių sveikatos įrašų sistemas ir biuro aparatinę įrangą. Kad ligoninės ir sveikatos priežiūros paslaugų teikėjai galėtų vykdyti savo veiklą, reikia patikimų ir saugių IRT sistemų ir paslaugų. Siekdama padėti sveikatos sektoriui spręsti kibernetinio saugumo uždavinius, TIS bendradarbiavimo grupė turėtų atlikti **koordinuotą saugumo rizikos vertinimą: įvertinti techninę ir strateginę riziką, susijusią su medicinos priemonių tiekimo grandinėmis, ir pasiūlyti rizikos mažinimo priemonių**[31]. Prireikus TIS bendradarbiavimo grupė turėtų dirbti kartu su Medicinos priemonių koordinavimo grupe.

Kibernetinio atsparumo aktas – tai nauja visapusė sistema, kurioje nustatyti kibernetinio saugumo reikalavimai, taikytini planuojant, projektuojant ir kuriant beveik visus aparatinės ir programinės įrangos produktus kiekviename vertės grandinės etape, taip pat tvarkantis su aktyviai išnaudojamu pažeidžiamumu, diegiant pataisas spragoms užtaisyti ir apie jį pranešant[32]. Medicinos prietaisai yra gaminių rūšis, naudojama vienoje jautriausių mūsų visuomenei sričių. Kibernetinio saugumo reikalavimai šiems gaminiams keliami jau kuris laikas galiojančiame Medicinos priemonių reglamente ir Reglamente dėl *in vitro* diagnostikos medicinos priemonių[33]. Dabar atliekant šių reglamentų vertinimą nagrinėjama, ar galima pasiekti didesnę šių sistemų dermę ir sinergiją, kad jos būtų paprastesnės, o kibernetinis saugumas būtų užtikrinamas naujoviškai.

Be to, rizikos vertinimo išvados turėtų padėti sveikatos priežiūros organizacijoms peržiūrėti savo tiekimo grandinės kibernetinio saugumo praktikas pagal TIS 2 direktyvos reikalavimus ir galėtų būti naudingos

[31] Pagal TIS 2 direktyvos 22 straipsnį.
[32] Pirmuoju etapu nuo 2025 m. rugpjūčio 1 d. bus reikalaujama, kad bendrojoje rinkoje pateikiami į Medicinos priemonių reglamento ir Reglamento dėl *in vitro* diagnostikos medicinos priemonių taikymo sritį nepatenkantys daugelio kategorijų radijo įrenginiai atitiktų su kibernetiniu saugumu susijusius esminius Radijo įrenginių direktyvos reikalavimus. Antrajame etape, nuo 2027 m. gruodžio 11 d., bus pradėtas taikyti Kibernetinio atsparumo aktas.
[33] 2019 m. gruodžio mėn. Bendradarbiavimo medicinos priemonių srityje grupė paskelbė gaires dėl medicinos priemonių kibernetinio saugumo, kad padėtų gamintojams laikytis abiejų reglamentų I priedo reikalavimų: https://ec.europa.eu/docsroom/documents/41863.

rengiant naujas **viešųjų pirkimų gaires**[34]. Šios gairės, kurias parengtų ENISA pasitelkdama jai priklausantį pagalbos centrą, turėtų atspindėti pastarojo meto tendencijas, pvz., pacientų duomenų kėlimą į debesį, taip pat poreikį elektroninius sveikatos duomenis į debesijos aplinką perkelti saugiai. Be to, naujosiose gairėse organizacijoms turėtų būti pasiūlyta praktinių priemonių, kad jos galėtų stebėti savo tiekimo grandines, be kita ko, pasitelkdamos valdomų saugumo paslaugų teikėjus ir naudodamosi atestavimo ataskaitomis ar trečiųjų subjektų rizikos vertinimais.

Debesijos srityje reikia imtis tolesnių veiksmų, kad būtų sprendžiamos specifinės su neskelbtinų sveikatos priežiūros duomenų tvarkymu susijusios problemos, be kita ko, valdoma didesnė saugumo, privatumo ir veiklos rizika. Siekdami sustiprinti apsaugos priemones, ekspertai rekomenduoja debesijos paslaugoms taikyti integruotojo ir pritaikytojo saugumo principus. Taikant šį požiūrį pirmenybė teikiama saugiai infrastruktūrai, iniciatyviam pažeidžiamumo valdymui ir valstybinių bei privačių debesijos sprendinių kompleksui. Siekiant užtikrinti patikimas saugumo praktikas taip pat labai svarbūs yra nuolatinė stebėsena ir konkrečių pardavėjų atestavimas, pvz., saugumo paslaugų teikėjų sertifikavimas ir atitikties nacionaliniams ir tarptautiniams standartams auditas.

Kai teikiamos tokios paslaugos kaip paslauginė infrastruktūra (IaaS), paslauginė platforma (PaaS) ir paslauginė programinė įranga (SaaS), užtikrinti saugumą dažnai tenka klientui. Tačiau daugeliui sveikatos priežiūros organizacijų trūksta išteklių, kurie leistų savarankiškai įvykdyti šiuos reikalavimus. Siekiant spręsti šią problemą, **debesijos paslaugų teikėjai turėtų būti raginami standartiškai įdiegti bazines saugumo priemones**. Šios priemonės sumažintų neteisingos konfigūracijos riziką, išlaikytų nuoseklią apsaugą visose vartotojų valdomose aplinkose ir suteiktų daugiau garantijų naudotojams. Nustatant numatytąjį bazinį saugumo lygį būtų siekiama patikimos apsaugos ir praktiškumo pusiausvyros pasirūpinant, kad jį būtų galima taikyti įvairiose sveikatos priežiūros organizacijose. Tam reikalingas glaudus debesijos paslaugų teikėjų ir sveikatos sektoriaus bendradarbiavimas, kuris sudarytų sąlygas naudojantis geriausia pramonės patirtimi sukurti veiksmingus kintamo masto sprendinius.

Mokymas ir įgūdžių ugdymas

Norint Europoje užtikrinti ilgalaikį tvarų augimą ir konkurencingumą, taip pat aukštos kokybės paslaugas, įskaitant sveikatos priežiūrą, svarbu apsirūpinti reikiamų įgūdžių turinčia darbo jėga. Kvalifikuotų kibernetinio saugumo specialistų trūkumas yra didelis iššūkis visoje Europoje – apskaičiuota, kad ES darbo rinkos poreikiams patenkinti trūksta 299 000 specialistų[35]. 2024 m. „Eurobarometro“ apklausos dėl kibernetinių įgūdžių[36] duomenimis, 81 proc. įmonių mano, kad sunkumai rasti kibernetinio saugumo darbuotojų kelia didelę riziką nukentėti nuo galimų kibernetinių išpuolių. Švietimo, sveikatos ir socialinio darbo sektoriuose 66 proc. kibernetinio saugumo funkcijų

[34] Remiantis 2020 m. ENISA parengtomis viešųjų pirkimų gairėmis dėl kibernetinio saugumo ligoninėse (2020 m. vasario mėn.). Skelbiama adresu https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

[35] 2024 m. kibernetinio saugumo panorama:ISC2 kibernetinio saugumo darbuotojų tyrimo įžvalgos | Skaitmeninių įgūdžių ir darbo vietų platforma

[36] Greitoji „Eurobarometro“ apklausa Nr. 547 dėl kibernetinių įgūdžių.

atlieka darbuotojai, kurie anksčiau dirbo kitokį darbą, o tai rodo, kad yra skubu persikvalifikuoti ir kelti kvalifikaciją.

Siekdamas spręsti šį uždavinį, pagalbos centras turėtų bendradarbiauti su būsimu kibernetinio saugumo įgūdžiams skirtu Europos skaitmeninės infrastruktūros konsorciumu (ESIK), numatytu Komisijos komunikate dėl Kibernetinio saugumo įgūdžių akademijos[37]. Šis darbas turėtų palengvinti sveikatos sektoriaus kibernetinio saugumo specialistų, pvz., vyriausiųjų informacijos saugumo pareigūnų (CISO), bendravimą. Vienas iš galimų veiksmų būtų sukurti **Europos sveikatos sektoriaus CISO tinklą**, pradedant ekspertų bendrija, kuri dalytųsi geriausia patirtimi ir ją kauptų, kurtų specialistų išlaikymo strategijas ir sprendimus, kaip pritraukti kibernetinio saugumo specialistus į sveikatos sektorių. Be to, pasitelkiant Kibernetinio saugumo įgūdžių akademiją turėtų būti plėtojami ištekliai, kurie, pramonei ir akademinei bendruomenei padedant, sveikatos sektoriuje stiprintų su kibernetiniu saugumu susijusius darbuotojus. Šioje srityje pramonės suinteresuotieji subjektai turėtų būti skatinami įsipareigoti remti kibernetinio saugumo mokymą.

Žmogaus klaidos ir toliau lemia daug sveikatos priežiūros kibernetinio saugumo incidentų, taigi būtinas visapusis darbuotojų mokymas ir kibernetinis sąmoningumas. Kadangi sveikatos priežiūros specialistai skaitmenines priemones naudoja dažnai, labai svarbu suteikti jiems žinių, kaip tai daryti saugiai. Tikslingas mokymas ir informuotumo didinimo kampanijos gali gerokai sumažinti riziką. Todėl pagalbos centras turėtų bendradarbiauti su sveikatos priežiūros specialistais ir paslaugų teikėjais, taip pat su švietimo ir mokymo paslaugų teikėjais, pramonės atstovais, Kibernetinio saugumo įgūdžiams skirtu ESIK ir valstybių narių institucijomis, kad būtų kuriami **išsamūs, lengvai prieinami internetiniai mokymo moduliai ir kursai** ir vyktų jų sklaida.

Siekiant sukurti tvirtą pagrindą sveikatos priežiūros kibernetiniam saugumui labai svarbu į švietimo programas įtraukti skaitmeninės kompetencijos ir kibernetinio saugumo modulius. Šiuose moduliuose turėtų būti kalbama sektoriui aktualiomis temomis, pavyzdžiui, apie pacientų duomenų apsaugą ir medicinos priemonių saugumo pažeidžiamumą. Plėtojant šiuos išteklius reikėtų atsižvelgti į ankstesnius veiksmus, pavyzdžiui, į projektą „BeWell“[38], finansuojamą pagal programą „Erasmus+“, ir PANACEA projektą[39], finansuojamą pagal programą „Horizontas 2020“.

3.2.Kibernetinių grėsmių sveikatos sektoriui nustatymo europiniai pajėgumai

[37] Komisijos komunikatas Europos Parlamentui ir Tarybai „Kibernetinio saugumo srities talentų trūkumo problemos sprendimas siekiant didinti ES konkurencingumą ir atsparumą bei skatinti jos augimą (Kibernetinio saugumo įgūdžių akademija)“, COM(2023) 207 *final*.
[38] „BeWell“ – aljansas būsimai sveikatos sektoriaus darbuotojų skaitmeninių ir žaliųjų įgūdžių strategijai parengti. Susipažinti galima adresu https://bewell-project.eu/.
[39] PANACEA – ligoninių ir sveikatos infrastruktūros apsauga ir privatumas taikant duomenims ir žmonėms naudingą pažangaus kibernetinio saugumo ir kovos su kibernetinėmis grėsmėmis priemonių rinkinį. Susipažinti galima adresu https://cordis.europa.eu/project/id/826293.

Siekiant greitai reaguoti į incidentus, labai svarbu veiksmingai nustatyti kibernetines grėsmes. Grėsmę keliantys subjektai gali naudotis įsibrovimo aptikimą apsunkinančiais metodais, kurie sudaro sąlygas ilgai naudotis neleistina sistemos landa[40]. Todėl pagerinus grėsmių aptikimo pajėgumus gali būti lengviau sustabdyti įsibėgėjančius kibernetinius išpuolius. Pvz., naudojant išpirkos reikalavimo programinę įrangą prieš Suomijos psichoterapijos paslaugų teikėją „Vastaamo“ įvykdyto išpuolio, kai kaltininkas prievartavo pacientus, kurių konfidencialūs įrašai buvo pavogti, pradinis įsibrovimas įvyko 2018 m., tačiau paslaugų teikėjas apie jį sužinojo tik 2020 m.[41]

Norint geriau nustatyti grėsmes ir gerinti informuotumą apie padėtį visoje ES, labai svarbu efektyviai dalytis informacija ir bendradarbiauti. Reagavimo į kompiuterinius saugumo incidentus tarnybos (CSIRT) atlieka labai svarbų vaidmenį, nes gauna pranešimus apie įvykusius ir vos neįvykusius incidentus bei galimas grėsmes ir teikia gaires dėl rizikos mažinimo nacionalinio lygmens priemonių. Tačiau tam**, kad būtų užtikrintas informuotumas apie padėtį ES, valstybės narės primygtinai raginamos dalytis su ENISA pagalbos centru visais ligoninių ir sveikatos priežiūros paslaugų teikėjų pranešimais apie kibernetinius incidentus**. Idealiu atveju kartu reikėtų pateikti dalykiškus įvairių aktualių incidento aspektų apibūdinimus, be kita ko, aptarti žinomą pamatinį pažeidžiamumą, sveikatos priežiūros paslaugų ir pacientų atžvilgiu nepageidaujamus reiškinius. Be to, medicinos ir *in vitro* diagnostikos priemonių gamintojai raginami savanoriškai per bendrą pranešimų teikimo platformą, kurią pagal Kibernetinio atsparumo aktą turi sukurti ir valdyti ENISA, pranešti apie aktyviai išnaudojamą pažeidžiamumą arba sunkius kibernetinius incidentus, darančius poveikį šių prietaisų saugumui, taip pat apie galimą kitą pažeidžiamumą, incidentus, įvykius be padarinių ar kibernetines grėsmes, kurie gali turėti įtakos šių prietaisų rizikos charakteristikai.

Pasinaudodamas ataskaitų informacija, kuri jau nėra neskelbtina, pagalbos centras galėtų, padedamas ENISA, sukurti europinį žinomo ir išnaudojamo medicinos priemonių, elektroninių sveikatos įrašų sistemų ir sveikatos srities IRT įrenginių bei programinės įrangos teikėjų pažeidžiamumo katalogą. Spręsdamas sudėtingus grėsmių nustatymo uždavinius, pagalbos centras turėtų sukurti **sveikatos sektoriui skirtą visoje ES prieinamą užsakomąją ankstyvojo perspėjimo paslaugą, kuri leistų apie pavojų perspėti beveik tikruoju laiku**. Šiai paslaugai būtų naudojami CSIRT, sveikatos priežiūros subjektų ir gamintojų, atvirųjų šaltinių žvalgybos (OSINT) ir kitų atitinkamų subjektų, pavyzdžiui, kibernetinio saugumo centrų, dalijimosi informacija ir analizės centrų (DIAC) ir teisėsaugos institucijų apdoroti duomenys. Informuotumą apie padėtį dar labiau pagerintų tvirtesnis ENISA ir Europos Sąjungos teisėsaugos bendradarbiavimo agentūros (Europolo) bendradarbiavimas, pavyzdžiui, prieš sveikatos sektorių nukreiptų elektroninių nusikaltimų modelių klausimais.

DIAC yra pagrindiniai žvalgybos informacijos apie kibernetines grėsmes ištekliai, jie puoselėja abipusį viešojo ir privačiojo sektorių keitimąsi informacija ir padeda stiprinti pasitikėjimą. Pagalbos centras turėtų labiau remti **Europos sveikatos sektoriaus DIAC** – aprūpinti priemonėmis, dalytis informacija, teikti sektorines informuotumo apie padėtį ataskaitas, taip pat puoselėti pasitikėjimu grįstą taktiškai ir strategiškai bendradarbiaujančią bendruomenę. Valstybės narės turėtų skatinti nacionalinių sveikatos

[40] ENISA Health Threat Landscape 2023.
[41] Suomijos duomenų apsaugos ombudsmeno sprendimas 1150/161/2021.

srities DIAC kūrimą[42]. DIAC taip pat turėtų būti raginami suvesti sveikatos priežiūros paslaugų teikėjus su gamintojais, kad būtų pasiektas bendras supratimas apie kibernetinio saugumo grėsmes, be kita ko, tiekimo grandinėje, ir lengviau megztųsi dialogas apie tai, kaip saugiai projektuoti produktus realiai atsižvelgiant į diegimo vietoje realijas.

3.3. Greitas reagavimas ir veiklos atkūrimas

Turint omenyje didelį pacientų sveikatos duomenų jautrumą ir galimai žlugdantį kibernetinių išpuolių poveikį sveikatos priežiūros paslaugoms, į kibernetinio saugumo incidentus labai svarbu reaguoti greitai ir efektyviai, kad būtų užtikrinta pacientų sauga. Kai ligoninė ar sveikatos priežiūros paslaugų teikėjas patiria kibernetinį išpuolį, pirmiausia reikia susisiekti su atitinkama nacionaline CSIRT[43]. CSIRT yra atsakinga, kad pagalba būtų suteikta laiku, geriausia – per 24 valandas, ir padėtų susitvarkyti su reikšmingais incidentais. Tačiau jei CSIRT su incidentu nesusidoroja, turėtų būti prieinama ES pagalba, kad reagavimas būtų greitas ir veiksmingas.

Pagal Kibernetinio solidarumo aktą įsteigtas ES kibernetinio saugumo rezervas, užtikrindamas patikimų valdomų saugumo paslaugų teikėjų teikiamas reagavimo į incidentus paslaugas, padeda susitvarkyti su reikšmingais arba didelio masto kibernetinio saugumo incidentais ir imtis pradinių veiklos atkūrimo darbų. Šis rezervas suformuotas taip, kad papildytų valstybių narių CSIRT pastangas: jos gali prašyti papildomos pagalbos su ypatingos svarbos sektoriais, pvz., sveikata, susijusiais atvejais. Stiprindamos šią sistemą, **Komisija ir ENISA turėtų užtikrinti, kad į rezervą būtų įtraukta konkrečiai sveikatos sektoriui skirta greitojo reagavimo tarnyba**. Kai nepakanka nacionalinės pagalbos, reikšmingiems ar didelio masto kibernetinio saugumo incidentams sveikatos priežiūros srityje valdyti ši tarnyba nedelsdama paskirs ekspertus, taip papildydama kitas veikiančias sistemas.

Siekdamas pagerinti reagavimą ir veiklos atkūrimą, pagalbos centras, bendradarbiaudamas su TIS bendradarbiavimo grupe, CSIRT tinklu ir, kai aktualu, Europolu, turėtų parengti **sveikatos priežiūrai pritaikytus reagavimo į kibernetinius incidentus žinynus**. Šie žinynai padėtų tiek CSIRT, tiek sveikatos priežiūros organizacijoms reaguoti į specifines kibernetinio saugumo grėsmes, įskaitant išpirkos reikalavimo programinę įrangą. Kadangi reaguojant į nusikalstamo pobūdžio kibernetinio saugumo incidentus ir juos tiriant labai svarbus veiksmingas CSIRT ir teisėsaugos institucijų bendradarbiavimas, žinynuose, be kita ko, turėtų būti paaiškinta, kaip apie tokius incidentus pranešti teisėsaugos institucijoms. Pagalbos centras taip pat galėtų **sudaryti palankesnes sąlygas plačiai organizuoti nacionalines kibernetinio saugumo pratybas, remiantis patirtimi, įgyta per ENISA**

[42] Pavyzdžiui, Suomija turi nacionalinį socialinės gerovės ir sveikatos priežiūros sektoriaus DIAC. Nuoroda į Suomijos nacionalinį kibernetinio saugumo centrą (DIAC dalijimosi informacija grupes) https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

[43] TIS 2 direktyvos 23 straipsnio 1 dalies nuostatomis esminiai ir svarbūs subjektai įpareigoti pranešti apie didelius incidentus atitinkamai CSIRT arba, kai taikytina, kompetentingai institucijai.

surengtas „Cyber Europe 2022“ ir panašias pratybas, kad žinynai būtų išbandyti ir būtų patobulinti reagavimo į incidentus protokolai.

Siekiant politiką pagrįsti informacija ir įvertinti priemonių, taikytų ginantis nuo išpuolių, kuriems naudota išpirkos reikalavimo programinė įranga, veiksmingumą, būtina surinkti daugiau duomenų. Todėl valstybės narės turėtų reikalauti, kad subjektai, kuriems taikoma TIS 2 direktyva, įskaitant sveikatos priežiūros organizacijas, pateikdami informaciją apie reikšmingus kibernetinio saugumo incidentus kartu praneštų apie visus atliktus ir ketinamus atlikti išpirkos mokėjimus. Tokie pranešimai padeda veiksmingai tirti incidentus, susijusius su išpirkos reikalavimo programine įranga, be kita ko, atsekti mokėjimus kriptovaliutos mainų platformose, kad būtų nustatyti gavėjai.

Labai svarbus atsparumo ir visuomenės pasitikėjimo išsaugojimo veiksnys yra veiklos atkūrimo sparta, ypač sveikatos priežiūros srityje, kurioje dėl prastovų gali sutrikti pacientų priežiūra. Kad galėtų veiksmingai atsigauti po išpuolių, susijusių su išpirkos reikalavimo programine įranga, sveikatos priežiūros paslaugų teikėjai turi turėti greitai atkuriamas saugias, atnaujintas ir izoliuotas atsargines kopijas. Pagalbos centras savo paslaugų kataloge galėtų pasiūlyti **užsakomąją išpirkos reikalavimo programinės įrangos sutrikdytos veiklos atkūrimo paslaugą, kuri padėtų ligoninėms ir sveikatos priežiūros paslaugų teikėjams iš anksto parengti veiklos atkūrimo planus**. ENISA ir Europolas dirbdami išvien turėtų nustatyti prieš sveikatos priežiūros organizacijas dažniausiai naudojamos išpirkos reikalavimo programinės įrangos atmainas ir **plėsti iššifravimo priemonių saugyklą**, sukurtą įgyvendinant projektą „No More Ransom“[44]. Jie taip pat turėtų parengti ir populiarinti prieinamas gaires, kurios padėtų sveikatos priežiūros paslaugų teikėjams naudotis iššifravimo priemonėmis ir taip išvengti išpirkos mokėjimo.

Tarptautinė kovos su išpirkos reikalavimo programine įranga iniciatyva[45] yra platforma, kuri padeda keistis informacija apie konkrečius incidentus, susijusius su išpirkos reikalavimo programine įranga, ir gerinti valstybių narių gebėjimus stiprinti savo kibernetinio saugumo sistemas ir tirti išpirkos reikalavimo programinę įrangą naudojančius subjektus. Bendradarbiaudama su vyriausiuoju įgaliotiniu, Komisija toliau skatins bendradarbiavimą įgyvendinant Kovos su išpirkos reikalavimo programine įranga iniciatyvą, be kita ko, kovojant su sveikatos sektoriui išpirkos reikalavimo programinės įrangos keliamomis grėsmėmis. Be to, Komisija sieks bendradarbiauti **G7 kibernetinio saugumo darbo grupėje**, kad būtų sustiprintas sveikatos sektoriaus kibernetinis saugumas. Konkrečiai, darbo grupė galėtų apsvarstyti galimybes remti sveikatos sektorių kovoje su tokiomis grėsmėmis kaip išpirkos reikalavimo programinė įranga, pasinaudodama tokiais argumentais kaip Jungtinių Tautų Saugumo Tarybos kontekste pateiktas 2024 m. lapkričio 8 d. bendras pareiškimas dėl išpuolių prieš sveikatos priežiūros objektus naudojant išpirkos reikalavimo programinę įrangą[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. Nacionalinio lygmens veiksmai

Šis veiksmų planas padės padidinti kibernetinį saugumą sveikatos sektoriuje tiek, kiek aktyviai ir ryžtingai įsitrauks valstybės narės. Kad veiksmų planas būtų sėkmingai įgyvendintas, valstybės narės galėtų paskirti **nacionalinius kibernetinio saugumo pagalbos centrus, skirtus specialiai ligoninėms ir sveikatos priežiūros** paslaugų teikėjams. Šie centrai veiktų kaip pirminiai sveikatos sektoriaus nacionalinio lygmens kontaktiniai centrai ir glaudžiai bendradarbiautų su ENISA pagalbos centru. Kai įmanoma ir aktualu, valstybės narės turėtų nacionaliniais kibernetinio saugumo pagalbos centrais paskirti esamas įstaigas, pavyzdžiui, nacionalines sveikatos priežiūros srities CSIRT arba atitinkamas institucijas.

Valstybės narės taip pat raginamos parengti **nacionalinius sveikatos sektoriaus kibernetiniam saugumui skirtus veiksmų planus**. Šiuose planuose būtų apibrėžta specifinė kibernetinio saugumo rizika, su kuria susiduria sveikatos priežiūros sistemos, ir nacionaliniai veiksmai, kurių imamasi jai pašalinti, kartu užtikrinant veiksmingą Europos lygmens išteklių naudojimą ir praktiką. ENISA pagalbos centras gali padėti rengti šiuos planus, atsižvelgdamas į jau egzistuojančius nacionalinius planus ir koordinuodamas pastangas užtikrinti, kad atskirų valstybių narių ištekliai ir strategijos papildytų vieni kitus.

Kitas svarbus valstybių narių darbo baras – sudaryti sveikatos priežiūros paslaugų teikėjams palankesnes sąlygas dalytis ištekliais, o tai galima pasiekti **vykdant bendrus viešuosius pirkimus arba sutelkiant išteklius** nacionaliniu, regioniniu ar net Europos lygmeniu. Toks požiūris sumažintų atskiriems subjektams tenkančią finansinę naštą ir padidintų jų derybinę galią kalbantis su kibernetinio saugumo paslaugų teikėjais.

Pavyzdžiui, pagal Prancūzijos CaRE programą[47] yra sukurtos įvairios nacionalinio ir regioninio lygmenų priemonės, kuriomis sprendžiamos su ištekliais susijusios problemos: kibernetinio saugumo kataloge galima susipažinti su kibernetiniais sprendiniais ir paketais, kuriuos ligoninėms siūlo nacionalinė kibernetinio saugumo agentūra, skaitmeninės sveikatos agentūra, regioninės agentūros ir nacionalinės perkančiosios organizacijos, taip pat su komerciniais sprendiniais. Be to, papildomai finansuojamos regioninės agentūros, kad jos galėtų pasiūlyti bendrų išteklių.

Valstybės narės taip pat turėtų spręsti nepakankamo investicijų į sveikatos sektoriaus kibernetinį saugumą lygio problemą. Siekdamos užtikrinti tinkamą finansavimą, jos turėtų nustatyti **neprivalomus lyginamuosius standartus ir stebėti būtent kibernetiniam saugumui skirto finansavimo tikslinius rodiklius**, kartu užtikrindamos, kad šios investicijos nenukreiptų dėmesio nuo būtinosios pacientų priežiūros. Šie finansavimo tiksliniai rodikliai taip pat turėtų padėti integruoti saugumo aspektus į visas šio sektoriaus skaitmenizavimo investicijas. Informacija apie su šiais tiksliniais rodikliais susijusias

[47]Prancūzijos skaitmeninės sveikatos agentūra *Cybersécurité acceleration et Résilience des Établissements* (CaRE) pasiekiama adresu https://esante.gouv.fr/strategie-nationale/cybersecurite.

geriausias praktikas ir patarimais valstybės narės galės dalytis per tokias platformas kaip E. sveikatos tinklas[48].

5. Viešojo ir privačiojo sektorių bendradarbiavimas

Norint sėkmingai įgyvendinti veiksmų planą labai svarbu, kad viešasis ir privatusis sektoriai bendradarbiautų ir konsultuotųsi su sveikatos priežiūros paslaugų teikėjais, kitais sveikatos sektoriaus subjektais ir atitinkamais kibernetinio saugumo sektoriaus subjektais. Siekdama labiau prisidėti prie pagalbos centro veiklos, iš abiejų sričių – sveikatos priežiūros ir kibernetinio saugumo – aukšto lygio atstovų **Komisija, padedama ENISA, suburs jungtinę sveikatos sektoriaus kibernetinio saugumo patariamąją tarybą**, kuri galės konsultuoti Komisiją ir paramos centrą dėl paveikių veiksmų ir svarstys tolesnį viešojo ir privačiojo sektorių partneryščių plėtojimą šioje srityje. Taryba bus buriama atsižvelgiant į esamas viešojo ir privačiojo sektorių partnerystės pastangas, įskaitant Europos sveikatos DIAC.

Be to, Komisija paskelbs **kvietimą veikti** kibernetinio saugumo įmonėms, fondams, švietimo įstaigoms ir pramonės suinteresuotiesiems subjektams, kad jie **įsipareigotų imtis sveikatos sektoriaus iššūkiams skirtų veiksmų**. Pasinaudodami Kibernetinio saugumo įgūdžių akademijos patirtimi, jie galėtų įsipareigoti (pavyzdžiui, Kibernetinio saugumo įgūdžių akademijos kontekste) parengti į sveikatos sektorių orientuotus mokymo kursus ir medžiagą kibernetinio saugumo specialistams[49]. Taip pat galima įsipareigoti vykdyti informuotumo didinimo veiklą arba teikti valdomas saugumo paslaugas subjektams, kurie yra pažeidžiami tam tikru aspektu, nemokamai arba už mažesnę kainą, siekiant padidinti jų parengtį ir kibernetiniu saugumu pagrįstą atsparumą. Be to, būtų galima įsipareigoti dalytis žvalgybos informacija apie kibernetines grėsmes su ENISA pagalbos centru. Pagalbos centras turėtų nuolat gauti pagal kvietimą imtis veiksmų prisiimtų įsipareigojimų apžvalgą, kad būtų užtikrinta jų dermė ir papildomumas.

6. Kibernetines grėsmes keliančių subjektų atgrasymas

ES vidaus ir išorės kibernetinio saugumo politika turėtų padėti siekti tikslo atgrasyti kibernetines grėsmes keliančius subjektus nuo išpuolių prieš Europos sveikatos priežiūros sistemas. Kibernetiniai išpuoliai prieš sveikatos priežiūros organizacijas yra ypač smerktina kibernetinės kenkimo veiklos atmaina, nes gali kelti grėsmę pacientų saugai ir gyvybei. Todėl turėtų būti pasinaudota visais kibernetinio saugumo ir teisėsaugos europiniais atgrasymo pajėgumais, kad būtų suardytas visas sveikatos sektoriui grėsmę keliančių subjektų verslo modelis ir lengvas pelnas taptų jiems nepasiekiamas. Pavyzdžiui, skatintini tarpvalstybiniai tyrimai, per kuriuos būtų aktyviau dalijamasi užvaldymo rodikliais ir kitais aktualiais duomenimis, ir daugiau dėmesio reikia skirti didelės vertės taikiniams ir pagrindiniams nusikaltėlių tarpininkams, pvz., nepramušamos prieglobos ar kriptovaliutų maišymo paslaugų teikėjams.

[48] E. sveikatos tinklas yra savanoriškas tinklas, vienijantis valstybių narių paskirtas nacionalines institucijas, kurios yra atsakingos už e. sveikatos sistemą, sukurtą vadovaujantis Direktyvos 2011/24/ES 14 straipsniu.

[49] Kibernetinio saugumo įgūdžių akademija: dalyvaukite | Skaitmeninių įgūdžių ir darbo vietų platforma

Kibernetinio saugumo diplomatijos priemonių rinkinys – tai sistema, kuria siekiama užkirsti kelią kibernetiniams išpuoliams prieš ES, valstybes nares ir šalis partneres, atgrasyti nuo jų ir į juos reaguoti. Reaguodamas į sveikatos sistemoms kylančias grėsmes, vyriausiasis įgaliotinis toliau naudosis esama sankcijų už kibernetinius nusikaltimus sistema.

Svarbi atgrasomoji priemonė – patraukti nusikalstamus subjektus atsakomybėn už jų veiksmus. Todėl valstybės narės turėtų užtikrinti, kad į jų nacionalinius veiksmų planus būtų visapusiškai integruota teisėsauga. Visų pirma jos turėtų naudotis visomis Direktyvos dėl atakų prieš informacines sistemas[50] ir Europos Tarybos Budapešto konvencijos dėl elektroninių nusikaltimų nuostatomis, kad atgrasytų nuo išpuolių, patrauktų nusikaltėlius baudžiamojon atsakomybėn ir išardytų nusikalstamas infrastruktūras, kurios palengvina išpuolius[51]. Sėkmingas šių priemonių įgyvendinimas turėtų užtikrinti, kad už nusikalstamus piktavališkus veiksmus prieš sveikatos priežiūrą būtų baudžiama.

7. Veiksmų plano įgyvendinimas ir stebėsena

Keletas šio veiksmų plano užduočių numatyta ENISA struktūroje įsteigtinam pagalbos centrui. Taip bus užtikrintas visapusis ir nuoseklus veiksmų plano įgyvendinimas, kartu išvengiant naujų subjektų steigimo, dėl kurio gali atsirasti dubliavimosi ir pridėtinių išlaidų. Komisija ketina pasiekti, kad pagalbos centrui būtų skirta pakankamai išteklių.

Kai pagalbos centras pradės veikti, ENISA, konsultuodamasi su Komisija, turėtų reguliariai teikti naujausią informaciją apie šio centro darbą ENISA valdančiajai tarybai ir atitinkamiems valstybių narių tinklams, visų pirma TIS bendradarbiavimo grupei, CSIRT tinklui, E. sveikatos tinklui ir, kai tinka, Europos sveikatos duomenų erdvės valdybai. Be to, ENISA turėtų nuolat dalytis informacija apie pagalbos centro veiksmų įgyvendinimą su viešajam ir privačiajam sektoriams atstovaujančia sveikatos sektoriaus kibernetinio saugumo patariamąja taryba.

Kaip galimybe paskelbti aktualius duomenis, padedančius vykdyti veiksmų plano stebėseną, reikėtų pasinaudoti reguliariomis ENISA ataskaitomis, pavyzdžiui, kibernetinio saugumo padėties Sąjungoje ataskaita, kurioje apibendrintai įvertinamas kibernetinio saugumo pajėgumų brandos lygis ir ištekliai visoje ES, taip pat ir sveikatos sektoriuje. O iš ENISA ES kibernetinio saugumo indekso[52] galima gauti kiekybinių ir kokybinių duomenų, kuriais, kaip įrodymais, galima remtis vertinant sveikatos sektoriaus reikšmę ir brandą.

8. Tolesni veiksmai

[50] 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR, https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng.
[51] Kovos su elektroniniais nusikaltimais konvencija (Budapešto konvencija, ETS Nr. 185) ir jos protokolai, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

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

Šiame komunikate išdėstyta plataus užmojo darbotvarkė, kaip padidinti ES sveikatos sektoriaus kibernetinį saugumą. Veiksmų plane siūloma ENISA struktūroje įsteigti kibernetinio saugumo pagalbos ligoninėms ir sveikatos priežiūros paslaugų teikėjams centrą ir nubrėžta kryptis, į kurią orientuojantis reikia kurti nuoseklų bendrą Europos požiūrį į sektoriaus kibernetinio saugumo problemą.

Šis komunikatas turėtų būti laikomas sveikatos sektoriaus kibernetinio saugumo gerinimo proceso pradžia. Todėl, siekiant surinkti įžvalgų, priėmus veiksmų planą bus pradėtos išsamios konsultacijos su suinteresuotaisiais subjektais ir toliau bendraujama su valstybėmis narėmis ir atitinkamais tinklais. Remdamasi konsultacijų rezultatais, 2025 m. ketvirtąjį ketvirtį Komisija ketina pateikti rekomendacijas dėl tolesnio veiksmų plano tobulinimo.

Komisija ragina valstybes nares ir visus suinteresuotuosius subjektus bendradarbiauti įgyvendinant veiksmų plano užmojus.

PRIEDAS. Siūlomų veiksmų apžvalga

Komisijai:

ENISA kibernetinio saugumo pagalbos ligoninėms ir sveikatos priežiūros paslaugų teikėjams centras	
Užtikrinti tinkamus išteklius kibernetinio saugumo pagalbos centrui. Bendradarbiaujant su ECCC inicijuoti bandomuosius projektus, per kuriuos būtų plėtojama geriausia kibernetinės higienos ir saugumo rizikos vertinimo praktika, ir pagal poreikius nuolat stebėti kibernetinį saugumą, rinkti žvalgybinę informaciją apie grėsmes ir reaguoti į incidentus naudojant pažangiausius kibernetinio saugumo sprendinius, kad būtų sudarytas Europos kibernetinio saugumo pagalbos centro paslaugų katalogas.	2025 m.
Kibernetinio saugumo incidentų prevencija	
Konsultuojantis su TIS bendradarbiavimo grupe, EU-CyCLONe ir ENISA, išnagrinėti, ar reikia nustatyti, kad sveikatos sektorius yra toks sektorius, kurio koordinuotą parengties testavimą galima remti pagal Kibernetinio solidarumo aktą.	2025 m. I ketvirtis
Greitas reagavimas ir veiklos atkūrimas	
Kartu su ENISA užtikrinti, kad į ES kibernetinio saugumo rezervą būtų įtraukta konkrečiai sveikatos sektoriui skirta greitojo reagavimo paslauga.	2025 m. IV ketvirtis
Viešojo ir privačiojo sektorių bendradarbiavimas	
Padedant ENISA įsteigti bendrą sveikatos sektoriaus kibernetinio saugumo patariamąją tarybą.	2025 m. I ketvirtis
Paskelbti kvietimą veikti kibernetinio saugumo įmonėms, fondams, švietimo įstaigoms ir pramonės suinteresuotiesiems subjektams, kad jie įsipareigotų imtis sveikatos sektoriaus iššūkiams skirtų veiksmų.	2025 m. II ketvirtis
Kibernetines grėsmes keliančių subjektų atgrasymas	
Kartu su vyriausiuoju įgaliotiniu apsvarstyti kibernetinio saugumo diplomatijos priemonių rinkinio priemonių naudojimą siekiant užkirsti kelią prieš	2025 m.

sveikatos sistemas nukreiptai piktavališkai veiklai, atgrasyti nuo jos ir į ją reaguoti.	
Dirbant su vyriausiuoju įgaliotiniu skatinti tarptautinį bendradarbiavimą kovoje su išpirkos reikalavimo programinę įrangą naudojančiais subjektais, konkrečiai, pagal Tarptautinę kovos su išpirkos reikalavimo programine įranga iniciatyvą.	2025–2026 m.
Siekti bendradarbiavimo G7 kibernetinio saugumo darbo grupėje, kad būtų sustiprintas sveikatos sektoriaus kibernetinis saugumas.	2025–2026 m.
Tolesni veiksmai	
Pradėti išsamias konsultacijas su suinteresuotaisiais subjektais.	2025 m. I ketvirtis
Priimti rekomendacijas dėl tolesnio veiksmų plano tobulinimo.	2025 m. IV ketvirtis

ENISA:

ES kibernetinio saugumo pagalbos ligoninėms ir sveikatos priežiūros paslaugų teikėjams centras	
Pradėti kurti Europos kibernetinio saugumo pagalbos ligoninėms ir sveikatos priežiūros paslaugų teikėjams centrą.	2025 m. II ketvirtis
Parengti išsamų kibernetinio saugumo pagalbos centro teikiamų paslaugų katalogą	Nuo 2025 m. IV ketvirčio
Kibernetinio saugumo incidentų prevencija	
Parengti gaires, kuriose būtų aiškiai nurodytos svarbiausios kibernetinio saugumo praktikos, ir padėti sveikatos priežiūros paslaugų teikėjams jas įgyvendinti.	2025 m. III ketvirtis
Glaudžiai bendradarbiaujant su Komisija ir valstybėmis narėmis sukurti reguliavimo priemonių inventorizacijos įrankį.	2025 m. I ketvirtis
Sukurti specialiai sveikatos priežiūrai skirtų kibernetinio saugumo brandos vertinimų sistemą.	2025 m. III ketvirtis
Atlikti metinį sveikatos sektoriaus kibernetinio saugumo brandos vertinimą.	2025–2026 m.

Bendradarbiauti su valstybėmis narėmis ir regioninėmis už programas atsakingomis institucijomis, kad būtų sukurtos pavyzdinės kibernetinio saugumo čekių programos.	2025–2026 m.
Parengti naujas ligoninių ir sveikatos priežiūros paslaugų teikėjų kibernetinio saugumo viešųjų pirkimų gaires.	2025 m. III ketvirtis
Sukurti Europos sveikatos sektoriaus CISO tinklą.	2026 m. I ketvirtis
Parengti ir propaguoti sveikatos priežiūros specialistų mokymo modulius ir kursus.	2026 m. I ketvirtis
Kibernetinių grėsmių sveikatos sektoriui nustatymo europiniai pajėgumai	
Sukurti europinį žinomo ir išnaudojamo medicinos priemonių, elektroninių sveikatos įrašų sistemų ir sveikatos srities IRT įrenginių bei programinės įrangos teikėjų pažeidžiamumo katalogą.	2025 m. IV ketvirtis
Įdiegti sveikatos sektoriui skirtą visoje ES prieinamą užsakomąją ankstyvojo perspėjimo paslaugą	Nuo 2026 m.
Remti Europos sveikatos sektoriaus DIAC suteikiant priemonių ir dalijantis informacija	2025–2026 m.
Greitas reagavimas ir veiklos atkūrimas	
Kartu su Komisija užtikrinti, kad į ES kibernetinio saugumo rezervą būtų įtraukta konkrečiai sveikatos sektoriui skirta greitojo reagavimo paslauga.	2025 m. IV ketvirtis
Bendradarbiaujant su CSIRT tinklu parengti sveikatos priežiūrai pritaikytus reagavimo į kibernetinius incidentus žinynus.	2025 m. III ketvirtis
Sudaryti palankesnes sąlygas plačiu mastu vykdyti nacionalines kibernetinio saugumo pratybas, kad būtų galima išbandyti žinynus ir patobulinti reagavimo į incidentus protokolus.	Nuo 2025 m. IV ketvirčio
Teikti užsakomąją išpirkos reikalavimo programinės įrangos sutrikdytos veiklos atkūrimo paslaugą.	Nuo 2026 m.
Kartu su Europolu nustatyti prieš sveikatos priežiūros organizacijas dažniausiai naudojamos išpirkos reikalavimo programinės įrangos atmainas ir išplėsti iššifravimo priemonių saugyklą, sukurtą įgyvendinant projektą „No More Ransom“.	2025 m. IV ketvirtis

Kartu su Europolu parengti prieinamas gaires, kurios padėtų sveikatos priežiūros paslaugų teikėjams išvengti išpirkos mokėjimo.	2025 m. III ketvirtis
Nacionalinio lygmens veiksmai	
Padėti valstybėms narėms parengti nacionalinius veiksmų planus.	2025 m.
Koordinuoti pastangas užtikrinti, kad atskirų valstybių narių ištekliai ir strategijos papildytų vieni kitus.	2025–2026 m.
Veiksmų plano įgyvendinimas ir stebėsena	
Konsultuojantis su Komisija reguliariai teikti naujausią informaciją apie kibernetinio saugumo pagalbos centro darbą atitinkamiems valstybių narių tinklams.	2025–2026 m.
Nuolat dalytis informacija su Sveikatos sektoriaus kibernetinio saugumo patariamąja taryba.	2025–2026 m.

Valstybėms narėms:

Kibernetinių grėsmių sveikatos sektoriui nustatymo europiniai pajėgumai	
Pagal TIS 2 perdavinėti Europos kibernetinio saugumo pagalbos centrui ligoninių ir sveikatos priežiūros paslaugų teikėjų pranešimus apie incidentus.	Nuo 2025 m. IV ketvirčio
Skatinti nacionalinių sveikatos srities DIAC kūrimą.	2025–2026 m.
Kibernetinio saugumo incidentų prevencija	
TIS bendradarbiavimo grupėje atlikti koordinuotą saugumo rizikos vertinimą, įvertinant techninę ir strateginę su medicinos priemonių tiekimo grandinėmis susijusią riziką.	2025 m. IV ketvirtis
Greitas reagavimas ir veiklos atkūrimas	
Organizuoti nacionalines kibernetinio saugumo pratybas, kad būtų galima išbandyti žinynus ir patobulinti reagavimo į incidentus protokolus.	Nuo 2026 m.
Nacionalinio lygmens veiksmai	

Paskirti nacionalinius kibernetinio saugumo pagalbos ligoninėms ir sveikatos priežiūros paslaugų teikėjams centrus.	2025 m. II ketvirtis
Parengti nacionalinius sveikatos sektoriaus kibernetiniam saugumui skirtus veiksmų planus.	2025 m. IV ketvirtis
Sudaryti palankesnes sąlygas sveikatos priežiūros paslaugų teikėjams dalytis ištekliais.	2025–2026 m.
Nustatyti neprivalomus konkrečiai kibernetiniam saugumui skirtus lyginamuosius standartus ir stebėti, kaip siekiama jam skirto finansavimo tikslinių rodiklių.	2025 m. IV ketvirtis
Pareikalauti, kad sveikatos priežiūros organizacijos ir kiti subjektai, kuriems taikoma TIS 2 direktyva, praneštų apie ketinimus mokėti išpirką.	2025 m. IV ketvirtis