Svet
Evropske unije

Bruselj, 16. januar 2025
(OR. en)

5426/25

CYBER 21
SAN 15

SPREMNI DOPIS

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Datum prejema:	15. januar 2025
Prejemnik:	Thérèse BLANCHET, generalna sekretarka Sveta Evropske unije
Št. dok. Kom.:	COM(2025) 10 final
Zadeva:	SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ Akcijski načrt za kibernetsko varnost bolnišnic in izvajalcev zdravstvenih dejavnosti

Delegacije prejmejo priloženi dokument COM(2025) 10 final.

Priloga: COM(2025) 10 final

EVROPSKA
KOMISIJA

Bruselj, 15.1.2025
COM(2025) 10 final

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ

Akcijski načrt za kibernetsko varnost bolnišnic in izvajalcev zdravstvenih dejavnosti

1. Uvod

Varnostno okolje EU se hitro spreminja, saj je vse več hibridnih in kibernetskih napadov, katerih cilj je destabilizirati našo družbo ter povzročati razdor in motnje, pa tudi služiti s kibernetsko kriminaliteto. Evropa mora zato nujno okrepiti svojo pripravljenost na to novo resničnost in odpornost proti njej, in sicer v vseh sektorjih ter v skladu z vsedružbenim in vsevladnim pristopom, kot je v poročilu pozval posebni svetovalec predsednice Evropske komisije Sauli Niinistö.

Varni in odporni zdravstveni sistemi so temelj socialnega modela EU. Vendar se bolnišnice in zdravstveni sistemi srečujejo z vse večjimi grožnjami, zlasti s strani tolp, ki uporabljajo izsiljevalsko programje, ki jih zaradi velike vrednosti podatkov o pacientih, vključno z elektronskimi zdravstvenimi zapisi, napadajo zaradi finančnih koristi. Zdravstveni sektor je v zadnjih štirih letih namreč postal največkrat napadena panoga v EU, tudi med pandemijo COVID-19, ko je bila zdravstvena infrastruktura vse pogosteje tarča kibernetskih napadov. Kibernetski napadi na bolnišnice in izvajalce zdravstvene dejavnosti neposredno škodujejo ljudem, saj povzročajo zamude pri medicinskih posegih in čakalne vrste v urgentnih centrih, v skrajnih primerih pa lahko privedejo do izgube življenj.

Izziv je še toliko večji, ker je sektor v procesu pomembne digitalne preobrazbe. Digitalno zdravje ter uporaba in ponovna uporaba zdravstvenih podatkov lahko omogočijo modele oskrbe, ki so bolje prilagojeni potrebam in željam ljudi in pacientov, saj lahko preprečijo nastanek bolezni ali omogočijo zgodnejše zdravljenje. Vključevanje digitalnih orodij in rešitev v klinične procese ter uporaba in ponovna uporaba zdravstvenih podatkov lahko prispevajo k boljšim kliničnim odločitvam, avtomatizaciji v zdravstvu ter hitrejši in boljši oskrbi pacientov. Digitalna orodja, uporaba podatkov in medicinski pripomočki, ki so pogosto povezani z internetom in jih poganja umetna inteligenca, so ključni tudi za reševanje izzivov, kot je pomanjkanje zdravstvenih delavcev.

Hkrati se zaradi digitalnih orodij širi tudi nabor potencialnih tarč storilcev kaznivega dejanja kibernetske kriminalitete. Poleg tega se nekateri državni akterji ne izogibajo napadom na zdravstvene ustanove, kot je razvidno iz ruske vojne agresije proti Ukrajini. Zato je ta sektor potencialna tarča kibernetskih napadov v okviru širše hibridne kampanje. Kibernetski napadi ne ogrožajo le varnosti pacientov, temveč tudi zmanjšujejo zaupanje javnosti v zdravstveno infrastrukturo in povzročajo velike stroške okrevanja. Odporna in varna digitalna infrastruktura je poleg zaščite pred kibernetskimi napadi bistvena tudi za podporo izvajanju in polni uvedbi evropskega zdravstvenega podatkovnega prostora[1].

Zato je čas, da se povečata in okrepita kibernetska varnost ter odpornost evropskih bolnišnic in izvajalcev zdravstvenih dejavnosti, kot je predsednica Ursula von der Leyen poudarila v svojih političnih usmeritvah za Komisijo za obdobje 2024–2029[2]. Ta akcijski načrt je odziv na nujnost razmer in edinstvene grožnje, s katerimi se srečuje zadevni sektor. Za izzive na področju kibernetske varnosti v zdravstvu ni preproste, čudežne rešitve. Namesto tega akcijski načrt poziva k okrepljenemu preprečevanju, pripravljenosti in bolj usklajenemu pristopu k solidarnosti ob izkoriščanju strokovnega znanja evropske industrije kibernetske varnosti. Akcijski načrt kot tak odraža pristop EU k varnosti, ki bo nadalje razvit in formaliziran v prihodnji evropski strategiji notranje varnosti, pri čemer je v njem

[1] https://www.consilium.europa.eu/sl/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_sl.

opredeljen celovit odziv na vse notranje varnostne grožnje, poudarek pa je na zmožnosti predvidevanja groženj, preprečevanju škode in zaščiti ljudi, pri čemer deluje na vseh ravneh z vsedružbenim pristopom.

Zdravstveni sektor vključuje številne subjekte in akterje, vključno z bolnišnicami, klinikami, domovi za starejše, rehabilitacijskimi centri in različnimi izvajalci zdravstvenih dejavnosti ter farmacevtsko, medicinsko in biotehnološko industrijo, proizvajalci medicinskih pripomočkov in zdravstvenimi raziskovalnimi ustanovami. Ta akcijski načrt se osredotoča predvsem na kibernetsko varnost bolnišnic in izvajalcev zdravstvenih dejavnosti, tj. vsake fizične ali pravne ali katere koli druge osebe, ki zakonito izvaja zdravstveno varstvo na ozemlju države članice[3]. Bolnišnice in izvajalci zdravstvenih dejavnosti so soodvisni z drugimi zdravstvenimi subjekti in so najbližje ljudem. Hkrati bi bilo treba z ukrepi za izboljšanje kibernetske varnosti bolnišnic in izvajalcev zdravstvenih dejavnosti obravnavati tudi tveganja, ki vplivajo na širšo dobavno verigo in ekosistem ter izhajajo na primer iz subjektov, ki uporabljajo zdravstvene podatke za raziskave in strojno učenje ali proizvajajo medicinske pripomočke, in sicer zlasti digitalno podprte medicinske pripomočke, ki se povezujejo z internetom ali drugimi pripomočki (t. i. internet stvari).

Zagotavljanje zdravstvenih sistemov je predvsem v nacionalni pristojnosti, vendar je zdravstvo tudi kritični sektor v skladu z direktivo o ukrepih za visoko skupno raven kibernetske varnosti v EU (NIS 2)[4]. Storilci kaznivega dejanja kibernetske kriminalitete in drugi akterji groženj delujejo čezmejno, izzivi na področju kibernetske varnosti, s katerimi se srečujejo zdravstvene organizacije, pa so podobni v vseh državah članicah. Sodelovanje na evropski ravni je dragoceno za izmenjavo in razširitev dobrih praks na ravni EU in nacionalni ravni. Zato so v akcijskem načrtu predlagani usklajevanje in ukrepi na ravni EU, hkrati pa se države članice poziva, naj sprejmejo ukrepe, ki bodo prispevali k boljšemu zdravstvenemu varstvu in širšemu zdravstvenemu ekosistemu.

Akcijski načrt je v prvi vrsti osredotočen zlasti na krepitev zmogljivosti sektorja za **preprečevanje** kibernetskih incidentov, saj je vedno bolje preprečiti kot odpravljati posledice. Drugič, v akcijskem načrtu so podrobno opisani ukrepi za izboljšanje izmenjave informacij o kibernetski varnosti in zmogljivosti za **odkrivanje** kibernetskih groženj, kar bo omogočilo hitrejše odzivanje. Tretjič, zagotavlja ukrepe za boljše **odzivanje** na incidente in **okrevanje** po njih. Poleg tega so v akcijskem načrtu predvideni načini za **odvračanje** akterjev kibernetskih groženj od napadov na zdravstvene sisteme v Evropi.

Akcijski načrt se bo izvajal v sodelovanju z izvajalci zdravstvenih dejavnosti in širšim zdravstvenim ekosistemom, državami članicami in skupnostjo za kibernetsko varnost. Sodelovalni pristop je ključen za nadaljnjo opredelitev in izpopolnitev najučinkovitejših ukrepov, da bodo imeli od njih koristi vsi ključni izvajalci zdravstvenih dejavnosti v Evropi. Zato bo to sporočilo spremljal začetek celovitega posvetovanja z deležniki, industrijo in državami članicami. Mednarodno sodelovanje je za kibernetsko varnost pomembno zaradi brezmejne narave in medsebojne povezanosti kibernetskih groženj. Primerljive kibernetske grožnje so prisotne tudi v državah širitve in državah evropskega sosedstva ter

[3] Člen 3, točka (g), Direktive 2011/24/EU Evropskega parlamenta in Sveta o uveljavljanju pravic pacientov pri čezmejnem zdravstvenem varstvu, https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=celex:32011L0024.
[4] Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (direktiva NIS 2), https://eur-lex.europa.eu/eli/dir/2022/2555.

drugih strateških partnerskih državah EU. To lahko na koncu ogrozi varnost kritične infrastrukture v EU. Zato bo treba izkušnje, pridobljene pri izvajanju akcijskega načrta, upoštevati tudi pri sodelovanju EU z državami širitve in drugimi partnerskimi državami glede na stopnje ogroženosti, ki so jim te države izpostavljene.

2. Izzivi na področju kibernetske varnosti za bolnišnice in izvajalce zdravstvenih dejavnosti

Kibernetske grožnje zdravstvenemu sektorju

Kibernetski napadi so po vsem svetu in v EU vse pogostejši, grožnje pa so vse bolj zapletene in dinamične. Storilci kaznivih dejanj in zlonamerni akterji imajo zaradi napredka na področju umetne inteligence na voljo zmogljiva orodja za povečanje natančnosti in učinka svojih operacij, zaradi tega napredka pa se spreminjajo tudi možnosti kibernetske obrambe, saj omogoča avtomatizirano ukrepanje proti napadom v realnem času.

Izsiljevalsko programje ostaja ključni izziv na področju kibernetske varnosti v EU in po svetu, pri čemer so v enem poročilu letni stroški na globalni ravni ocenjeni na več kot 250 milijard EUR do leta 2031[5]. Ko napadejo storilci kaznivih dejanj, ki uporabljajo izsiljevalsko programje, poleg šifriranja podatkov žrtev za odkupnino vse pogosteje tudi razkrijejo občutljive informacije, da bi izvajali dodaten pritisk. Drug pomemben izziv so ranljivosti v programski in strojni opremi: po navedbah Agencije Evropske unije za kibernetsko varnost (ENISA)[6] je zdravstveno varstvo sektor, v katerem je bilo prijavljenih največ varnostnih incidentov, povezanih s takimi ranljivostmi[7]. Med vse večjimi grožnjami so tudi porazdeljeni napadi za zavrnitev storitve, katerih namen je ciljni sistem preobremeniti s prometom, zaradi česar ni več dostopen zakonitim uporabnikom[8].

Zdravstveni sektor se srečuje s podobnimi trendi groženj kibernetski varnosti, pri čemer je velik poudarek na napadih z izsiljevalskim programjem. Po podatkih agencije ENISA je bilo izsiljevalsko programje v obdobju 2021–2023 uporabljeno v 54 % analiziranih kibernetskih incidentov v zdravstvenem sektorju. 83 % napadov je bilo finančno motiviranih zaradi visoke vrednosti zdravstvenih podatkov, 10 % napadov pa je bilo ideološko motiviranih[9]. Podobno je bilo v poročilu Komisije iz

[5] Cybersecurity Ventures (1. junij 2024): „Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031“ (Stroški škode zaradi izsiljevalske programske opreme na globalni ravni naj bi do leta 2031 presegli 265 milijard USD). Na voljo na povezavi https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

[6] Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (Akt o kibernetski varnosti), https://eur-lex.europa.eu/eli/reg/2019/881/oj/slv.

[7] ENISA Threat Landscape: Health Sector (Poročilo agencije ENISA o naravi groženj v zdravstvenem sektorju), julij 2023.

[8] ENISA Threat Landscape 2024 (Poročilo agencije ENISA o naravi groženj iz leta 2024).

[9] ENISA Threat Landscape: Health Sector (Poročilo agencije ENISA o naravi groženj v zdravstvenem sektorju), julij 2023. V poročilu so bili analizirani izvajalci zdravstvenih dejavnosti ter druge vrste organizacij, vključno z organizacijami, ki izvajajo zdravstvene raziskave, subjekti, ki proizvajajo nekatere izdelke, povezane z zdravjem, zdravstvenimi organi,

leta 2024 ugotovljeno, da je bilo v 71 % napadov, ki so vplivali na oskrbo pacientov, kot so zamude pri zdravljenju, zapoznela diagnoza in oviran dostop do storitev v sili, uporabljeno izsiljevalsko programje[10]. Napadi z izsiljevalskim programjem lahko še posebno moteče vplivajo na zagotavljanje zdravstvenih storitev in ogrožajo varnost pacientov. Poleg tega so pogosto povezani s kršitvami varstva podatkov o pacientih[11], kar pogosto zajema občutljive zdravstvene podatke in s čimer se krši temeljna pravica ljudi do varstva osebnih podatkov.

Hkrati se z vse večjo digitalizacijo zdravstvenega varstva povečuje napadna površina. Glede na poročilo o stanju digitalnega desetletja za leto 2024 ima v povprečju 79 % državljanov EU spletni dostop do svojih elektronskih zdravstvenih zapisov v primarnem zdravstvenem varstvu[12]. Elektronski zdravstveni zapisi, klinični informacijski sistemi, sistemi delovnega postopka v bolnišnicah, informacijski sistemi za obravnavanje povračil stroškov zdravljenja, sistemi za medicinsko slikanje in medicinski pripomočki, ki se uporabljajo za diagnostične namene ali spremljanje pacientov, so primeri digitalnih orodij, ki imajo lahko pomembno vlogo pri povečanju učinkovitosti in uspešnosti zdravstvenega sektorja, vendar so tudi potencialne tarče kibernetskega napada. Določene zdravstvene dejavnosti, kot sta intenzivna nega in radiološko slikanje, ali medicinska področja, kot sta onkologija in kardiologija, ki so močno odvisna od digitalno podprtih pripomočkov, so še posebno izpostavljeni kibernetskim napadom. Poleg tega se lahko zaradi težav v dobavni verigi nabavijo pripomočki z nezadostno kibernetsko varnostjo, kar še poveča obstoječa splošna tveganja.

Med pandemijo COVID-19 je na primer napad z izsiljevalskim programjem ohromil velik del irskega sistema zdravstvenega varstva, zaradi česar je bilo zjutraj na dan incidenta odpovedanih vsaj nekaj storitev v 31 od 54 akutnih bolnišnic[13]. Zdravstvene službe so se morale vrniti na papirno dokumentacijo, kar je upočasnilo učinkovitost delovanja. Napad je izviral iz lažnega elektronskega sporočila, ki je vsebovalo zlonamerno priponko[14]. Incident je pokazal, da se kibernetski napadi lahko razširijo po različnih sistemih in da je zato pomembno zaščititi celotno napadno površino zdravstvene organizacije. Poudaril je tudi pomen zagotavljanja temeljne kibernetske higiene in kulture kibernetske varnosti v vseh organizacijah.

Kibernetskovarnostna zrelost bolnišnic in izvajalcev zdravstvenih dejavnosti

zdravstvenimi zavarovalnicami, centri, ki nudijo bolnišnično zdravljenje, in ponudniki socialnih storitev. Na voljo na povezavi: https://www.enisa.europa.eu/publications/health-threat-landscape.

[10] Evropska komisija: Skupno raziskovalno središče, Reina, V., in 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 (Kibernetska varnost v zdravstvu in medicini – študija o razpoložljivih dokazih o posledicah kibernetskih incidentov za zdravje pacientov v zdravstvenih ustanovah), Urad za publikacije EU, 2024, https://data.europa.eu/doi/10.2760/693487.

[11] Po podatkih agencije ENISA iz poročila o naravi groženj v zdravstvenem sektorju je bila kršitev varnosti podatkov ali kraja podatkov potrjena v 43 % analiziranih incidentov z izsiljevalskim programjem.

[12] Poročilo o stanju digitalnega desetletja za leto 2024.

[13] Irska zdravstvena služba (Health Service Executive) (2021): „Conti cyber attack on the HSE: Independent Post Incident Review“ (Kibernetski napad skupine Conti na HSE: neodvisni pregled po napadu).

[14] Irska zdravstvena služba (Health Service Executive): „Cyber-attack and HSE response“ (Kibernetski napad in odziv HSE). Na voljo na povezavi: https://www2.hse.ie/services/cyber-attack/what-happened/.

Področje zdravstvenega varstva v EU je zelo raznoliko, saj se bolnišnice in drugi izvajalci zdravstvenih dejavnosti med državami članicami zelo razlikujejo glede na lastništvo, strukturo in velikost. V nekaterih primerih lahko upravljanje zdravstvenega varstva temelji na centraliziranem pristopu na nacionalni ravni, v drugih pa na regionalni in lokalni ravni; izvajalci zdravstvenih dejavnosti so lahko v javni ali zasebni lasti. Poleg tega lahko razlike obstajajo tudi znotraj iste države, na primer kadar so med regijami znatne socialno-ekonomske in teritorialne razlike, kar vodi do zapletene slike. To zapleteno zdravstveno okolje lahko ogrožajo pomembne zdravstvene krize zaradi nalezljivih bolezni, kot je pandemija COVID-19, pa tudi druga zdravstvena tveganja, ki so povezana na primer s podnebnimi spremembami. Poleg tega je stopnja digitalizacije in uporabe tehnologije pri izvajalcih zdravstvenih dejavnosti zelo raznolika in razdrobljena. Primer te zapletenosti je, da lahko nerazpoložljivost storitev zaradi kibernetskega incidenta povzroči resno škodo pacientom tudi v manjših zdravstvenih ustanovah, vključno s klinikami ali službami nujne medicinske pomoči, ki zagotavljajo bistveno storitev razmeroma majhnemu številu uporabnikov.

V skladu s poročilom agencije ENISA o stanju kibernetske varnosti v Uniji za leto 2024[15] je kibernetskovarnostna zrelost zdravstvenega sektorja EU zmerna, med zdravstvenimi subjekti po Evropi pa obstajajo velike razlike v stopnji te zrelosti. Pomanjkljivosti je mogoče opaziti na ključnih področjih, kot so zadostni človeški viri, znanje organizacij o njihovih dobavnih verigah informacijske in komunikacijske tehnologije (IKT) ter namestitev sodobnih varnostnih elementov v izdelke. Sektor ima težave z osnovno kibernetsko higieno in temeljnimi varnostnimi ukrepi, kot je razvidno iz dejstva, da se skoraj vse zdravstvene organizacije, vključene v raziskavo, srečujejo z izzivi pri izvajanju ocen tveganja za kibernetsko varnost, skoraj polovica pa jih še nikoli ni izvedla analize tveganja[16].

Drug pomemben izziv za kibernetsko varnost bolnišnic je stičišče informacijske in operativne tehnologije, kjer se srečajo različne varnostne prednostne naloge glede zaupnosti, razpoložljivosti in zanesljivosti ter kjer lahko kršitev na enem področju vpliva na drugo. V poročilu agencije ENISA o stanju kibernetske varnosti v Uniji za leto 2024 je nadalje poudarjeno, da se v zdravstvenem sektorju zaradi veliko različnih zdravstvenih subjektov, pripomočkov in izdelkov ne zagotavlja ustrezna varnost izdelkov in postopkov IKT, ki se v njem uporabljajo.

Ta raznolikost skupaj z različnimi ravnmi kibernetske ozaveščenosti med bolnišničnim osebjem in vodstvom predstavlja zapleten izziv za zagotavljanje kibernetske varnosti zdravstvenih sistemov. Glede na raziskavo Eurobarometer o kibernetskih veščinah iz leta 2024 je na primer samo 25 % anketiranih podjetij v sektorju zdravstva, izobraževanja in socialnega varstva v zadnjih 12 mesecih zagotovilo usposabljanje ali ozaveščanje o kibernetski varnosti[17]. Potrebni so ukrepi za spodbujanje kulture ozaveščanja o kibernetski varnosti med najbolj izpostavljenimi zdravstvenimi delavci. Prerazporejanje osebja, uporaba skupnih delovnih postaj, slabo upravljanje avtentikacije in uporaba izmenljivih nosilcev

[15] ENISA: 2024 Report on the State of Cybersecurity in the Union (Poročilo o stanju kibernetske varnosti v Uniji za leto 2024), september 2024. Na voljo na povezavi: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
[16] ENISA Threat Landscape: Health Sector (Poročilo agencije ENISA o naravi groženj v zdravstvenem sektorju), julij 2023. Na voljo na povezavi: https://www.enisa.europa.eu/publications/health-threat-landscape.
[17] Raziskava Flash Eurobarometer 547 o kibernetskih veščinah (maj 2024). Na voljo na povezavi:https://europa.eu/eurobarometer/surveys/detail/3176.

podatkov so na primer dodatni viri ranljivosti, ki vplivajo na kibernetsko varnost izvajalcev zdravstvenih dejavnosti[18].

V mnogih primerih se informacijska in operativna tehnologija vsaj delno oddata v zunanje izvajanje. Raziskava Eurobarometer iz leta 2024 je pokazala, da je delež podjetij, ki vsaj nekatere vidike svoje kibernetske varnosti oddajo v zunanje izvajanje, največji v sektorju zdravstva, izobraževanja in socialnega varstva, kjer to počne 57 % anketiranih podjetij[19]. Podobno obstaja močan trend prehoda na računalništvo v oblaku, ki je posledica potrebe po nadgradljivem shranjevanju in upravljanju podatkov, stroškovni učinkovitosti, boljšem sodelovanju in podpori naprednim tehnologijam, kot sta umetna inteligenca in internet medicinskih stvari. Leta 2022 je 58 % zdravstvenih organizacij uporabljalo digitalno platformo za zdravstvene storitve v oblaku[20]. S tem premikom se lahko znatno poveča učinkovitost, vendar so prisotna tudi tveganja, glede katerih je treba sprejemati informirane odločitve o javnem naročanju in varni konfiguraciji.

Nad vsemi temi izzivi je vprašanje krepitve zmogljivosti in financiranja. Financiranje kibernetske varnosti v zdravstvenem sektorju je omejeno in ostaja univerzalni izziv po vsej EU[21]. Poleg tega se ti izzivi v zvezi s financiranjem pojavljajo v kontekstu staranja prebivalstva, ki naj bi v prihodnjih desetletjih povzročilo obsežne proračunske pritiske na evropske zdravstvene sisteme.

Nadaljnja uporaba zastarelih orodij in obstoječih sistemov, omejeni viri za preprečevanje incidentov ali odzivanje nanje ter vrzeli v kibernetskovarnostni zrelosti so pogosto posledica pomanjkanja sredstev. Bolnišnice se srečujejo s stalnim izzivom, kako uravnotežiti sodobno varno in digitalno infrastrukturo z drugimi potrebnimi naložbami za izboljšanje oskrbe pacientov, kot so zaposlovanje zdravnikov in drugih zdravstvenih delavcev, izvajanje novih diagnostičnih metod in metod zdravljenja ter nakup pripomočkov. Po podatkih agencije ENISA[22] je zdravstveni sektor šele na sedmem mestu od 12 obravnavanih sektorjev glede na delež izdatkov za informacijsko varnost v skupnih izdatkih za informacijsko tehnologijo, pri čemer je mediana v zdravstvenem sektorju 8,3 %.

3. Evropski podporni center za kibernetsko varnost za bolnišnice in izvajalce zdravstvenih dejavnosti

Okvir EU za kibernetsko varnost ponuja širok nabor orodij, ki bi jih bilo treba uporabiti za izboljšanje varnosti in odpornosti bolnišnic in izvajalcev zdravstvenih dejavnosti. Za reševanje številnih zgoraj

[18] Panacea – People-centric cybersecurity in healthcare (Kibernetska varnost na področju zdravstvenega varstva, osredotočena na ljudi), 2021: White Paper – Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres (Bela knjiga – Izkušnje, pridobljene v okviru projekta PANACEA, o kibernetski zaščiti bolnišnic in centrov za oskrbo).

[19] Raziskava Flash Eurobarometer 547 o kibernetskih veščinah (maj 2024). Na voljo na povezavi:https://europa.eu/eurobarometer/surveys/detail/3176.

[20] ENISA: NIS Investments Report 2022 (Poročilo o naložbah na področju varnosti omrežij in informacijskih sistemov za leto 2022), november 2022. Na voljo na povezavi: https://www.enisa.europa.eu/publications/nis-investments-2022.

[21] Organizacija in zagotavljanje zdravstvenih storitev in zdravstvene oskrbe sta v nacionalni pristojnosti v skladu s členom 168 Pogodbe o delovanju Evropske unije, financiranje sistemov zdravstvenega varstva pa se med državami članicami razlikuje.

[22] ENISA: NIS Investments Report 2022 (Poročilo o naložbah na področju varnosti omrežij in informacijskih sistemov za leto 2022), november 2022. Na voljo na povezavi: https://www.enisa.europa.eu/publications/nis-investments-2022.

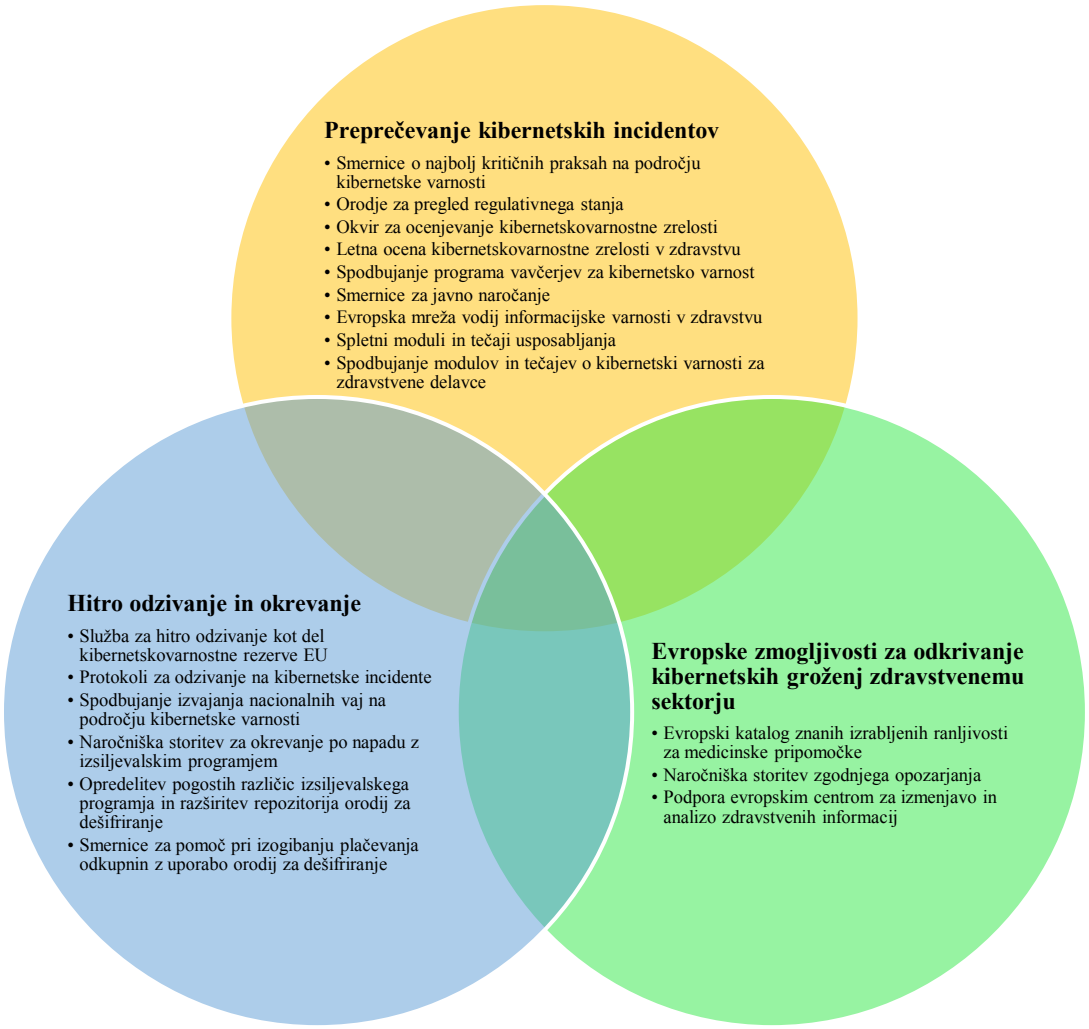
navedenih izzivov je treba razviti enoten strateški pristop na ravni EU, ki bo združeval potrebne vire, strokovno znanje in orodja za učinkovito spoprijemanje s kibernetskimi grožnjami. Celovit pregled ter boljše načrtovanje in usklajevanje so bistveni za pomoč izvajalcem zdravstvenih dejavnosti po vsej EU pri krepitvi njihove obrambe. Za dosego tega cilja je agencija ENISA najprimernejša, da znotraj svoje organizacije ustanovi namenski **Evropski podporni center za kibernetsko varnost za bolnišnice in izvajalce zdravstvenih dejavnosti**[23] v okviru svojega mandata[24] za zaščito kritične infrastrukture EU in njeno podporo.

Podporni center bi moral postopoma **razviti celovit katalog storitev za potrebe bolnišnic in izvajalcev zdravstvenih dejavnosti**, v katerem bi bil opisan obseg razpoložljivih storitev za pripravljenost, preprečevanje, odkrivanje in odzivanje. V sodelovanju z organi držav članic ter na podlagi izkušenj bolnišnic in izvajalcev zdravstvenih dejavnosti bi moral razviti uporabniku prijazen in lahko dostopen repozitorij vseh razpoložljivih instrumentov na evropski, nacionalni in regionalni ravni. Pri izvajanju svojih dejavnosti bi moral zagotoviti ustrezno usklajevanje z državami članicami ter podpirati določanje prednostnih nalog in po potrebi izvajanje ukrepov v realnem času.

Komisija bo predlagala, da se kot pomemben gradnik za razvoj kataloga storitev podpornega centra po vsej EU uvedejo pilotni projekti za razvoj dobrih praks za kibernetsko higieno in oceno varnostnih tveganj ter obravnavanje potrebe po stalnem spremljanju kibernetske varnosti, obveščanju o grožnjah in odzivanju na incidente z uporabo najsodobnejših rešitev na področju kibernetske varnosti. Rezultati teh pilotnih projektov, ki se bodo financirali iz programa Digitalna Evropa, izvajal pa jih bo Evropski kompetenčni center za kibernetsko varnost (ECCC), bodo podlaga za nadaljnje ukrepe na ravni EU, vključno z delom podpornega centra.

[23] V tem dokumentu se kot sopomenka uporablja izraz „podporni center“.

[24] Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15).



Slika 1: Koncepti za katalog storitev podpornega centra za bolnišnice in izvajalce zdravstvenih dejavnosti

3.1 Preprečevanje kibernetskih incidentov

Preprosta dejanja za zmanjšanje možnosti kibernetskega incidenta

Osnovni ukrepi za kibernetsko varnost, kot so zagotavljanje ažurnosti sistemov, upravljanje varnostnih kopij in izvajanje dvofaktorske avtentikacije, lahko po eni od ocen organizacije zaščitijo pred do 98 % napadov[25]. Številne najučinkovitejše ukrepe za kibernetsko higieno in obvladovanje tveganj je

[25] Microsoft Digital Defense Report 2022 (Microsoftovo poročilo o digitalni obrambi za leto 2022). Na voljo na povezavi: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

razmeroma preprosto sprejeti, zato so najprimernejši za izboljšanje kibernetske varnosti. Ena od ključnih vlog podpornega centra bi zato morala biti **priprava jasnih in ciljno usmerjenih smernic, v katerih bodo poudarjene najbolj kritične prakse na področju kibernetske varnosti in ki bodo izvajalcem zdravstvenih dejavnosti v pomoč pri njihovem izvajanju**. Ta podpora ne sme biti namenjena le velikim bolnišnicam in mora vključevati prilagojeno svetovanje za manjše subjekte, kot so lokalne ambulante splošnih zdravnikov in specialistične klinike, ki pogosto nimajo sredstev za posebne ekipe za kibernetsko varnost, vendar so prav tako izpostavljene napadom. Poleg tega je treba upoštevati regionalni pomen posebnih zdravstvenih subjektov za zagotavljanje oskrbe pacientov, na primer na redko poseljenih območjih. Zdravstvenim raziskovalnim inštitutom, ki obdelujejo velike količine občutljivih osebnih podatkov, bi prav tako lahko koristile smernice o osnovnih ukrepih za kibernetsko varnost, da bi povečali svojo odpornost.

Za zdravstvene organizacije veljajo tudi številne obveznosti v zvezi s kibernetsko varnostjo, ki izhajajo iz zakonodaje EU[26]. Obveznosti so ključne za zagotavljanje visokega skupnega izhodišča za kibernetsko varnost in varnost podatkov, vendar je treba zagotoviti, da delovanje v regulativnem okolju ni po nepotrebnem težavno in obremenjujoče. Velik poudarek na skladnosti ne bi smel biti v nasprotju s ciljem spodbujanja močne kulture kibernetske varnosti. **Enostavno dostopno orodje za pregled regulativnega stanja lahko pomaga zmanjšati upravno breme za subjekte, za katere velja več regulativnih instrumentov**. Podporni center bi moral poleg priprave smernic in naborov orodij tesno sodelovati s Komisijo in državami članicami, da bi čim prej razvil in razširil tako orodje. Zato bi imel pomembno vlogo pri zagotavljanju lažjega razumevanja in izvajanja pravil o kibernetski varnosti, na primer z zagotavljanjem smernic za izvajanje[27] in po potrebi s spodbujanjem ustreznih standardov.

Prihodnje **evropske denarnice za digitalno identiteto** so še eno orodje za olajšanje preprostega izvajanja dobrih praks kibernetske higiene. Da bi se zmanjšala tveganja nepooblaščenega dostopa do zdravstvenih podatkov, je bistveno zmanjšati zanašanje na šibke mehanizme identifikacije, kot so gesla. Prehod na varne rešitve za prijavo, ki temeljijo na zanesljivi identifikaciji, je ključnega pomena. Evropska denarnica za digitalno identiteto ponuja usklajen, vseevropski pristop k elektronski identifikaciji za zdravstvene delavce ter zagotavlja zanesljivo in enotno rešitev od konca leta 2026. Vsi

[26] Kot so revidirana direktiva o varnosti omrežij in informacijskih sistemov (NIS 2); Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi (Akt o kibernetski odpornosti), https://eur-lex.europa.eu/eli/reg/2024/2847/oj/slv; Uredba (EU) 2017/745 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o medicinskih pripomočkih, https://eur-lex.europa.eu/eli/reg/2017/745/oj/slv (uredba o medicinskih pripomočkih); Uredba (EU) 2017/746 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o *in vitro* diagnostičnih medicinskih pripomočkih (uredba o *in vitro* diagnostičnih medicinskih pripomočkih), https://eur-lex.europa.eu/eli/reg/2017/746/oj/slv; Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Splošna uredba o varstvu podatkov), https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:32016R0679; Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci (Akt o umetni inteligenci), https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:32024R1689, ter Predlog uredbe Evropskega parlamenta in Sveta o evropskem zdravstvenem podatkovnem prostoru (COM(2022) 197 final), https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=celex:52022PC0197. Pogajanja so se zaključila s političnim dogovorom spomladi 2024, po koncu postopka pa je spomladi 2025 predvidena objava v Uradnem listu.

[27] Priprava smernic za razlago splošne uredbe o varstvu podatkov je v pristojnosti Evropskega odbora za varstvo podatkov (EOVP). Agencija ENISA bi morala pri pripravi smernic v celoti upoštevati pristojnosti EOVP.

spletni zdravstveni informacijski sistemi, potrebni za izvajanje močne avtentikacije uporabnika, bodo morali od konca leta 2027 sprejemati denarnico za namene identifikacije[28].

Pripravljenost in ciljno usmerjena podpora

Preskušanje pripravljenosti, ki vključuje ukrepe, kot je penetracijsko testiranje, je temelj učinkovite kibernetske varnosti, Komisija pa je agenciji ENISA že dodelila sredstva za pilotne pobude za pripravljenost, ki so pokazale, da je zdravstveni sektor med najbolj iskanimi področji za testiranje in nadaljnje ocene, da se opredelijo vrzeli v kibernetskovarnostni zrelosti. Z začetkom veljavnosti akta o kibernetski solidarnosti se bodo ta prizadevanja znatno razširila, pri čemer bo vodilno vlogo prevzel Evropski kompetenčni center za kibernetsko varnost. Komisija bo za zadovoljitev te potrebe v posvetovanju s Skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov, mrežo EU-CyCLONe[29] in agencijo ENISA predlagala, da se zdravje opredeli kot sektor, za katerega se lahko zagotovi podpora za **usklajeno preskušanje pripravljenosti** v skladu z aktom o kibernetski solidarnosti. Poleg tega bi moral podporni center razviti **prilagojen okvir za ocenjevanje kibernetskovarnostne zrelosti, specifičen za zdravstveno varstvo**. Take ocene zrelosti bi subjektom zagotovile uporaben vpogled v njihove ranljivosti, hkrati pa bi jim omogočile, da pacientom in deležnikom dokažejo svojo pripravljenost na področju kibernetske varnosti ter tako okrepijo zaupanje v svoje storitve. Na zbirni ravni bi moral podporni center izvajati **letno oceno kibernetskovarnostne zrelosti v zdravstvu**, ki bi omogočila jasen pregled kibernetske varnosti v zdravstvenem sektorju na nacionalni ravni in na ravni EU.

Zdravstveni sektor je pri storitvah kibernetske varnosti močno odvisen od zunanjih izvajalcev[30], kar kaže na potrebo po ciljno usmerjeni podpori za krepitev obrambe. Države članice bi morale na podlagi uspešnih pobud, kot so inovacijski boni EU, **razmisliti o ciljno usmerjenih ukrepih, kot so vavčerji za kibernetsko varnost za mikro, male in srednje bolnišnice ter izvajalce zdravstvenih dejavnosti**. S temi vavčerji bi se zagotovila finančna pomoč za uvedbo posebnih ukrepov za kibernetsko varnost. Prednostna razvrstitev dodelitve vavčerjev bi morala temeljiti na ugotovitvah preskušanja pripravljenosti in ocen zrelosti.

Lokalno znanje in okvir sta ključna za učinkovito uvedbo vavčerjev ali drugih podpornih programov, saj zagotavljata ustreznost in dostopnost. Skladi EU, kot je Evropski sklad za regionalni razvoj, že dejavno podpirajo pobude na področju kibernetske varnosti in digitalnega zdravja, zato bi se lahko v njihovem okviru razvile ciljno usmerjene sheme vavčerjev za kibernetsko varnost za izvajalce zdravstvenih dejavnosti. Podporni center bi pri teh prizadevanjih sodeloval z državami članicami in regionalnimi organi, pristojnimi za programe, da bi podprl razvoj takih regionalnih shem vavčerjev, pri čemer bi se

[28] Člen 5f(1) in (2) Uredbe (EU) št. 910/2014.
[29] Evropska organizacijska mreža za povezovanje v kibernetski krizi.
[30] Glej ENISA NIS Investments Report 2023 (Poročilo agencije ENISA o naložbah na področju varnosti omrežij in informacijskih sistemov za leto 2023) iz novembra 2023, v katerem je poudarjen pomen zunanje podpore za revizijo in skladnost na področju kibernetske varnosti. Na voljo na povezavi: https://www.enisa.europa.eu/publications/nis-investments-2023.

oprl na izkušnje iz obstoječih nacionalnih projektov in ukrepov, financiranih v okviru programa Digitalna Evropa, da bi zagotovil praktično in učinkovito izvajanje.

Poleg tega imajo programi Obzorje od leta 2014 ključno vlogo pri financiranju vrste raziskovalnih pobud, usmerjenih na krepitev odpornosti zdravstvenih ustanov, kot so bolnišnice, proti kibernetskim grožnjam in zmanjševanje tveganj, povezanih z zlorabo nastajajočih tehnologij. Končni rezultati vključujejo nabor specializiranih orodij, okvirov in sistemov, kot so orodja za oceno tveganja, platforme za izmenjavo podatkov, ki ohranjajo zasebnost, kriptografske rešitve, programi usposabljanja za ozaveščanje o kibernetski varnosti in sistemi za odkrivanje groženj v realnem času. Te rešitve so bile skrbno potrjene s pilotnim izvajanjem v okoljih zdravstvenega varstva v realnih okoliščinah, s čimer sta se zagotovili njihova učinkovitost in praktična uporabnost pri zaščiti pred kibernetskimi grožnjami.

Zagotavljanje zanesljivosti dobavnih verig na področju zdravstvenega varstva

Ključni izziv za zdravstvene organizacije je upravljanje zapletenih dobavnih verig IKT, ki vključujejo vrsto izdelkov, kot so povezani medicinski pripomočki, sistemi elektronskih zdravstvenih zapisov in pisarniška strojna oprema. Bolnišnice in izvajalci zdravstvenih dejavnosti za svoje delovanje potrebujejo zanesljive in varne sisteme in storitve IKT. Za pomoč pri reševanju izzivov na področju kibernetske varnosti v zdravstvenem sektorju bi morala Skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov izvesti **usklajeno oceno varnostnih tveganj, v kateri so ocenjena tehnična in strateška tveganja, povezana z dobavnimi verigami medicinskih pripomočkov, ter predlagani blažilni ukrepi**[31]. Skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov bi morala po potrebi sodelovati s Koordinacijsko skupino za medicinske pripomočke.

Akt o kibernetski odpornosti je nov, celovit okvir, ki določa zahteve glede kibernetske varnosti za načrtovanje, zasnovo, razvoj ter obravnavanje, nameščanje popravkov in poročanje o aktivno izrabljenih ranljivostih v zvezi s skoraj vsemi izdelki strojne in programske opreme v vsaki fazi vrednostne verige[32]. Medicinski pripomočki so vrsta izdelkov, ki se uporabljajo na enem najobčutljivejših področij naše družbe. Zahteve glede kibernetske varnosti za te izdelke izhajajo iz že obstoječe uredbe o medicinskih pripomočkih in uredbe o *in vitro* diagnostičnih medicinskih pripomočkih[33]. V okviru tekočega ocenjevanja navedenih uredb se proučujejo možnosti za večjo skladnost in sinergije med temi okviri, da bi se zagotovili poenostavitev in najsodobnejša kibernetska varnost.

Poleg tega bi morale ugotovitve iz ocene tveganja podpirati zdravstvene organizacije pri pregledu njihovih praks na področju kibernetske varnosti dobavnih verig, kot se zahteva v skladu z revidirano direktivo o varnosti omrežij in informacijskih sistemov, in bi lahko bile podlaga za razvoj novih **smernic**

[31] V skladu s členom 22 revidirane direktive o varnosti omrežij in informacijskih sistemov.
[32] V prvem koraku bodo morale širše kategorije radijske opreme, ki ne spadajo na področje uporabe uredbe o medicinskih pripomočkih in uredbe o *in vitro* diagnostičnih medicinskih pripomočkih, od 1. avgusta 2025 pri dajanju na enotni trg izpolnjevati bistvene zahteve iz direktive o radijski opremi, ki se nanašajo na kibernetsko varnost. V drugi fazi, 11. decembra 2027, se bo začel uporabljati akt o kibernetski odpornosti.
[33] Skupina za sodelovanje na področju medicinskih pripomočkov je decembra 2019 izdala smernice o kibernetski varnosti za medicinske pripomočke, s katerimi je proizvajalce podprla pri izpolnjevanju zahtev iz Priloge I k obema uredbama: https://ec.europa.eu/docsroom/documents/41863?locale=sl.

za javno naročanje[34]. Te smernice, ki jih je agencija ENISA pripravila v okviru svojega podpornega centra, bi morale odražati nedavne trende, kot je prenos shranjevanja podatkov o pacientih v oblak, vključno s potrebo po varnem prenosu elektronskih zdravstvenih podatkov v okolja v oblaku. Poleg tega bi morale nove smernice organizacijam ponuditi praktična orodja za spremljanje njihovih dobavnih verig, vključno s ponudniki upravljanih varnostnih storitev, poročili o potrjevanju ali ocenami tveganja, ki jih izvedejo tretje osebe.

Kar zadeva računalništvo v oblaku, so potrebni nadaljnji ukrepi za reševanje edinstvenih izzivov upravljanja občutljivih zdravstvenih podatkov, vključno s povečanimi varnostnimi in operativnimi tveganji ter tveganji za zasebnost. Da bi se okrepili zaščitni ukrepi, strokovnjaki priporočajo, da se v storitve v oblaku vključita „privzeta in vgrajena varnost“. Pri tem pristopu so v ospredju varna infrastruktura, proaktivno obvladovanje ranljivosti ter kombinacija vladnih in zasebnih rešitev v oblaku. Za zagotavljanje zanesljivih varnostnih praks so bistveni tudi stalno spremljanje in potrdila posameznih ponudnikov, kot so certifikati ponudnikov varnostnih storitev ter revizije skladnosti z nacionalnimi in mednarodnimi standardi.

Pri storitvah, kot so infrastruktura kot storitev, platforma kot storitev in programska oprema kot storitev, je za izvajanje varnosti pogosto odgovorna stranka. Vendar številne zdravstvene organizacije nimajo dovolj sredstev za samostojno izpolnjevanje teh zahtev. Da bi to rešili, **bi bilo treba ponudnike storitev v oblaku spodbujati k izvajanju osnovnih varnostnih ukrepov kot standardne funkcije**. S temi ukrepi bi se zmanjšalo tveganje napačne konfiguracije in ohranila dosledna zaščita v okoljih, ki jih upravljajo stranke, uporabniki pa bi dobili večje zagotovilo. Cilj vzpostavitve privzete varnostne osnove bi bil uravnotežiti zanesljivo zaščito s praktičnostjo, s čimer bi se zagotovila uporabnost za najrazličnejše zdravstvene organizacije. Ta prizadevanja bi vključevala tesno sodelovanje med ponudniki storitev v oblaku in zdravstvenim sektorjem, pri čemer bi se izkoristile dobre prakse industrije za oblikovanje učinkovitih in nadgradljivih rešitev.

Usposabljanje in razvoj spretnosti

Delovna sila z najbolj iskanimi spretnostmi je pomembna za dolgoročno trajnostno rast in konkurenčnost v Evropi, pa tudi za visokokakovostne storitve, vključno z zdravstvenimi storitvami. Pomanjkanje usposobljenih strokovnjakov za kibernetsko varnost je velik izziv po vsej Evropi, saj se ocenjuje, da je v EU za zapolnitev potreb po delovni sili potrebnih 299 000 strokovnjakov[35]. Glede na raziskavo Eurobarometer o kibernetskih veščinah iz leta 2024[36] so po mnenju 81 % podjetij težave pri zaposlovanju osebja s področja kibernetske varnosti ključno tveganje za morebitne kibernetske napade. V sektorjih izobraževanja, zdravstva in socialnega dela 66 % vlog na področju kibernetske varnosti zasedajo

[34] Na podlagi smernic agencije ENISA za javno naročanje na področju kibernetske varnosti v bolnišnicah iz leta 2020 (februar 2020). Na voljo na povezavi: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

[35] The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study (Področje kibernetske varnosti v letu 2024: spoznanja iz študije ISC2 o delovni sili na področju kibernetske varnosti) | Platforma za digitalne spretnosti in delovna mesta.

[36] Raziskava Flash Eurobarometer 547 o kibernetskih veščinah.

zaposleni, ki prehajajo s položajev, ki niso povezani s kibernetsko varnostjo, kar kaže na nujno potrebo po preusposabljanju in izpopolnjevanju.

Podporni center bi moral pri reševanju tega izziva sodelovati s prihodnjim Konzorcijem evropske digitalne infrastrukture za kibernetske veščine, predvidenim v sporočilu Komisije o akademiji za kibernetske veščine[37]. Opravljeno delo bi moralo olajšati izmenjave med strokovnjaki za kibernetsko varnost v zdravstvenem sektorju, kot so vodje informacijske varnosti. Eden od možnih ukrepov bi bila ustanovitev **Evropske mreže vodij informacijske varnosti v zdravstvu**, ki bi sprva zajemala nabor strokovnjakov za izmenjavo in razvoj dobrih praks, strategij za zadržanje talentov in rešitev za privabljanje strokovnjakov za kibernetsko varnost v zdravstveni sektor. Poleg tega bi bilo treba pod okriljem akademije za kibernetske veščine razviti vire za okrepitev delovne sile na področju kibernetske varnosti v zdravstvenem sektorju ob podpori industrije in akademskih krogov. V zvezi s tem bi bilo treba deležnike iz industrije spodbujati, naj podprejo okrepitev usposabljanja na področju kibernetske varnosti.

Človeška napaka je še vedno glavni dejavnik za kibernetske incidente na področju zdravstvenega varstva, kar poudarja ključno potrebo po celovitem usposabljanju osebja in kibernetski ozaveščenosti. Glede na to, da zdravstveni delavci pogosto uporabljajo digitalna orodja, jih je treba opremiti z znanjem o varnih praksah. S ciljno usmerjenim usposabljanjem in kampanjami ozaveščanja se lahko znatno zmanjšajo tveganja. Da bi se to rešilo, bi moral podporni center sodelovati z zdravstvenimi delavci in izvajalci zdravstvenih dejavnosti, izvajalci izobraževanja in usposabljanja, industrijo, Konzorcijem evropske digitalne infrastrukture za kibernetske veščine ter organi držav članic pri oblikovanju in razširjanju **obsežnih, lahko dostopnih spletnih modulov in tečajev usposabljanja**.

Vključitev modulov o digitalnih kompetencah in kibernetski varnosti v učne načrte je ključnega pomena za vzpostavitev trdnih temeljev kibernetske varnosti na področju zdravstvenega varstva. V okviru teh modulov bi bilo treba obravnavati vprašanja, specifična za posamezne sektorje, kot so varstvo podatkov o pacientih in ranljivosti pri varnosti medicinskih pripomočkov. Pri razvoju teh virov bi bilo treba upoštevati predhodne ukrepe, kot sta projekt BeWell, financiran v okviru programa Erasmus+[38], in projekt PANACEA, financiran v okviru pobude Obzorje 2020[39].

3.2 Evropske zmogljivosti za odkrivanje kibernetskih groženj zdravstvenemu sektorju

[37] Sporočilo Komisije Evropskemu parlamentu in Svetu Zapolnitev vrzeli na področju strokovnjakov za kibernetsko varnost za povečanje konkurenčnosti, rasti in odpornosti EU („akademija za kibernetske veščine“). COM(2023) 207 final.
[38] BeWell – Blueprint alliance for a future health workforce strategy on digital and green skills (Okvirno zavezništvo za prihodnjo strategijo za zdravstveno osebje na področju digitalnih in zelenih spretnosti). Na voljo na povezavi: https://bewell-project.eu/.
[39] PANACEA – Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people (Zaščita in zasebnost bolnišničnih in zdravstvenih infrastruktur z zbirko pametnih orodij za kibernetsko varnost in kibernetske grožnje za podatke in ljudi). Na voljo na povezavi: https://cordis.europa.eu/project/id/826293.

Učinkovito odkrivanje kibernetskih groženj je bistveno za hiter odziv na incidente. Akterji groženj lahko uporabljajo tehnike, ki otežujejo odkrivanje vdorov in omogočajo daljše obdobje nedovoljenega dostopa do sistema[40]. Zato se lahko z boljšimi zmogljivostmi za odkrivanje groženj kibernetski napadi zaustavijo že na začetku. Na primer, v napadu z izsiljevalskim programjem na finskega ponudnika psihoterapevtskih storitev Vastaamo, med katerim je storilec izsiljeval paciente, ki jim je bila ukradena zaupna zdravstvena dokumentacija, se je prvi vdor zgodil leta 2018, ponudnik pa je zanj izvedel šele leta 2020[41].

Učinkovita izmenjava informacij in sodelovanje sta bistvena za izboljšanje odkrivanja groženj in situacijskega zavedanja po vsej EU. Skupine za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT) imajo ključno vlogo pri prejemanju poročil o incidentih, skorajšnjih dogodkih in morebitnih grožnjah ter zagotavljajo smernice za blažilne ukrepe na nacionalni ravni. Vendar **se države članice močno spodbuja, naj vsa obvestila o kibernetskih incidentih bolnišnic in izvajalcev zdravstvenih dejavnosti posredujejo tudi podpornemu centru agencije ENISA, da se omogoči situacijsko zavedanje EU.** Najbolje bi bilo, če bi to spremljala smiselna opredelitev različnih pomembnih razsežnosti incidentov, vključno z znanimi temeljnimi ranljivostmi ter učinki na zdravstvene storitve in neželenimi dogodki v zvezi s pacienti. Poleg tega se proizvajalce medicinskih in *in vitro* diagnostičnih pripomočkov spodbuja, naj prek enotne platforme za poročanje, ki jo bo vzpostavila in upravljala agencija ENISA v okviru akta o kibernetski odpornosti, prostovoljno poročajo o aktivno izrabljenih ranljivostih ali resnih kibernetskih incidentih, ki vplivajo na varnost teh pripomočkov, ter morebitnih drugih ranljivostih, incidentih, skorajšnjih dogodkih ali kibernetskih grožnjah, ki lahko vplivajo na profil tveganja teh pripomočkov.

Kadar informacije v poročilih niso več občutljive, bi lahko podporni center oblikoval evropski katalog znanih izrabljenih ranljivosti za medicinske pripomočke, sisteme za vodenje elektronskih zdravstvenih zapisov ter ponudnike IKT opreme in programske opreme na področju zdravja, ki bi ga sponzorirala agencija ENISA. Za reševanje pomembnih izzivov pri odkrivanju groženj bi moral podporni center uvesti **vseevropsko naročniško storitev zgodnjega opozarjanja za zdravstveni sektor, ki bi zagotavljala opozorila v skoraj realnem času**. Ta storitev bi temeljila na obdelanih podatkih skupin CSIRT, zdravstvenih subjektov in proizvajalcev, obveščevalnih podatkih iz javnih virov (OSINT) in podatkih drugih ustreznih akterjev, kot so kibernetska vozlišča, centri za izmenjavo in analizo informacij ter organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Situacijsko zavedanje bi se še izboljšalo z okrepljenim sodelovanjem med agencijo ENISA in Agencijo Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Europol), na primer glede vzorcev kibernetske kriminalitete v zdravstvenem sektorju.

Centri za izmenjavo in analizo informacij so osrednji viri za obveščevalne podatke o kibernetskih grožnjah, ki spodbujajo dvosmerno izmenjavo informacij med javnim in zasebnim sektorjem ter krepijo zaupanje. Podporni center bi moral okrepiti podporo **evropskemu centru za izmenjavo in analizo zdravstvenih informacij** z orodji in izmenjavo informacij, poročili o situacijskem zavedanju v sektorjih

[40] ENISA Health Threat Landscape 2023 (Poročilo agencije ENISA o naravi groženj v zdravstvenem sektorju iz leta 2023).
[41] Sklep 1150/161/2021 finskega pooblaščenca za varstvo podatkov.

ter spodbujanjem zaupanja vredne skupnosti za taktično in strateško sodelovanje. Države članice bi morale spodbujati razvoj nacionalnih centrov za izmenjavo in analizo zdravstvenih informacij[42]. Prav tako bi bilo treba centre za izmenjavo in analizo informacij spodbujati, naj izvajalce zdravstvenih dejavnosti povežejo s proizvajalci, da bi se doseglo skupno razumevanje kibernetskih groženj, tudi v dobavni verigi, in olajšal dialog o varni zasnovi izdelkov, pri kateri bi se resnično upoštevale razmere pri uvajanju na terenu.

3.3 Hitro odzivanje in okrevanje

Glede na visoko občutljivost zdravstvenih podatkov pacientov in potencialno uničujoče učinke kibernetskih napadov na zdravstvene storitve je hiter in učinkovit odziv na kibernetske incidente ključen za zagotavljanje varnosti pacientov. Kadar bolnišnica ali izvajalec zdravstvenih dejavnosti utrpi kibernetski napad, je prva kontaktna točka ustrezna nacionalna skupina CSIRT[43]. Skupina CSIRT je odgovorna za zagotavljanje pravočasne podpore, po možnosti v 24 urah, za pomoč pri obvladovanju pomembnih incidentov. Če pa incident presega zmogljivosti skupine CSIRT, bi morala biti na voljo podpora EU, da se zagotovi hiter in učinkovit odziv.

Kibernetskovarnostna rezerva EU, vzpostavljena na podlagi akta o kibernetski solidarnosti, zagotavlja storitve odzivanja na incidente, ki jih nudijo zaupanja vredni ponudniki upravljanih varnostnih storitev, in sicer za pomoč pri pomembnih kibernetskih incidentih ali kibernetskih incidentih velikih razsežnosti in začetnih prizadevanjih za okrevanje. Ta rezerva je zasnovana tako, da dopolnjuje prizadevanja skupin CSIRT držav članic in jim omogoča, da zaprosijo za dodatno podporo v primerih, ki vključujejo kritične sektorje, kot je zdravje. Za izboljšanje tega sistema bi morali **Komisija in agencija ENISA zagotoviti, da rezerva vključuje službo za hitro odzivanje, ki je posebej namenjena zdravstvenemu sektorju**. V okviru te službe, ki bi dopolnjevala druge obstoječe okvire, bi bili brez odlašanja napoteni strokovnjaki za obvladovanje pomembnih kibernetskih incidentov ali kibernetskih incidentov velikih razsežnosti na področju zdravstvenega varstva, kadar nacionalna podpora ne bi zadostovala.

Da bi se izboljšala odzivanje in okrevanje, bi moral podporni center v sodelovanju s Skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov, mrežo skupin CSIRT in po potrebi Europolom razviti **protokole za odzivanje na kibernetske incidente, prilagojene področju zdravstvenega varstva**. Ti protokoli bi skupine CSIRT in zdravstvene organizacije usmerjali pri odzivanju na posebne kibernetske grožnje, vključno z izsiljevalskim programjem. Glede na pomen učinkovitega sodelovanja med skupinami CSIRT ter organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj pri odzivanju na kibernetske incidente kazenske narave in njihovem preiskovanju bi morali protokoli med drugim zagotavljati jasne smernice o poročanju o takih incidentih organom

[42] Finska ima na primer nacionalni center za izmenjavo in analizo informacij za sektor socialnega in zdravstvenega varstva. Glej Finski nacionalni center za kibernetsko varnost: „ISAC information sharing groups“ (Skupine za izmenjavo informacij v okviru centra za izmenjavo in analizo informacij), na voljo na povezavi: https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

[43] Člen 23(1) revidirane direktive o varnosti omrežij in informacijskih sistemov določa, da morajo bistveni in pomembni subjekti pomembne incidente priglasiti zadevni skupini CSIRT ali, kadar je to potrebno, pristojnemu organu.

preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Poleg tega bi lahko podporni center **omogočil obsežno uvedbo nacionalnih vaj na področju kibernetske varnosti na podlagi izkušenj z vajami, kot je vaja agencije ENISA Cyber Europe 2022, da se preizkusijo zadevni protokoli in okrepijo protokoli za odzivanje na incidente**.

Da bi se lahko oblikovale politike in ocenila učinkovitost ukrepov, sprejetih proti napadom z izsiljevalskim programjem, je treba zbrati dodatne podatke. V ta namen bi morale države članice od subjektov, za katere se uporablja revidirana direktiva o varnosti omrežij in informacijskih sistemov, vključno z zdravstvenimi organizacijami, zahtevati, da poročajo o vseh izvedenih in načrtovanih plačilih odkupnine, skupaj z drugimi informacijami, ki jih zagotovijo pri poročanju o pomembnih kibernetskih incidentih. Tako poročanje podpira učinkovito preiskovanje incidentov z izsiljevalskim programjem, vključno s sledenjem plačilom na platformah za izmenjavo kriptovalut, da se identificirajo prejemniki.

Hitrost okrevanja je ključni dejavnik pri ohranjanju odpornosti in zaupanja javnosti, zlasti na področju zdravstvenega varstva, kjer lahko izpadi ovirajo oskrbo pacientov. Za učinkovito okrevanje po napadih z izsiljevalskim programjem morajo imeti izvajalci zdravstvenih dejavnosti varne, posodobljene in izolirane varnostne kopije, ki jih je mogoče hitro obnoviti. Podporni center bi lahko v okviru svojega kataloga storitev nudil **naročniško storitev za okrevanje po napadu z izsiljevalskim programjem, ki bi bolnišnicam in izvajalcem zdravstvenih dejavnosti pomagal vnaprej pripraviti načrte za okrevanje**. Agencija ENISA in Europol bi morala sodelovati pri opredelitvi najpogostejših različic izsiljevalskega programja, usmerjenih v zdravstvene organizacije, in **razširiti repozitorij orodij za dešifriranje**, ki so na voljo v okviru projekta No More Ransom[44]. Razviti in spodbujati bi morala tudi dostopne smernice, ki bodo izvajalcem zdravstvenih dejavnosti pomagale, da se z uporabo orodij za dešifriranje izognejo plačilu odkupnin.

Mednarodna pobuda za boj proti izsiljevalskemu programju[45] je dragocen prostor za izmenjavo informacij o posameznih incidentih z izsiljevalskim programjem ter za gradnjo zmogljivosti držav članic za krepitev njihovih okvirov kibernetske varnosti in preiskovalnih zmogljivosti zoper akterje, ki uporabljajo izsiljevalsko programje. Komisija bo v sodelovanju z visokim predstavnikom še naprej spodbujala sodelovanje v pobudi za boj proti izsiljevalskemu programju, tudi proti grožnjam z izsiljevalskim programjem zdravstvenemu sektorju. Poleg tega si bo prizadevala za sodelovanje v **delovni skupini G7 za kibernetsko varnost**, da bi se okrepila kibernetska varnost zdravstvenega sektorja. Delovna skupina bi lahko zlasti proučila možnosti za podporo zdravstvenemu sektorju pri grožnjah, kot je izsiljevalsko programje, in se pri tem oprla na razmisleke, kot je skupna izjava o napadih z izsiljevalskim programjem na zdravstvene ustanove z dne 8. novembra 2024, predstavljena v okviru Varnostnega sveta Združenih narodov[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. Nacionalni ukrepi

Zmogljivost tega akcijskega načrta za izboljšanje kibernetske varnosti v zdravstvenem sektorju je odvisna od dejavnega sodelovanja in zavezanosti držav članic. Za uspešno izvajanje akcijskega načrta bi lahko države članice imenovale **nacionalne podporne centre za kibernetsko varnost posebej za bolnišnice in izvajalce zdravstvenih dejavnosti**. Ti centri bi delovali kot glavne kontaktne točke za zdravstveni sektor na nacionalni ravni in tesno sodelovali s podpornim centrom agencije ENISA. Če je to mogoče in ustrezno, bi morale države članice za nacionalne podporne centre za kibernetsko varnost imenovati obstoječe organe, kot so nacionalne skupine CSIRT za zdravstvo ali ustrezni organi.

Države članice se spodbuja tudi k pripravi **nacionalnih akcijskih načrtov za kibernetsko varnost v zdravstvenem sektorju**. V teh načrtih bi bila opisana posebna tveganja za kibernetsko varnost, s katerimi se srečujejo sistemi zdravstvenega varstva, in nacionalni ukrepi, sprejeti za njihovo odpravo, hkrati pa bi se zagotovila učinkovita uporaba virov in praks na evropski ravni. Podporni center agencije ENISA lahko pomaga pri pripravi teh načrtov, pri čemer upošteva že obstoječe nacionalne načrte in usklajuje prizadevanja za zagotovitev, da se viri in strategije posameznih držav članic med seboj dopolnjujejo.

Drug ključni poudarek za države članice je olajšanje souporabe virov med izvajalci zdravstvenih dejavnosti, kar bi bilo mogoče doseči s **skupnim javnim naročanjem ali združenimi viri** na nacionalni, regionalni ali celo evropski ravni. S tem pristopom bi se zmanjšalo finančno breme za posamezne subjekte in hkrati povečala njihova pogajalska moč pri ponudnikih storitev kibernetske varnosti.

Na primer, v okviru francoskega programa CaRE[47] so bili na nacionalni in regionalni ravni uvedeni številni ukrepi za reševanje izzivov pri zagotavljanju sredstev: kibernetski katalog vsebuje pregled kibernetskih rešitev in svežnjev, ki so bolnišnicam na voljo prek nacionalne agencije za kibernetsko varnost, agencije za digitalno zdravje, regionalnih agencij, nacionalnih nabavnih organizacij in komercialnih rešitev. To dopolnjuje dodatno financiranje regionalnih agencij za zagotavljanje skupnih virov.

Države članice bi morale obravnavati tudi nezadostne ravni naložb v kibernetsko varnost v zdravstvenem sektorju. Da bi se zagotovilo ustrezno financiranje, bi morale določiti **nezavezujoča referenčna merila in spremljati cilje financiranja, ki so posebej namenjeni kibernetski varnosti**, ter ob tem zagotoviti, da te naložbe ne bodo vplivale na osnovno oskrbo pacientov. Namen teh ciljev financiranja bi moral biti tudi vključitev varnostnih vidikov v vse digitalne naložbe v sektorju. Države članice si lahko izmenjujejo dobre prakse in nasvete o teh ciljih prek platform, kot je mreža e-zdravje[48].

[47]Francoska agencija za digitalno zdravje: Cybersécurité acceleration et Résilience des Établissements (CaRE). Na voljo na povezavi: https://esante.gouv.fr/strategie-nationale/cybersecurite.

[48] Mreža e-zdravje je prostovoljna mreža nacionalnih organov, pristojnih za e-zdravje, ki jih imenujejo države članice in je ustanovljena na podlagi člena 14 Direktive 2011/24/EU.

5. Javno-zasebno sodelovanje

Za uspešno izvajanje akcijskega načrta sta bistvena javno-zasebno sodelovanje in posvetovanje z izvajalci zdravstvenih dejavnosti, drugimi subjekti zdravstvenega sektorja ter ustreznimi akterji iz industrije kibernetske varnosti. Da bi se dodatno prispevalo k delu podpornega centra, **bo Komisija ob podpori agencije ENISA ustanovila skupni svetovalni odbor za kibernetsko varnost na področju zdravja**, v katerem bodo visoki predstavniki obeh področij, tj. zdravstvenega varstva in kibernetske varnosti, in ki bo Komisiji in podpornemu centru svetoval o učinkovitih ukrepih ter razpravljal o nadaljnjem razvoju javno-zasebnih partnerstev na tem področju. Odbor bo gradil na obstoječih prizadevanjih za javno-zasebna partnerstva, vključno z evropskim centrom za izmenjavo in analizo zdravstvenih informacij.

Poleg tega bo Komisija objavila **poziv k ukrepanju**, s katerim bo podjetja, fundacije, izobraževalne ustanove in deležnike iz industrije na področju kibernetske varnosti pozvala, naj se **zavežejo k sprejetju ukrepov za reševanje izzivov v sektorju**. Na podlagi izkušenj akademije za kibernetske veščine bi lahko bile take zaveze na primer zaveze v okviru akademije za kibernetske veščine, ki bi vključevale zagotavljanje tečajev in gradiva za usposabljanje strokovnjakov za kibernetsko varnost s poudarkom na zdravstvenem sektorju[49]. V okviru drugih zavez bi bilo mogoče obravnavati tudi dejavnosti ozaveščanja ali zagotavljanje upravljanih varnostnih storitev posebej ranljivim subjektom brezplačno ali po znižani ceni, da bi se povečala njihova pripravljenost in odpornost na področju kibernetske varnosti. Poleg tega bi lahko zaveze vključevale izmenjavo obveščevalnih podatkov o kibernetskih grožnjah s podpornim centrom agencije ENISA. Podporni center bi moral imeti pregled nad zavezami, sprejetimi v okviru poziva k ukrepanju, da bi zagotovil njihovo skladnost in dopolnjevanje.

6. Odvračanje akterjev kibernetskih groženj

Notranje in zunanje politike EU na področju kibernetske varnosti bi morale podpirati cilj odvračanja akterjev kibernetskih groženj od napadov na evropske zdravstvene sisteme. Kibernetski napadi na zdravstvene organizacije so še posebno nesprejemljiva vrsta zlonamerne kibernetske dejavnosti, saj lahko ogrozijo varnost pacientov in človeška življenja. Zato bi bilo treba v celoti izkoristiti odvračilne zmogljivosti EU na področjih kibernetske varnosti ter preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, da bi oslabili splošni poslovni model akterjev, ki ogrožajo zdravstveni sektor, in jim onemogočili lahek zaslužek. To bi vključevalo spodbujanje čezmejnih preiskav z okrepljeno izmenjavo kazalnikov ogroženosti in drugih ustreznih podatkov ter večjo osredotočenost na cilje visoke vrednosti in ključne spodbujevalce kaznivih dejanj, kot so neprebojno gostovanje ali storitve mešanja kriptovalut.

Zbirka orodij za kibernetsko diplomacijo zagotavlja okvir za preprečevanje kibernetskih napadov na EU, države članice in partnerje, odvračanje od njih ter odzivanje nanje. Visoki predstavnik bo za

[49] Cyber Skills Academy: Get Involved (Akademija za kibernetske veščine: vključite se) | Platforma za digitalne spretnosti in delovna mesta.

odzivanje na grožnje, usmerjene v zdravstvene sisteme, še naprej uporabljal obstoječi okvir sankcij proti kibernetskim napadom.

Pregon storilcev kaznivih dejanj je pomemben odvračilni dejavnik. Zato bi morale države članice zagotoviti, da so preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v celoti vključeni v njihove nacionalne akcijske načrte. Zlasti bi morale za odvračanje napadov, kaznovanje storilcev kaznivih dejanj in uničenje kriminalne infrastrukture, ki omogoča napade, v celoti izkoristiti določbe direktive o napadih na informacijske sisteme[50] in Budimpeške konvencije Sveta Evrope o kibernetski kriminaliteti[51]. Z uspešnim izvajanjem teh orodij bi se moralo zagotoviti kaznovanje kaznivih in zlonamernih dejanj zoper zdravstveno varstvo.

7. Izvajanje in spremljanje akcijskega načrta

V tem akcijskem načrtu so bile predvidene številne naloge za podporni center, ki bo vzpostavljen v okviru agencije ENISA. S tem se bo zagotovilo celostno in skladno izvajanje akcijskega načrta ter hkrati preprečilo ustanavljanje novih subjektov, ki bi lahko povzročilo prekrivanje in režijske stroške. Komisija namerava zagotoviti ustrezno financiranje podpornega centra.

Ko podporni center začne delovati, bi morala agencija ENISA v posvetovanju s Komisijo upravnemu odboru agencije ENISA in ustreznim mrežam držav članic, zlasti Skupini za sodelovanje na področju varnosti omrežnih in informacijskih sistemov, mreži skupin CSIRT, mreži e-zdravje in po potrebi odboru za evropski zdravstveni podatkovni prostor redno zagotavljati najnovejše informacije o delu podpornega centra. Poleg tega bi morala agencija ENISA z javno-zasebnim svetovalnim odborom za kibernetsko varnost na področju zdravja stalno izmenjevati informacije o izvajanju ukrepov, ki jih zagotavlja podporni center.

Redna poročila agencije ENISA, kot je poročilo o stanju kibernetske varnosti v Uniji, ki vsebuje zbirno oceno ravni zrelosti zmogljivosti in virov za kibernetsko varnost po vsej EU, tudi v zdravstvenem sektorju, bi morala biti priložnost za objavo ustreznih podatkov v podporo spremljanju akcijskega načrta. Poleg tega lahko indeks kibernetske varnosti EU agencije ENISA[52] zagotovi kvantitativne in kvalitativne podatke, ki so lahko dokazna podlaga za oceno kritičnosti in zrelosti zdravstvenega sektorja.

8. Naslednji koraki

V tem sporočilu je predstavljena ambiciozna agenda za večjo kibernetsko varnost zdravstvenega sektorja v EU. Akcijski načrt s predlaganim razvojem podpornega centra za kibernetsko varnost za bolnišnice in

[50] Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa Sveta 2005/222/PNZ: https://eur-lex.europa.eu/eli/dir/2013/40/oj/slv.
[51] Konvencija o kibernetski kriminaliteti (Budimpeška konvencija, ETS št. 185) in njeni protokoli: https://www.coe.int/en/web/cybercrime/the-budapest-convention.
[52] ENISA, EU Cybersecurity Index, Framework and Methodological Note (Indeks kibernetske varnosti EU, okvir in metodološka opomba), 2024. Na voljo na povezavi: https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

izvajalce zdravstvenih dejavnosti v središču agencije ENISA določa pot do oblikovanja skladnega in skupnega evropskega pristopa k izzivu kibernetske varnosti v sektorju.

To sporočilo bi bilo treba obravnavati kot začetek procesa za izboljšanje kibernetske varnosti v zdravstvenem sektorju. Zato se bodo ob sprejetju akcijskega načrta začela celovita posvetovanja z deležniki ter nadaljevale izmenjave z državami članicami in ustreznimi mrežami, da bi zbrali nova spoznanja. Komisija namerava na podlagi rezultatov posvetovanj v zadnjem četrtletju 2025 pripraviti priporočila za nadaljnjo izpopolnitev akcijskega načrta.

Komisija poziva države članice in vse deležnike, naj si skupaj prizadevajo za uresničitev ciljev akcijskega načrta.

PRILOGA – Pregled predlaganih ukrepov

Komisija:

Podporni center agencije ENISA za kibernetsko varnost za bolnišnice in izvajalce zdravstvenih dejavnosti	
Zagotavljanje ustreznih virov za podporni center za kibernetsko varnost. Sodelovanje z Evropskim kompetenčnim centrom za kibernetsko varnost pri izvajanju pilotnih projektov za razvoj dobrih praks za kibernetsko higieno in oceno varnostnega tveganja ter obravnavanju potrebe po stalnem spremljanju kibernetske varnosti, obveščanju o grožnjah in odzivanju na incidente z uporabo najsodobnejših rešitev na področju kibernetske varnosti, in sicer za razvoj kataloga storitev Evropskega podpornega centra za kibernetsko varnost.	2025
Preprečevanje kibernetskih incidentov	
V posvetovanju s Skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov, mrežo EU-CyCLONe in agencijo ENISA proučitev možnosti, da se zdravje opredeli kot sektor, za katerega se lahko zagotovi podpora za usklajeno preskušanje pripravljenosti v skladu z aktom o kibernetski solidarnosti.	Prvo četrtletje 2025
Hitro odzivanje in okrevanje	
Skupaj z agencijo ENISA zagotavljanje, da bo kibernetskovarnostna rezerva EU vključevala službo za hitro odzivanje, ki je posebej namenjena zdravstvenemu sektorju.	Četrto četrtletje 2025
Javno-zasebno sodelovanje	
Ob podpori agencije ENISA ustanovitev skupnega svetovalnega odbora za kibernetsko varnost na področju zdravja.	Prvo četrtletje 2025
Objava poziva k ukrepanju, s katerim bodo podjetja, fundacije, izobraževalne ustanove in deležniki iz industrije na področju kibernetske varnosti pozvani, naj se zavežejo, da bodo sprejeli ukrepe za reševanje izzivov v zdravstvenem sektorju.	Drugo četrtletje 2025

Odvračanje akterjev kibernetskih groženj	
Skupaj z visokim predstavnikom proučitev uporabe ukrepov iz zbirke orodij za kibernetsko diplomacijo za preprečevanje in onemogočanje zlonamernih dejavnosti proti zdravstvenim sistemom, odvračanje od njih ter odzivanje nanje.	2025
Spodbujanje mednarodnega sodelovanja v boju proti akterjem, ki uporabljajo izsiljevalsko programje, zlasti v okviru Mednarodne pobude za boj proti izsiljevalskemu programju, v sodelovanju z visokim predstavnikom.	2025–2026
Prizadevanje za sodelovanje v delovni skupini G7 za kibernetsko varnost, da bi se okrepila kibernetska varnost zdravstvenega sektorja.	2025–2026
Naslednji koraki	
Začetek celovitih posvetovanj z deležniki.	Prvo četrtletje 2025
Sprejetje priporočil za nadaljnjo izpopolnitev akcijskega načrta.	Četrto četrtletje 2025

ENISA:

Podporni center agencije EU za kibernetsko varnost za bolnišnice in izvajalce zdravstvenih dejavnosti	
Začetek dela za ustanovitev Evropskega podpornega centra za kibernetsko varnost za bolnišnice in izvajalce zdravstvenih dejavnosti.	Drugo četrtletje 2025
Razvoj celovitega kataloga storitev, ki ga bo zagotavljal podporni center za kibernetsko varnost.	Od četrtega četrtletja 2025
Preprečevanje kibernetskih incidentov	
Objava smernic, v katerih so poudarjene najbolj kritične prakse na področju kibernetske varnosti in so izvajalcem zdravstvenih dejavnosti v pomoč pri njihovem izvajanju.	Tretje četrtletje 2025
Priprava orodja za pregled regulativnega stanja v tesnem sodelovanju s Komisijo in državami članicami.	Prvo četrtletje 2025
Razvoj okvira za ocenjevanje kibernetskovarnostne zrelosti, specifičnega za zdravstveno varstvo.	Tretje četrtletje 2025

Izvedba letne ocene kibernetskovarnostne zrelosti v zdravstvu.	2025–2026
Sodelovanje z državami članicami in regionalnimi organi, pristojnimi za programe, pri oblikovanju vzorčnih programov vavčerjev za kibernetsko varnost.	2025–2026
Razvoj novih smernic za javno naročanje na področju kibernetske varnosti bolnišnic in izvajalcev zdravstvenih dejavnosti.	Tretje četrtletje 2025
Vzpostavitev evropske mreže vodij informacijske varnosti v zdravstvu.	Prvo četrtletje 2026
Oblikovanje in spodbujanje modulov in tečajev o kibernetski varnosti za zdravstvene delavce.	Prvo četrtletje 2026
Evropske zmogljivosti za odkrivanje kibernetskih groženj zdravstvenemu sektorju	
Vzpostavitev evropskega kataloga znanih izrabljenih ranljivosti za medicinske pripomočke, sisteme za vodenje elektronskih zdravstvenih zapisov ter ponudnike IKT opreme in programske opreme na področju zdravja.	Četrto četrtletje 2025
Uvedba vseevropske naročniške storitve zgodnjega opozarjanja za zdravstveni sektor.	Od leta 2026
Podpora evropskemu centru za izmenjavo in analizo zdravstvenih informacij z orodji in izmenjavo informacij.	2025–2026
Hitro odzivanje in okrevanje	
Skupaj s Komisijo zagotavljanje, da bo kibernetskovarnostna rezerva EU vključevala službo za hitro odzivanje, ki je posebej namenjena zdravstvenemu sektorju.	Četrto četrtletje 2025
V sodelovanju z mrežo skupin CSIRT razvoj protokolov za odzivanje na kibernetske incidente, prilagojenih področju zdravstvenega varstva.	Tretje četrtletje 2025
Olajšanje široke uvedbe nacionalnih vaj na področju kibernetske varnosti za preskušanje zadevnih protokolov in okrepitev protokolov za odzivanje na incidente.	Od četrtega četrtletja 2025
Zagotavljanje naročniške storitve za okrevanje po napadu z izsiljevalskim programjem.	Od leta 2026

Skupaj z Europolom opredelitev najpogostejših različic izsiljevalskega programja, usmerjenih v zdravstvene organizacije, in razširitev repozitorija orodij za dešifriranje v okviru projekta No More Ransom.	Četrto četrtletje 2025
Skupaj z Europolom razvoj dostopnih smernic, ki bodo izvajalcem zdravstvenih dejavnosti pomagale, da se izognejo plačilu odkupnin.	Tretje četrtletje 2025
Nacionalni ukrepi	
Pomoč državam članicam pri razvoju nacionalnih akcijskih načrtov.	2025
Usklajevanje prizadevanj za zagotovitev, da se viri in strategije posameznih držav članic med seboj dopolnjujejo.	2025–2026
Izvajanje in spremljanje akcijskega načrta	
V posvetovanju s Komisijo redno zagotavljanje najnovejših informacij o delu podpornega centra za kibernetsko varnost ustreznim mrežam držav članic.	2025–2026
Stalna izmenjava mnenj s svetovalnim odborom za kibernetsko varnost na področju zdravja.	2025–2026

Države članice:

Evropske zmogljivosti za odkrivanje kibernetskih groženj zdravstvenemu sektorju	
Izmenjava obvestil o incidentih bolnišnic in izvajalcev zdravstvenih dejavnosti na podlagi revidirane direktive o varnosti omrežij in informacijskih sistemov z Evropskim podpornim centrom za kibernetsko varnost.	Od četrtega četrtletja 2025
Spodbujanje razvoja nacionalnih centrov za izmenjavo in analizo zdravstvenih informacij.	2025–2026
Preprečevanje kibernetskih incidentov	
V okviru Skupine za sodelovanje na področju varnosti omrežnih in informacijskih sistemov izvedba usklajene ocene varnostnih tveganj, v kateri so ocenjena tehnična in strateška tveganja, povezana z dobavnimi verigami medicinskih pripomočkov.	Četrto četrtletje 2025

Hitro odzivanje in okrevanje	
Uvedba nacionalnih vaj na področju kibernetske varnosti za preskušanje zadevnih protokolov in okrepitev protokolov za odzivanje na incidente.	Od leta 2026
Nacionalni ukrepi	
Imenovanje nacionalnih podpornih centrov za kibernetsko varnost za bolnišnice in izvajalce zdravstvenih dejavnosti.	Drugo četrtletje 2025
Priprava nacionalnih akcijskih načrtov za kibernetsko varnost v zdravstvenem sektorju.	Četrto četrtletje 2025
Olajšanje souporabe virov med izvajalci zdravstvenih dejavnosti.	2025–2026
Določitev nezavezujočih referenčnih meril in spremljanje ciljev financiranja, ki so posebej namenjeni kibernetski varnosti.	Četrto četrtletje 2025
Zahteva, da zdravstvene organizacije in drugi subjekti, za katere se uporablja revidirana direktiva o varnosti omrežij in informacijskih sistemov, poročajo o svojih namerah glede plačila odkupnin.	Četrto četrtletje 2025