Съвет на
Европейския съюз

Брюксел, 16 януари 2025 г.
(OR. en)

5426/25

CYBER 21
SAN 15

ПРИДРУЖИТЕЛНО ПИСМО

От:	Генералния секретар на Европейската комисия, подписано от г-жа Martine DEPREZ, директор
Дата на получаване:	15 януари 2025 г.
До:	Г-жа Thérèse BLANCHET, генерален секретар на Съвета на Европейския съюз
№ док. Ком.:	COM(2025) 10 final
Относно:	СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, СЪВЕТА, ЕВРОПЕЙСКИЯ ИКОНОМИЧЕСКИ И СОЦИАЛЕН КОМИТЕТ И КОМИТЕТА НА РЕГИОНИТЕ Европейски план за действие относно киберсигурността на болниците и доставчиците на здравно обслужване

Приложено се изпраща на делегациите документ COM(2025) 10 final.

Приложение: COM(2025) 10 final

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 15.1.2025 г.
COM(2025) 10 final

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, СЪВЕТА, ЕВРОПЕЙСКИЯ ИКОНОМИЧЕСКИ И СОЦИАЛЕН КОМИТЕТ И КОМИТЕТА НА РЕГИОНИТЕ

Европейски план за действие относно киберсигурността на болниците и доставчиците на здравно обслужване

1. Въведение

Средата на сигурност в ЕС се променя бързо, като се наблюдава ескалация на хибридните атаки и кибератаките, насочени към дестабилизиране на обществото ни с цел е да се породи разделение и смущение, но също да се генерират печалби от киберпрестъпността. Ето защо Европа трябва спешно да засили готовността и устойчивостта си срещу тази нова реалност във всички сектори и в съответствие с подхода, обхващащ цялото общество и всички нива на управление, както се призовава в доклада на специалния съветник на председателя на Европейската комисия Саули Нийнистьо.

Сигурните и устойчиви здравни системи са крайъгълен камък на социалния модел на ЕС. Болниците и здравните системи обаче са изправени пред нарастващи заплахи, особено от страна на престъпни групи, използващи софтуер за изнудване, които се прицелват в тях с оглед на финансова изгода поради високата стойност на данните на пациентите, в това число електронните здравни досиета. Секторът на здравеопазването действително се превърна в най-атакувания отрасъл в ЕС през последните четири години, включително по време на пандемията от COVID-19, когато здравната инфраструктура все по-често ставаше обект на кибератаки. Кибератаките срещу болници и доставчици на здравно обслужване водят до преки вреди за хората, забавяне на медицинските процедури, претоварване в спешните отделения и в крайни случаи потенциално до загуба на човешки живот.

Залогът е още по-висок сега, когато секторът преминава през съществена цифрова трансформация. Благодарение на цифровото здравеопазване и използването и повторното използване на здравни данни може да се развиват модели на грижи, които отговарят в по-голяма степен на нуждите и предпочитанията на хората и пациентите, като чрез тях се предотвратява появата на заболявания или се дава възможност за тяхното по-ранно лечение. Интегрирането на цифрови инструменти и решения в клиничните процеси, както и използването и повторното използване на здравни данни могат да послужат за вземане на по-добри клинични решения и да допринесат за автоматизацията в областта на здравеопазването, както и за по-бързи и по-добри грижи за пациентите. Цифровите инструменти, използването на данни и медицинските изделия — често свързани с интернет и използващи изкуствен интелект (ИИ) — са от основно значение и за справянето с предизвикателства като недостига на медицински специалисти.

Същевременно цифровите инструменти умножават потенциалните цели на киберпрестъпниците. Освен това някои държавни субекти не се притесняват да осъществяват атаки срещу здравни заведения, както виждаме по време на продължаващата агресивна война на Русия срещу Украйна. Така секторът се превръща в потенциална цел за кибератаки като част от по-широка хибридна кампания. Кибератаките не само застрашават безопасността на пациентите, но и подкопават общественото доверие в здравната инфраструктура и водят до значителни разходи за възстановяване. Освен като защита срещу кибератаки, устойчивата и сигурна цифрова инфраструктура е от съществено значение и за подпомагане на прилагането и пълноценното разгръщане на европейското пространство на здравни данни[1] (ЕПЗД).

[1] https://www.consilium.europa.eu/bg/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/

Ето защо е време да се повишат и укрепят киберсигурността и устойчивостта на европейските болници и доставчици на здравно обслужване, както подчерта председателят на ЕК Урсула Фон дер Лайен в своите политически насоки за периода 2024—2029 г.[2] Предлаганият план за действие представлява отговор на неотложността на ситуацията и изключителните заплахи, пред които е изправен секторът. Просто универсално решение за предизвикателствата пред киберсигурността в областта на здравеопазването не съществува. Затова в плана за действие се призовава за засилване на превенцията, подготвеност и прилагане на по-координиран подход към солидарността, като същевременно се използва експертният опит в европейския сектор на киберсигурността. Планът за действие е отражение на подхода на ЕС към сигурността, който ще бъде доразвит и формализиран в предстоящата европейска стратегия за вътрешната сигурност, с която ще се определи цялостен отговор за справяне с всички заплахи за вътрешната сигурност и ще се наблегне на способността за предвиждане на заплахите, предотвратяване на вредите и защита на хората, като се действа на всички равнища, следвайки подхода за обхващане на цялото общество.

Секторът на здравеопазването включва много и разнообразни субекти и участници, в това число болници, клиники, домове за грижи, рехабилитационни центрове и различни доставчици на здравно обслужване, наред с фармацевтичната, медицинската и биотехнологичната промишленост, производителите на медицински изделия и институциите за изследвания в областта на здравеопазването. Настоящият план за действие е насочен предимно към киберсигурността на болниците и доставчиците на здравно обслужване, под които се разбира всяко физическо или юридическо лице или всяка друга структура, законно предоставяща здравно обслужване на територията на държава членка[3]. Болниците и доставчиците на здравно обслужване функционират във взаимозависимост с другите здравни организации и са най-близо до хората. Същевременно мерките за повишаване на киберсигурността на болниците и доставчиците на здравно обслужване следва да са насочени и към рисковете, засягащи по-общо веригата на доставки и екосистемата и произлизащи например от субекти, които използват здравни данни за научни изследвания и машинно обучение или които произвеждат медицински изделия, по-специално медицински изделия, които се основават на цифрови технологии и се свързват с интернет или с други устройства („интернет на предметите“).

Въпреки че сигурността на здравните системи е преди всичко въпрос от национална компетентност, здравеопазването е и критичен сектор съгласно Директивата относно мерки за високо общо ниво на киберсигурност (МИС 2)[4]. Киберпрестъпниците и другите източници на заплаха действат трансгранично, а и предизвикателствата пред киберсигурността, пред които са изправени здравните организации, също са сходни в отделните държави членки. Сътрудничеството на европейско равнище е ценно с оглед на споделянето и разпространението на най-добрите практики на равнището на ЕС и на национално равнище. Поради това в плана за

[2] https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_bg

[3] Член 3, буква ж) от Директива 2011/24/ЕС на Европейския парламент и на Съвета за упражняване на правата на пациентите при трансгранично здравно обслужване, https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=celex:32011L0024

[4] Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза (Директива МИС 2), https://eur-lex.europa.eu/eli/dir/2022/2555

действие се предлагат координация и мерки на равнището на ЕС, като същевременно държавите членки се призовават да предприемат действия с цел постигане на промяна в областта на здравеопазването и по-общо в здравната екосистема.

Планът за действие е насочен, на първо място, към изграждането на капацитета на сектора за **предотвратяване** на инциденти в областта на киберсигурността, тъй като винаги е по-добре да се предотврати един проблем, отколкото да се вземат мерки впоследствие. На второ място, в плана за действие се описват подробно действия за подобряване на обмена на информация в областта на киберсигурността и на способността за **откриване** на киберзаплахи, което прави възможна по-бързата реакция. На трето място, се предвиждат мерки за по-добро **реагиране** при инциденти и за **възстановяване** след тях. И на последно място, в плана за действие се предвиждат начини за **възпиране** на източниците на киберзаплахи от осъществяване на атаки срещу здравните системи в Европа.

Планът за действие ще се изпълнява в сътрудничество с доставчиците на здравно обслужване и с другите участници в здравната екосистема, държавите членки и експертната общност в областта на киберсигурността. Сътрудничеството като подход е от основно значение за по-нататъшното определяне и усъвършенстване на действията, които биха имали най-голямо въздействие, така че те да могат да са от полза за всички критични доставчици на здравно обслужване в Европа. Поради това паралелно с настоящото съобщение ще бъде проведена и задълбочена консултация със заинтересованите страни, сектора и държавите членки. Международното сътрудничество е важно за киберсигурността, тъй като по принцип киберзаплахите са свързани помежду си и при тях границите не са от значение. Подобни заплахи за киберсигурността съществуват и в страните, обхванати от процеса на разширяване, и в съседните на Съюза държави, както и в други държави, които са стратегически партньори на ЕС. В крайна сметка, те може да застрашат сигурността на критичната инфраструктура в ЕС. Поради тази причина ще бъде важно поуките, извлечени при изпълнението на плана за действие, да имат отражение и в сътрудничеството на ЕС както със страните, обхванати от процеса на разширяване, така и с други държави партньори предвид съответното равнище на заплаха, на което са изложени.

2. Предизвикателството пред киберсигурността на болниците и доставчиците на здравно обслужване

Киберзаплахите срещу сектора на здравеопазването

Кибератаките се увеличават в световен мащаб и в рамките на ЕС, като картината на заплахите става все по-сложна и динамична. В резултат на напредъка в областта на изкуствения интелект (ИИ) престъпниците и злонамерените участници разполагат с мощни инструменти за повишаване на прецизността и въздействието на своите операции, но същевременно се променят и възможностите за киберзащита, като вече има възможност срещу атаките да се използват автоматизирани действия в реално време.

Софтуерът за изнудване продължава да бъде основно предизвикателство пред киберсигурността в ЕС и в световен мащаб, като в неотдавнашен доклад годишните разходи на световно равнище се оценяват на над 250 милиарда евро до 2031 г.[5] Когато използващите софтуер за изнудване престъпници провеждат атаки, те не само криптират данните на жертвите, за да получат откуп, но и все по-често предизвикват изтичане на чувствителна информация, за да упражнят допълнителен натиск. Друго важно предизвикателство представляват уязвимостите в софтуера и хардуера: според Агенцията на Европейския съюз за киберсигурност (ENISA)[6] здравеопазването е секторът, в който се докладват най-много инциденти в областта на сигурността, свързани с такива уязвимости.[7] Сред другите нарастващи заплахи са разпределените атаки от типа „отказ от обслужване“ (DDoS), чиято цел е да претоварят целевата система с поток от трафик, за да я направят недостъпна за легитимни потребители[8].

Секторът на здравеопазването е изправен пред подобни тенденции при заплахите пред киберсигурността, с особен акцент върху атаките със софтуер за изнудване. Според ENISA при 54 % от анализираните инциденти в областта на киберсигурността в сектора на здравеопазването за периода 2021–2023 г. е използван софтуер за изнудване. Поради високата стойност на здравните данни 83 % от атаките са финансово мотивирани, а 10 % са с идеологическа мотивация[9]. Аналогично доклад на Комисията от 2024 г. установи, че при 71 % от атаките, които повлияват на грижите за пациентите, например поради забавено лечение, диагностика и нарушен достъп до спешни услуги, се използва софтуер за изнудване[10]. Атаките със софтуер за изнудване могат да имат особено неблагоприятно въздействие върху предоставянето на здравни услуги, в резултат на което се излага на риск безопасността на пациентите. Освен това атаките със софтуер за изнудване нерядко са съчетани с компрометиране на сигурността на данните на пациентите[11], при което

[5] Cybersecurity Ventures (1 юни 2024 г.): Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031 [„Разходите за щети от атаки със софтуер за изнудване на световно равнище се очаква да надхвърлят 265 милиарда долара до 2031 г.“]. Достъпно на https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

[6] Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии (Акт за киберсигурността), https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

[7] Доклад относно картината на заплахите на ENISA: сектор „Здравеопазване“ (юли 2023 г.).

[8] Доклад относно картината на заплахите на ENISA, 2024 г..

[9] Доклад относно картината на заплахите на ENISA: сектор „Здравеопазване“ (юли 2023 г.). В доклада се анализират доставчиците на здравно обслужване, както и други видове организации, в това число организации, провеждащи изследвания, свързани със здравето, субекти производители на определени продукти, свързани със здравето, здравни органи, здравноосигурителни организации и заведения за резиденциално лечение, както и доставчици на социални услуги. Достъпен на https://www.enisa.europa.eu/publications/health-threat-landscape

[10] Европейска комисия: Съвместен изследователски център, Reina, V. и 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 [„Киберсигурност в сектора на здравеопазването и медицината — проучване на наличните доказателства за последиците за здравето на пациентите, произтичащи от киберинциденти в здравни заведения“], Служба за публикации на ЕС, 2024 г., https://op.europa.eu/bg/publication-detail/-/publication/9d3355cf-591f-11ef-acbc-01aa75ed71a1

[11] Според доклада на ENISA относно картината на заплахите за сектор „Здравеопазване“ в 43 % от анализираните инциденти със софтуер за изнудване се потвърждава нарушаване на сигурността на данни или кражба на данни.

често се засягат чувствителни данни, свързани с тяхното здравословно състояние, и се нарушава основното право на защита на личните данни.

Същевременно с нарастващото цифровизиране на здравеопазването се увеличава и повърхността, уязвима на атаки. Съгласно доклада за състоянието на цифровото десетилетие за 2024 г. средно 79 % от гражданите на ЕС имат онлайн достъп до своите електронни здравни досиета в областта на първичната медицинска помощ.[12] Електронните здравни досиета, клиничните информационни системи, системите за управление на работните процеси в болниците, информационните системи за възстановяване на разходите за лечение, системите за медицинска образна диагностика и медицинските изделия, използвани за диагностични цели или за мониториране на пациентите, са примери за цифрови инструменти, които могат да играят важна роля за повишаване на ефективността и резултатите в сектора на здравеопазването, но също така са потенциални мишени на атаките срещу киберсигурността. Специфични здравни дейности като интензивното лечение и рентгенологичните изображения или области на медицината като онкологията и кардиологията, които са силно зависими от цифрови устройства, са изложени на особен риск от кибератаки. Освен това е възможно при проблеми с веригата на доставки да се стигне до закупуване на устройства с недостатъчно ниво на киберсигурност, което изостря съществуващите общи рискове.

Например по време на пандемията от COVID-19 атака със софтуер за изнудване парализира голяма част от здравната система в Ирландия, което доведе до отмяна на поне няколко от услугите в 31 от 54-те болници за активно лечение в сутрешните часове в деня на инцидента.[13] В здравните заведения трябваше отново да се използват записи на хартия, което доведе до забавяне на ефективността на дейностите. Атаката бе в резултат на фишинг по електронна поща с прикачен злонамерен файл.[14] Инцидентът бе доказателство за потенциала на кибератаките, които могат да обхващат различни системи, и следователно за това колко важно е да бъде защитена цялата повърхност, уязвима на атаки, в дадена здравна организация. От този инцидент стана ясно също така колко важно е да се осигури основна киберхигиена и култура на киберсигурност във всички организации.

Зрялост по отношение на киберсигурността на болниците и доставчиците на здравно обслужване

Секторът на здравеопазването в ЕС е много разнообразен, като болниците и другите доставчици на здравно обслужване в отделните държави членки се различават значително по отношение на собствеността, структурата и размера. В някои случаи управлението на здравеопазването може да се основава на централизиран подход на национално равнище, а в други — на регионално и местно равнище; доставчиците на здравно обслужване могат да са публична или частна собственост. Освен това различия могат да съществуват и в рамките на една и съща държава, например когато има значителни социално-икономически и териториални различия между

[12] Доклад за състоянието на цифровото десетилетие 2024 г.
[13] Национална здравна служба на Ирландия (2021 г.): Conti cyber attack on the HSE: Independent Post Incident Review [„Кибератака с Conti срещу Националната здравна служба на Ирландия: независим преглед след инцидента“].
[14] Национална здравна служба на Ирландия: Cyber-attack and HSE response [„Кибератаката и реакцията на Националната здравна служба на Ирландия“]. Достъпно на https://www2.hse.ie/services/cyber-attack/what-happened/.

регионите, което води до сложна обща картина. В сложния контекст на сектора на здравеопазването предизвикателства могат да представляват значителни здравни кризи, дължащи се на заразни болести, като пандемията от COVID-19, но и други рискове за здравето, например тези във връзка с изменението на климата. И на последно място, налице са значителни различия и разпокъсаност по отношение на цифровата зрялост и нивото на внедряване на технологии от страна на доставчиците на здравно обслужване. Пример за тази сложност е фактът, че недостъпността на услугите, причинена от инциденти в областта на киберсигурността, може да доведе до сериозни щети и вреди за пациентите дори и в малки здравни заведения, в това число клиники или служби за спешна медицинска помощ, които предоставят основна услуга на относително малък брой потребители.

Съгласно доклада на ENISA за състоянието на киберсигурността в Съюза за 2024 г.[15] зрелостта по отношение на киберсигурността в сектора на здравеопазването в ЕС се оценява като умерена, като съществуват големи разлики в нивото на зрялост по отношение на киберсигурността между здравните субекти в цяла Европа. Наблюдават се недостатъци в основни области като наличието на достатъчно човешки ресурси, познанията на организациите за техните вериги на доставки в областта на информационните и комуникационните технологии (ИКТ) и инсталирането на съвременни елементи за сигурност в продуктите. Секторът не успява да се справи с основната киберхигиена и базовите мерки за сигурност, както е видно от факта, че почти всички анкетирани здравни организации се сблъскват с предизвикателства, когато става въпрос за извършване на оценка на рисковете за киберсигурността, а почти половината от тях никога не са правили такъв анализ на риска.[16]

Друго значително предизвикателство пред киберсигурността на болниците е пресечната точка между информационните технологии (ИТ) и операционните технологии (ОТ), в която се срещат различни приоритети в областта на сигурността по отношение на поверителността, наличността и надеждността и където евентуален пробив в едната област може да засегне и другата. В доклада за състоянието на киберсигурността в Съюза на ENISA за 2024 г. се подчертава още, че секторът на здравеопазването не постига адекватни резултати при гарантирането на сигурността на използваните от него ИКТ продукти и процеси поради голямото разнообразие от здравни субекти, медицински изделия и продукти.

Това разнообразие, съчетано с различни нива на осведоменост в областта на киберсигурността сред персонала и ръководството на болниците, води до сложно предизвикателство при гарантирането на киберсигурността на здравните системи. Например съгласно проучването на уменията в областта на киберсигурността на „Евробарометър“ за 2024 г. само 25 % от анкетираните дружества в секторите на здравеопазването, образованието и социалните грижи са предоставили обучения или други дейности за повишаване на осведомеността в областта на

[15] ENISA: Доклад за състоянието на киберсигурността в Съюза за 2024 г. (септември 2024 г.). Достъпен на https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[16] Доклад относно картината на заплахите на ENISA: сектор „Здравеопазване“ (юли 2023 г.). Достъпен на https://www.enisa.europa.eu/publications/health-threat-landscape

киберсигурността през предходните 12 месеца.[17] Необходими са действия за насърчаване на култура на осведоменост в областта на киберсигурността сред медицинските специалисти, работещи на първа линия. Например ротацията на персонала, използването на споделени работни станции, лошото управление на удостоверяването на автентичността и използването на преносими носители представляват допълнителни източници на уязвимости, които засягат киберсигурността на доставчиците на здравно обслужване[18].

В много случаи ИТ и ОТ са поне частично възложени на външни изпълнители. С проучването „Евробарометър“ за 2024 г. се установи, че делът на дружествата, които възлагат на външни изпълнители поне някои аспекти на своята киберсигурност, е най-висок в секторите на здравеопазването, образованието и социалните грижи, като 57 % от анкетираните дружества попадат в тази група.[19] По същия начин се наблюдава силна тенденция на мигриране към компютърни услуги „в облак“ поради необходимостта от възможности за разрастрастване при съхранението и управлението на данни, ефективност на разходите, подобрено сътрудничество и подкрепа за модерните технологии като ИИ и интернет на предметите в медицината. През 2022 г. 58 % от здравните организации са използвали платформа за цифрово здравеопазване „в облак“.[20] Въпреки че в резултат на тази промяна може да бъде постигната значителна ефективност, тя води и до рискове, които изискват информирани решения относно възлагането на обществени поръчки и защитените конфигурации.

Като общ проблем сред всички тези предизвикателства стоят въпросите за изграждането на капацитет и финансирането. Финансирането за киберсигурност в сектора на здравеопазването е ограничено и продължава да бъде всеобщо предизвикателство в целия ЕС.[21] Освен това предизвикателствата, свързани с финансирането, възникват в контекста на застаряване на населението, което се очаква да доведе до повсеместен натиск върху бюджетите на здравните системи в Европа през следващите десетилетия.

Фактът, че продължават да се използват остарели инструменти и наследени системи, ограничените ресурси за предотвратяване или реагиране на инциденти, както и разликите в нивото на зрялост по отношение на киберсигурността често произтичат от недостиг на финансиране. Болниците са непрекъснато изправени пред предизвикателството да търсят баланс между инвестициите в съвременна, сигурна и цифрова инфраструктура и други необходими инвестиции, насочени към подобряване на грижите за пациентите, като например наемането на

[17] Flash Eurobarometer 547 on Cyberskills [„Експресно проучване „Евробарометър“ № 547 на уменията в областта на киберсигурността“] (май 2024 г.). Достъпно на https://europa.eu/eurobarometer/surveys/detail/3176.
[18] Panacea — People-centric cybersecurity in healthcare (2021): White Paper — Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres. [„Panacea — Ориентирана към хората киберсигурност в здравеопазването (2021 г.): Бяла книга — Поуки от PANACEA относно киберзащитата на болниците и заведенията за грижи“].
[19] Експресно проучване „Евробарометър“ № 547 на уменията в областта на киберсигурността (май 2024 г.). Достъпно на https://europa.eu/eurobarometer/surveys/detail/3176.
[20] ENISA: NIS Investments Report 2022 [Доклад за инвестициите в мрежова и информационна сигурност (МИС) за 2022 г.] (ноември 2022 г.). Достъпен на https://www.enisa.europa.eu/publications/nis-investments-2022.
[21] Съгласно член 168 от Договора за функционирането на Европейския съюз организацията и предоставянето на здравно обслужване и медицински грижи попадат в обхвата на националната компетентност, а финансирането на здравните системи е различно в отделните държави членки.

лекари и други медицински специалисти, внедряването на нови методи за диагностика и лечение и закупуването на медицински изделия. Според ENISA[22] секторът на здравеопазването се нарежда едва на 7-мо място измежду 12-те сектора, включени в проучването, по отношение на дела, който разходите за информационна сигурност имат от общите разходи за ИТ, като медианата в сектора на здравеопазването е 8,3 %.

3. Европейски център за подкрепа в областта на киберсигурността за болници и доставчици на здравно обслужване

Рамката на ЕС в областта на киберсигурността предлага широк набор от инструменти, които следва да се използват за подобряване на сигурността и устойчивостта на болниците и доставчиците на здравно обслужване. За да се преодолеят многобройните предизвикателства, изтъкнати по-горе, е необходимо да се разработи единен стратегически подход на равнището на ЕС, чрез който да се обединят необходимите ресурси, експертен опит и инструменти за ефективно справяне с киберзаплахите. Цялостният преглед, както и по-доброто планиране и координация са от съществено значение, за да се помогне на доставчиците на здравно обслужване в целия ЕС да бъдат по-добре защитени. С оглед на постигането на тази цел ENISA е в най-добра позиция да създаде, в рамките на своята организация, специален **Европейски център за подкрепа в областта на киберсигурността за болници и доставчици на здравно обслужване**[23] като част от мандата си[24] за защита и подкрепа на критичната инфраструктура на ЕС.

Центърът за подкрепа следва постепенно да **разработи подробен каталог на услугите, насочен към нуждите на болниците и доставчиците на здравно обслужване**, в който да се очертае обхватът на наличните услуги за готовност, предотвратяване, откриване и реагиране на заплахи. В сътрудничество с органите на държавите членки и въз основа на опита на болниците и доставчиците на здравно обслужване Центърът за подкрепа следва да разработи лесно за ползване и леснодостъпно хранилище на всички налични инструменти на европейско, национално и регионално равнище. Когато осъществява дейностите си той следва да осигури подходяща координация с държавите членки и да подкрепя приоритизирането и изпълнението на действия в реално време при необходимост.

Като важен градивен елемент за разработването на каталога с услуги на Центъра за подкрепа Комисията ще предложи да се стартират пилотни проекти в целия ЕС с цел разработване на най-добри практики за оценка на киберхигиената и рисковете за сигурността, както и предприемане на мерки по отношение на необходимостта от непрекъснато наблюдение на киберсигурността, разузнавателни сведения за заплахи и реагиране при инциденти, като се използват най-съвременни решения в областта на киберсигурността. Резултатите от тези пилотни проекти, които

[22] ENISA: NIS Investments Report 2022 [Доклад за инвестициите в мрежова и информационна сигурност (МИС) за 2022 г.] (ноември 2022 г.). Достъпен на https://www.enisa.europa.eu/publications/nis-investments-2022.
[23] В настоящия документ наричан също „Център за подкрепа“.
[24] Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 15—69).

ще бъдат финансирани по програма „Цифрова Европа“, изпълнявана от Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността, ще послужат за основа за по-нататъшни действия на равнището на ЕС, в това число работата на Центъра за подкрепа.

Фигура 1: Концепции за каталога с услуги на Центъра за подкрепа за болници и доставчици на здравно обслужване

3.1. Предотвратяване на инциденти в областта на киберсигурността

Прости действия, които водят до промяна в нивото на риска

Съгласно неотдавнашна оценка основните мерки за киберсигурност, като например гарантирането, че системите са актуализирани, управлението на архивирането и внедряването на многофакторно удостоверяване на автентичността, могат да помогнат на организациите да се защитят от до 98 % от атаките[25]. Много от най-ефективните мерки за киберхигиена и управление на риска са относително лесни за приемане, поради което те са естествен избор за подобряване на киберсигурността. Следователно една от основните роли на Центъра за подкрепа следва да бъде **разработването на ясни, конкретни насоки, в които се изтъкват най-важните практики в областта на киберсигурността и се подпомагат доставчиците на здравно обслужване при прилагането им**. Тази подкрепа трябва да обхване не само големите болници, но да включва и персонализирани съвети за по-малки субекти, като например кабинети на местните общопрактикуващи лекари и специализирани клиники, които често не разполагат с ресурси за специализирани екипи по киберсигурност, но са еднакво уязвими на атаки. Освен това е необходимо да се вземе предвид регионалното значение на конкретни здравни субекти за осигуряване на грижи за пациентите, например в слабо населените райони. За институциите за изследвания в областта на здравеопазването, които обработват големи количества чувствителни лични данни, също може да е полезно да получат насоки относно основни мерки за киберсигурност, които да подобрят тяхната устойчивост.

Освен това здравните организации са натоварени с редица задължения, свързани с киберсигурността, произтичащи от законодателството на ЕС[26]. Въпреки че тези задължения са от

[25] Microsoft Digital Defense Report 2022 [Доклад относно цифровата защита на Microsoft за 2022 г.]. Достъпен на https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

[26] Като например Директивата МИС 2; Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета от 23 октомври 2024 г. относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи (Акт за киберустойчивост), https://eur-lex.europa.eu/eli/reg/2024/2847/oj/enghttps://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng; Регламент (ЕС) 2017/745 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия https://eur-lex.europa.eu/eli/reg/2017/745/oj/enghttps://eur-lex.europa.eu/eli/reg/2017/745/oj/eng (Регламент за медицинските изделия) https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng Регламента за медицинските изделия; Регламент (ЕС) 2017/746 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия за инвитро диагностика (Регламент за медицинските изделия за инвитро диагностика), https://eur-lex.europa.eu/eli/reg/2017/746/oj/enghttps://eur-lex.europa.eu/eli/reg/2017/746/oj/eng; Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Общ регламент относно защитата на данните), https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32016R0679https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32016R0679; Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. за определяне на хармонизирани правила за изкуствения интелект (Акт за изкуствения интелект), https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32024R1689; Предложение за РЕГЛАМЕНТ НА

решаващо значение, за да се осигури висока обща база по отношение на киберсигурността и сигурността на данните, от съществено значение е да се гарантира, че регулаторната среда не е ненужно сложна и прекомерно тежка за навигиране. Силният акцент върху съответствието следва да не противоречи на целта да се насърчава стабилна култура на киберсигурност. Наличието на **лесно достъпен инструмент за регулаторно картографиране може да спомогне да се сведе до минимум административната тежест за субектите, които са обект на множество регулаторни инструменти.** Успоредно с разработването на насоки и инструментариуми Центърът за подкрепа следва да работи в тясно сътрудничество с Комисията и държавите членки за разработването и разпространението на такъв инструмент възможно най-скоро. Поради това Центърът за подкрепа ще играе важна роля за това правилата за киберсигурност да бъдат лесни за разбиране и прилагане, например като предоставя насоки за тяхното прилагане[27], и, при необходимост, популяризира съответните стандарти.

Бъдещите **европейски портфейли за цифрова самоличност** са друг инструмент, с който се улеснява опростеното прилагане на добри практики за киберхигиена. Намаляването на зависимостта от слаби механизми за установяване на самоличността, например пароли, е от съществено значение за намаляване на рисковете от неразрешен достъп до здравни данни. Преминаването към сигурни решения за влизане, основани на надеждно установяване на самоличността, е от решаващо значение. С европейския портфейл за цифрова самоличност се предлага хармонизиран общоевропейски подход към електронната идентификация на медицинските специалисти, с което от края на 2026 г. ще се осигури стабилно и единно решение. Всички онлайн информационни системи в сектора на здравеопазването, при които се изисква надеждно удостоверяване на автентичността на потребителите, ще бъдат задължени от края на 2027 г. да приемат портфейла за целите на установяване на автентичността.[28]

Готовност и целенасочена подкрепа

Тестването на готовността, което включва действия като тестване за пробив, е крайъгълен камък на ефективната киберсигурност и Комисията вече отпусна финансиране на ENISA за пилотни инициативи в областта на готовността, при което стана ясно, че секторът на здравеопазването е сред най-търсените области за тестване и провеждане на допълнителни оценки с цел установяване на пропуски по отношение на киберсигурността. С влизането в сила на Законодателния акт за киберсолидарност тези усилия ще се разширят значително, като Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността ще поеме водеща роля. За да отговори на тази необходимост, Комисията ще

ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА относно европейското пространство на здравни данни (COM(2022) 197 final), https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=celex:52022PC0197. Преговорите приключиха с политическо споразумение през пролетта на 2024 г. и след като бъде финализиран, се очаква да бъде публикуван в Официален вестник през пролетта на 2025 г.

[27] Разработването на насоки за тълкуване на Общия регламент за защита на данните (GDPR) е от компетентността на Европейския комитет по защита на данните (ЕКЗД). При разработването на своите насоки ENISA следва да зачита изцяло прерогативите на ЕКЗД.

[28] Член 5, буква е), параграфи 1—2 от Регламент (ЕС) № 910/2014.

предложи, след консултация с групата за сътрудничество за МИС, EU-CyCLONe[29] и ENISA, здравеопазването да бъде определено за сектор, който може да получава подкрепа за **координирано тестване на готовността** съгласно Законодателния акт за киберсолидарност. Освен това Центърът за подкрепа следва да разработи **адаптирана рамка за оценки на зрелостта по отношение на киберсигурността, която да е специфична за сектора на здравеопазването.** Чрез такива оценки на зрелостта субектите ще получават осъществими на практика идеи във връзка с техните уязвимости и същевременно ще могат да докажат готовността си в областта на киберсигурността пред пациентите и заинтересованите страни и така да изградят доверие в своите услуги. Освен това Центърът за подкрепа следва да извършва обобщена **годишна оценка на зрелостта по отношение на киберсигурността на сектора на здравеопазването**, с която ще прави преглед на киберсигурността в сектора на здравеопазването както на национално равнище, така и на равнището на ЕС.

Секторът на здравеопазването разчита в голяма степен на външни изпълнители за услуги в областта на киберсигурността[30], което подчертава необходимостта от целенасочена подкрепа за засилване на защитните механизми. Предвид други успешни инициативи като ваучерите на ЕС за иновации **държавите членки следва да обмислят целенасочени мерки като ваучери за киберсигурност за микро-, малки и средни болници и доставчици на здравно обслужване.** Чрез тези ваучери ще се предоставя финансова помощ за въвеждане на специфични мерки за киберсигурност. Приоритетите при разпределението на ваучери следва да се основават на констатациите от тестовете за готовност и оценките на зрелостта.

Местните познания и контекст са от решаващо значение за ефективното разгръщане на ваучерите или други програми за подкрепа, като се гарантира тяхната целесъобразност и достъпност. Фондовете на ЕС, като например Европейският фонд за регионално развитие, вече активно подкрепят инициативи в областта на киберсигурността и цифровото здравеопазване и поради тази причина могат да бъдат от полза при разработването на целеви схеми за ваучери за киберсигурност за доставчиците на здравно обслужване. За да стимулира тези усилия, Центърът за подкрепа ще си сътрудничи с държавите членки и регионалните програмни органи, за да подкрепи разработването на такива регионални схеми за ваучери, като има предвид извлечените поуки от съществуващите национални проекти, както и действията, финансирани по програма „Цифрова Европа“, с оглед да се гарантира тяхното практическо и ефективно изпълнение.

Освен това от 2014 г. насам програмите по „Хоризонт“ имат важна роля във финансирането на редица научноизследователски инициативи, насочени към повишаване на устойчивостта към киберзаплахи на здравните институции, например болниците, и намаляване на рисковете, свързани със злоупотребата с нововъзникващи технологии. Получените резултати включват набор от специализирани инструменти, рамки и системи, например инструменти за оценка на риска, платформи за споделяне на данни при запазване на поверителността, криптографски решения, програми за обучение по повишаване на осведомеността в областта на киберсигурността и

[29] Мрежа за връзка на организациите при кибернетични кризи

[30] Вж. ENISA NIS Investments Report 2023 [„Доклад за инвестициите в мрежова и информационна сигурност (МИС) на ENISA за 2023 г.“] (ноември 2023 г.), в който се подчертава значението на външната подкрепа за одит и съответствие в областта на киберсигурността. Достъпен на https://www.enisa.europa.eu/publications/nis-investments-2023

системи за откриване на заплахи в реално време. Важно е да се отбележи, че тези решения са преминали стриктно валидиране чрез пилотни внедрявания при реални условия в сектора на здравеопазването, с което се гарантира тяхната ефективност и практическа приложимост за защита срещу киберзаплахи.

Гарантиране на сигурността на веригите на доставките в сектора на здравеопазването

Основно предизвикателство за здравните организации е управлението на сложни вериги на доставки на ИКТ, които включват множество продукти, като например свързани медицински изделия, системи за електронни здравни досиета и офисен хардуер. Болниците и доставчиците на здравно обслужване се нуждаят от надеждни и сигурни ИКТ системи и услуги, за да осъществяват дейността си. За да окаже подкрепа за справяне с предизвикателствата пред киберсигурността в сектора на здравеопазването, групата за сътрудничество за МИС следва да извърши **координирана оценка на риска за сигурността, като оцени както техническите, така и стратегическите рискове, свързани с веригите на доставки на медицински изделия, и да предложи мерки за смекчаване.**[31] Когато е целесъобразно, групата за сътрудничество за МИС следва да си сътрудничи с Координационната група по медицинските изделия.

Законодателният акт за киберустойчивост представлява нова, всеобхватна рамка, с която се определят изискванията за киберсигурност с цел планиране, проектиране, разработване, както и обработка, коригиране и докладване на активно използвани уязвимости по отношение на почти всички хардуерни и софтуерни продукти на всеки етап от веригата за създаване на стойност[32]. Медицинските изделия са вид продукт, използван в една от най-чувствителните области на нашето общество. Изискванията в областта на киберсигурността за тези продукти произтичат от вече съществуващите Регламент за медицинските изделия и Регламент за медицинските изделия за инвитро диагностика[33]. При извършваната в момента оценка на посочените регламенти се проучва потенциалът за повече съгласуваност и полезни взаимодействия между тези рамки с цел да се гарантира опростяване и най-съвременна киберсигурност.

Освен това констатациите от оценката на риска следва да подпомогнат здравните организации при преразглеждането на практиките им за киберсигурност във веригите на доставките, както се изисква съгласно Директивата МИС 2, и могат да послужат за основа за разработването на нови **насоки за възлагане на обществени поръчки**[34]. Разработени от ENISA чрез Центъра за

[31] В съответствие с член 22 от Директивата за МИС 2.

[32] Като първа стъпка, считано от 1 август 2025 г., големи категории радиосъоръжения, които не попадат в обхвата на Регламента за медицинските изделия и Регламента за медицинските изделия за инвитро диагностика, ще трябва да отговарят, при пускането си на единния пазар, на основните изисквания, свързани с киберсигурността, на Директивата за радиосъоръженията. На втори етап, считано от 11 декември 2027 г., ще влезе в сила Законодателният акт за киберустойчивост.

[33] През декември 2019 г. групата за сътрудничество за медицинските изделия издаде насоки относно киберсигурността на медицинските изделия, с които подпомага производителите в изпълнението на изискванията на приложение I към двата регламента: https://ec.europa.eu/docsroom/documents/41863.

[34] Building on the 2020 ENISA Procurement Guidelines for Cybersecurity in Hospitals [„Надграждане на насоките на ENISA за възлагане на обществени поръчки в областта на киберсигурността в болниците от 2020 г.“] (февруари 2020 г.). Достъпни на https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

подкрепа, тези насоки следва да отразяват най-новите тенденции, като например преминаването към съхранение на данните на пациентите „в облак“, в това число необходимостта от сигурна миграция на електронните здравни данни към облака. Освен това с новите насоки на организациите следва да се предложат практически инструменти за проследяване на техните вериги на доставки, включително доставчиците на управлявани услуги за сигурност, атестационни доклади или оценки на риска от трети страни.

Що се отнася до облака, необходими са допълнителни действия за справяне със специфичните предизвикателства при управлението на чувствителни здравни данни, в това число повишени рискове по отношение на сигурността и поверителността, както и повишени оперативни рискове. За да се засилят предпазните мерки, експертите препоръчват в облачните услуги да се вгради „сигурност по подразбиране и сигурност на етапа на проектирането“. С този подход се дава приоритет на сигурната инфраструктура, проактивното управление на уязвимостите и комбинирането на държавни и частни облачни решения. Непрекъснатото наблюдение и специфичните за всеки вид доставчик удостоверения — например сертификати за доставчиците на решения за сигурност, както и одити за съответствие с националните и международните стандарти — също са от основно значение, за да се гарантират надеждни практики в областта на сигурността.

За услугите инфраструктура като услуга (IaaS), платформа като услуга (PaaS) и софтуер като услуга (SaaS) внедряването на мерки за сигурност често е отговорност на клиента. Много здравни организации обаче не разполагат с необходимите ресурси, за да отговорят на тези изисквания сами. За да решат този въпрос, **доставчиците на компютърни услуги „в облак“ следва да бъдат насърчавани да прилагат базови мерки за сигурност като стандартна характеристика**. Тези мерки ще доведат до намаляване на риска от неправилни конфигурации, поддържане на постоянно ниво на защита в управляваните от клиента среди и осигуряване на по-голяма сигурност на потребителите. Чрез установяване на единна база по подразбиране по отношение на сигурността ще се цели да се постигне баланс между стабилната защита и практичността, като се гарантира използваемост за широк кръг здравни организации. Това ще включва тясно сътрудничество между доставчиците на компютърни услуги „в облак“ и сектора на здравеопазването, като ще се използват най-добрите практики в сектора с цел създаване на ефективни и мащабируеми решения.

Обучение и развитие на умения

Наличието на работна сила с търсените умения е важно условие за устойчивия растеж и конкурентоспособността в дългосрочен план в Европа, както и за висококачествените услуги, в това число здравното обслужване. Недостигът на квалифицирани специалисти в областта на киберсигурността е значително предизвикателство в цяла Европа, като се очаква да бъдат необходими 299 000 специалисти, за да се посрещнат нуждите по отношение на работната сила в

ЕС[35]. Според проучването „Евробарометър“ на уменията в областта на киберсигурността за 2024 г.[36] 81 % от дружествата считат трудностите при наемането на персонал в областта на киберсигурността за основен риск от потенциални кибератаки. В секторите на образованието, здравеопазването и социалната дейност 66 % от позициите в областта на киберсигурността се заемат от служители, осъществяващи преход от други позиции, несвързани с киберсигурността, което подчертава спешната нужда от преквалификация и повишаване на квалификацията.

За да се справи с това предизвикателство, Центърът за подкрепа следва да си сътрудничи с бъдещия консорциум за умения в областта на киберсигурността — консорциума за европейска цифрова инфраструктура (КЕЦИ), предвиден в съобщението на Комисията относно Академията на ЕС за киберумения[37]. Неговата работа следва да улеснява обмена между специалистите по киберсигурност в сектора на здравеопазването, например старшите служители по въпросите на сигурността на информацията (CISO). Едно потенциално действие би било създаването на **Европейска мрежа на CISO в сектора на здравеопазването**, като се започне с група от експерти, които да споделят и разработват най-добри практики, стратегии за задържане на таланти и решения за привличане на специалисти по киберсигурност в сектора на здравеопазването. Освен това под шапката на Академията за киберумения с подкрепата на промишлеността и академичните среди следва да бъдат разработени ресурси за усъвършенстване на работната сила в областта на киберсигурността в сектора на здравеопазването. Във връзка с това заинтересованите страни от сектора следва да бъдат насърчавани да поемат ангажименти в подкрепа на подобряването на обучението по киберсигурност.

Човешките грешки продължават да имат основна роля при инцидентите в областта на киберсигурността в сектора на здравеопазването, което подчертава критичната нужда от цялостно обучение на персонала и осведоменост в областта на киберсигурността. Като се има предвид колко често медицинските специалисти използват цифрови инструменти, от жизненоважно значение е те да придобият знания как да правят това по сигурен начин. Целенасочените кампании за обучение и повишаване на осведомеността могат да доведат до значително намаляване на рисковете. За да реши този въпрос, Центърът за подкрепа следва да работи с медицинските специалисти и доставчиците на здравно обслужване и да си сътрудничи с доставчиците на образование и обучение, промишлеността, КЕЦИ за киберумения, както и с органите на държавите членки за създаване и разпространение на **подробни лесно достъпни онлайн модули и курсове за обучение**.

Включването на модули за цифрова компетентност и киберсигурност в образователните програми е от решаващо значение за изграждането на стабилна основа за високо ниво на киберсигурност в сектора на здравеопазването. В тези модули следва да се разглеждат

[35] Картината на киберсигурността за 2024 година: Изводи от проучването на работната сила в областта на киберсигурността на ISC2 | Платформа за умения и работни места в областта на цифровите технологии

[36] Експресно проучване „Евробарометър“ № 547 на уменията в областта на киберсигурността.

[37] Съобщение на Комисията до Европейския парламент и Съвета: Преодоляване на недостига на таланти в областта на киберсигурността за повишаване на конкурентоспособността, растежа и устойчивостта на ЕС („Академия на ЕС за киберумения“). COM(2023) 207 final.

специфични за сектора въпроси, например защитата на данните на пациентите и уязвимостите в сигурността на медицинските изделия. При разработването на тези ресурси следва да се вземат предвид предишни действия, например проекта BeWell, финансиран по програма „Еразъм+“[38], и проекта PANACEA, финансиран по „Хоризонт 2020“[39].

3.2.Европейски способности за откриване на киберзаплахи срещу сектора на здравеопазването

Ефективното откриване на киберзаплахи е от съществено значение за бързата реакция при инциденти. Източниците на заплахи могат да използват техники, с които да затруднят откриването на проникванията, което може да доведе до продължителни периоди на неразрешен достъп до дадена система[40]. Следователно наличието на по-добри възможности за откриване на заплахи може да спомогне за прекратяване на кибератаките, още докато се подготвят. Например при атаката със софтуер за изнудване срещу финландския доставчик на психотерапевтични услуги Vastaamo, по време на която извършителят изнудва пациенти, чиито поверителни здравни досиета са били откраднати, първоначалното проникване е станало през 2018 г., но става известно на доставчика едва през 2020 г.[41]

Ефективният обмен на информация и сътрудничеството са от съществено значение за подобряване на откриването на заплахи и ситуационната осведоменост в целия ЕС. Екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС) имат жизненоважна роля при получаването на доклади за инциденти, ситуации, близки до инциденти, и потенциални заплахи и в предоставянето на насоки за мерки за смекчаване на национално равнище. **Държавите членки обаче също настоятелно се насърчават да споделят всички уведомления за киберинциденти от страна на болници и доставчици на здравно обслужване с Центъра за подкрепа на ENISA, за да подпомогнат така ситуационната осведоменост на ЕС.** В идеалния случай уведомлението следва да бъде придружено от съдържателна характеристика, включваща различни съответни измерения на инцидента, в това число известните основни уязвимости и ефектите върху здравните услуги, както и неблагоприятните въздействия за пациентите. Освен това производителите на медицински изделия и изделия за инвитро диагностика се насърчават доброволно да докладват чрез единната платформа за докладване, която ще бъде създадена и управлявана от ENISA в рамките на Законодателния акт за киберустойчивост, за активно използвани уязвимости или тежки киберинциденти, които оказват въздействие върху сигурността

[38] BeWell — Blueprint alliance for a future health workforce strategy on digital and green skills. [„BeWell — Алианс за бъдеща стратегия за работната сила в сектора на здравеопазването по отношение на цифровите и зелените умения“]. Достъпно на 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. [„ПАНАЦЕЯ — Защита и неприкосновеност на личния живот в болнични и здравни инфраструктури със smArt Cyber sEcurity и инструментариум срещу киберзаплахи за данните и хората“]. Достъпно на https://cordis.europa.eu/project/id/826293.
[40] Доклад относно картината на заплахите в сектора на здравеопазването на ENISA, 2023 г..
[41] Решение № 1150/161/2021 на финландския омбудсман за защита на данните.

на тези изделия, както и потенциално за други уязвимости, инциденти, ситуации, близки до инциденти, или киберзаплахи, които могат да повлияят на профила на риска на тези изделия.

Когато информацията в докладите вече не е чувствителна, Центърът за подкрепа може да създаде спонсориран от ENISA европейски каталог на известни експлоатирани уязвимости (KEV) на медицинските изделия, системите за електронни здравни досиета и доставчиците на ИКТ оборудване и софтуер в сектора на здравеопазването. За да се справи със значителните предизвикателства при откриването на заплахи, Центърът за подкрепа следва да въведе **абонаментна услуга за ранно предупреждение за сектора на здравеопазването в целия ЕС, чрез която да се подават сигнали почти в реално време**. Тази услуга ще се основава на обработени данни от ЕРИКС, здравни организации и производители, разузнаване от открити източници (OSINT) и други съответни участници като киберцентрове, центрове за споделяне и анализ на информация (ISAC) и правоприлагащи органи. Засиленото сътрудничество между ENISA и Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол) — например по отношение на моделите на киберпрестъпност срещу сектора на здравеопазването — ще доведе до допълнително повишаване на ситуационната осведоменост.

Центровете за споделяне и анализ на информация са основни ресурси за събиране на разузнавателни сведения за киберзаплахи, като насърчават двупосочния обмен на информация между публичния и частния сектор и подпомагат изграждането на доверие. Центърът за подкрепа следва да засили подкрепата за **Европейския център за споделяне и анализ на информация за сектора на здравеопазването** чрез инструменти и обмен на информация, секторни доклади за ситуационна осведоменост, както и да насърчава развитието на надеждна общност за тактическо и стратегическо сътрудничество. Държавите членки следва да насърчават разработването на национални центрове за споделяне и анализ на информация за сектора на здравеопазването[42]. Освен това центровете за споделяне и анализ на информация следва да бъдат насърчавани да провеждат срещи между доставчиците на здравно обслужване и производителите, за да се постигне общо разбиране за заплахите за киберсигурността, включително във веригите на доставки, и да насърчават диалога във връзка със сигурното проектиране на продуктите, при което действително се отчита реалността при внедряването на място.

3.3.Бързо реагиране и възстановяване

Като се има предвид високата чувствителност на здравните данни на пациентите и потенциално опустошителните последици от кибератаките върху здравните услуги, бързата и ефективна реакция на инцидентите в областта на киберсигурността е от решаващо значение, за да се

[42] Например Финландия има национален център за споделяне и анализ на информация за сектора на социалното подпомагане и здравеопазването. Вж. Национален център за киберсигурност на Финландия: ISAC information sharing groups [„Групи за споделяне на информация от типа Център за споделяне и анализ на информация“], достъпно на https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

гарантира безопасността на пациентите. Когато една болница или един доставчик на здравно обслужване се сблъска с кибератака, първото звено за контакт е съответният национален ЕРИКС[43]. ЕРИКС отговаря за предоставянето на навременна подкрепа, в идеалния случай в рамките на 24 часа, която да подпомогне управлението на значителни инциденти. Ако обаче по отношение на даден инциденткапацитетът на ЕРИКС не е достатъчен, следва да има подкрепа от ЕС, за да се гарантира бърза и ефективна реакция.

Чрез резерва за киберсигурност на ЕС, създаден съгласно Законодателния акт за киберсолидарност, се предоставят услуги за реагиране при инциденти от надеждни доставчици на управлявани услуги за сигурност, за да се окаже подкрепа при значителни или мащабни инциденти в областта на киберсигурността и да се предприемат първоначални мерки за възстановяване. Целта на този резерв е да се допълнят усилията на ЕРИКС на държавите членки, като им се даде възможност да поискат допълнителна подкрепа в случаи, засягащи критични сектори като здравеопазването. С цел подобряване на тази система **Комисията и ENISA следва да гарантират, че резервът включва услуга за бързо реагиране, предназначена специално за сектора на здравеопазването.** В допълнение към други съществуващи рамки, в случаи, когато националната подкрепа е недостатъчна, по линия на тази услуга ще бъдат изпращани експерти за незабавно управление на значителни или мащабни инциденти в областта на киберсигурността в сектора на здравеопазването.

С цел подобряване на реагирането и възстановяването Центърът за подкрепа, в сътрудничество с групата за сътрудничество за МИС, мрежата на ЕРИКС и, ако е приложимо, Европол следва да разработят **наръчници за реагиране при киберинциденти, адаптирани за сектора на здравеопазването**. Чрез тези наръчници ще се предоставят насоки както на ЕРИКС, така и на здравните организации как да отговорят на конкретни заплахи за киберсигурността, включително такива със софтуер за изнудване. Като се има предвид значимостта на ефективното сътрудничество между ЕРИКС и правоприлагащите органи при реагирането и разследването на инциденти в областта на киберсигурността от престъпен характер, наръчниците следва, наред с други аспекти, да включват ясни насоки относно докладването на такива инциденти към правоприлагащите органи. Освен това Центърът за подкрепа може да **улесни мащабно разгръщане на национални учения в областта на киберсигурността, като се основава на опита от Cyber Europe 2022 на ENISA, с цел тестване на наръчниците и укрепване на протоколите за реагиране при инциденти.**

За да се подплатят политиките с информация и да се оцени ефективността на мерките, предприети срещу атаките със софтуер за изнудване, е необходимо да се съберат допълнителни данни. За тази цел държавите членки следва да поискат от субектите, обхванати от Директивата МИС 2, в това число от здравните организации, да докладват за всички извършени плащания на откупи и за плащанията на откупи, които възнамеряват да извършат, наред с останалата информация, която предоставят, когато докладват за значителни инциденти в областта на киберсигурността. Този вид докладване подпомага ефективното разследване на инциденти със софтуер за изнудване,

[43] В член 23, параграф 1 от Директивата МИС 2 се установява изискване съществените и важните субекти да уведомяват за значителни инциденти съответния ЕРИКС или, ако е приложимо, компетентния орган.

включително проследяването на плащанията в платформи за обмен на криптовалути, за да се установи самоличността на получателите.

Скоростта на възстановяване е критичен фактор за поддържане на устойчивостта и общественото доверие, особено в сектора на здравеопазването, където неналичността на компютърните системи може да доведе до нарушаване на грижите за пациентите. За ефективно възстановяване от атаки със софтуер за изнудване доставчиците на здравно обслужване трябва да разполагат със сигурни, актуални и изолирани резервни копия, които да могат да бъдат бързо възстановени. Като част от своя каталог с услуги, Центърът за подкрепа може да предлага **абонаментна услуга за възстановяване след атаки със софтуер за изнудване, с която да помага на болниците и доставчиците на здравно обслужване предварително да подготвят планове за възстановяване.** ENISA и Европол следва да си сътрудничат, за да установят най-често срещаните видове софтуер за изнудване, насочени към здравните организации, и да **разширят списъка на инструменти за декриптиране**, наличен благодарение на проекта No More Ransom[44]. Освен това те следва да разработят и популяризират достъпни насоки, които да помогнат на доставчиците на здравно обслужване да избегнат плащането на откупи, като използват инструменти за декриптиране.

Международната инициатива за борба със софтуера за изнудване[45] е ценен форум за обмен на информация относно конкретни инциденти със софтуер за изнудване, както и за изграждане на капацитета на държавите членки за укрепване на техните рамки за киберсигурност и способности за разследване срещу участници в атаки със софтуер за изнудване. Комисията, заедно с върховния представител, ще продължи да развива сътрудничеството в рамките на инициативата за борба със софтуера за изнудване, включително срещу заплахите от атаки със софтуер за изнудване в сектора на здравеопазването. Освен това Комисията ще търси възможности за сътрудничество в **работната група по киберсигурност на Г-7** с цел укрепване на киберсигурността в сектора на здравеопазването. По-специално работната група може да разгледа възможностите да се окаже подкрепа на сектора на здравеопазването срещу заплахи, например срещу атаки със софтуер за изнудване, като продължи по този начин документи за размисъл като съвместното изявление относно атаките със софтуер за изнудване срещу здравни заведения от 8 ноември 2024 г., представено в контекста на Съвета за сигурност на ООН[46].

4. Действия на национално равнище

Капацитетът на настоящия план за действие за подобряване на киберсигурността в сектора на здравеопазването зависи от активното участие и ангажираност на държавите членки. За

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

успешното изпълнение на плана за действие държавите членки могат да определят **национални центрове за подкрепа в областта на киберсигурността, предназначени специално за болниците и доставчиците на здравно обслужване.** Тези центрове ще действат като основни звена за контакт за сектора на здравеопазването на национално равнище, като ще си сътрудничат тясно с Центъра за подкрепа на ENISA. Когато е възможно и целесъобразно, държавите членки следва да определят като такива вече съществуващи органи, например националните ЕРИКС за сектора на здравеопазването или съответните органи, като например националните центрове за подкрепа в областта на киберсигурността.

Освен това държавите членки се насърчават да създадат **национални планове за действие, насочени към киберсигурността в сектора на здравеопазването**. В тези планове ще бъдат очертани специфичните рискове за киберсигурността, пред които са изправени здравните системи, и националните действия, предприети за справяне с тях, като същевременно се гарантира ефективното използване на ресурсите и практиките на европейско равнище. Центърът за подкрепа на ENISA може да съдейства за разработването на тези планове, като взема предвид вече съществуващите национални планове и координира усилията, за да се гарантира, че ресурсите и стратегиите на отделните държави членки се допълват взаимно.

Друг основен акцент за държавите членки е улесняването на споделянето на ресурси между доставчиците на здравно обслужване, което може да бъде постигнато чрез **съвместни обществени поръчки или обединени ресурси** на национално, регионално или дори европейско равнище. Този подход ще допринесе за намаляване на финансовата тежест за отделните субекти, като същевременно ще спомогне за засилване на позициите им при договарянето с доставчиците на услуги в областта на киберсигурността.

Например с френската програма CaRE[47] бяха въведени редица мерки на национално и регионално равнище за справяне с предизвикателствата при осигуряването на ресурси: киберкаталогът дава възможност за общ преглед на киберрешенията и пакетите, предоставяни на болниците чрез Националната агенция за киберсигурност, Агенцията за цифрово здравеопазване, регионалните агенции, националните организации за закупуване, както и наличните търговски решения. Освен това на регионалните агенции се предоставя допълнително финансиране, за да предлагат споделени ресурси.

Държавите членки следва също да предприемат мерки спрямо недостатъчното ниво на инвестиции в областта на киберсигурността за сектора на здравеопазването. За да гарантират подходящо финансиране, те следва да определят **необвързващи референтни показатели и да проследяват целите по отношение на финансирането, които се отнасят конкретно за киберсигурността,** като същевременно гарантират, че тези инвестиции не водят до ограничаване на основните грижи за пациентите. Тези цели по отношение на финансирането следва също да бъдат ориентирани към интегриране на съображенията за сигурност във всички цифрови

[47] Агенция за цифрово здравеопазване на Франция: Cybersécurité acceleration et Résilience des Établissements (CaRE). Достъпно на https://esante.gouv.fr/strategie-nationale/cybersecurite.

инвестиции в сектора. Държавите членки могат да обменят най-добри практики и съвети във връзка с тези цели чрез платформи като мрежата за електронно здравеопазване[48].

5. Публично-частно сътрудничество

Публично-частното сътрудничество и консултациите с доставчиците на здравно обслужване, други субекти от сектора на здравеопазването, както и съответните участници в сектора на киберсигурността са от съществено значение за успешното изпълнение на плана за действие. За да допринесе за работата на Центъра за подкрепа, **Комисията, със съдействието на ENISA, ще създаде съвместен консултативен съвет по киберсигурност в сектора на здравеопазването** с участието на високопоставени представители от двете области — здравеопазване и киберсигурност, който може да съветва Комисията и Центъра за подкрепа относно ефективните действия и да провежда обсъждания относно по-нататъшното развитие на публично-частните партньорства в тази област. Съветът ще надгражда вече съществуващите действия в областта на публично-частните партньорства, в това число Европейския център за споделяне и анализ на информация за сектора на здравеопазването.

Освен това Комисията ще отправи **призив за действие** към дружества, фондации, образователни институции и други заинтересовани страни в областта на киберсигурността, **за да се ангажират с мерки за справяне с предизвикателствата в сектора**. Въз основа на опита на Академията за киберумения това могат да бъдат например ангажименти в рамките на Академията за киберумения за включване на предоставянето на курсове и материали за обучение на специалисти в областта на киберсигурността с акцент върху сектора на здравеопазването[49]. Други ангажименти могат да бъдат насочени и към дейности за повишаване на осведомеността или предоставяне на управлявани услуги за сигурност на специално уязвими субекти безплатно или на по-ниска цена с цел да се повиши тяхната готовност и устойчивост в областта на киберсигурността. Освен това ангажиментите могат да се състоят в споделяне на разузнавателни данни за киберзаплахи с Центъра за подкрепа на ENISA. Центърът за подкрепа следва да поддържа общ преглед на ангажиментите, поети в рамките на призива за действие, за да гарантира тяхната съгласуваност и взаимно допълване.

6. Възпиране на участниците в киберзаплахи

Вътрешните и външните политики на ЕС в областта на киберсигурността следва да бъдат в подкрепа на целта за възпиране на участниците в киберзаплахи от атаки срещу европейските здравни системи. Кибератаките срещу здравни организации са особено неприемливи сред злонамерените действия в киберпространството, като се има предвид, че могат да застрашат безопасността на пациентите и човешкия живот. Поради това ЕС следва да използва изцяло

[48] Мрежата за електронно здравеопазване е доброволна мрежа на определените от държавите членки национални органи, отговарящи за електронното здравеопазване, създадена на основание член 14 от Директива 2011/24/ЕС.
[49] Академия за киберумения:Включете се |Платформа за умения и работни места в областта на цифровите технологии

капацитета си в областта на киберсигурността и правоприлагането за възпиране на такива атаки и той следва да влезе в действие, за да се подкопае цялостният бизнес модел на участниците в заплахите, насочени към сектора на здравеопазването, и те да бъдат лишени от възможността за лесни печалби. Това ще включва насърчаване на трансграничните разследвания чрез засилен обмен на информация относно признаци за нарушена сигурност и други съответни данни, както и засилен акцент върху цели с висока стойност и ключови за престъпна дейност фактори, като например брониран хостинг или услуги за смесване на криптовалути.

С **инструментариума за кибердипломация** се предлага рамка за предотвратяване, възпиране и реагиране на кибератаки срещу ЕС, държавите членки и партньорите. Върховният представител ще продължи да използва съществуващата рамка за киберсанкции в отговор на заплахи, насочени към здравните системи.

Търсенето на отговорност от престъпниците за действията им е важен възпиращ фактор. Поради това държавите членки следва да гарантират, че правоприлагането е напълно интегрирано в националните им планове за действие. По-специално те следва да използват пълноценно разпоредбите на Директивата относно атаките срещу информационните системи[50] и на Конвенцията от Будапеща за престъпленията в кибернетичното пространство на Съвета на Европа, за да възпират атаки, да изправят престъпниците пред съда и да разбиват престъпните инфраструктури, с чиято помощ се осъществяват атаките[51]. С успешното прилагане на тези инструменти следва да се гарантира, че престъпните и злонамерените действия срещу сектора на здравеопазването се наказват.

7. Изпълнение и мониторинг на плана за действие

В плана за действие са предвидени редица задачи с оглед на създаването на Център за подкрепа в рамките на ENISA. По този начин се гарантира цялостно и съгласувано изпълнение на плана за действие, като същевременно се избягва създаването на нови субекти, което може да доведе до потенциални припокривания и допълнителни общопроизводствени разходи. Комисията възнамерява да осигури подходящи ресурси за Центъра за подкрепа.

След като Центърът за подкрепа започне да функционира, ENISA, след консултация с Комисията, следва редовно да предоставя актуална информация за работата на Центъра за подкрепа на управителния съвет на ENISA, както и на съответните мрежи на държавите членки, по-специално на групата за сътрудничество за МИС, мрежата на ЕРИКС, мрежата за електронно здравеопазване и, ако е приложимо, на Комитета по въпросите на европейското пространство на здравни данни. Освен това ENISA следва непрекъснато да обменя информация с публично-частния консултативен

[50] Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng

[51] Конвенция за престъпленията в кибернетичното пространство (Конвенция от Будапеща, ETS № 185) и протоколите към нея: https://www.coe.int/en/web/cybercrime/the-budapest-convention

съвет по киберсигурност в сектора на здравеопазването относно изпълнението на действията, извършвани от Центъра за подкрепа.

Редовните доклади на ENISA, например доклада за състоянието на киберсигурността в Съюза, с който се предоставя обобщена оценка на степента на зрялост на способностите и ресурсите по отношение на киберсигурността в целия ЕС, включително в сектора на здравеопазването, следва бъдат повод да се публикуват съответни данни, което ще бъде в подкрепа на мониторинга на плана за действие. Освен това индексът за киберсигурност на ЕС на ENISA[52] може да бъде източник на количествени и качествени данни, което ще послужи като доказателствена база за оценка на критичността и зрелостта на сектора на здравеопазването.

8. По-нататъшни стъпки

В настоящото съобщение се установява амбициозна програма за повишено ниво на киберсигурност в сектора на здравеопазването в ЕС. С предложения Център за подкрепа в областта на киберсигурността за болници и доставчици на здравно обслужване, който да стои в основата на ENISA, в плана за действие се очертава пътят към създаването на съгласуван и споделен европейски подход към предизвикателството, което представлява киберсигурността за сектора.

Настоящото съобщение следва да се разглежда като начало на процеса на подобряване на киберсигурността в сектора на здравеопазването. Поради това наред с приемането на плана за действие ще започнат задълбочени консултации със заинтересованите страни и ще продължи обменът с държавите членки и съответните мрежи за събиране на информация. Въз основа на резултатите от консултациите през четвъртото тримесечие на 2025 г. Комисията възнамерява да представи препоръки за по-нататъшно усъвършенстване на плана за действие.

Комисията призовава държавите членки и всички заинтересовани страни да работят заедно за постигане на амбициозните цели на плана за действие.

[52] ENISA, Индекс за киберсигурност на ЕС, рамка и методологическа бележка (2024 г.). Достъпно на https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

ПРИЛОЖЕНИЕ — Преглед на предложените действия

Комисията:

Европейски център за подкрепа в областта на киберсигурността за болници и доставчици на здравно обслужване в рамките на ENISA	
Осигуряване на подходящи ресурси за Центъра за подкрепа в областта на киберсигурността Работа с Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността за стартиране на пилотни проекти с цел разработване на най-добри практики за киберхигиена и оценка на риска за сигурността, както и справяне с необходимостта от непрекъснато наблюдение на киберсигурността, разузнавателни сведения за заплахи и реагиране при инциденти, като се използват най-съвременни решения в областта на киберсигурността, с оглед на разработването на каталога с услугите на Европейския център за подкрепа в областта на киберсигурността	2025 г.
Предотвратяване на инциденти в областта на киберсигурността	
След консултация с групата за сътрудничество за МИС, EU-CyCLONe и ENISA, проучване на възможността здравеопазването да бъде определено като сектор, който може да получава подкрепа за координирано тестване на готовността съгласно Законодателния акт за киберсолидарност.	първо тримесечие на 2025 г.
Бързо реагиране и възстановяване	
Заедно с ENISA, гарантиране, че резервът за киберсигурност на ЕС включва служба за бързо реагиране, специално за сектора на здравеопазването	четвърто тримесечие на 2025 г.
Публично-частно сътрудничество	
С подкрепата на ENISA, създаване на съвместен консултативен съвет по киберсигурност в здравеопазването	първо тримесечие на 2025 г.
Отправяне на призив за действие към дружества, фондации, образователни институции и други заинтересовани страни в областта на	второ тримесечие на 2025 г.

киберсигурността, за да се ангажират с мерки за справяне с предизвикателствата в сектора	
Възпиране на участниците в киберзаплахи	
Заедно с върховния представител, проучване на възможността да се използват мерки от инструментариума за кибердипломация с цел предотвратяване, възпиране и реагиране на злонамерени действия срещу здравните системи	2025 г.
Постигане на напредък в международното сътрудничество срещу участниците в атаки със софтуер за изнудване, по-специално в рамките на Международната инициатива за борба със софтуера за изнудване, като се работи съвместно с върховния представител	2025—2026 г.
Търсене на възможности за сътрудничество в работната група по киберсигурност на Г-7 с цел укрепване на киберсигурността в сектора на здравеопазването	2025—2026 г.
По-нататъшни стъпки	
Започване на задълбочени консултации със заинтересованите страни	първо тримесечие на 2025 г.
Приемане на препоръки за по-нататъшно усъвършенстване на плана за действие	четвърто тримесечие на 2025 г.

ENISA:

Европейски център за подкрепа в областта на киберсигурността за болници и доставчици на здравно обслужване в рамките на EU	
Започване на работа по създаването на Европейски център за подкрепа в областта на киберсигурността за болници и доставчици на здравно обслужване	второ тримесечие на 2025 г.
Разработване на подробен каталог на услугите, който да бъде предоставен от Центъра за подкрепа в областта на киберсигурността	от четвъртото тримесечие на 2025 г.
Предотвратяване на инциденти в областта на киберсигурността	
Издаване на насоки, в които се изтъкват най-важните практики в областта на киберсигурността	трето тримесечие на 2025 г.

и се подпомагат доставчиците на здравно обслужване при прилагането им	
В тясно сътрудничество с Комисията и държавите членки, разработване на инструмент за регулаторно картографиране	първо тримесечие на 2025 г.
Разработване на рамка за оценки на зрелостта по отношение на киберсигурността, която да е специфична за сектора на здравеопазването	трето тримесечие на 2025 г.
Извършване на годишна оценка на зрелостта по отношение на киберсигурността на сектора на здравеопазването	2025—2026 г.
В сътрудничество с държавите членки и регионалните програмни органи, създаване на модели на ваучери за киберсигурност	2025—2026 г.
Разработване на нови насоки за възлагане на обществени поръчки в областта на киберсигурността на болници и доставчици на здравно обслужване	трето тримесечие на 2025 г.
Създаване на Европейска мрежа на главните служители по въпросите на информационната сигурност в сектора на здравеопазването	първо тримесечие на 2026 г.
Разработване и популяризиране на модули и курсове за обучение на медицински специалисти	първо тримесечие на 2026 г.
Европейски способности за откриване на киберзаплахи срещу сектора на здравеопазването	
Създаване на европейски каталог на известни експлоатирани уязвимости (KEV) на медицинските изделия, системите за електронни здравни досиета и доставчиците на ИКТ оборудване и софтуер в сектора на здравеопазването	четвърто тримесечие на 2025 г.
Въвеждане на абонаментна услуга за ранно предупреждение в целия ЕС за сектора на здравеопазването	от 2026 г. нататък
Подкрепа за Европейския център за споделяне и анализ на информация за сектора на здравеопазването с инструменти и обмен на информация	2025—2026 г.
Бързо реагиране и възстановяване	

Заедно с Комисията гарантиране, че резервът за киберсигурност на ЕС включва служба за бързо реагиране, специално за сектора на здравеопазването	четвърто тримесечие на 2025 г.
В сътрудничество с мрежата на ЕРИКС, разработване на наръчници за реагиране при киберинциденти, адаптирани за сектора на здравеопазването	трето тримесечие на 2025 г.
Улесняване на мащабно разгръщане на национални учения в областта на киберсигурността с цел тестване на наръчниците и укрепване на протоколите за реагиране при инциденти	четвърто тримесечие на 2025 г.
Предоставяне на абонаментна услуга за възстановяване след атака със софтуер за изнудване	от 2026 г. нататък
Заедно с Европол, установяване на най-често срещаните видове софтуер за изнудване, насочени към здравните организации, и разширяване на списъка с инструменти за декриптиране чрез проекта No More Ransom.	четвърто тримесечие на 2025 г.
Заедно с Европол, разработване на достъпни насоки, с които да се помогне на доставчиците на здравно обслужване да избягват плащането на откупи	трето тримесечие на 2025 г.
Действия на национално равнище	
Подпомагане на държавите членки при разработването на национални планове за действие	2025 г.
Координиране на усилията, за да се гарантира, че ресурсите и стратегиите на отделните държави членки се допълват взаимно	2025—2026 г.
Изпълнение и мониторинг на плана за действие	
След консултация с Комисията, редовно предоставяне на актуална информация за работата на Центъра за подкрепа в областта на киберсигурността на съответните мрежи на държавите членки	2025—2026 г.

Непрекъснат обмен с консултативния съвет по киберсигурност в сектора на здравеопазването	2025—2026 г.

Държави членки:

Европейски способности за откриване на киберзаплахи срещу сектора на здравеопазването	
Споделяне на уведомления за киберинциденти от страна на болници и доставчици на здравно обслужване по Директива МИС 2 с Европейския център за подкрепа в областта на киберсигурността	четвърто тримесечие на 2025 г.
Насърчаване на разработването на национални центрове за споделяне и анализ на информация за сектора на здравеопазването	2025—2026 г.
Предотвратяване на инциденти в областта на киберсигурността	
В рамките на групата за сътрудничество за МИС, провеждане на координирана оценка на риска за сигурността, като се оценят както техническите, така и стратегическите рискове, свързани с веригите за доставки на медицински изделия	четвърто тримесечие на 2025 г.
Бързо реагиране и възстановяване	
Разгръщане на национални учения в областта на киберсигурността с цел тестване на наръчниците и укрепване на протоколите за реагиране при инциденти	от 2026 г. нататък
Действия на национално равнище	
Определяне на национални центрове за подкрепа в областта на киберсигурността за болници и доставчици на здравно обслужване	второ тримесечие на 2025 г.
Създаване на национални планове за действие, насочени към киберсигурността в сектора на здравеопазването	четвърто тримесечие на 2025 г.
Улесняване на споделянето на ресурси между доставчиците на здравно обслужване	2025—2026 г.
Определяне на необвързващи референтни показатели и проследяване на целите по	четвърто тримесечие на 2025 г.

отношение на финансирането, които се отнасят конкретно за киберсигурността	
Изискване от здравните организации и други субекти, които са обект на Директивата МИС 2, да докладват намеренията си да плащат откупи	четвърто тримесечие на 2025 г.