Europeiska unionens råd

Bryssel den 16 januari 2025
(OR. en)

5426/25

CYBER 21
SAN 15

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	15 januari 2025
till:	Thérèse BLANCHET, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2025) 10 final
Ärende:	MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN Europeisk handlingsplan för cybersäkerhet för sjukhus och vårdgivare

För delegationerna bifogas dokument – COM(2025) 10 final.

Bilaga: COM(2025) 10 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 15.1.2025
COM(2025) 10 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN

Europeisk handlingsplan för cybersäkerhet för sjukhus och vårdgivare

1. Inledning

EU:s säkerhetsmiljö förändras snabbt, med en upptrappning av hybrid- och cyberattacker som syftar till att destabilisera vårt samhälle och skapa splittring och störningar – men också tjäna pengar – genom it-brottslighet. EU måste därför snarast stärka sin beredskap för och resiliens mot denna nya verklighet, inom alla sektorer och i linje med ett samhälls- och myndighetsövergripande tillvägagångssätt, vilket efterlyses i rapporten från den särskilda rådgivaren till Europeiska kommissionens ordförande, Sauli Niinistö.

Säkra och resilienta hälso- och sjukvårdssystem är en hörnsten i EU:s sociala modell. Sjukhus och hälso- och sjukvårdssystem står dock inför allt större hot, särskilt från gäng med utpressningsprogram som attackerar dem för ekonomisk vinning, med anledning av det höga värdet av patientuppgifter, inklusive elektroniska patientjournaler. Faktum är att hälso- och sjukvårdssektorn har blivit den hårdast drabbade sektorn i EU under de senaste fyra åren, bland annat under covid-19-pandemin då hälso- och sjukvårdsinfrastrukturen i allt högre grad utsattes för cyberattacker. Cyberattacker mot sjukhus och vårdgivare vållar direkt skada för människor, försenar behandlingar, skapar kaos på akutmottagningar och kan i yttersta fall leda till dödsfall.

Utmaningen blir ännu större med tanke på att sektorn genomgår en viktig digital omställning. E-hälsa och användning och återanvändning av hälsodata kan skapa vårdmodeller som är bättre lämpade för människor och patienters behov och preferenser, genom att förhindra sjukdomsutbrott eller möjliggöra tidigare behandling. Integreringen av digitala verktyg och lösningar i kliniska processer samt användningen och återanvändningen av hälsodata kan leda till bättre kliniska beslut, mer automatiserad hälso- och sjukvård och snabbare och bättre patientvård. Digitala verktyg, dataanvändning och medicintekniska produkter – som ofta är uppkopplade till internet och drivs av artificiell intelligens (AI) – är också avgörande för att hantera problem som bristen på hälso- och sjukvårdspersonal.

Samtidigt gör de digitala verktygen hälso- och sjukvårdssektorn till en större måltavla för it-brottslingar. Vissa statliga aktörer väjer inte heller för att angripa vårdinrättningar, vilket framgår av Rysslands pågående anfallskrig mot Ukraina. Detta gör sektorn till ett potentiellt mål för cyberattacker som en del av en bredare hybridkampanj. Cyberattacker äventyrar inte bara patientsäkerheten, utan undergräver också allmänhetens förtroende för hälso- och sjukvårdsinfrastrukturen och medför betydande återställningskostnader. Utöver att skydda mot cyberattacker är en resilient och säker digital infrastruktur också avgörande för att stödja genomförandet och den fullständiga tillämpningen av det europeiska hälsodataområdet[1].

Det är därför hög tid att vidta åtgärder och stärka cybersäkerheten och resiliensen för EU:s sjukhus och vårdgivare, vilket framhölls av ordförande Ursula von der Leyen i hennes politiska riktlinjer för kommissionen för 2024–2029[2]. Denna handlingsplan är ett svar på det brådskande läget och de unika hot som sektorn står inför. Det finns ingen enkel patentlösning på cybersäkerhetsutmaningarna inom hälso- och sjukvården. I handlingsplanen efterlyses i stället förstärkta åtgärder för förebyggande och beredskap samt en mer samordnad och solidarisk strategi samtidigt som sakkunskapen inom den

[1] https://www.consilium.europa.eu/sv/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_sv.

europeiska cybersäkerhetsbranschen utnyttjas. Handlingsplanen återspeglar EU:s säkerhetsstrategi, som kommer att vidareutvecklas och formaliseras i den kommande europeiska strategin för inre säkerhet. Strategin kommer att omfatta övergripande åtgärder för att ta itu med alla inre säkerhetshot, med fokus på förmågan att förutse hot, förebygga skada och skydda människor. Den kommer att tillämpas på alla nivåer utifrån ett samhälleligt helhetsgrepp.

Hälso- och sjukvårdssektorn omfattar ett stort antal enheter och aktörer, däribland sjukhus, vårdcentraler, vårdhem, rehabiliteringscenter och olika vårdgivare, tillsammans med läkemedelsindustrin, den medicinska industrin, bioteknikindustrin, tillverkare av medicintekniska produkter och forskningsinstitut på hälsoområdet. Denna handlingsplan är främst inriktad på cybersäkerhet för sjukhus och vårdgivare, dvs. alla fysiska eller juridiska personer – eller andra enheter – som lagligen bedriver hälso- och sjukvård på en medlemsstats territorium[3]. Sjukhus och vårdgivare är beroende av andra vårdinrättningar och de har den närmaste kontakten med människor. Samtidigt bör åtgärder för att öka cybersäkerheten för sjukhus och vårdgivare också ta itu med risker som påverkar den bredare leveranskedjan och det bredare ekosystemet, till exempel risker som härrör från enheter som använder hälsodata för forskning och maskininlärning eller som tillverkar medicintekniska produkter, särskilt digitala medicintekniska produkter som kopplas upp till internet eller andra anordningar (sakernas internet).

Även om skyddet av hälso- och sjukvårdssystemen i första hand är en nationell behörighet är hälso- och sjukvårdssektorn även en kritisk sektor enligt direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2)[4]. It-brottslingar och andra fientliga aktörer verkar över gränserna, och de cybersäkerhetsutmaningar som hälso- och sjukvårdsorganisationer står inför är också likartade i alla medlemsstater. Samarbete på EU-nivå är värdefullt för att dela och förbättra bästa praxis i EU och nationellt. I handlingsplanen föreslås därför samordning och åtgärder på EU-nivå, samtidigt som medlemsstaterna uppmanas att vidta åtgärder för att göra skillnad för hälso- och sjukvården och det bredare hälsoekosystemet.

Handlingsplanen inriktas på att bygga upp sektorns kapacitet att **förhindra** cybersäkerhetsincidenter från att ske över huvud taget, eftersom det alltid är bättre att förebygga än att bota. För det andra innehåller handlingsplanen åtgärder för att förbättra informationsutbytet om cybersäkerhet och förmågan att **upptäcka** cyberhot så att man ska kunna reagera snabbare. För det tredje innehåller den åtgärder för att bättre **bemöta** incidenter och **återhämta sig** från dem. Slutligen omfattar handlingsplanen metoder för att **avskräcka** cyberhotande aktörer från att attackera hälso- och sjukvårdssystemen i EU.

Handlingsplanen kommer att genomföras i samarbete med vårdgivare och det bredare hälsoekosystemet, medlemsstaterna och cybersäkerhetsbranschen. Samarbete är avgörande för att ytterligare fastställa och förfina de mest verkningsfulla åtgärderna så att alla kritiska vårdgivare i EU kan dra nytta av dem. Detta meddelande kommer därför att åtföljas av ett omfattande samråd med berörda parter, branschen och medlemsstaterna. Internationellt samarbete är viktigt för cybersäkerheten på grund av cyberhotens gränsöverskridande och sammanlänkade karaktär. Jämförbara cybersäkerhetshot förekommer även i

[3] Artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård, https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=celex:32011L0024.
[4] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2-direktivet), https://eur-lex.europa.eu/eli/dir/2022/2555.

utvidgnings- och grannskapsländerna och andra strategiska partnerländer till EU. Detta kan i förlängningen äventyra säkerheten för kritisk infrastruktur i EU. Det kommer därför att vara viktigt att återspegla lärdomarna från genomförandet av handlingsplanen i EU:s samarbete med både utvidgningsländerna och andra partnerländer, mot bakgrund av hotnivån mot dessa länder.

2. Cybersäkerhetsutmaningar för sjukhus och vårdgivare

Cyberhot mot hälso- och sjukvårdssektorn

Cyberattackerna ökar globalt och inom EU, och hoten blir alltmer komplexa och dynamiska. Utvecklingen inom AI ger brottslingar och fientliga aktörer kraftfulla verktyg för att angripa med ökad precision och effekt. Samtidigt ger AI-utvecklingen upphov till nya möjligheter att försvara sig genom automatiserade åtgärder i realtid mot attacker.

Utpressningsprogram är fortfarande en kritisk cybersäkerhetsutmaning i EU och globalt. I en rapport uppskattas den globala årliga kostnaden uppgå till över 250 miljarder euro fram till 2031[5]. När brottslingar med utpressningsprogram slår till krypterar de inte bara offrens data för en lösensumma, utan de har även i allt större utsträckning börjat läcka känslig information för att utöva ytterligare påtryckningar. Ett annat stort problem är sårbarheter i programvara och hårdvara. Enligt Europeiska unionens cybersäkerhetsbyrå (Enisa)[6] är hälso- och sjukvård den sektor som har rapporterat flest säkerhetsincidenter kopplade till sådana sårbarheter[7]. Andra växande hot är samordnade överbelastningsattacker, som är utformade för att överbelasta det attackerade systemet med trafik så att legitima användare inte kan komma åt det[8].

Hälso- och sjukvårdssektorn står inför liknande cybersäkerhetshot, framför allt i form av utpressningsattacker. Enligt Enisa stod utpressningsprogram för 54 % av de analyserade cybersäkerhetsincidenterna inom hälso- och sjukvårdssektorn 2021–2023. Av attackerna var 83 % ekonomiskt motiverade, med anledning av det höga värdet av hälso- och sjukvårdsdata, medan 10 % hade en ideologisk bakgrund[9]. På samma sätt konstaterade kommissionen i en rapport från 2024 att 71 % av attacker med inverkan på patientvården, såsom fördröjd behandling och diagnos samt försämrad

[5] Cybersecurity Ventures (1 juni 2024): *Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031*. Finns på https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[6] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten), https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.
[7] *ENISA Threat Landscape: Health Sector* (juli 2023).
[8] Enisas hotbildsrapport 2024.
[9] *ENISA Threat Landscape: Health Sector* (juli 2023). I rapporten analyserades vårdgivare samt andra typer av organisationer, däribland organisationer som bedriver hälsorelaterad forskning, enheter som tillverkar vissa hälsorelaterade produkter, hälsomyndigheter, sjukförsäkringsorgan, inrättningar för slutenvård och leverantörer av sociala tjänster. Finns på https://www.enisa.europa.eu/publications/health-threat-landscape.

tillgång till alarmeringstjänster, hade genomförts med utpressningsprogram[10]. Utpressningsattacker kan ha en särskilt störande effekt på tillhandahållandet av hälso- och sjukvård, vilket äventyrar patientsäkerheten. Utpressningsattacker kombineras dessutom ofta med intrång i patientuppgifter[11], vilka ofta inbegriper känsliga hälsorelaterade uppgifter och kränker människors grundläggande rätt till skydd av personuppgifter.

Samtidigt växer attackytan i takt med den ökande digitaliseringen av hälso- och sjukvården. Enligt lägesrapporten om det digitala decenniet 2024 har i genomsnitt 79 % av EU-medborgarna tillgång till sina elektroniska patientjournaler inom primärvården online[12]. Elektroniska patientjournaler, kliniska informationssystem, system för sjukhusens arbetsflöde, it-system för hantering av ersättning för behandlingar, system för bilddiagnostik och medicintekniska produkter som används för diagnostik eller för patientövervakning är alla exempel på digitala verktyg som kan spela en viktig roll för att öka effektiviteten och resultaten inom hälso- och sjukvårdssektorn, men som också är potentiella mål för en cybersäkerhetsattack. Särskild hälso- och sjukvårdsverksamhet som intensivvård och radiologisk avbildning, eller medicinska områden som onkologi och kardiologi, som är starkt beroende av digitala enheter, löper en särskilt stor risk att utsättas för cyberattacker. Dessutom kan problem med leveranskedjan leda till upphandling av enheter som inte är tillräckligt cybersäkra och därmed förvärrar de befintliga allmänna riskerna.

Under covid-19-pandemin ledde till exempel en utpressningsattack till att stora delar av det irländska hälso- och sjukvårdssystemet paralyserades, vilket i sin tur medförde att åtminstone vissa tjänster ställdes in vid 31 av 54 akutsjukhus den morgon då incidenten ägde rum[13]. Hälso- och sjukvården tvingades återgå till pappersjournaler, vilket bromsade verksamhetens effektivitet. Attacken utlöstes av ett nätfiskemeddelande via e-post som innehöll en skadlig bilaga[14]. Incidenten visade potentialen hos cyberattacker som sprider sig till olika system och följaktligen vikten av att skydda en hälso- och sjukvårdsorganisations hela attackyta. Det blev också tydligt hur viktigt det är att säkerställa grundläggande it-hygien och cybersäkerhet inom alla organisationer.

Sjukhusens och vårdgivarnas cybersäkerhetsmognad

Hälso- och sjukvårdslandskapet i EU är mycket varierat, och sjukhus och andra vårdgivare skiljer sig kraftigt åt vad gäller ägande, struktur och storlek i olika medlemsstater. I vissa fall kan styrningen på hälsoområdet vara centraliserad på nationell nivå, medan den i andra sköts på regional och lokal nivå. Vårdgivare kan vara offentligt eller privat ägda. Det kan dessutom finnas skillnader inom samma land, till exempel där det finns betydande socioekonomiska och territoriella skillnader mellan regionerna,

[10] Europeiska kommissionen, gemensamma forskningscentrumet, Reina, V. och 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*, Europeiska unionens publikationsbyrå, 2024, https://data.europa.eu/doi/10.2760/693487.
[11] Enligt Enisas hotbildsrapport om hälso- och sjukvårdssektorn kunde dataintrång eller datastöld bekräftas vid 43 % av de analyserade utpressningsincidenterna.
[12] Lägesrapport om det digitala decenniet 2024.
[13] Irish Health Service Executive (2021): *Conti cyber attack on the HSE: Independent Post Incident Review*.
[14] Irish Health Service Executive: *Cyber-attack and HSE response*. Finns på https://www2.hse.ie/services/cyber-attack/what-happened/.

vilket ger en komplex bild. Detta komplexa hälso- och sjukvårdslandskap kan drabbas av viktiga hälsokriser, på grund av smittsamma sjukdomar, såsom covid-19-pandemin, men även av andra hälsorisker, till exempel i samband med klimatförändringarna. Slutligen förekommer betydande variation och fragmentering när det gäller vårdgivarnas digitalisering och införande av teknik. Ett exempel på denna komplexitet är om tjänster blir otillgängliga till följd av en cybersäkerhetsincident och detta leder till allvarlig skada för patienter även vid små vårdinrättningar, däribland vårdcentraler eller akutsjukvårdstjänster som tillhandahåller en samhällsviktig tjänst för relativt få personer.

Enligt Enisas rapport om cybersäkerhetssituationen i unionen från 2024[15] är cybersäkerhetsmognaden i EU:s hälso- och sjukvårdssektor måttlig och skiljer sig markant mellan olika vårdinrättningar i EU. Det förekommer brister på viktiga områden, såsom tillräckliga personalresurser, organisationernas kunskap om sina leveranskedjor för informations- och kommunikationsteknik (IKT) samt installation av de senaste säkerhetsfunktionerna i produkter. Sektorn kämpar med elementär it-hygien och grundläggande säkerhetsåtgärder, vilket illustreras av att nästan samtliga undersökta hälsoorganisationer står inför utmaningar när det gäller att utföra bedömningar av cybersäkerhetsrisker, medan nästan hälften aldrig har utfört en riskanalys[16].

En annan stor utmaning för sjukhusens cybersäkerhet är skärningspunkten mellan informationsteknik och operativ teknik, där olika säkerhetsprioriteringar möts vad gäller konfidentialitet, tillgänglighet och tillförlitlighet, och där ett intrång på ett område kan påverka ett annat. I Enisas rapport om cybersäkerhetssituationen i unionen från 2024 betonas vidare att hälso- och sjukvårdssektorn inte fungerar på ett tillfredsställande sätt när det gäller att säkerställa säkerheten för de IKT-produkter och IKT-processer som den använder, på grund av den stora variationen av olika vårdinrättningar, anordningar och produkter.

Denna mångfald, i kombination med varierande nivåer av cybermedvetenhet bland sjukhusens personal och ledning, skapar en komplex utmaning i fråga om att säkerställa cybersäkerheten i hälso- och sjukvårdssystemen. Enligt Eurobarometerundersökningen om cyberkompetens 2024 hade till exempel bara 25 % av de undersökta företagen inom sektorn för hälso- och sjukvård, utbildning och social omsorg tillhandahållit utbildning eller information om cybersäkerhet under de senaste tolv månaderna[17]. Det krävs åtgärder för att främja en kultur av cybersäkerhetsmedvetenhet bland hälso- och sjukvårdspersonal i första ledet. Till exempel är personalrotation, användningen av delade arbetsstationer, dålig autentiseringshantering och användningen av flyttbara medier ytterligare källor till sårbarheter som påverkar vårdgivarnas cybersäkerhet[18].

I många fall läggs informationsteknik och operativ teknik åtminstone delvis ut på entreprenad. I 2024 års Eurobarometerundersökning konstaterades att andelen företag som lägger ut åtminstone vissa aspekter av sin cybersäkerhet på entreprenad är högst inom sektorn för hälso- och sjukvård, utbildning

[15] Enisa, 2024 års rapport om cybersäkerhetssituationen i unionen (september 2024). Finns på https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
[16] *ENISA Threat Landscape: Health Sector* (juli 2023). Finns på https://www.enisa.europa.eu/publications/health-threat-landscape.
[17] Flash Eurobarometer 547 om cyberkompetens (maj 2024). Finns på 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*.

och social omsorg, där 57 % av de undersökta företagen gör detta[19]. På samma sätt finns det en stark tendens att migrera till molntjänster, på grund av behovet av skalbar datalagring och datahantering, kostnadseffektivitet, förbättrat samarbete och stöd för avancerad teknik som AI och sakernas internet inom medicin. Under 2022 använde 58 % av hälsoorganisationerna en molnbaserad e-hälsoplattform[20]. Denna övergång kan medföra betydande effektivitetsvinster, men den ger även upphov till risker som kräver välgrundade beslut om upphandling och säker konfiguration.

En fråga som genomsyrar alla dessa utmaningar är den om kapacitetsuppbyggnad och finansiering. Finansieringen av cybersäkerhet inom hälso- och sjukvårdssektorn har varit begränsad och är fortfarande ett universellt problem i hela EU[21]. Dessutom uppstår dessa finansieringsutmaningar mot bakgrund av en åldrande befolkning, som förväntas skapa ett omfattande budgettryck på EU:s hälso- och sjukvårdssystem under de kommande årtiondena.

Den fortsatta användningen av föråldrade verktyg och system, begränsade resurser för att förebygga eller hantera incidenter samt bristande cybersäkerhetsmognad beror ofta på finansieringsunderskott. Sjukhusen står inför en ständig utmaning att balansera en uppdaterad säker och digital infrastruktur med andra nödvändiga investeringar för att förbättra patientvården, såsom anställning av läkare och annan vårdpersonal, införande av nya diagnos- och behandlingsmetoder samt förvärv av produkter. Enligt Enisa[22] hamnar hälso- och sjukvårdssektorn bara på sjunde plats av de tolv undersökta sektorerna när det gäller andelen utgifter för informationssäkerhet av de totala it-utgifterna, med ett medianvärde på 8,3 %.

3. Europeiskt stödcentrum för cybersäkerhet för sjukhus och vårdgivare

EU:s cybersäkerhetsram erbjuder en lång rad olika verktyg som bör användas för att förbättra säkerheten och resiliensen för sjukhus och vårdgivare. För att ta itu med de många utmaningar som presenteras ovan är det nödvändigt att utarbeta en enhetlig strategi på EU-nivå som sammanför de resurser, den sakkunskap och de verktyg som krävs för att effektivt hantera cyberhot. En omfattande översikt samt bättre planering och samordning är avgörande för att hjälpa vårdgivare i hela EU att stärka sitt försvar. För att uppnå detta är Enisa den som är bäst lämpad att inom sin organisation inrätta ett särskilt **europeiskt stödcentrum för cybersäkerhet för sjukhus och vårdgivare**[23] som en del av sitt mandat[24] att skydda och stödja EU:s kritiska infrastruktur.

Stödcentrumet bör successivt **utarbeta en omfattande tjänstekatalog för att tillgodose sjukhusens och vårdgivarnas behov**, med en beskrivning av de tillgängliga tjänsterna för beredskap, förebyggande,

[19] Flash Eurobarometer 547 om cyberkompetens (maj 2024). Finns på https://europa.eu/eurobarometer/surveys/detail/3176.
[20] Enisa, *NIS Investments Report 2022* (november 2022). Finns på https://www.enisa.europa.eu/publications/nis-investments-2022.
[21] Organiseringen och tillhandahållandet av hälso- och sjukvård är en nationell behörighet enligt artikel 168 i fördraget om Europeiska unionens funktionssätt, och finansieringen av hälso- och sjukvårdssystemen varierar mellan medlemsstaterna.
[22] Enisa, *NIS Investments Report 2022* (november 2022). Finns på https://www.enisa.europa.eu/publications/nis-investments-2022.
[23] Även kallat *stödcentrumet* i det här dokumentet.
[24] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

upptäckt och insatser. I samarbete med medlemsstaternas myndigheter och med hjälp av sjukhusens och vårdgivarnas erfarenheter bör stödcentrumet utveckla en användarvänlig och lättillgänglig databas över alla tillgängliga instrument på europeisk, nationell och regional nivå. I sin verksamhet bör stödcentrumet säkerställa lämplig samordning med medlemsstaterna och stödja prioritering och genomförande av åtgärder vid behov i realtid.

Som en viktig byggsten för utarbetandet av stödcentrumets tjänstekatalog kommer kommissionen att föreslå att pilotprojekt lanseras i hela EU för att utveckla bästa praxis för bedömning av it-hygien och cybersäkerhetsrisker samt för att tillgodose behovet av kontinuerlig cybersäkerhetsövervakning, underrättelser om hot och hantering av incidenter med hjälp av de senaste cybersäkerhetslösningarna. Resultaten av dessa pilotprojekt, som kommer att finansieras genom programmet för ett digitalt Europa, vilket genomförs av Europeiska kompetenscentrumet för cybersäkerhet, kommer att ligga till grund för ytterligare åtgärder på EU-nivå, inbegripet stödcentrumets arbete.

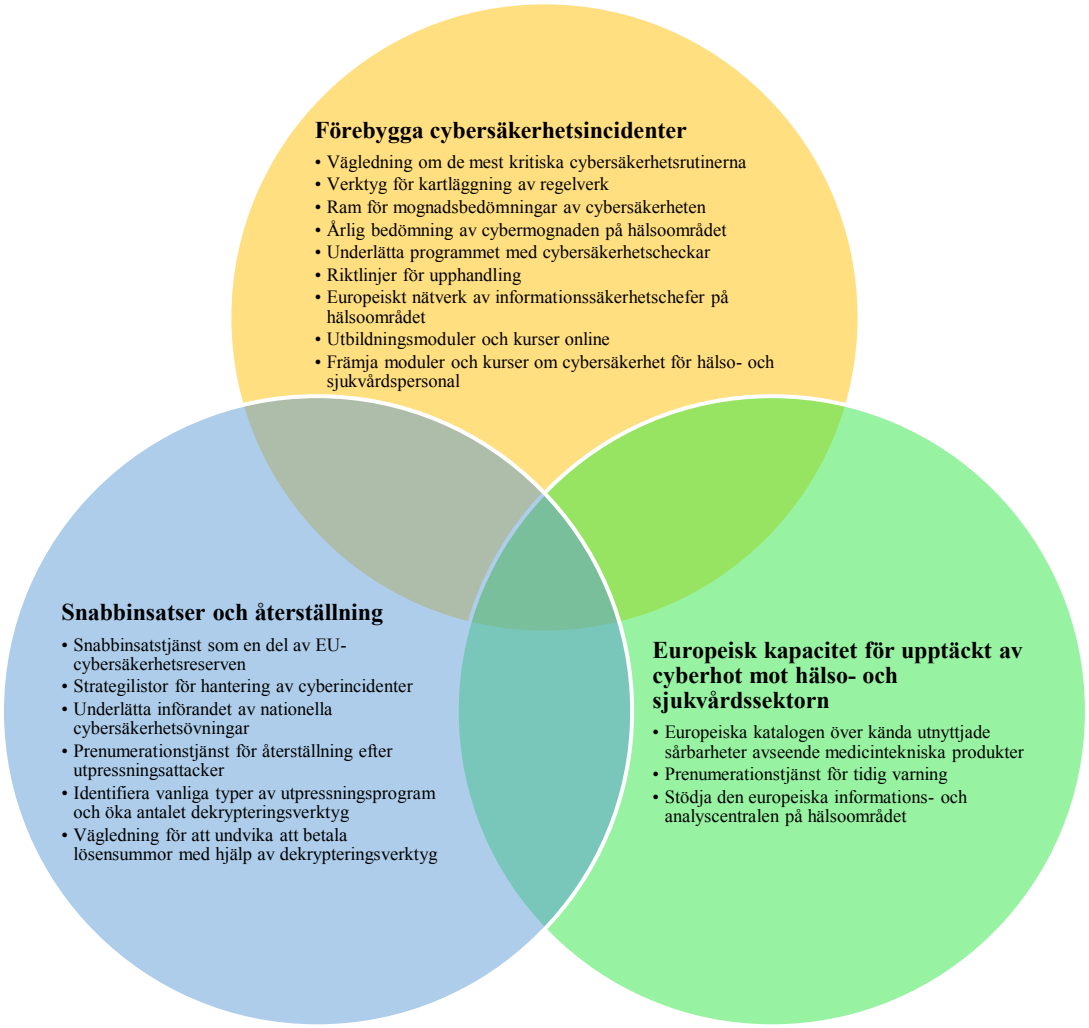

Diagram 1: Koncept för stödcentrumets tjänstekatalog för sjukhus och vårdgivare

3.1. Förebygga cybersäkerhetsincidenter

Enkla åtgärder som ändrar förutsättningarna

Grundläggande cybersäkerhetsåtgärder, såsom att se till att systemen är uppdaterade, hantera säkerhetskopior och införa flerfaktorsautentisering, kan enligt en uppskattning skydda organisationer mot upp till 98 % av attackerna[25]. Många av de mest verkningsfulla it-hygien- och riskhanteringsåtgärderna är relativt enkla att vidta, vilket gör dem till tacksamma mål för att förbättra cybersäkerheten. En av stödcentrumets viktigaste uppgifter bör därför vara att **utarbeta tydlig och riktad vägledning som lyfter fram de mest kritiska cybersäkerhetsrutinerna och hjälper vårdgivarna att genomföra dem**. Detta stöd får inte bara gå till större sjukhus och det måste omfatta skräddarsydd rådgivning för mindre inrättningar, såsom lokala vårdcentraler och specialistkliniker, som ofta saknar resurser för särskilda cybersäkerhetsteam men är lika sårbara för attacker. Det är dessutom nödvändigt att beakta de specifika vårdinrättningarnas regionala betydelse när det gäller att säkerställa patientvården, till exempel i glesbefolkade områden. Forskningsinstitut på hälsoområdet som hanterar stora mängder känsliga personuppgifter skulle också kunna dra nytta av vägledning om grundläggande cybersäkerhetsåtgärder för att förbättra sin resiliens.

Hälso- och sjukvårdsorganisationer omfattas även av en rad cybersäkerhetsrelaterade skyldigheter i EU-lagstiftningen[26]. Även om skyldigheterna är avgörande för att säkerställa ett högt gemensamt utgångsläge för cyber- och datasäkerhet är det även viktigt att se till att lagstiftningen inte är onödigt svår och betungande att navigera i. Ett starkt fokus på efterlevnad bör inte stå i vägen för målet att främja en stark cybersäkerhetskultur. Ett **lättåtkomligt verktyg för kartläggning av regelverk kan hjälpa till att minimera den administrativa bördan för enheter som omfattas av flera lagstiftningsinstrument**. Tillsammans med utarbetandet av vägledning och verktygslådor bör stödcentrumet bedriva ett nära

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

[26] Såsom NIS 2-direktivet, Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element (cyberresiliensförordningen), https://eur-lex.europa.eu/eli/reg/2024/2847/oj/swe, Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, https://eur-lex.europa.eu/eli/reg/2017/745/oj/swe, Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för *in vitro*-diagnostik, https://eur-lex.europa.eu/eli/reg/2017/746/oj/swe, Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän dataskyddsförordning), https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:32016R0679, Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens (förordning om artificiell intelligens), https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:32024R1689, förslag till Europaparlamentets och rådets förordning om ett europeiskt hälsodataområde, COM(2022) 197 final, https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=celex:52022PC0197. Förhandlingarna ledde till en politisk överenskommelse våren 2024. Efter slutförandet förväntas offentliggörandet i *Europeiska unionens officiella tidning* äga rum våren 2025.

samarbete med kommissionen och medlemsstaterna för att utveckla och sprida ett sådant verktyg så snart som möjligt. Stödcentrumet skulle därmed spela en viktig roll för att göra cybersäkerhetsreglerna enkla att förstå och genomföra, till exempel genom att ge vägledning om genomförandet[27] och vid behov främja relevanta standarder.

De kommande **europeiska digitala identitetsplånböckerna** är ett annat verktyg för att underlätta ett enkelt genomförande av god praxis för it-hygien. Att minska beroendet av svaga identifieringsmekanismer, såsom lösenord, är avgörande för att minska riskerna för obehörig åtkomst till hälsodata. En övergång till säkra inloggningslösningar som bygger på tillförlitlig identifiering är av yttersta vikt. EU:s digitala identitetsplånbok erbjuder en harmoniserad, EU-omfattande strategi för elektronisk identifiering för hälso- och sjukvårdspersonal. Denna robusta och enhetliga lösning ska tas i bruk i slutet av 2026. Alla hälsoinformationssystem online som är ålagda att införa stark användarautentisering kommer att vara skyldiga att godta plånboken för identifiering från och med slutet av 2027[28].

Beredskap och riktat stöd

Beredskapstestning, däribland penetrationstestning, är en grundförutsättning för effektiv cybersäkerhet, och kommissionen har redan anslagit medel till Enisa för pilotprojekt för beredskap. Det framgick då att hälso- och sjukvårdssektorn är ett av områdena med störst efterfrågan på tester och ytterligare bedömningar för att identifiera brister beträffande cybersäkerhetsmognaden. I samband med cybersolidaritetsaktens ikraftträdande kommer dessa insatser att öka avsevärt, med Europeiska kompetenscentrumet för cybersäkerhet i spetsen. För att tillgodose detta behov kommer kommissionen, i samråd med samarbetsgruppen för nät- och informationssäkerhet, EU-CyCLONe[29] och Enisa, att fastställa hälso- och sjukvårdssektorn som en sektor som kan ges stöd för **samordnad beredskapstestning** inom ramen för cybersolidaritetsakten. Dessutom bör stödcentrumet utarbeta en **skräddarsydd ram för mognadsbedömningar av cybersäkerheten som är specifik för hälso- och sjukvården**. Sådana mognadsbedömningar skulle ge enheterna agerbara insikter om sina sårbarheter samtidigt som de skulle få möjlighet att visa sin cybersäkerhetsberedskap för patienter och intressenter och därmed bygga upp förtroendet för sina tjänster. På aggregerad nivå bör stödcentrumet genomföra en **årlig mognadsbedömning av cybersäkerheten inom hälso- och sjukvården**, vilken skulle ge en tydlig översikt över hälso- och sjukvårdssektorns cybersäkerhet på både nationell nivå och EU-nivå.

Hälso- och sjukvårdssektorn är starkt beroende av externa uppdragstagare för cybersäkerhetstjänster[30], vilket betonar behovet av riktat stöd för att stärka dess försvar. Med utgångspunkt i framgångsrika initiativ som EU:s innovationscheckar **bör medlemsstaterna överväga riktade åtgärder som cybersäkerhetscheckar för små och medelstora sjukhus och vårdgivare, inklusive mikrosjukhus**

[27] Det är Europeiska dataskyddsstyrelsens ansvar att utarbeta riktlinjer om tolkningen av den allmänna dataskyddsförordningen. Enisas utarbetande av vägledning bör ske i full överensstämmelse med Europeiska dataskyddsstyrelsens befogenheter.
[28] Artikel 5f.1–5f.2 i förordning (EU) 910/2014.
[29] Europeiska kontaktnätverket för cyberkriser.
[30] Se Enisa, *NIS Investments Report 2023* (november 2023), där betydelsen av externt stöd för revision och efterlevnad av cybersäkerhet framhålls. Finns på https://www.enisa.europa.eu/publications/nis-investments-2023.

och mikrovårdgivare. Dessa checkar skulle ge ekonomiskt stöd för införandet av särskilda cybersäkerhetsåtgärder. Prioriteringen av tilldelningen av checkar bör motiveras av resultaten av beredskapstester och mognadsbedömningar.

Lokala kunskaper och sammanhang är avgörande för ett effektivt införande av checkar eller andra stödprogram och säkerställer relevans och tillgänglighet. EU-fonder, såsom Europeiska regionala utvecklingsfonden, är redan aktiva när det gäller att stödja initiativ inom cybersäkerhet och e-hälsa och skulle därför kunna fungera som ett verktyg för att utveckla program för cybersäkerhetscheckar riktade till vårdgivare. För att driva på denna insats skulle stödcentrumet samarbeta med medlemsstaterna och regionala programmyndigheter för att stödja utvecklingen av sådana regionala checkprogram, med utgångspunkt i lärdomar från befintliga nationella projekt samt åtgärder som finansieras inom programmet för ett digitalt Europa i syfte att säkerställa ett praktiskt och effektivt genomförande.

Vidare har Horisont-programmen sedan 2014 varit avgörande för att finansiera en rad forskningsinitiativ som inriktas på att förbättra sjukhusens och andra sjukvårdsinrättningars resiliens mot cyberhot samt minska riskerna i samband med missbruk av ny teknik. Detta har resulterat i en rad specialiserade verktyg, ramar och system, såsom riskbedömningsverktyg, integritetsbevarande plattformar för datadelning, kryptografiska lösningar, utbildningsprogram för cybersäkerhetsmedvetenhet och system för att upptäcka hot i realtid. Dessa lösningar har validerats noggrant genom verkliga pilotprojekt i hälso- och sjukvårdsmiljöer, vilket säkerställer att de är effektiva och praktiskt tillämpbara när det gäller att skydda mot cyberhot.

Trygga leveranskedjorna för hälso- och sjukvård

En viktig utmaning för hälso- och sjukvårdsorganisationer är hanteringen av komplexa IKT-leveranskedjor, vilka omfattar en rad produkter såsom uppkopplade medicintekniska produkter, elektroniska patientjournalsystem och kontorshårdvara. Sjukhus och vårdgivare behöver tillförlitliga och säkra IKT-system och IKT-tjänster för sin verksamhet. För att hjälpa till att hantera cybersäkerhetsutmaningar inom hälso- och sjukvårdssektorn bör samarbetsgruppen för nät- och informationssäkerhet utföra en **samordnad säkerhetsriskbedömning, med beaktande av både tekniska och strategiska risker kopplade till leveranskedjor för medicintekniska produkter och med förslag till riskreducerande åtgärder**[31]. Samarbetsgruppen för nät- och informationssäkerhet bör vid behov samarbeta med samordningsgruppen för medicintekniska produkter.

Cyberresiliensförordningen är ett nytt, omfattande regelverk med cybersäkerhetskrav för planering, utformning, utveckling samt hantering, korrigering och rapportering av aktivt utnyttjade sårbarheter rörande nästan alla hårdvaru- och programvaruprodukter i varje steg av värdekedjan[32]. Medicintekniska

[31] Enligt artikel 22 i NIS 2-direktivet.

[32] I ett första steg, från och med den 1 augusti 2025, kommer breda kategorier av radioutrustning som inte omfattas av förordningen om medicintekniska produkter och förordningen om medicintekniska produkter för *in vitro*-diagnostik att behöva uppfylla de grundläggande kraven i radioutrustningsdirektivet som rör cybersäkerhet när dessa produkter släpps ut på den inre marknaden. I ett andra steg, från och med den 11 december 2027, kommer cyberresiliensförordningen att börja tillämpas.

produkter är en typ av produkt som används inom ett av de känsligaste områdena i vårt samhälle. Cybersäkerhetskraven för dessa produkter härrör från de befintliga förordningarna om medicintekniska produkter respektive om medicintekniska produkter för *in vitro*-diagnostik[33]. Under den pågående utvärderingen av dessa förordningar undersöks möjligheterna till större samstämmighet och synergieffekter mellan dessa ramar för att garantera förenkling och de senaste cybersäkerhetslösningarna.

Vidare bör resultaten av riskbedömningen hjälpa hälso- och sjukvårdsorganisationer att se över sina cybersäkerhetsrutiner för leveranskedjan i enlighet med NIS 2-direktivet, och resultaten skulle även kunna ligga till grund för utarbetandet av nya **riktlinjer för upphandling**[34]. Dessa riktlinjer, som utarbetas av Enisa genom dess stödcentrum, bör återspegla den senaste tidens trender, såsom övergången till molntjänster för lagring av patientuppgifter, inklusive behovet av säker migrering av elektroniska hälsodata till molnmiljöer. Dessutom bör de nya riktlinjerna erbjuda praktiska verktyg som hjälper organisationer att bevaka sina leveranskedjor, däribland leverantörer av utlokaliserade säkerhetstjänster, attesteringsrapporter eller riskbedömningar av tredje parter.

För molnet krävs ytterligare åtgärder för att ta itu med de unika utmaningarna med att hantera känsliga hälso- och sjukvårdsuppgifter, inklusive åtgärder för ökad säkerhet och integritet samt för att hantera operativa risker. För att stärka skyddet rekommenderar experter att säkerhet som standard och inbyggd säkerhet integreras i molntjänsterna. Denna strategi prioriterar säker infrastruktur, proaktiv sårbarhetshantering och en kombination av statliga och privata molnlösningar. Kontinuerlig övervakning och leverantörsspecifika intyg, såsom certifieringar av säkerhetsleverantörer och revisioner för att kontrollera efterlevnaden av nationella och internationella standarder, är också avgörande för att säkerställa robusta säkerhetsrutiner.

För tjänster som infrastruktur som en tjänst, plattform som en tjänst och program som nättjänst är det ofta upp till kunden att vidta säkerhetsåtgärder. Många hälso- och sjukvårdsorganisationer saknar dock resurser att på egen hand uppfylla dessa krav. För att komma till rätta med detta **bör leverantörer av molntjänster uppmuntras att vidta grundläggande säkerhetsåtgärder som en standardfunktion**. Dessa åtgärder skulle minska risken för felkonfigurering, upprätthålla ett konsekvent skydd i alla kundhanterade miljöer och ge användarna större säkerhet. Införandet av en standardsäkerhetsgrund skulle syfta till att balansera ett robust skydd med praktisk genomförbarhet samt säkerställa användbarhet för en mängd olika hälso- och sjukvårdsorganisationer. Denna insats skulle omfatta ett nära samarbete mellan molnleverantörer och hälso- och sjukvårdssektorn och utnyttja branschens bästa praxis för att skapa effektiva och skalbara lösningar.

[33] I december 2019 utfärdade samordningsgruppen för medicintekniska produkter vägledning om cybersäkerhet för medicintekniska produkter för att hjälpa tillverkarna att uppfylla kraven i bilaga I till de båda förordningarna: https://ec.europa.eu/docsroom/documents/41863.

[34] Med utgångspunkt i Enisas upphandlingsriktlinjer för cybersäkerhet på sjukhus från 2020 (*Procurement Guidelines for Cybersecurity in Hospitals*, februari 2020). Finns på https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

Utbildning och kompetensutveckling

Att ha en arbetskraft med efterfrågad kompetens är viktigt för långsiktig hållbar tillväxt och konkurrenskraft i EU samt för högkvalitativa tjänster, inklusive hälso- och sjukvårdstjänster. Bristen på kvalificerade cybersäkerhetsspecialister är ett stort problem i hela EU. Uppskattningsvis saknas 299 000 yrkesverksamma inom cybersäkerhet för att tillfredsställa arbetskraftsbehoven i EU[35]. Enligt 2024 års Eurobarometerundersökning om cyberkompetens[36] ser 81 % av företagen svårigheter med att anställa cybersäkerhetspersonal som en central risk för potentiella cyberattacker. Inom sektorerna utbildning, hälsa och socialt arbete innehas 66 % av cybersäkerhetsrollerna av personer utan tidigare erfarenhet inom cybersäkerhet, vilket visar på ett brådskande behov av omskolning och kompetenshöjning.

För att åtgärda detta problem bör stödcentrumet samarbeta med det framtida Edic-konsortium för cyberkompetens (europeiskt konsortium för digital infrastruktur) som planeras i kommissionens meddelande om EU-akademin för cyberkompetens[37]. Arbetet bör underlätta utbyten mellan cybersäkerhetspersonal inom hälso- och sjukvårdssektorn, däribland informationssäkerhetschefer. En möjlig åtgärd skulle vara att skapa ett **europeiskt nätverk av informationssäkerhetschefer på hälsoområdet**, med utgångspunkt i en expertpool för att dela och utveckla bästa praxis, strategier för att behålla talanger samt lösningar för att locka cybersäkerhetsspecialister till hälso- och sjukvårdssektorn. Dessutom bör resurser utvecklas inom ramen för EU-akademin för cyberkompetens för att öka kompetensen hos cybersäkerhetsanställda inom hälso- och sjukvårdssektorn med stöd av branschen och den akademiska världen. I detta avseende bör branschaktörer uppmuntras att utlova stöd för att förbättra cybersäkerhetsutbildningen.

Mänskliga misstag fortsätter att vara en viktig bidragande faktor till cybersäkerhetsincidenter inom hälso- och sjukvården, vilket understryker det kritiska behovet av att utbilda och öka medvetenheten hos personalen. Hälso- och sjukvårdspersonalen använder regelbundet digitala verktyg, och det är därför viktigt att de får kunskap om säker praxis. Riktade utbildnings- och informationskampanjer kan minska riskerna avsevärt. Mot denna bakgrund bör stödcentrumet samarbeta med hälso- och sjukvårdspersonal och vårdgivare samt med utbildningsanordnare, branschen, Edic-konsortiet för cyberkompetens och medlemsstaternas myndigheter för att skapa och sprida **omfattande och lättillgängliga utbildningsmoduler och kurser online**.

Att införliva moduler om digital kompetens och cybersäkerhet i läroplanerna är avgörande för att bygga upp en stark cybersäkerhetsgrund inom hälso- och sjukvården. Dessa moduler bör behandla sektorsspecifika frågor såsom skydd av patientuppgifter och sårbarheter i fråga om säkerheten hos medicintekniska produkter. Utvecklingen av dessa resurser bör ta hänsyn till tidigare insatser, såsom

[35] *The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study* | Plattformen för digital kompetens och digitala arbetstillfällen.
[36] Flash Eurobarometer 547 om cyberkompetens.
[37] Meddelande från kommissionen till Europaparlamentet och rådet: *Minska kompetensbristen på cybersäkerhetsområdet för att främja EU:s konkurrenskraft, tillväxt och resiliens (EU-akademin för cyberkompetens)*, COM(2023) 207 final.

BeWell-projektet som finansieras genom Erasmus+-programmet[38] och Panacea-projektet som finansieras genom Horisont 2020[39].

3.2. Europeisk kapacitet för upptäckt av cyberhot mot hälso- och sjukvårdssektorn

Effektiv upptäckt av cyberhot är avgörande för snabba insatser vid incidenter. Fientliga aktörer kan använda metoder för att göra det svårt att upptäcka intrång, vilket möjliggör längre perioder av obehörig åtkomst till ett system[40]. En bättre förmåga att upptäcka hot kan därför bidra till att stoppa cyberattacker. I en utpressningsattack mot den finska leverantören av psykoterapitjänster Vastaamo, där gärningsmannen utpressade patienter vars konfidentiella patientjournaler hade stulits, skedde till exempel det första intrånget 2018, men kom till leverantörens kännedom först 2020[41].

Ett effektivt informationsutbyte och samarbete är avgörande för att öka hotidentifieringen och situationsmedvetenheten i hela EU. Enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter) spelar en viktig roll när det gäller att ta emot rapporter om incidenter, tillbud och potentiella hot, och ger vägledning om riskreducerande åtgärder på nationell nivå. **Medlemsstaterna uppmanas dock starkt att även dela alla rapporter om cyberincidenter från sjukhus och vårdgivare med Enisas stödcentrum för att möjliggöra situationsmedvetenhet i EU**. Detta bör helst inbegripa en meningsfull karakterisering av olika relevanta dimensioner av incidenten, däribland kända bakomliggande sårbarheter samt effekter på hälso- och sjukvårdstjänsterna och patienterna. Dessutom uppmuntras tillverkare av medicintekniska produkter, inklusive medicintekniska produkter för *in vitro*-diagnostik, att, via den gemensamma rapporteringsplattform som ska inrättas och skötas av Enisa inom ramen för cyberresiliensförordningen, frivilligt rapportera aktivt utnyttjade sårbarheter eller allvarliga cyberincidenter som påverkar dessa produkters säkerhet samt eventuella andra sårbarheter, incidenter, tillbud eller cyberhot som kan påverka dessa produkters riskprofil.

Om informationen i rapporterna inte längre är känslig kan stödcentrumet bygga upp en Enisa-sponsrad europeisk katalog över kända utnyttjade sårbarheter avseende medicintekniska produkter, elektroniska patientjournalsystem och leverantörer av IKT-utrustning och IKT-programvara på hälsoområdet. För att ta itu med betydande utmaningar när det gäller att upptäcka hot bör stödcentrumet införa **en EU-omfattande prenumerationstjänst för tidig varning för hälso- och sjukvårdssektorn med varningar i nära realtid**. Denna tjänst skulle bygga på behandlade uppgifter från CSIRT-enheter, vårdinrättningar och tillverkare, underrättelseinhämtning genom öppna källor och andra berörda aktörer såsom cybernav, informations- och analyscentraler och brottsbekämpande myndigheter. Ett fördjupat samarbete mellan Enisa och Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol)

[38] BeWell – *Blueprint alliance for a future health workforce strategy on digital and green skills*. Finns på 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*. Finns på https://cordis.europa.eu/project/id/826293.
[40] Enisa, *Health Threat Landscape 2023*.
[41] Beslut 1150/161/2021 av den finska dataombudsmannen.

– till exempel om mönster för it-brottslighet riktad mot hälso- och sjukvårdssektorn – skulle ytterligare öka situationsmedvetenheten.

Informations- och analyscentraler fungerar som centrala resurser för underrättelser om cyberhot. De verkar för informationsutbyte i båda riktningarna mellan den offentliga och den privata sektorn och främjar förtroendeskapande. Stödcentrumet bör intensifiera stödet till den **europeiska informations- och analyscentralen på hälsoområdet** genom verktyg och informationsutbyte, sektorsspecifika rapporter om situationsmedvetenheten samt främjande av en tillförlitlig gemenskap för taktiskt och strategiskt samarbete. Medlemsstaterna bör uppmuntra utvecklingen av nationella informations- och analyscentraler[42]. Informations- och analyscentralerna bör i sin tur uppmuntras att skapa kontakter mellan vårdgivare och tillverkare för att bidra till en gemensam förståelse av cybersäkerhetshot, även i leveranskedjan, samt verka för en dialog om säker produktutformning som verkligen tar hänsyn till den faktiska användningen i praktiken.

3.3.Snabbinsatser och återställning

Med tanke på den höga känsligheten hos patienters hälsodata och de potentiellt förödande effekterna av cyberattacker på hälso- och sjukvårdstjänster är ett snabbt och effektivt svar på cybersäkerhetsincidenter avgörande för att skydda patientsäkerheten. När ett sjukhus eller en vårdgivare utsätts för en cyberattack är den första kontaktpunkten den relevanta nationella CSIRT-enheten[43]. CSIRT-enheten ansvarar för att tillhandahålla snabbt stöd, helst inom 24 timmar, för att hjälpa till att hantera större incidenter. Om en incident överskrider CSIRT-enhetens kapacitet bör dock EU-stöd finnas tillgängligt för att säkerställa snabba och effektiva insatser.

EU-cybersäkerhetsreserven, som inrättades genom cybersolidaritetsakten, tillhandahåller incidenthanteringstjänster från betrodda leverantörer av utlokaliserade säkerhetstjänster för att bistå vid betydande eller storskaliga cyberincidenter och de initiala återställningsinsatserna. Denna reserv är utformad för att komplettera insatserna från medlemsstaternas CSIRT-enheter så att de kan begära ytterligare stöd i ärenden som rör kritiska sektorer som hälso- och sjukvård. För att förbättra detta system **bör kommissionen och Enisa se till att reserven inbegriper en specifik snabbinsatstjänst för hälso- och sjukvårdssektorn**. Som komplement till andra befintliga regelverk skulle denna tjänst utan dröjsmål utplacera experter för att hantera betydande eller storskaliga cyberincidenter inom hälso- och sjukvården när det nationella stödet inte är tillräckligt.

För att förbättra insatserna och återställningen bör stödcentrumet, i samarbete med samarbetsgruppen för nät- och informationssäkerhet, CSIRT-nätverket och, i förekommande fall, Europol, utarbeta **hälso- och**

[42] Finland har till exempel en nationell informations- och analyscentral (ISAC) för social- och hälsovårdssektorn. Se Finlands nationella cybersäkerhetscenter: *ISAC-grupper för utbyte av information*. Finns på https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/isac-grupper-utbyte-av-information.

[43] Enligt artikel 23.1 i NIS 2-direktivet ska väsentliga och viktiga entiteter underrätta sin CSIRT-enhet eller, i tillämpliga fall, sin behöriga myndighet om betydande incidenter.

sjukvårdsspecifika strategilistor för hantering av cyberincidenter. Dessa strategilistor skulle hjälpa både CSIRT-enheterna och hälso- och sjukvårdsorganisationerna att bemöta specifika cybersäkerhetshot, inklusive utpressningsprogram. Med tanke på vikten av ett effektivt samarbete mellan CSIRT-enheterna och de brottsbekämpande myndigheterna för att hantera och utreda brottsliga cybersäkerhetsincidenter bör strategilistorna bland annat ge tydlig vägledning om rapporteringen av sådana incidenter till brottsbekämpande myndigheter. Stödcentrumet skulle dessutom kunna **underlätta ett omfattande införande av nationella cybersäkerhetsövningar, baserat på erfarenheter från övningar som Enisas ”Cyber Europe 2022”-övning, för att testa strategilistorna och stärka rutinerna för incidenthantering**.

För att fatta informerade politiska beslut och bedöma effektiviteten hos de åtgärder som vidtagits mot utpressningsattacker är det nödvändigt att samla in ytterligare data. Medlemsstaterna bör därför begära att enheter som omfattas av NIS 2-direktivet, däribland hälso- och sjukvårdsorganisationer, rapporterar om eventuella lösensummor som de betalat eller avser att betala, tillsammans med annan information som de tillhandahåller när de rapporterar om betydande cybersäkerhetsincidenter. Sådan rapportering stöder en effektiv utredning av incidenter som involverar utpressningsprogram, inbegripet spårning av betalningar på växelplattformar för kryptovalutor för att identifiera mottagarna.

Återställningshastigheten är en avgörande faktor för att upprätthålla resiliensen och allmänhetens förtroende, särskilt inom hälso- och sjukvården, där verksamhetsstopp kan störa patientvården. För en effektiv återställning efter utpressningsattacker måste vårdgivarna ha säkra, uppdaterade och isolerade säkerhetskopior som snabbt kan återställas. Som en del av sin tjänstekatalog skulle stödcentrumet kunna erbjuda **en prenumerationstjänst för återställning efter utpressningsattacker som hjälper sjukhus och vårdgivare att på förhand utarbeta återställningsplaner**. Enisa och Europol bör tillsammans identifiera de vanligaste typerna av utpressningsprogram som riktar in sig på hälso- och sjukvårdsorganisationer och **öka antalet dekrypteringsverktyg** som finns tillgängliga genom projektet No More Ransom[44]. De bör också utarbeta och lyfta fram lättillgänglig vägledning för att hjälpa vårdgivare att undvika att betala lösensummor genom användning av dekrypteringsverktyg.

International Counter Ransomware Initiative[45] är ett värdefullt forum för utbyte kring specifika utpressningsincidenter samt för att förbättra medlemsstaternas förmåga att stärka sina cybersäkerhetsramar och sin kapacitet att utreda brott som begås med utpressningsprogram. Kommissionen kommer, i samarbete med den höga representanten, att fortsätta att främja samarbetet inom ramen för International Counter Ransomware Initiative, bland annat mot utpressningshot riktade mot hälso- och sjukvårdssektorn. Dessutom kommer kommissionen att söka samarbete i **G7-arbetsgruppen för cybersäkerhet** för att stärka cybersäkerheten inom hälso- och sjukvårdssektorn. Arbetsgruppen skulle särskilt kunna överväga möjligheter att stödja hälso- och sjukvårdssektorn mot hot såsom utpressningsprogram, med utgångspunkt i reflektioner såsom det gemensamma uttalandet om

[44] https://www.nomoreransom.org/sv/index.html.
[45] https://www.counter-ransomware.org/.

utpressningsattacker mot vårdinrättningar av den 8 november 2024, som lades fram för FN:s säkerhetsråd[46].

4. Nationella åtgärder

Handlingsplanens kapacitet att förbättra cybersäkerheten inom hälso- och sjukvårdssektorn är beroende av medlemsstaternas aktiva deltagande och engagemang. För att framgångsrikt genomföra handlingsplanen skulle medlemsstaterna kunna utse **nationella stödcentrum för cybersäkerhet som riktar sig särskilt till sjukhus och vårdgivare**. Dessa centrum skulle fungera som de främsta kontaktpunkterna för hälso- och sjukvårdssektorn på nationell nivå och bedriva ett nära samarbete med Enisas stödcentrum. När så är möjligt och relevant bör medlemsstaterna utse befintliga organ till nationella stödcentrum för cybersäkerhet, såsom nationella CSIRT-enheter på hälsoområdet eller relevanta myndigheter.

Medlemsstaterna uppmanas också att utarbeta **nationella handlingsplaner för cybersäkerhet inom hälso- och sjukvårdssektorn**. Dessa planer skulle innehålla en beskrivning av de specifika cybersäkerhetsrisker som hälso- och sjukvårdssystemen står inför och de nationella åtgärder som vidtas för att hantera dem, samtidigt som det säkerställs att resurser och praxis på EU-nivå används på ett effektivt sätt. Enisas stödcentrum kan bidra till utarbetandet av dessa planer, med beaktande av redan befintliga nationella planer, och samordna insatserna för att se till att enskilda medlemsstaters resurser och strategier kompletterar varandra.

Ett annat viktigt fokus för medlemsstaterna är att underlätta resursdelning mellan vårdgivare, vilket kan uppnås genom **gemensam upphandling eller samlade resurser** på nationell eller regional nivå eller till och med på EU-nivå. Detta tillvägagångssätt skulle minska den ekonomiska bördan för enskilda enheter och samtidigt förbättra deras förhandlingsposition i förhållande till leverantörer av cybersäkerhetstjänster.

Det franska CaRE-programmet[47] har till exempel infört ett antal åtgärder på nationell och regional nivå för att ta itu med svårigheterna med att anskaffa resurser. En cyberkatalog ger en översikt över digitala lösningar och paket som görs tillgängliga för sjukhus via den nationella cybersäkerhetsmyndigheten, myndigheten för digital hälsa, regionala myndigheter, nationella inköpsorganisationer samt kommersiella lösningar. Denna kompletteras med ytterligare finansiering för regionala myndigheter för att erbjuda delade resurser.

[46] https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/.
[47] Franska myndigheten för digital hälsa (*Agence du Numérique en Santé*): *Cybersécurité acceleration et Résilience des Établissements* (CaRE). Finns på https://esante.gouv.fr/strategie-nationale/cybersecurite.

Medlemsstaterna bör även komma till rätta med de otillräckliga investeringarna i cybersäkerhet inom hälso- och sjukvårdssektorn. För att säkerställa tillräcklig finansiering bör de fastställa **icke-bindande riktmärken och övervaka finansieringsmål som är särskilt inriktade på cybersäkerhet**, samtidigt som de säkerställer att dessa investeringar inte försämrar den grundläggande patientvården. Dessa finansieringsmål bör också syfta till att integrera säkerhetsöverväganden i alla digitala investeringar i sektorn. Medlemsstaterna kan utbyta bästa praxis och råd om dessa mål via plattformar såsom nätverket för e-hälsa[48].

5. Samarbete mellan den offentliga och den privata sektorn

Offentlig-privat samarbete och samråd med vårdgivare, andra enheter inom hälso- och sjukvårdssektorn samt berörda aktörer inom cybersäkerhetsbranschen är avgörande för att handlingsplanen ska kunna genomföras. För att ytterligare bidra till stödcentrumets arbete **kommer kommissionen, med stöd av Enisa, att inrätta ett gemensamt rådgivande organ för cybersäkerhet på hälsoområdet** med företrädare på hög nivå från både hälso- och sjukvårdssektorn och cybersäkerhetsbranschen. Detta organ kommer att bistå kommissionen och stödcentrumet med rådgivning om verkningsfulla åtgärder och diskutera vidareutvecklingen av offentlig-privata partnerskap på detta område. Organet kommer att bygga vidare på befintliga insatser för offentlig-privata partnerskap, inklusive den europeiska informations- och analyscentralen på hälsoområdet.

Vidare kommer kommissionen att utlysa **en ansökningsomgång** där cybersäkerhetsföretag, stiftelser, utbildningsinstitutioner och branschaktörer kan **göra utfästelser om åtgärder för att ta itu med utmaningarna inom sektorn**. Med utgångspunkt i erfarenheterna från EU-akademin för cyberkompetens skulle det till exempel kunna handla om utfästelser inom ramen för akademin om att erbjuda kurser och utbildningsmaterial med inriktning på hälso- och sjukvårdssektorn för cybersäkerhetsspecialister[49]. Andra åtaganden skulle även kunna omfatta medvetandehöjande verksamhet eller tillhandahållande av utlokaliserade säkerhetstjänster för särskilt sårbara enheter, antingen kostnadsfritt eller till en lägre kostnad, för att öka deras beredskap och cybersäkerhetsresiliens. Åtagandena skulle dessutom kunna bestå i att dela underrättelser om cyberhot med Enisas stödcentrum. Stödcentrumet bör ha en översikt över de utfästelser som görs inom ramen för ansökningsomgången, i syfte att säkerställa deras samstämmighet och komplementaritet.

6. Avskräcka cyberhotande aktörer

EU:s interna och externa cybersäkerhetspolitik bör stödja målet att avskräcka cyberhotande aktörer från att angripa europeiska hälso- och sjukvårdssystem. Cyberattacker mot hälso- och sjukvårdsorganisationer är en särskilt oacceptabel typ av skadlig cyberverksamhet, med tanke på deras förmåga att hota patientsäkerheten och människoliv. Därför bör EU:s avskräckande kapacitet på området cybersäkerhet och brottsbekämpning användas med full kraft för att undergräva den övergripande

[48] Nätverket för e-hälsa är ett frivilligt nätverk av nationella myndigheter med ansvar för e-hälsa, som medlemsstaterna har utsett och inrättat i enlighet med artikel 14 i direktiv 2011/24/EU.

[49] *Cyber Skills Academy - Get Involved* | Plattformen för digital kompetens och digitala arbetstillfällen.

affärsmodellen för fientliga aktörer som angriper hälso- och sjukvårdssektorn och för att beröva dem lätta vinster. Detta inbegriper främjande av gränsöverskridande utredningar genom ökat utbyte av angreppsindikatorer och andra relevanta uppgifter samt ett större fokus på mål med högt värde och centrala kriminella mellanhänder, däribland så kallad bulletproof hosting eller mixertjänster avseende kryptovalutor.

Verktygslådan för cyberdiplomati erbjuder en ram för att förebygga, avskräcka från och bemöta cyberattacker mot EU, medlemsstaterna och deras partner. Den höga representanten kommer att fortsätta att använda den befintliga ramen för cybersanktioner för att bemöta hot mot hälso- och sjukvårdssystemen.

Att hålla kriminella aktörer ansvariga för sina handlingar är ett viktigt avskräckande medel. Medlemsstaterna bör därför se till att brottsbekämpning till fullo integreras i deras nationella handlingsplaner. De bör särskilt dra full nytta av bestämmelserna i direktivet om angrepp mot informationssystem[50] och Europarådets Budapestkonvention om it-relaterad brottslighet för att avskräcka från angrepp, ställa brottslingar inför rätta och avveckla kriminella infrastrukturer som underlättar angrepp[51]. Ett framgångsrikt genomförande av dessa verktyg bör säkerställa att brottsliga och illvilliga handlingar mot hälso- och sjukvården bestraffas.

7. Genomförande och övervakning av handlingsplanen

I denna handlingsplan har ett antal uppgifter planerats för ett stödcentrum som ska inrättas inom Enisa. Detta säkerställer ett övergripande och konsekvent genomförande av handlingsplanen, samtidigt som man undviker skapandet av nya enheter som leder till potentiella överlappningar och allmänna omkostnader. Kommissionen avser att se till att stödcentrumet får lämpliga resurser.

När stödcentrumet är operativt bör Enisa, i samråd med kommissionen, regelbundet tillhandahålla uppdateringar om stödcentrumets arbete till Enisas styrelse samt berörda nätverk av medlemsstater, särskilt samarbetsgruppen för nät- och informationssäkerhet, CSIRT-nätverket, nätverket för e-hälsa och, i tillämpliga fall, styrelsen för det europeiska hälsodataområdet. Dessutom bör Enisa ha ett kontinuerligt utbyte med det offentlig-privata rådgivande organet för cybersäkerhet på hälsoområdet om genomförandet av stödcentrumets åtgärder.

Enisas regelbundna rapporter, såsom rapporten om cybersäkerhetssituationen i unionen, vilken ger en aggregerad bedömning av mognadsnivån på cybersäkerhetskapaciteten och cybersäkerhetsresurserna i hela EU, bland annat inom hälso- och sjukvårdssektorn, bör fungera som tillfällen att offentliggöra relevanta uppgifter och därmed stödja övervakningen av handlingsplanen. Dessutom kan Enisas

[50] Europaparlamentets och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF: https://eur-lex.europa.eu/eli/dir/2013/40/oj/swe.
[51] Konventionen om it-relaterad brottslighet (Budapestkonventionen, ETS nr 185) och dess protokoll: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

cybersäkerhetsindex för EU[52] tillhandahålla kvantitativa och kvalitativa uppgifter och därmed fungera som en evidensbas för att bedöma hälso- och sjukvårdssektorns kritikalitet och mognad.

8. Nästa steg

I detta meddelande fastställs en ambitiös agenda för en mer cybersäker hälso- och sjukvårdssektor i EU. I handlingsplanen föreslås utvecklingen av ett stödcentrum för cybersäkerhet för sjukhus och vårdgivare inom ramen för Enisa och därigenom en väg mot att skapa en enhetlig och gemensam europeisk strategi för cybersäkerhetsutmaningen i sektorn.

Detta meddelande bör ses som början på en process för att förbättra cybersäkerheten inom hälso- och sjukvårdssektorn. Antagandet av handlingsplanen kommer därför att åtföljas av omfattande samråd med berörda parter och fortsatta utbyten med medlemsstaterna och berörda nätverk för att samla in synpunkter. På grundval av resultaten av samråden avser kommissionen att lägga fram rekommendationer under fjärde kvartalet 2025 för att ytterligare finjustera handlingsplanen.

Kommissionen uppmanar medlemsstaterna och alla berörda parter att arbeta tillsammans för att förverkliga handlingsplanens ambition.

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

Bilaga – Översikt över föreslagna åtgärder

Kommissionen:

Enisas stödcentrum för cybersäkerhet för sjukhus och vårdgivare	
Säkerställa lämpliga resurser för stödcentrumet för cybersäkerhet Arbeta med Europeiska kompetenscentrumet för cybersäkerhet för att lansera pilotprojekt i syfte att utveckla bästa praxis för bedömning av it-hygien och cybersäkerhetsrisker och tillgodose behovet av kontinuerlig cybersäkerhetsövervakning, underrättelser om hot och hantering av incidenter med hjälp av de senaste cybersäkerhetslösningarna, för utvecklingen av stödcentrumets tjänstekatalog	2025
Förebygga cybersäkerhetsincidenter	
I samråd med samarbetsgruppen för nät- och informationssäkerhet, EU-CyCLONe och Enisa, undersöka möjligheten att fastställa hälso- och sjukvårdssektorn som en sektor som kan ges stöd för samordnad beredskapstestning inom ramen för cybersolidaritetsakten	Första kvartalet 2025
Snabbinsatser och återställning	
Tillsammans med Enisa, se till att EU-cybersäkerhetsreserven inbegriper en specifik snabbinsatstjänst för hälso- och sjukvårdssektorn	Fjärde kvartalet 2025
Samarbete mellan den offentliga och den privata sektorn	
Med stöd av Enisa, inrätta ett gemensamt rådgivande organ för cybersäkerhet på hälsoområdet	Första kvartalet 2025
Utlysa en ansökningsomgång där cybersäkerhetsföretag, stiftelser, utbildningsinstitutioner och branschaktörer kan göra utfästelser om åtgärder för att ta itu med utmaningarna inom hälso- och sjukvårdssektorn	Andra kvartalet 2025
Avskräcka cyberhotande aktörer	
Tillsammans med den höga representanten undersöka användningen av åtgärder i verktygslådan för cyberdiplomati för att förebygga, avskräcka från,	2025

motverka och bemöta fientlig verksamhet riktad mot hälso- och sjukvårdssystemen	
Främja internationellt samarbete mot aktörer bakom utpressningsprogram, särskilt inom det internationella initiativet för att motverka utpressningsprogram, i samarbete med den höga representanten	2025–2026
Söka samarbete i G7-arbetsgruppen för cybersäkerhet för att stärka cybersäkerheten inom hälso- och sjukvårdssektorn	2025–2026
Nästa steg	
Inleda omfattande samråd med berörda parter	Första kvartalet 2025
Anta rekommendationer för att ytterligare finjustera handlingsplanen	Fjärde kvartalet 2025

Enisa:

Europeiskt stödcentrum för cybersäkerhet för sjukhus och vårdgivare	
Börja arbetet med att inrätta ett europeiskt stödcentrum för cybersäkerhet för sjukhus och vårdgivare	Andra kvartalet 2025
Ta fram en omfattande tjänstekatalog som ska tillhandahållas av stödcentrumet för cybersäkerhet	Från och med fjärde kvartalet 2025
Förebygga cybersäkerhetsincidenter	
Utfärda vägledning som lyfter fram de mest kritiska cybersäkerhetsrutinerna och hjälper vårdgivarna att genomföra dem	Tredje kvartalet 2025
Utveckla ett verktyg för kartläggning av regelverk, i nära samarbete med kommissionen och medlemsstaterna	Första kvartalet 2025
Ta fram en ram för mognadsbedömningar av cybersäkerheten som är specifik för hälso- och sjukvården	Tredje kvartalet 2025
Utföra en årlig mognadsbedömning av cybersäkerheten inom hälso- och sjukvården	2025–2026

Samarbeta med medlemsstaterna och regionala programmyndigheter för att skapa pilotprogram för cybersäkerhetscheckar	2025–2026
Utarbeta nya upphandlingsriktlinjer för cybersäkerhet för sjukhus och vårdgivare	Tredje kvartalet 2025
Skapa ett europeiskt nätverk av informationssäkerhetschefer på hälsoområdet	Första kvartalet 2026
Utforma och synliggöra utbildningsmoduler och kurser om cybersäkerhet för hälso- och sjukvårdspersonal	Första kvartalet 2026
Europeisk kapacitet för upptäckt av cyberhot mot hälso- och sjukvårdssektorn	
Skapa en europeisk katalog över kända utnyttjade sårbarheter avseende medicintekniska produkter, elektroniska patientjournalsystem och leverantörer av IKT-utrustning och IKT-programvara på hälsoområdet	Fjärde kvartalet 2025
Införa en EU-omfattande prenumerationstjänst för tidig varning för hälso- och sjukvårdssektorn	Från och med 2026
Bistå den europeiska informations- och analyscentralen på hälsoområdet med verktyg och informationsutbyte	2025–2026
Snabbinsatser och återställning	
Tillsammans med kommissionen se till att EU-cybersäkerhetsreserven inbegriper en specifik snabbinsatstjänst för hälso- och sjukvårdssektorn	Fjärde kvartalet 2025
I samarbete med CSIRT-nätverket, utarbeta hälso- och sjukvårdsspecifika strategilistor för hantering av cyberincidenter	Tredje kvartalet 2025
Underlätta ett brett införande av nationella cybersäkerhetsövningar för att testa strategilistorna och stärka rutinerna för incidenthantering	Från och med fjärde kvartalet 2025
Tillhandahålla en prenumerationstjänst för återställning efter attacker från utpressningsprogram	Från och med 2026
Tillsammans med Europol identifiera de vanligaste typerna av utpressningsprogram som riktar in sig på hälso- och sjukvårdsorganisationer och öka antalet dekrypteringsverktyg genom projektet No More Ransom	Fjärde kvartalet 2025

Tillsammans med Europol utarbeta lättillgänglig vägledning för att hjälpa vårdgivare att undvika att betala lösensummor	Tredje kvartalet 2025
Nationella åtgärder	
Hjälpa medlemsstaterna att utarbeta nationella handlingsplaner	2025
Samordna insatserna för att se till att enskilda medlemsstaters resurser och strategier kompletterar varandra	2025–2026
Genomförande och övervakning av handlingsplanen	
I samråd med kommissionen, lämna regelbundna uppdateringar om det arbete som utförs av stödcentrumet för cybersäkerhet till de relevanta nätverken i medlemsstaterna	2025–2026
Kontinuerligt utbyte med det rådgivande organet för cybersäkerhet på hälsoområdet	2025–2026

Medlemsstaterna:

Europeisk kapacitet för upptäckt av cyberhot mot hälso- och sjukvårdssektorn	
Dela incidentrapporter från sjukhus och vårdgivare inom ramen för NIS 2 med det europeiska stödcentrumet för cybersäkerhet	Från och med fjärde kvartalet 2025
Uppmuntra utvecklingen av nationella informations- och analyscentraler på hälsoområdet	2025–2026
Förebygga cybersäkerhetsincidenter	
Inom samarbetsgruppen för nät- och informationssäkerhet utföra en samordnad säkerhetsriskbedömning, med beaktande av både tekniska och strategiska risker kopplade till leveranskedjor för medicintekniska produkter	Fjärde kvartalet 2025
Snabbinsatser och återställning	
Införa nationella cybersäkerhetsövningar för att testa strategilistorna och stärka rutinerna för incidenthantering	Från och med 2026

Nationella åtgärder	
Utse nationella stödcentrum för cybersäkerhet för sjukhus och vårdgivare	Andra kvartalet 2025
Upprätta nationella handlingsplaner med fokus på cybersäkerhet inom hälso- och sjukvårdssektorn	Fjärde kvartalet 2025
Underlätta resursdelning mellan vårdgivare	2025–2026
Fastställa icke-bindande riktmärken och övervaka finansieringsmål som särskilt avser cybersäkerhet	Fjärde kvartalet 2025
Begära att hälso- och sjukvårdsorganisationer och andra inrättningar som omfattas av NIS 2-direktivet rapporterar sina avsikter att betala lösensummor	Fjärde kvartalet 2025