Rådet for
Den Europæiske Union

Bruxelles, den 16. januar 2025
(OR. en)

5426/25

CYBER 21
SAN 15

FØLGESKRIVELSE

fra:	Martine DEPREZ, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget:	15. januar 2025
til:	Thérèse BLANCHET, generalsekretær for Rådet for Den Europæiske Union
Komm. dok. nr.:	COM(2025) 10 final
Vedr.:	MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET, DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET Europæisk handlingsplan for cybersikkerhed for hospitaler og sundhedstjenesteydere

Hermed følger til delegationerne dokument COM(2025) 10 final.

Bilag: COM(2025) 10 final

EUROPA-
KOMMISSIONEN

Bruxelles, den 15.1.2025
COM(2025) 10 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET, DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET

Europæisk handlingsplan for cybersikkerhed for hospitaler og sundhedstjenesteydere

1. Indledning

EU's sikkerhedsmiljø er under hurtig forandring med en optrapning af hybride angreb og cyberangreb, der har til formål at destabilisere samfundet, skabe splittelse og forstyrrelser, men også generere profit fra cyberkriminalitet. Derfor må Europa hurtigst muligt styrke sit beredskab og sin modstandsdygtighed over for denne nye situation i alle sektorer og i overensstemmelse med en tilgang, der inddrager hele samfundet og går på tværs af ministerier og myndigheder, som omhandlet i rapporten fra den særlige rådgiver for Europa-Kommissionens formand, Sauli Niinistö.

Sikre og modstandsdygtige sundhedssystemer er en hjørnesten i EU's sociale model. Hospitaler og sundhedssystemer står imidlertid over for stigende trusler, navnlig fra ransomwarebander, der går målrettet efter dem med økonomisk gevinst for øje på grund af den høje værdi af patientdata, herunder elektroniske patientjournaler. Faktisk er sundhedssektoren blevet den mest angrebne industri i EU i de seneste fire år, også under covid-19-pandemien, hvor sundhedsinfrastruktur i stigende grad var genstand for cyberangreb. Cyberangreb mod hospitaler og sundhedstjenesteydere forårsager direkte skade på mennesker, forsinker medicinske procedurer, skaber fastlåste situationer på skadestuer og kan i ekstreme tilfælde føre til tab af menneskeliv.

Der er endnu mere spil, når sektoren gennemgår en afgørende digital omstilling. Digital sundhed og anvendelse og videreanvendelse af sundhedsdata kan muliggøre plejemodeller, der er bedre tilpasset mennesker og patienternes behov og præferencer ved at forebygge sygdomme eller gøre det muligt at behandle tidligt. Integrationen af digitale værktøjer og løsninger i kliniske processer samt anvendelsen og videreanvendelsen af sundhedsdata kan danne grundlag for bedre kliniske beslutninger og bidrage til automatisering på sundhedsområdet og hurtigere og bedre patientpleje. Digitale værktøjer, dataanvendelse og medicinsk udstyr – som ofte er forbundet med internettet og drivet af kunstig intelligens – er også vigtige for at håndtere udfordringer såsom manglen på sundhedsprofessionelle.

Samtidig udvider digitale værktøjer også de potentielle målområder for cyberkriminelle. Derudover er visse statslige aktører ikke tilbageholdende med at gå målrettet efter sundhedsfaciliteter, som det ses i Ruslands igangværende angrebskrig mod Ukraine. Dette gør sektoren til et potentielt mål for cyberangreb som led i en bredere hybridkampagne. Cyberangreb bringer ikke blot patientsikkerheden i fare, men svækker også offentlighedens tillid til sundhedsinfrastrukturen og medfører betydelige genoprettelsesomkostninger. Ud over at give beskyttelse mod cyberangreb er en modstandsdygtig og sikker digital infrastruktur også afgørende for at støtte gennemførelsen og den fulde udrulning af det europæiske sundhedsdataområde[1].

Det er derfor på tide at øge og styrke cybersikkerheden og modstandsdygtigheden for europæiske hospitaler og sundhedstjenesteydere som understreget af kommissionsformand Ursula von der Leyen i hendes politiske retningslinjer for Kommissionen 2024-2029[2]. Denne handlingsplan er en reaktion på situationens hastende karakter og de særlige trusler, som sektoren står over for. Der findes ingen simpel løsning på cybersikkerhedsudfordringerne på sundhedområdet. Snarere opfordres der i handlingsplanen til styrket forebyggelse, beredskab og en mere koordineret tilgang til solidaritet, samtidig med at den

[1] https://www.consilium.europa.eu/da/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_da.

europæiske cybersikkerhedsindustris ekspertise udnyttes. Handlingsplanen afspejler således EU's tilgang til sikkerhed, som vil blive videreudviklet og formaliseret i den kommende europæiske strategi for den indre sikkerhed, som fastlægger et omfattende beredskab med henblik på at imødegå alle indre sikkerhedstrusler og fokuserer på evnen til at foregribe trusler, forebygge skade og beskytte mennesker ved at handle på alle niveauer med en tilgang, der inddrager hele samfundet.

Sundhedssektoren består af en lang række enheder og aktører, som omfatter hospitaler, klinikker, plejehjem, rehabiliteringscentre og forskellige sundhedstjenesteydere foruden medicinal-, mediko- og bioteknologiindustrien, producenter af medicinsk udstyr og sundhedsforskningsinstitutioner. Denne handlingsplan fokuserer primært på cybersikkerheden for hospitaler og sundhedstjenesteydere, forstået som enhver fysisk eller juridisk person – eller enhver anden enhed – der lovligt leverer sundhedsydelser på en medlemsstats område[3]. Hospitaler og sundhedstjenesteydere er indbyrdes afhængige med andre sundhedsenheder, og de er tættest på mennesker. Samtidig bør foranstaltninger til forbedring af cybersikkerheden for hospitaler og sundhedstjenesteydere også imødegå risici, der påvirker forsyningskæden og økosystemet i en bredere forstand, f.eks. risici, der hidrører fra enheder, der anvender sundhedsdata til forskning og maskinlæring eller producerer medicinsk udstyr, navnlig digitalt understøttet medicinsk udstyr, der opretter forbindelse til internettet eller andet udstyr ("tingenes internet").

Selv om sikring af sundhedssystemer primært er en national kompetence, er sundhed også en kritisk sektor i henhold til direktivet om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele EU (NIS 2-direktivet)[4]. Cyberkriminelle og andre trusselsaktører opererer på tværs af grænserne, og de cybersikkerhedsudfordringer, som sundhedsorganisationerne står over for, ligner også hinanden på tværs af medlemsstaterne. Samarbejde på europæisk plan er værdifuldt for at udveksle og opskalere bedste praksis på EU-plan og nationalt plan. Derfor foreslås der i handlingsplanen koordinering og foranstaltninger på EU-plan, samtidig med at medlemsstaterne opfordres til at træffe foranstaltninger til at gøre en forskel for sundhedsplejen og det bredere sundhedsøkosystem.

Handlingsplanens fokus er først og fremmest på at opbygge sektorens kapacitet til at **forebygge** cybersikkerhedshændelser, da det altid er bedre at forebygge end at helbrede. For det andet redegøres der i handlingsplanen for tiltag til at forbedre udvekslingen af cybersikkerhedsoplysninger og kapaciteten til at **opdage** cybertrusler, hvilket gør det muligt at reagere hurtigere. For det tredje indeholder den foranstaltninger til bedre at kunne **reagere** på hændelser og **genoprette** efter dem. Endelig omfatter handlingsplanen forslag til, hvordan cybertrusselsaktører kan **afskrækkes** fra at iværksætte angreb mod sundhedssystemer i Europa.

Handlingsplanen vil blive gennemført sammen med sundhedstjenesteydere og det bredere sundhedsøkosystem, medlemsstaterne og cybersikkerhedssektoren. En samarbejdsbaseret tilgang er afgørende for yderligere at fastlægge og finjustere de tiltag, der er mest virkningsfulde, så alle kritiske sundhedstjenesteydere i Europa kan drage fordel af dem. Derfor vil denne meddelelse blive ledsaget af

[3] Jf. artikel 3, litra g), i Europa-Parlamentets og Rådets direktiv 2011/24/EU om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32011L0024.

[4] Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (NIS 2-direktivet), https://eur-lex.europa.eu/eli/dir/2022/2555.

iværksættelsen af en omfattende høring af interessenter, industrien og medlemsstaterne. Internationalt samarbejde er vigtigt for cybersikkerheden på grund af cybertruslernes grænseløse og indbyrdes forbundne karakter. Sammenlignelige cybersikkerhedstrusler er også at finde i udvidelses- og naboskabslandene og andre af EU's strategiske partnerlande. Dette kan i sidste ende bringe sikkerheden af kritisk infrastruktur i EU i fare. Det vil derfor være vigtigt også at tage erfaringerne fra gennemførelsen af handlingsplanen med i EU's samarbejde med både udvidelseslande og andre partnerlande i betragtning af de trusselsniveauer, som de er udsat for.

2. Den cybersikkerhedsmæssige udfordring for hospitaler og sundhedstjenesteydere

Cybertrusler mod sundhedssektoren

Cyberangreb er i stigning på verdensplan og inden for EU, og trusselsbilledet bliver stadig mere komplekst og dynamisk. Fremskridtene inden for kunstig intelligens giver kriminelle og ondsindede aktører kraftfulde værktøjer til at gøre deres aktiviteter mere præcise og virkningsfulde, men ændrer samtidig cyberforsvarsmulighederne ved at muliggøre automatiseret handling og handling i realtid over for angreb.

Ransomware er fortsat en kritisk udfordring for cybersikkerheden i EU og på verdensplan, og i en rapport anslås det, at de årlige omkostninger på verdensplan vil beløbe sig til mere end 250 mia. EUR i 2031[5]. Når ransomwarekriminelle slår til, krypterer de ikke blot ofrenes data mod løsepenge, men lækker i stigende grad følsomme oplysninger for at udøve yderligere pres. En anden fremtrædende udfordring er sårbarheder i software og hardware: Ifølge Den Europæiske Unions Agentur for Cybersikkerhed (ENISA)[6] er sundhedssektoren den sektor, der meldte om flest sikkerhedshændelser i forbindelse med sådanne sårbarheder[7]. Andre stigende trusler omfatter distributed denial of service-angreb (DDoS-angreb), der har til formål at overbebyrde det system, der er mål for angrebet, med en overflod af trafik, så det bliver utilgængeligt for legitime brugere[8].

Sundhedssektoren står over for lignende tendenser med hensyn til cybersikkerhedstrusler, og ransomwareangreb er i udpræget grad fremherskende. Ifølge ENISA tegnede ransomware sig for 54 % af de analyserede cybersikkerhedshændelser i sundhedssektoren i perioden 2021-2023. 83 % af angrebene var økonomisk motiverede på grund af den høje værdi af sundhedsdata, mens 10 % af angrebene var ideologisk motiverede[9]. Tilsvarende blev det i en rapport fra Kommissionen fra 2024

[5] Cybersecurity Ventures (1. juni 2024): *Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031*. Findes på https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[6] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed) og om cybersikkerhedscertificering af informations- og kommunikationsteknologi (forordningen om cybersikkerhed), https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.
[7] ENISA Threat Landscape: Health Sector (July 2023).
[8] ENISA Threat Landscape 2024.
[9] ENISA Threat Landscape: Health Sector (July 2023). I rapporten analyseredes sundhedstjenesteydere samt andre typer organisationer, herunder organisationer, der udfører sundhedsrelateret forskning, enheder, der fremstiller visse

konstateret, at 71 % af de angreb, der havde en indvirkning på patientplejen såsom forsinket behandling eller diagnose eller forringet adgang til beredskabstjenester, var af ransomwaretypen[10]. Ransomwareangreb kan have en særlig forstyrrende virkning på leveringen af sundhedsydelser og bringe patientsikkerheden i fare. Desuden kombineres ransomwareangreb ofte med patientdatabrud[11], som ofte omfatter følsomme sundhedsrelaterede oplysninger og krænker menneskers grundlæggende ret til beskyttelse af personoplysninger.

Samtidig vokser angrebsfladen i omfang med den stigende digitalisering af sundhedsplejen. Ifølge rapporten fra 2024 om status over det digitale årti har i gennemsnit 79 % af EU-borgerne onlineadgang til deres elektroniske patientjournaler inden for primær sundhedspleje[12]. Elektroniske patientjournaler, kliniske informationssystemer, hospitalers workflowsystemer, IT-systemer til håndtering af refusion for behandlinger, medicinske billedbehandlingssystemer og medicinsk udstyr, der anvendes til diagnostiske formål eller til patientovervågning, er alle eksempler på digitale værktøjer, der kan spille en vigtig rolle med hensyn til at øge effektiviteten og produktiviteten i sundhedssektoren, men de er også potentielle mål for cybersikkerhedsangreb. Specifikke sundhedsplejeaktiviteter, som f.eks. intensiv behandling og radiologisk billeddannelse, eller medicinske områder såsom onkologi og kardiologi, der er stærkt afhængige af digitalt understøttet udstyr, er i særlig risiko for cyberangreb. Desuden kan problemer i forsyningskæderne føre til indkøb af udstyr med utilstrækkelig cybersikkerhed, hvilket forværrer de eksisterende generelle risici.

F.eks. lammede et ransomwareangreb under covid-19-pandemien store dele af det irske sundhedssystem, hvilket førte til aflysning af i hvert fald nogle tjenester på 31 af de 54 akutsygehuse den formiddag, hændelsen indtraf[13]. Sundhedstjenesterne var nødt til at gå tilbage til papirjournaler, hvilket hæmmede effektiviteten. Angrebet udsprang fra en phishing-e-mail med en ondsindet fil vedhæftet[14]. Hændelsen viste muligheden for, at cyberangreb kan sprede sig på tværs af forskellige systemer, og dermed hvor vigtigt det er at beskytte hele sundhedsorganisationens angrebsflade. Hændelsen fremhævede også vigtigheden af at sikre en grundlæggende cyberhygiejne og cybersikkerhedskultur i hele organisationen.

Hospitalers og sundhedstjenesteyderes cybersikkerhedsmodenhed

Sundhedslandskabet i EU er meget forskelligartet, idet hospitaler og andre sundhedstjenesteydere varierer meget med hensyn til ejerskab, struktur og størrelse fra medlemsstat til medlemsstat. I nogle

sundhedsrelaterede produkter, sundhedsmyndigheder, sygesikringsorganisationer og døgnbehandlingscentre og udbydere af sociale tjenesteydelser. Findes på https://www.enisa.europa.eu/publications/health-threat-landscape (foreligger ikke på dansk).

[10] Europa-Kommissionen: Det Fælles Forskningscenter, Reina, V. og 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, Den Europæiske Unions Publikationskontor, 2024, https://data.europa.eu/doi/10.2760/693487 (foreligger ikke på dansk).

[11] Ifølge ENISA's rapport om trusselsbilledet for sundhedssektoren blev der konstateret databrud eller datatyveri i 43 % af de analyserede ransomwarehændelser.

[12] Rapport om status over det digitale årti 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"*. Findes på https://www2.hse.ie/services/cyber-attack/what-happened/.

tilfælde kan sundhedsforvaltningen være baseret på en centraliseret tilgang på nationalt plan, i andre tilfælde på regionalt og lokalt plan, og sundhedstjenesteyderne kan være offentligt ejede eller privatejede. Desuden kan der også være forskelle inden for det samme land, f.eks. hvis der er betydelige socioøkonomiske og territoriale forskelle mellem områder, hvilket giver et komplekst billede. Det komplekse sundhedslandskab kan blive udfordret af større sundhedskriser som følge af overførbare sygdomme, som f.eks. covid-19-pandemien, men også andre sundhedsrisici, f.eks. i forbindelse med klimaændringer. Endelig er der betydelige forskelle og fragmentering i sundhedstjenesteydernes digitaliseringsniveau og teknologianvendelse. Et eksempel på denne kompleksitet er, at tjenesters utilgængelighed som følge af en cybersikkerhedshændelse kan medføre alvorlig skade eller tab for patienter, selv i små sundhedsfaciliteter, herunder klinikker eller akutmedicinske tjenester, som leverer en væsentlig tjeneste til et relativt lavt antal brugere.

Ifølge ENISA's rapport fra 2024 om cybersikkerhedssituationen i Unionen[15] er cybersikkerhedsmodenheden i sundhedssektoren i EU moderat, og der er store forskelle i modenhedsniveauet blandt sundhedsenheder på tværs af Europa. Der kan konstateres mangler på centrale områder såsom tilstrækkelige menneskelige ressourcer, organisationernes kendskab til deres forsyningskæder for informations- og kommunikationsteknologi (IKT) og installation af de seneste sikkerhedselementer i produkter. Sektoren kæmper med basal cyberhygiejne og grundlæggende sikkerhedsforanstaltninger, hvilket illustreres af, at næsten alle de adspurgte sundhedsorganisationer har udfordringer, når det gælder om at foretage cybersikkerhedsrisikovurderinger, og næsten halvdelen har aldrig foretaget en risikoanalyse[16].

En anden betydelig udfordring for hospitalernes cybersikkerhed er skæringspunktet mellem informationsteknologi (IT) og operationel teknologi (OT), hvor forskellige sikkerhedsprioriteter mødes med hensyn til fortrolighed, tilgængelighed og pålidelighed, og hvor et brud på et område kan påvirke et andet. I ENISA's rapport fra 2024 om cybersikkerhedssituationen i Unionen understreges det endvidere, at sundhedssektoren ikke klarer sig tilstrækkeligt med hensyn til at garantere sikkerheden af de IKT-produkter og -processer, der anvendes i sektoren, på grund af den store mængde sundhedsenheder, udstyr og produkter.

Denne mangfoldighed kombineret med forskellige niveauer af cyberbevidsthed blandt hospitalernes personale og ledelse skaber en kompleks udfordring, når det gælder om at garantere sundhedssystemernes cybersikkerhed. Ifølge Eurobarometerundersøgelsen fra 2024 om cyberfærdigheder havde f.eks. kun 25 % af de adspurgte virksomheder i sundheds-, uddannelses- og socialsektoren tilbudt uddannelse eller oplysning om cybersikkerhed i de foregående 12 måneder[17]. Der er behov for en indsats for at fremme en bevidsthedskultur om cybersikkerhed blandt sundhedsprofessionelle i forreste linje. F.eks. er personalerotationer, brug af fælles arbejdsstationer, ringe

[15] ENISA: 2024 Report on the State of Cybersecurity in the Union (September 2024). Findes på https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (foreligger ikke på dansk).
[16] ENISA Threat Landscape: Health Sector (July 2023). Findes på https://www.enisa.europa.eu/publications/health-threat-landscape (foreligger ikke på dansk).
[17] Flash Eurobarometer 547 on Cyberskills (May 2024). Findes på https://europa.eu/eurobarometer/surveys/detail/3176 (foreligger ikke på dansk).

autentifikationsstyring og anvendelse af flytbare medier yderligere kilder til sårbarheder, der påvirker sundhedstjenesteydernes cybersikkerhed[18].

I mange tilfælde er informationsteknologi og operationel teknologi som minimum delvist outsourcet. Eurobarometerundersøgelsen fra 2024 viste, at andelen af virksomheder, der outsourcer som minimum visse aspekter af deres cybersikkerhed, er højest i sundheds-, uddannelses- og socialsektoren, hvor andelen tegner sig for 57 % af de adspurgte virksomheder[19]. Ligeledes er der en stærk tendens til at migrere til cloudcomputing på grund af behovet for skalerbar datalagring og -forvaltning, omkostningseffektivitet, forbedret samarbejde og understøttelse af avanceret teknologi såsom kunstig intelligens og de medicinske tings internet. I 2022 benyttede 58 % af sundhedsorganisationerne en cloudbaseret digital sundhedsplatform[20]. Selv om dette skift kan medføre betydelige effektivitetsgevinster, indebærer det også risici, der nødvendiggør informerede beslutninger om udbud og sikker konfiguration.

Over alle disse udfordringer ligger spørgsmålet om kapacitetsopbygning og finansiering. Finansieringen af cybersikkerhed i sundhedssektoren har været begrænset og er fortsat en generel udfordring i hele EU[21]. Desuden opstår de finansieringsmæssige udfordringer på baggrund af en aldrende befolkning, som forventes at skabe et omfattende budgetpres for de europæiske sundhedssystemer i de kommende årtier.

Den fortsatte anvendelse af forældede værktøjer og nedarvede systemer, begrænsede ressourcer til forebyggelse af eller reaktion på hændelser og mangler med hensyn til cybersikkerhedsmodenhed skyldes ofte manglende finansiering. Hospitalerne står over for en vedvarende udfordring med hensyn til at balancere mellem en moderne, sikker og digital infrastruktur og andre investeringer, der er nødvendige for at forbedre patientplejen, som f.eks. ansættelse af læger og andre sundhedsprofessionelle, indførelse af nye diagnosticerings- og behandlingsmetoder og erhvervelse af udstyr. Ifølge ENISA[22] ligger sundhedssektoren kun på en syvendeplads blandt de 12 undersøgte sektorer, når det gælder andelen af udgifter til informationssikkerhed ud af de samlede IT-udgifter, idet 8,3 % er medianen i sundhedssektoren.

3. Europæisk støttecenter for cybersikkerhed for hospitaler og sundhedstjenesteydere

EU's ramme for cybersikkerhed tilbyder en bred vifte af værktøjer, der bør udnyttes til at forbedre sikkerheden og modstandsdygtigheden hos hospitaler og sundhedstjenesteydere. For at håndtere de

[18] Panacea – *People-centric cybersecurity in healthcare (2021): White Paper – Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres.*
[19] Flash Eurobarometer 547 on Cyberskills.(May 2024). Findes på https://europa.eu/eurobarometer/surveys/detail/3176 (foreligger ikke på dansk).
[20] ENISA: NIS Investments Report 2022 (November 2022). Findes på https://www.enisa.europa.eu/publications/nis-investments-2022 (foreligger ikke på dansk).
[21] Organisation og levering af sundhedstjenesteydelser og behandling på sundhedsområdet er en national kompetence i henhold til artikel 168 i traktaten om Den Europæiske Unions funktionsmåde, og finansieringen af sundhedssystemerne varierer fra medlemsstat til medlemsstat.
[22] ENISA: NIS Investments Report 2022 (November 2022). Findes på https://www.enisa.europa.eu/publications/nis-investments-2022 (foreligger ikke på dansk).

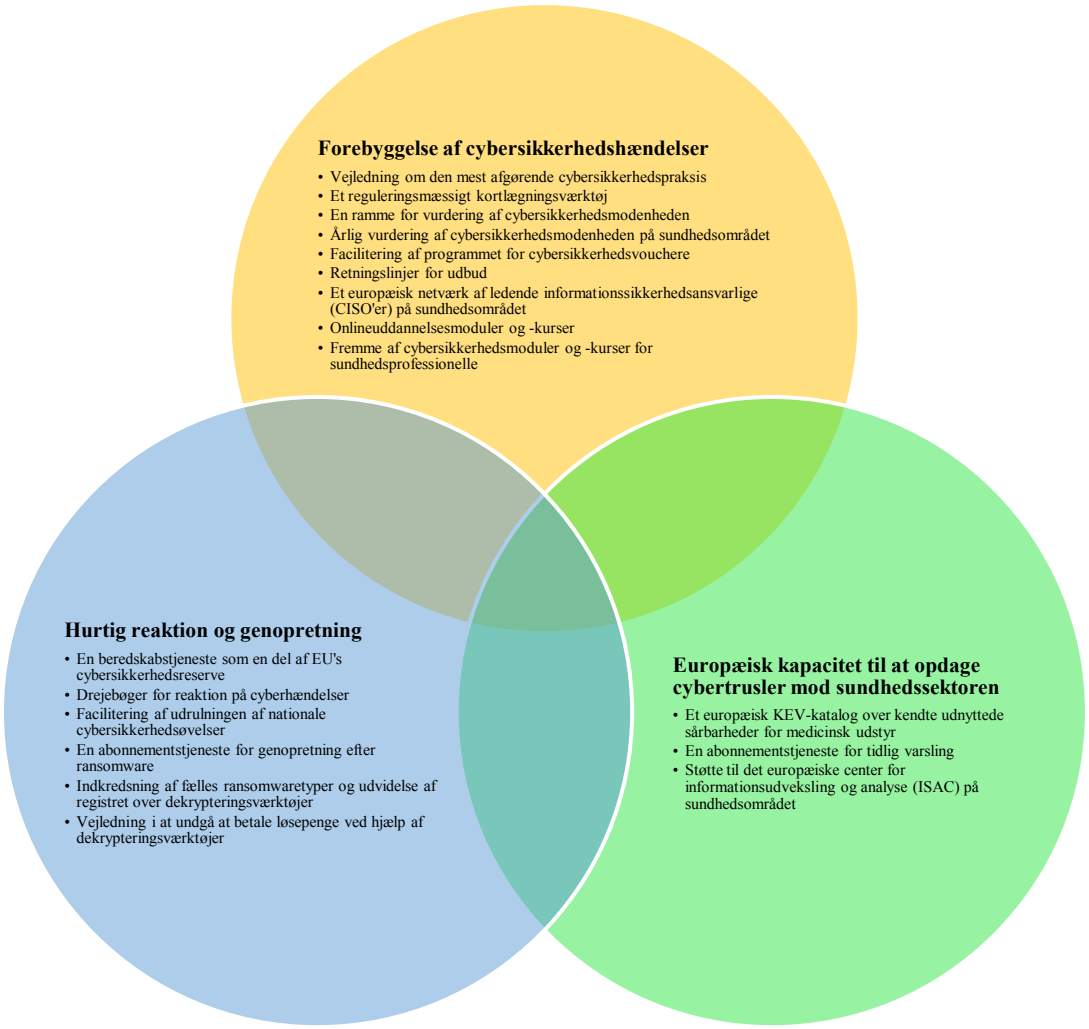
mange udfordringer, der er fremhævet ovenfor, er det nødvendigt at udvikle en samlet strategisk tilgang på EU-plan, der samler de nødvendige ressourcer og værktøjer og den nødvendige ekspertise til effektivt at imødegå cybertrusler. Et omfattende overblik samt bedre planlægning og koordinering er afgørende for at hjælpe sundhedstjenesteydere i hele EU med at styrke deres forsvar. Med henblik på at opnå dette er ENISA bedst i stand til inden for sin organisation at oprette et særligt **europæisk støttecenter for cybersikkerhed for hospitaler og sundhedstjenesteydere**[23] som led i sit mandat[24] til at beskytte og understøtte EU's kritiske infrastruktur.

Støttecentret bør gradvist **udarbejde et omfattende tjenestekatalog, der imødekommer hospitalernes og sundhedstjenesteydernes behov**, og som sammenfatter udvalget af tilgængelige tjenester til beredskab, forebyggelse, opdagelse og reaktion. Støttecentret bør i samarbejde med medlemsstaternes myndigheder og på grundlag af erfaringerne fra hospitaler og sundhedstjenesteydere udarbejde et brugervenligt og lettilgængeligt register over alle tilgængelige instrumenter på EU-plan og nationalt og regionalt plan. Støttecentret bør i forbindelse med udførelsen af sine aktiviteter sikre passende koordinering med medlemsstaterne og støtte prioritering og gennemførelse af foranstaltninger efter behov i realtid.

Som en vigtig byggesten i udarbejdelsen af støttecentrets tjenestekatalog vil Kommissionen foreslå at iværksætte pilotprojekter i hele EU for at udvikle bedste praksis for cyberhygiejne og sikkerhedsrisikovurdering samt imødekomme behovet for løbende cybersikkerhedsovervågning, trusselsefterretninger og reaktion på hændelser ved hjælp af de nyeste cybersikkerhedsløsninger. Resultaterne af disse pilotprojekter, som vil blive finansieret af programmet for et digitalt Europa og gennemført af Det Europæiske Kompetencecenter for Cybersikkerhed (ECCC), vil danne grundlag for yderligere tiltag på EU-plan, herunder støttecentrets arbejde.

[23] I dette dokument bruges som synonym også blot "støttecenter".

[24] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).



Figur 1: Koncepter for støttecentrets tjenestekatalog for hospitaler og sundhedstjenesteydere.

3.1. Forebyggelse af cybersikkerhedshændelser

Enkle tiltag, der vender oddsene

Grundlæggende cybersikkerhedsforanstaltninger, som f.eks. sikring af systemernes ajourholdelse, forvaltning af backups og gennemførelse af multifaktorautentificering, kan ifølge et skøn beskytte organisationer mod op til 98 % af angrebene[25]. Mange af de mest virkningsfulde foranstaltninger vedrørende cyberhygiejne og risikostyring er relativt enkle at træffe og derfor en lavthængende frugt,

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

når det gælder om at forbedre cybersikkerheden. En af støttecentrets centrale roller bør derfor være at **udarbejde klar, målrettet vejledning, der fremhæver den mest afgørende cybersikkerhedspraksis og hjælper sundhedstjenesteyderne med at gennemføre den**. Støtten skal række ud over store hospitaler og omfatte skræddersyet rådgivning til mindre enheder såsom lokale lægeklinikker og specialistklinikker, som ofte ikke har ressourcerne til særlige cybersikkerhedsteams, men er lige så sårbare over for angreb. Desuden er det nødvendigt at tage hensyn til specifikke sundhedsenheders regionale betydning med hensyn til at sikre patientplejen, f.eks. i tyndt befolkede områder. Sundhedsforskningsinstitutter, der håndterer store mængder følsomme personoplysninger, kan også drage fordel af at modtage vejledning om grundlæggende cybersikkerhedsforanstaltninger for at øge deres modstandsdygtighed.

Sundhedsorganisationer er også underlagt en række cybersikkerhedsrelaterede forpligtelser i EU-lovgivningen[26]. Selv om forpligtelserne er afgørende for at sikre et højt fælles referenceniveau for cyber- og datasikkerhed, er det vigtigt at sørge for, at det lovgivningsmæssige landskab ikke er unødigt vanskeligt og byrdefuldt at navigere i. Et stærkt fokus på overholdelse bør ikke være i strid med målet om at fremme en stærk cybersikkerhedskultur. Et **reguleringsmæssigt kortlægningsværktøj, som er let at få adgang til, kan være med til at minimere den administrative byrde for enheder, der er omfattet af flere reguleringsinstrumenter**. Sideløbende med udarbejdelsen af vejledning og udviklingen af værktøjskasser bør støttecentret arbejde tæt sammen med Kommissionen og medlemsstaterne om at udvikle og udbrede et sådant værktøj så hurtigt som muligt. Støttecentret vil derfor spille en vigtig rolle med hensyn til at gøre cybersikkerhedsreglerne enkle at forstå og gennemføre, f.eks. ved at yde gennemførelsesvejledning[27] og om nødvendigt fremme relevante standarder.

De kommende **europæiske digitale identitetstegnebøger** er endnu et redskab til at lette en enkel gennemførelse af god cyberhygiejnepraksis. For at mindske risikoen for uautoriseret adgang til sundhedsdata er det afgørende at mindske afhængigheden af svage identifikationsmekanismer såsom

[26] F.eks. NIS2-direktivet; Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer (forordningen om cyberrobusthed), https://eur-lex.europa.eu/eli/reg/2024/2847/oj/enghttps://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng; Europa-Parlamentets og Rådets forordning (EU) 2017/745 af 5. april 2017 om medicinsk udstyr, https://eur-lex.europa.eu/eli/reg/2017/745/oj/enghttps://eur-lex.europa.eu/eli/reg/2017/745/oj/eng (forordningen om medicinsk udstyr) https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng; Europa-Parlamentets og Rådets forordning (EU) 2017/746 af 5. april 2017 om medicinsk udstyr til in vitro-diagnostik (forordningen om medicinsk udstyr til in vitro-diagnostik), https://eur-lex.europa.eu/eli/reg/2017/746/oj/enghttps://eur-lex.europa.eu/eli/reg/2017/746/oj/eng; Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse), https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:32016R0679https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:32016R0679; Europa-Parlamentets og Rådets forordning (EU) 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens (forordningen om kunstig intelligens), https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:32024R1689; forslag til Europa-Parlamentets og Rådets forordning om det europæiske sundhedsdataområde (COM(2022) 197 final), https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=celex:52022PC0197. Forhandlingerne blev afsluttet med en politisk aftale i foråret 2024, og efter færdiggørelsen forventes offentliggørelse i EU-Tidende i foråret 2025.

[27] Udarbejdelsen af retningslinjer for fortolkningen af den generelle forordning om databeskyttelse (GDPR) henhører under Det Europæiske Databeskyttelsesråds ansvar. ENISA's udarbejdelse af vejledning bør fuldt ud respektere Databeskyttelsesrådets beføjelser.

passwords. Et skift i retningen af sikre loginløsninger baseret på pålidelig identifikation er af kritisk betydning. Den europæiske digitale identitetstegnebog tilbyder sundhedsprofessionelle en harmoniseret, EU-dækkende tilgang til elektronisk identifikation og tilvejebringer således en robust og samlet løsning fra udgangen af 2026. Alle onlinesundhedsinformationssystemer, der er forpligtet til at gennemføre stærk brugerautentifikation, vil være forpligtede til at acceptere identitetstegnebogen med henblik på identifikation fra udgangen af 2027[28].

Beredskab og målrettet støtte

Beredskabstest, der omfatter foranstaltninger såsom penetrationstest, er en hjørnesten i effektiv cybersikkerhed, og Kommissionen har allerede afsat midler til ENISA til pilotinitiativer vedrørende beredskab, som afslørede, at sundhedssektoren er et af de områder, hvor der er størst efterspørgsel efter test og videre vurdering for at afdække mangler i cybersikkerhedsmodenheden. Med ikrafttrædelsen af forordningen om cybersolidaritet vil disse bestræbelser blive udvidet betydeligt, og Det Europæiske Kompetencecenter for Cybersikkerhed vil føre an. For at imødekomme behovet vil Kommissionen i samråd med NIS-samarbejdsgruppen, EU-CyCLONe[29] og ENISA foreslå at udpege sundhed som en sektor, hvor der kan ydes støtte til **koordineret beredskabstestning** inden for rammerne af forordningen om cybersolidaritet. Desuden bør støttecentret udvikle en **skræddersyet ramme for vurdering af cybersikkerhedsmodenheden, der er specifik for sundhedsområdet**. Sådanne modenhedsvurderinger vil give enhederne handlingsrettet indsigt i deres sårbarheder og samtidig give dem mulighed for at vise deres cybersikkerhedsberedskab over for patienter og interessenter og opbygge tillid til deres tjenester. På aggregeret niveau bør støttecentret foretage en **årlig vurdering af cybersikkerhedsmodenheden på sundhedsområdet**, der vil give et klart overblik over sundhedssektorens cybersikkerhed på både nationalt plan og EU-plan.

Sundhedssektoren er stærkt afhængig af eksterne kontrahenter for cybersikkerhedstjenester[30], hvilket understreger behovet for målrettet støtte for at styrke forsvaret. På grundlag af vellykkede initiativer såsom EU's innovationsvouchere **bør medlemsstaterne overveje målrettede foranstaltninger, som f.eks. cybersikkerhedsvouchere for meget små, små og mellemstore hospitaler og sundhedstjenesteydere**. Voucherne vil yde finansiel bistand til at gennemføre specifikke cybersikkerhedsforanstaltninger. Prioriteringen i tildelingen af vouchere bør baseres på resultaterne af beredskabstest og modenhedsvurderinger.

Lokal viden og kontekst er afgørende for en effektiv udrulning af vouchere eller andre støtteprogrammer og sikrer relevans og tilgængelighed. EU-fonde såsom Den Europæiske Fond for Regionaludvikling er allerede aktive med hensyn til at støtte initiativer vedrørende cybersikkerhed og digital sundhed og kan derfor tjene som et middel til at udvikle målrettede cybersikkerhedsvoucherordninger for sundhedstjenesteydere. For at fremme denne indsats vil støttecentret samarbejde med medlemsstaterne og de regionale programmyndigheder om at støtte udviklingen af sådanne regionale voucherordninger

[28] Artikel 5f, stk. 1-2, i forordning (EU) nr. 910/2014.
[29] Det Europæiske Netværk af Forbindelsesorganisationer for Cyberkriser.
[30] Se ENISA's NIS-investeringsrapport 2023 (november 2023), hvori det fremhæves, hvor fremtrædende en plads ekstern støtte i forbindelse med cybersikkerhedsauditering og -overholdelse indtager. Findes på https://www.enisa.europa.eu/publications/nis-investments-2023 (foreligger ikke på dansk).

på grundlag af erfaringerne fra eksisterende nationale projekter samt tiltag, der finansieres under programmet for et digitalt Europa, for at sikre en praktisk og virkningsfuld gennemførelse.

Siden 2014 har Horisontprogrammerne desuden været medvirkende til at finansiere en række forskningsinitiativer med fokus på at øge modstandsdygtigheden over for cybertrusler hos sundhedsinstitutioner, f.eks. hospitaler, og afbøde de risici, der er forbundet med forkert brug af ny teknologi. De deraf følgende resultater omfatter en række specialiserede værktøjer, rammer og systemer, som f.eks. risikovurderingsværktøjer, datadelingsplatforme, der beskytter privatlivets fred, kryptografiske løsninger, uddannelsesprogrammer om cybersikkerhedsbevidsthed og systemer til opdagelse af trusler i realtid. Disse løsninger er navnlig blevet nøje valideret gennem pilotimplementeringer under faktiske forhold i sundhedsmiljøer, hvilket gør, at de er effektive og praktisk anvendelige, når det gælder beskyttelse mod cybertrusler.

Sikring af forsyningskæder på sundhedsområdet

En central udfordring for sundhedsorganisationer er at forvalte komplekse IKT-forsyningskæder, der omfatter en række produkter såsom netforbundet medicinsk udstyr, elektroniske patientjournalsystemer og hardware til kontorer. Hospitaler og sundhedstjenesteydere har brug for pålidelige og sikre IKT-systemer og -tjenester til deres aktiviteter. For at bidrage til at håndtere cybersikkerhedsudfordringer i sundhedssektoren bør NIS-samarbejdsgruppen foretage en **koordineret sikkerhedsrisikovurdering, hvor både tekniske og strategiske risici i forbindelse med forsyningskæder for medicinsk udstyr vurderes, og der foreslås afbødende foranstaltninger**[31]. I det omfang det er relevant, bør NIS-samarbejdsgruppen samarbejde med Koordinationsgruppen for Medicinsk Udstyr.

Forordningen om cyberrobusthed er en ny, omfattende ramme, der fastsætter cybersikkerhedskrav til planlægning, design, udvikling samt til håndtering, rettelse og indberetning af aktivt udnyttede sårbarheder for næsten alle hardware- og softwareprodukter i hvert led i værdikæden[32]. Medicinsk udstyr er en type produkt, der anvendes på et af de mest følsomme områder i samfundet. Cybersikkerhedskravene til sådanne produkter hidrører fra den allerede eksisterende forordning om medicinsk udstyr og forordningen om medicinsk udstyr til in vitro-diagnostik[33]. I den igangværende evaluering af disse forordninger undersøges potentialet for større sammenhæng og synergi mellem rammerne med henblik på forenkling og avanceret cybersikkerhed.

Derudover bør resultaterne af risikovurderingen støtte sundhedsorganisationerne i gennemgangen af deres cybersikkerhedspraksis i forbindelse med forsyningskæder som krævet af NIS 2-direktivet og kan

[31] Jf. NIS 2-direktivets artikel 22.
[32] I første omgang vil bredere kategorier af radioudstyr, der ikke er omfattet af anvendelsesområdet for forordningen om medicinsk udstyr og forordningen om medicinsk udstyr til in vitro-diagnostik, fra den 1. august 2025 skulle opfylde de væsentlige krav vedrørende cybersikkerhed i radioudstyrsdirektivet, når de bringes i omsætning på det indre marked. I anden fase, fra den 11. december 2027, vil forordningen om cyberrobusthed finde anvendelse.
[33] I december 2019 udsendte Samarbejdsgruppen for Medicinsk Udstyr en vejledning om cybersikkerhed i forbindelse med medicinsk udstyr, der skulle hjælpe producenterne med at opfylde kravene i bilag I til de to forordninger: https://ec.europa.eu/docsroom/documents/41863 (foreligger ikke på dansk).

danne grundlag for at udarbejde nye **retningslinjer for udbud**[34]. Retningslinjerne vil skulle udarbejdes af ENISA via dets støttecenter og bør afspejle de seneste tendenser, som f.eks. cloudificeringen af lagringen af patientdata, herunder behovet for sikker migration af elektroniske sundhedsdata til cloudmiljøer. Desuden bør de nye retningslinjer give organisationerne praktiske værktøjer til at have styr på deres forsyningskæder, herunder udbydere af administrerede sikkerhedstjenester, attesteringsrapporter eller tredjepartsrisikovurderinger.

Med hensyn til cloud er der behov for yderligere tiltag for at håndtere de særlige udfordringer i forbindelse med forvaltningen af følsomme sundhedsdata, herunder øget sikkerhed, privatlivets fred og operationelle risici. Med henblik på at styrke sikkerhedsforanstaltningerne anbefaler eksperter, at der i cloudtjenesterne indarbejdes "sikkerhed gennem standardindstillinger og indbygget sikkerhed". Med denne tilgang prioriteres sikker infrastruktur, proaktiv sårbarhedsstyring og en blanding af offentlige og private cloudløsninger. Løbende overvågning og leverandørspecifikke attesteringer – f.eks. sikkerhedsleverandørers certificeringer og kontrol af overensstemmelsen med nationale og internationale standarder – er også afgørende for at opnå en robust sikkerhedspraksis.

For tjenester som infrastruktur som en tjeneste (IaaS), platform som en tjeneste (PaaS) og software som en tjeneste (SaaS) falder gennemførelsen af sikkerheden ofte over på kunden. Mange sundhedsorganisationer har imidlertid ikke tilstrækkelige ressourcer til at opfylde disse krav på egen hånd. For at afhjælpe denne situation bør **cloudtjenesteudbydere tilskyndes til at gennemføre grundlæggende sikkerhedsforanstaltninger som en standardfunktion**. Sådanne foranstaltninger vil mindske risikoen for fejlkonfigureringer, opretholde en ensartet beskyttelse på tværs af kundestyrede miljøer og give brugerne større sikkerhed. Fastlæggelsen af et grundlæggende sikkerhedsreferenceniveau vil sigte mod at finde en balance mellem solid beskyttelse og praktisk gennemførlighed og dermed garantere anvendeligheden for en bred vifte af sundhedsorganisationer. Denne indsats vil indebære et tæt samarbejde mellem cloududbydere og sundhedssektoren, og at bedste praksis fra industrien udnyttes til at skabe effektive og skalerbare løsninger.

Uddannelse og kompetenceudvikling

Det er vigtigt at have en arbejdsstyrke med efterspurgte færdigheder for at opnå bæredygtig vækst og konkurrenceevne i Europa på lang sigt samt tjenesteydelser af høj kvalitet, herunder sundhedsydelser. Manglen på kvalificerede fagfolk inden for cybersikkerhed er en betydelig udfordring i hele Europa, og det anslås, at der mangler 299 000 fagfolk for at opfylde arbejdsstyrkens behov i EU[35]. Ifølge Eurobarometerundersøgelsen fra 2024 om cyberfærdigheder[36] betragter 81 % af virksomhederne vanskeligheder med at ansætte cybersikkerhedspersonale som en central risiko for potentielle cyberangreb. I uddannelses-, sundheds- og socialsektoren er 66 % af cybersikkerhedsstillingerne besat

[34] På grundlag af ENISA's retningslinjer for udbud med hensyn til cybersikkerhed på hospitaler fra februar 2020. Findes på https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services (foreligger ikke på dansk).
[35] The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study | Digital Skills and Jobs Platform.
[36] Flash Eurobarometer 547 on Cyberskills.

af medarbejdere, der kommer fra stillinger, der ikke vedrører cybersikkerhed, hvilket understreger det presserende behov for omskoling og opkvalificering.

For at håndtere denne udfordring bør støttecentret samarbejde med det fremtidige konsortium for en europæisk digital infrastruktur (EDIC) for cybersikkerhedsfærdigheder som omhandlet i Kommissionens meddelelse om EU's akademi for cybersikkerhedskompetencer[37]. Arbejdet bør lette udvekslingen mellem cybersikkerhedsfagfolk i sundhedssektoren, som f.eks. ledende informationssikkerhedsansvarlige (Chief Information Security Officers – CISO'er). Et muligt tiltag kan være at oprette et **europæisk netværk af ledende informationssikkerhedsansvarlige (CISO'er) på sundhedsområdet** med udgangspunkt i en pulje af eksperter, der skal udveksle og udvikle bedste praksis, strategier for fastholdelse af talent og løsninger til at tiltrække cybersikkerhedsfagfolk til sundhedssektoren. Desuden bør der inden for rammerne af akademiet for cybersikkerhedsfærdigheder udvikles ressourcer til at styrke cybersikkerhedsarbejdsstyrken i sundhedssektoren med støtte fra industrien og den akademiske verden. I den henseende bør interessenter fra industrien tilskyndes til at give tilsagn om at støtte en forbedring af uddannelsesmulighederne inden for cybersikkerhed.

Menneskelige fejl ligger fortsat i stort omfang til grund for cybersikkerhedshændelser på sundhedsområdet, hvilket understreger det kritiske behov hos personalet for omfattende uddannelse og cyberbevidsthed. I betragtning af sundhedsprofessionelles hyppige anvendelse af digitale værktøjer er det afgørende at udruste dem med viden om sikker praksis. Målrettede uddannelses- og oplysningskampagner kan reducere risiciene betydeligt. For at afhjælpe situationen bør støttecentret arbejde med sundhedsprofessionelle og sundhedstjenesteydere og samarbejde med uddannelsesudbydere, industrien, konsortiet for en europæisk digital infrastruktur for cybersikkerhedsfærdigheder og medlemsstaternes myndigheder om at skabe og udbrede **omfattende og lettilgængelige onlineuddannelsesmoduler og -kurser**.

For at opbygge et stærkt cybersikkerhedsgrundlag på sundhedsområdet er det afgørende at indarbejde digitale kompetencer og cybersikkerhedsmoduler i undervisningsplanerne. Modulerne bør omhandle sektorspecifikke spørgsmål såsom patientdatabeskyttelse og sårbarheder med hensyn til sikkerheden i forbindelse med medicinsk udstyr. I udviklingen af disse ressourcer bør der tages hensyn til tidligere tiltag, som f.eks. BeWell-projektet, der finansieres under Erasmus+-programmet[38], og PANACEA-projektet, der finansieres under Horisont 2020[39].

3.2.Europæisk kapacitet til at opdage cybertrusler mod sundhedssektoren

[37] Meddelelse fra Kommissionen til Europa-Parlamentet og Rådet: Opbygning af cybersikkerhedskompetencer skal styrke EU's konkurrenceevne, vækst og modstandsdygtighed ("EU's akademi for cybersikkerhedskompetencer") (COM(2023) 207 final).
[38] BeWell – Blueprint alliance for a future health workforce strategy on digital and green skills. Kan tilgås 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. Kan tilgås på https://cordis.europa.eu/project/id/826293.

Effektiv opdagelse af cybertrusler er afgørende for at kunne reagere hurtigt på hændelser. Trusselsaktører kan udnytte teknikker, der gør det vanskeligt at opdage indtrængen og dermed muliggør længere perioder med uautoriseret adgang til et system[40]. Derfor kan bedre evner til at opdage trusler være med til at stoppe cyberangreb tidligt. I ransomwareangrebet mod den finske udbyder af psykoterapeutiske tjenester Vastaamo, hvor gerningsmændene afpressede patienter, hvis fortrolige patientjournaler var blevet stjålet, skete den første indtrængen f.eks. i 2018, men kom først til udbyderens kendskab i 2020[41].

Effektiv informationsudveksling og samarbejde er afgørende for at øge trusselsopdagelsen og situationsbevidstheden i hele EU. Enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), spiller en afgørende rolle med hensyn til at modtage underretninger om hændelser, nærvedhændelser og potentielle trusler og tilbyder vejledning om afbødende foranstaltninger på nationalt plan. Dog **opfordres medlemsstaterne kraftigt til også at dele alle underretninger om cyberhændelser fra hospitaler og sundhedstjenesteydere med ENISA's støttecenter med henblik på situationsbevidsthed i EU**. Ideelt set bør dette ledsages af en meningsfuld beskrivelse af forskellige relevante dimensioner af hændelserne, herunder kendte årsagsmæssige sårbarheder samt indvirkninger på sundhedsydelser og utilsigtede hændelser hos patienter. Desuden opfordres producenter af medicinsk udstyr og udstyr til in vitro-diagnostik til frivilligt via den fælles indberetningsplatform, der skal oprettes og forvaltes af ENISA inden for rammerne af forordningen om cyberrobusthed, at indberette aktivt udnyttede sårbarheder eller alvorlige cyberhændelser, der har indvirkning på sikkerheden i forbindelse med sådant udstyr, samt eventuelle andre sårbarheder, hændelser, nærvedhændelser eller cybertrusler, der kan have indvirkning på udstyrets risikoprofil.

Når oplysningerne i indberetningerne ikke længere er følsomme, kan støttecentret opbygge et ENISA-støttet europæisk katalog over kendte udnyttede sårbarheder (KEV-katalog) for medicinsk udstyr, elektroniske patientjournalsystemer og udbydere af IKT-udstyr og -software på sundhedsområdet. Med henblik på at håndtere betydelige udfordringer i forbindelse med opdagelsen af trusler bør støttecentret indføre **en EU-dækkende abonnementstjeneste for tidlig varsling for sundhedssektoren, der giver varslinger i næsten realtid**. Tjenesten vil trække på behandlede data fra CSIRT'er, enheder og producenter på sundhedsområdet, efterretninger indhentet fra åbne kilder (OSINT) og andre relevante aktører såsom cyberknudepunkter, centre for informationsudveksling og analyse (ISAC'er) og retshåndhævende myndigheder. Et øget samarbejde mellem ENISA og Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol) – f.eks. om mønstre for cyberkriminalitet rettet mod sundhedssektoren – vil yderligere øge situationsbevidstheden.

Centrene for informationsudveksling og analyse fungerer som centrale ressourcer for efterretninger om cybertrusler, fremmer tovejsudveksling af oplysninger mellem den offentlige og den private sektor og styrker tillidsskabelsen. Støttecentret bør øge støtten til det **europæiske center for informationsudveksling og analyse på sundhedsområdet** med værktøjer, informationsudveksling og sektorspecifikke rapporter om situationsbevidstheden samt fremme et tillidspræget fællesskab for taktisk og strategisk samarbejde. Medlemsstaterne bør tilskynde til udvikling af nationale centre for

[40] ENISA Health Threat Landscape 2023.
[41] Afgørelse 1150/161/2021 af den finske ombudsmand for beskyttelse af personoplysninger.

informationsudveksling og analyse på sundhedsområdet[42]. Centrene for informationsudveksling og analyse bør også tilskyndes til at samle sundhedstjenesteydere og producenter for at give anledning til en fælles forståelse af cybersikkerhedstrusler, herunder i forsyningskæden, og facilitere en dialog om sikker udformning af produkter, hvor der tages hensyn til de faktiske forhold på stedet.

3.3.Hurtig reaktion og genopretning

I betragtning af den høje følsomhed af patienters sundhedsdata og de potentielt ødelæggende virkninger af cyberangreb på sundhedstjenesterne er en hurtig og effektiv reaktion på cybersikkerhedshændelser afgørende for at beskytte patientsikkerheden. Når et hospital eller en sundhedstjenesteyder står over for et cyberangreb, er det første kontaktpunkt den pågældende nationale CSIRT[43]. CSIRT'en er ansvarlig for at yde rettidig støtte, ideelt set inden for 24 timer, for at hjælpe med at håndtere væsentlige hændelser. Hvis en hændelse overstiger CSIRT'ens kapacitet, bør der imidlertid være EU-støtte til rådighed for at sikre en hurtig og effektiv reaktion.

EU's cybersikkerhedsreserve, som er oprettet i henhold til forordningen om cybersolidaritet, leverer tjenester til håndtering af hændelser fra betroede udbydere af administrerede sikkerhedstjenester for at bistå i forbindelse med væsentlige eller omfattende cybersikkerhedshændelser og den indledende genopretningsindsats. Reserven er udformet med henblik på at supplere medlemsstaternes CSIRT'ers indsats og sætter dem i stand til at anmode om yderligere støtte i tilfælde, der involverer kritiske sektorer såsom sundhed. For at forbedre dette system **bør Kommissionen og ENISA sikre, at reserven omfatter en beredskabstjeneste specifikt for sundhedssektoren**. Som supplement til andre eksisterende rammer vil denne tjeneste straks kunne udsende eksperter for at håndtere væsentlige eller omfattende cybersikkerhedshændelser på sundhedsområdet, hvis den nationale støtte er utilstrækkelig.

For at forbedre reaktionen og genopretningen bør støttecentret i samarbejde med NIS-samarbejdsgruppen, CSIRT-netværket og, i det omfang det er relevant, Europol udarbejde **drejebøger for reaktion på cyberhændelser, der er skræddersyede til sundhedsområdet**. Drejebøgerne skal vejlede både CSIRT'er og sundhedsorganisationer i, hvordan de bør reagere på specifikke cybersikkerhedstrusler, herunder ransomware. I betragtning af hvor vigtigt det er, at der er et effektivt samarbejde mellem CSIRT'er og retshåndhævende myndigheder om at reagere på og efterforske cybersikkerhedshændelser af kriminel karakter, bør drejebøgerne bl.a. indeholde klar vejledning i, hvordan sådanne hændelser indberettes til de retshåndhævende myndigheder. Desuden kan støttecentret **fremme en bred udrulning af nationale cybersikkerhedsøvelser på grundlag af erfaringer fra**

[42] F.eks. har Finland et nationalt center for informationsudveksling og analyse for social- og sundhedssektoren. Se Finnish National Cybersecurity Centre: "ISAC information sharing groups". Findes på https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

[43] I NIS 2-direktivets artikel 23, stk. 1, er der fastsat krav om, at væsentlige og vigtige enheder skal underrette den relevante CSIRT eller i givet fald den kompetente myndighed om væsentlige hændelser.

øvelser såsom ENISA's Cyber Europe-øvelse i 2022 med henblik på at afprøve drejebøgerne og styrke protokoller for reaktion på hændelser.

For at skabe grundlag for politikker og vurdere effektiviteten af de foranstaltninger, der træffes over for ransomwareangreb, er det nødvendigt at indsamle flere data. Derfor bør medlemsstaterne anmode de enheder, der er omfattet af NIS 2-direktivet, herunder sundhedsorganisationer, om at indberette enhver betaling af løsepenge, som de har foretaget eller planlægger at foretage, sammen med de andre oplysninger, de giver ved indberetning af væsentlige cybersikkerhedshændelser. En sådan indberetning understøtter en effektiv efterforskning af ransomwarehændelser, herunder sporing af betalinger på kryptovalutabørse med henblik på at identificere modtagerne.

Genopretningshastigheden er en afgørende faktor for at opretholde modstandsdygtigheden og offentlighedens tillid, navnlig på sundhedsområdet, hvor nedetid kan skabe forstyrrelser for patientplejen. For at sikre en effektiv genopretning efter ransomwareangreb skal sundhedstjenesteyderne have sikre, ajourførte og isolerede sikkerhedskopier, der hurtigt kan gendannes. Støttecentret kan som en del af sit tjenestekatalog tilbyde **en abonnementstjeneste for genopretning efter ransomware og hjælpe hospitaler og sundhedstjenesteydere med at udarbejde genopretningsplaner på forhånd**. ENISA og Europol bør samarbejde om at indkredse de mest almindelige ransomwaretyper, der bruges mod sundhedsorganisationer, og **udvide registret over dekrypteringsværktøjer**, der er tilgængeligt gennem No More Ransom-projektet[44]. De bør også udarbejde og fremme tilgængelig vejledning for at hjælpe sundhedstjenesteydere med at undgå at betale løsepenge ved hjælp af dekrypteringsværktøjer.

Det **internationale initiativ til bekæmpelse af ransomware**[45] er et værdifuldt forum for udveksling vedrørende specifikke ransomwarehændelser og opbygning af medlemslandenes evne til at styrke deres cybersikkerhedsrammer og efterforskningskapacitet over for aktører, der benytter sig af ransomware. Kommissionen vil i samarbejde med den højtstående repræsentant fortsætte med at fremme samarbejdet i initiativet til bekæmpelse af ransomware, herunder med henblik på imødegåelse af ransomwaretrusler mod sundhedssektoren. Derudover vil Kommissionen søge samarbejde i **G7-arbejdsgruppen om cybersikkerhed** for at styrke cybersikkerheden i sundhedssektoren. Arbejdsgruppen kan navnlig overveje mulighederne for at støtte sundhedssektoren over for trusler som ransomware på grundlag af overvejelser, som f.eks. den fælles erklæring om ransomwareangreb mod sundhedsfaciliteter af 8. november 2024, som blev fremsat i FN's Sikkerhedsråd[46].

4. Foranstaltninger på nationalt plan

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

Denne handlingsplans kapacitet til at forbedre cybersikkerheden i sundhedssektoren afhænger af, at medlemsstaterne inddrages og er aktivt engagerede. Med henblik på at handlingsplanen gennemføres korrekt, kan medlemsstaterne udpege **nationale støttecentre for cybersikkerhed specifikt for hospitaler og sundhedstjenesteydere**. Centrene vil fungere som de primære kontaktpunkter for sundhedssektoren på nationalt plan og arbejde tæt sammen med ENISA-støttecentret. Hvor det er muligt og relevant, bør medlemsstaterne udpege eksisterende organer som nationale støttecentre for cybersikkerhed, f.eks. nationale CSIRT'er på sundhedsområdet eller relevante myndigheder.

Medlemsstaterne opfordres også til at udarbejde **nationale handlingsplaner med fokus på cybersikkerhed i sundhedssektoren**. Planerne vil skulle skitsere de specifikke cybersikkerhedsrisici, som sundhedssystemerne står over for, og de nationale foranstaltninger, der træffes for at imødegå dem, og samtidig sikre, at ressourcerne og praksis på europæisk plan anvendes effektivt. ENISA-støttecentret kan bistå med at udarbejde planerne under hensyntagen til allerede eksisterende nationale planer og koordinere indsatsen for at sikre, at de enkelte medlemsstaters ressourcer og strategier supplerer hinanden.

Et andet centralt fokus for medlemsstaterne er at fremme ressourcedeling mellem sundhedstjenesteydere, hvilket kan opnås gennem **fælles udbud eller ved at samle ressourcer** på nationalt, regionalt eller endda europæisk plan. Denne tilgang vil mindske den finansielle byrde for de enkelte enheder og samtidig øge deres forhandlingsposition over for udbydere af cybersikkerhedstjenester.

F.eks. er der med det franske CaRE-program[47] indført en række foranstaltninger på nationalt og regionalt plan for at håndtere udfordringer med hensyn til ressourcer: et cyberkatalog giver et overblik over de cyberløsninger og -pakker, der stilles til rådighed for hospitaler gennem det nationale cybersikkerhedsagentur, agenturet for digital sundhed, regionale agenturer, nationale indkøbsorganisationer, samt kommercielle løsninger. Dette suppleres af yderligere finansiering til regionale agenturer, så de kan tilbyde delte ressourcer.

Medlemsstaterne bør også gøre noget ved de utilstrækkelige investeringer i cybersikkerhed i sundhedssektoren. For at sikre tilstrækkelig finansiering bør de fastsætte **ikkebindende benchmarks og overvåge finansieringsmål, der specifikt fokuserer på cybersikkerhed**, og samtidig sikre, at investeringerne ikke hæmmer væsentlig patientpleje. Med disse finansieringsmål bør der også sigtes mod at indarbejde sikkerhedshensyn i alle digitale investeringer i sektoren. Medlemsstaterne kan udveksle bedste praksis og rådgivning om målene via platforme såsom e-sundhedsnetværket[48].

5. Offentlig-privat samarbejde

[47] Det franske agentur for digital sundhed: Cybersécurité acceleration et Résilience des Établissements (CaRE). Kan tilgås på https://esante.gouv.fr/strategie-nationale/cybersecurite.

[48] E-sundhedsnetværket er et frivilligt netværk af nationale myndigheder med ansvar for e-sundhed, som er udpeget af medlemsstaterne. Netværket er oprettet i medfør af artikel 14 i direktiv 2011/24/EU.

Offentlig-privat samarbejde og høring af sundhedstjenesteydere, andre enheder i sundhedssektoren samt relevante aktører i cybersikkerhedsindustrien er afgørende for en vellykket gennemførelse af handlingsplanen. For yderligere at bidrage til støttecentrets arbejde **vil Kommissionen med støtte fra ENISA oprette et fælles rådgivende udvalg for cybersikkerhed på sundhedsområdet** bestående af højtstående repræsentanter fra både sundheds- og cybersikkerhedsområdet, som kan rådgive Kommissionen og støttecentret om virkningsfulde foranstaltninger og drøfte den videre udvikling af offentlig-private partnerskaber på området. Udvalget vil bygge videre på den eksisterende indsats for offentlig-private partnerskaber, herunder det europæiske center for informationsudveksling og analyse på sundhedsområdet.

Derudover vil Kommissionen iværksætte en **opfordring til handling**, der skal få cybersikkerhedsvirksomheder, fonde, uddannelsesinstitutioner og interessenter fra industrien til at **give tilsagn om at gøre en indsats for at håndtere udfordringerne i sektoren**. Med udgangspunkt i erfaringerne fra akademiet for cybersikkerhedsfærdigheder kan sådanne tilsagn f.eks. gives inden for rammerne af akademiet og omfatte levering af uddannelseskurser og -materialer med fokus på sundhedssektoren til fagfolk inden for cybersikkerhed[49]. Andre tilsagn kan også vedrøre oplysningsaktiviteter eller levering af administrerede sikkerhedstjenester til særligt sårbare enheder gratis eller til en nedsat pris med henblik på at øge deres beredskab og cybersikkerhedsmæssige robusthed. Desuden kan tilsagnene bestå i at dele efterretninger om cybertrusler med ENISA-støttecentret. Støttecentret bør fastholde et overblik over de tilsagn, der gives i forbindelse med opfordringen til handling, med det formål at sikre sammenhæng og komplementaritet.

6. Afskrækkelse af cybertrusselsaktører

EU's interne og eksterne cybersikkerhedspolitikker bør støtte målet om at afskrække cybertrusselsaktører fra at angribe europæiske sundhedssystemer. Cyberangreb mod sundhedsorganisationer er en særlig uacceptabel form for ondsindet cyberaktivitet, fordi de kan true patientsikkerheden og bringe menneskeliv i fare. Derfor bør EU's afskrækkelsesevne inden for cybersikkerhed og retshåndhævelse anvendes i fuldt omfang til at underminere den overordnede forretningsmodel for de trusselsaktører, der går efter sundhedssektoren, og til at fratage dem deres kilde til profit. Dette vil omfatte fremme af grænseoverskridende efterforskninger gennem øget udveksling af kompromitteringsindikatorer og andre relevante data samt et øget fokus på mål af høj værdi og centrale kriminelle formidlere såsom bulletproof hosting eller tjenester til blanding af kryptovaluta.

Den **cyberdiplomatiske værktøjskasse** udgør en ramme for forebyggelse, afskrækkelse og reaktion med hensyn til cyberangreb mod EU, medlemsstater og partnere. Den højtstående repræsentant vil fortsat anvende den eksisterende cybersanktionsramme til at reagere på trusler rettet mod sundhedssystemer.

Det er et vigtigt afskrækkende middel, at kriminelle aktører bliver draget til ansvar for deres handlinger. Medlemsstaterne bør derfor sikre, at retshåndhævelsen integreres fuldt ud i deres nationale handlingsplaner. De bør navnlig gøre fuld brug af bestemmelserne i medfør af direktivet om angreb på

[49] Cyber Skills Academy: Get Involved | Digital Skills and Jobs Platform.

informationssystemer[50] og Europarådets Budapestkonvention om IT-kriminalitet til at afskrække fra angreb, retsforfølge kriminelle og optrevle kriminelle infrastrukturer, der faciliterer angreb[51]. En vellykket gennemførelse af disse værktøjer bør sikre, at kriminelle og ondsindede handlinger mod sundhedsplejen straffes.

7. Gennemførelse og overvågning af handlingsplanen

Igennem hele denne handlingsplan er der opstillet en række opgaver for et støttecenter, der skal oprettes inden for rammerne af ENISA. Dette sikrer en holistisk og sammenhængende gennemførelse af handlingsplanen, samtidig med at det undgås, at der oprettes nye enheder, der kan føre til potentielle overlap og medføre generalomkostninger. Kommissionen agter at sikre passende ressourcer til støttecentret.

Når støttecentret er operationelt, bør ENISA i samråd med Kommissionen regelmæssigt give opdateringer om støttecentrets arbejde til ENISA's bestyrelse samt relevante netværk i medlemsstaterne, navnlig NIS-samarbejdsgruppen, CSIRT-netværket, e-sundhedsnetværket og, hvis det er relevant, Udvalget for det Europæiske Sundhedsdataområde. ENISA bør desuden løbende indgå i udvekslinger med det offentlig-private Rådgivende Udvalg for Cybersikkerhed på Sundhedsområdet om gennemførelsen af de foranstaltninger, som støttecentret tilbyder.

ENISA's regelmæssige rapporter, som f.eks. rapporten om cybersikkerhedssituationen i Unionen, som giver en samlet vurdering af modenheden af cybersikkerhedskapaciteter og -ressourcer i hele EU, herunder i sundhedssektoren, bør tjene som en lejlighed til at offentliggøre relevante data til støtte for overvågningen af handlingsplanen. Desuden kan ENISA's EU-cybersikkerhedsindeks[52] give kvantitative og kvalitative data, der kan udgøre et evidensgrundlag for at vurdere sundhedssektorens kritikalitet og modenhed.

8. Næste skridt

Med denne meddelelse er der opstillet en ambitiøs dagsorden for større cybersikkerhed i sundhedssektoren i EU. Med den foreslåede oprettelse af støttecentret for cybersikkerhed for hospitaler og sundhedstjenesteydere i hjertet af ENISA udstikker handlingsplanen en vej mod en sammenhængende og fælles europæisk tilgang til udfordringen i forbindelse med cybersikkerhed i sektoren.

Denne meddelelse bør ses som startskuddet til en proces, der skal forbedre cybersikkerheden i sundhedssektoren. Vedtagelsen af handlingsplanen vil derfor blive ledsaget af en iværksættelse af

[50] Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng.
[51] Konventionen om IT-kriminalitet (Budapestkonventionen, ETS nr. 185) og protokollerne hertil: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

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

omfattende høringer af interessenter og en videreførelse af udvekslingerne med medlemsstaterne og relevante netværk for at indsamle viden. På grundlag af resultaterne af høringerne agter Kommissionen at fremsætte henstillinger i fjerde kvartal af 2025 for yderligere at finjustere handlingsplanen.

Kommissionen opfordrer medlemsstaterne og alle interessenter til at samarbejde om at indfri handlingsplanens ambitioner.

BILAG – Oversigt over foreslåede foranstaltninger

Kommissionen:

ENISA-støttecenter for cybersikkerhed for hospitaler og sundhedstjenesteydere	
Sikre passende ressourcer til støttecentret for cybersikkerhed Samarbejde med Det Europæiske Kompetencecenter for Cybersikkerhed om at iværksætte pilotprojekter for at udvikle bedste praksis for cyberhygiejne og sikkerhedsrisikovurdering og om at imødekomme behovet for løbende cybersikkerhedsovervågning, trusselsefterretninger og reaktion på hændelser ved hjælp af de nyeste cybersikkerhedsløsninger med henblik på udarbejdelse af det europæiske støttecenter for cybersikkerheds tjenestekatalog	2025
Forebyggelse af cybersikkerhedshændelser	
I samråd med NIS-samarbejdsgruppen, EU-CyCLONe og ENISA undersøge muligheden for at udpege sundhed som en sektor, hvor der kan ydes støtte til koordineret beredskabstestning i henhold til forordningen om cybersolidaritet	Første kvartal 2025
Hurtig reaktion og genopretning	
Sammen med ENISA sikre, at EU's cybersikkerhedsreserve omfatter en beredskabstjeneste specifikt for sundhedssektoren	Fjerde kvartal 2025
Offentlig-privat samarbejde	
Med støtte fra ENISA oprette et fælles rådgivende udvalg for cybersikkerhed på sundhedsområdet	Første kvartal 2025
Iværksætte en opfordring til handling, der skal få cybersikkerhedsvirksomheder, fonde, uddannelsesinstitutioner og interessenter fra industrien til at give tilsagn om at gøre en indsats for at håndtere udfordringerne i sundhedssektoren	Andet kvartal 2025
Afskrækkelse af cybertrusselsaktører	
Sammen med den højtstående repræsentant undersøge anvendelsen af foranstaltninger i den cyberdiplomatiske værktøjskasse til at forebygge,	2025

modvirke, afskrække fra og reagere på ondsindede aktiviteter mod sundhedssystemer	
Fremme internationalt samarbejde mod aktører, der benytter sig af ransomware, navnlig inden for rammerne af det internationale initiativ til bekæmpelse af ransomware, i samarbejde med den højtstående repræsentant	2025-2026
Søge samarbejde i G7-arbejdsgruppen om cybersikkerhed for at styrke cybersikkerheden i sundhedssektoren	2025-2026
Næste skridt	
Iværksætte omfattende høringer af interessenter	Første kvartal 2025
Vedtage henstillinger for yderligere at finjustere handlingsplanen	Fjerde kvartal 2025

ENISA:

EU-støttecenter for cybersikkerhed for hospitaler og sundhedstjenesteydere	
Påbegynde arbejdet med at oprette et europæisk støttecenter for cybersikkerhed for hospitaler og sundhedstjenesteydere	Andet kvartal 2025
Udarbejde et omfattende tjenestekatalog, som støttecentret for cybersikkerhed skal stille til rådighed	Fra fjerde kvartal 2025
Forebyggelse af cybersikkerhedshændelser	
Give vejledning, der fremhæver den mest afgørende cybersikkerhedspraksis, og hjælpe sundhedstjenesteydere med at gennemføre den	Tredje kvartal 2025
I tæt samarbejde med Kommissionen og medlemsstaterne udvikle et reguleringsmæssigt kortlægningsværktøj	Første kvartal 2025
Udvikle en ramme for vurdering af cybersikkerhedsmodenheden, der er specifik for sundhedsområdet	Tredje kvartal 2025
Gennemføre en årlig vurdering af cybersikkerhedsmodenheden på sundhedsområdet	2025-2026

Samarbejde med medlemsstaterne og de regionale programmyndigheder om at udarbejde skabelonprogrammer for cybersikkerhedsvouchere	2025-2026
Udvikle nye retningslinjer for udbud for så vidt angår cybersikkerhed for hospitaler og sundhedstjenesteydere	Tredje kvartal 2025
Oprette et europæisk netværk af ledende informationssikkerhedsansvarlige (CISO'er) på sundhedsområdet	Første kvartal 2026
Udforme og fremme uddannelsesmoduler og -kurser om cybersikkerhed for sundhedsprofessionelle	Første kvartal 2026
Europæisk kapacitet til at opdage cybertrusler mod sundhedssektoren	
Opbygge et europæisk KEV-katalog for medicinsk udstyr, elektroniske patientjournalsystemer og udbydere af IKT-udstyr og -software på sundhedsområdet	Fjerde kvartal 2025
Indføre en EU-dækkende abonnementstjeneste for tidlig varsling i sundhedssektoren	Fra og med 2026
Støtte det europæiske center for informationsudveksling og analyse på sundhedsområdet med værktøjer og informationsudveksling	2025-2026
Hurtig reaktion og genopretning	
Sammen med Kommissionen sikre, at EU's cybersikkerhedsreserve omfatter en beredskabstjeneste specifikt for sundhedssektoren	Fjerde kvartal 2025
I samarbejde med CSIRT-netværket udarbejde drejebøger for reaktion på cyberhændelser, der er skræddersyede til sundhedsområdet	Tredje kvartal 2025
Facilitere en omfattende udrulning af nationale cybersikkerhedsøvelser for at afprøve drejebøgerne og styrke protokoller for reaktion på hændelser	Fra og med fjerde kvartal 2025
Tilbyde en abonnementstjeneste for genopretning efter ransomware	Fra og med 2026
Sammen med Europol indkredse de mest almindelige ransomwaretyper, der bruges mod sundhedsorganisationer, og udvide registret over	Fjerde kvartal 2025

dekrypteringsværktøjer gennem No More Ransom-projektet	
Sammen med Europol udarbejde tilgængelig vejledning for at hjælpe sundhedstjenesteydere med at undgå at betale løsepenge	Tredje kvartal 2025
Foranstaltninger på nationalt plan	
Bistå medlemsstaterne med at udarbejde nationale handlingsplaner	2025
Koordinere indsatsen for at sikre, at de enkelte medlemsstaters ressourcer og strategier supplerer hinanden	2025-2026
Gennemførelse og overvågning af handlingsplanen	
I samråd med Kommissionen regelmæssigt give opdateringer om arbejdet i støttecentret for cybersikkerhed til relevante netværk i medlemsstaterne	2025-2026
Løbende indgå i udvekslinger med Det Rådgivende Udvalg for Cybersikkerhed på Sundhedsområdet	2025-2026

Medlemsstaterne:

Europæisk kapacitet til at opdage cybertrusler mod sundhedssektoren	
Dele underretninger om hændelser fra hospitaler og sundhedstjenesteydere, der er omfattet af NIS 2-direktivet, med det europæiske støttecenter for cybersikkerhed	Fra og med fjerde kvartal 2025
Tilskynde til udvikling af nationale centre for informationsudveksling og analyse på sundhedsområdet	2025-2026
Forebyggelse af cybersikkerhedshændelser	
Inden for rammerne af NIS-samarbejdsgruppen foretage en koordineret sikkerhedsrisikovurdering, hvor både tekniske og strategiske risici i forbindelse med forsyningskæder for medicinsk udstyr vurderes	Fjerde kvartal 2025
Hurtig reaktion og genopretning	

Udrulle nationale cybersikkerhedsøvelser for at afprøve drejebøgerne og styrke protokoller for reaktion på hændelser	Fra og med 2026
Foranstaltninger på nationalt plan	
Udpege nationale støttecentre for cybersikkerhed for hospitaler og sundhedstjenesteydere	Andet kvartal 2025
Udarbejde nationale handlingsplaner med fokus på cybersikkerhed i sundhedssektoren	Fjerde kvartal 2025
Lette ressourcedeling mellem sundhedstjenesteydere	2025-2026
Fastsætte ikkebindende benchmarks og overvåge finansieringsmål, der specifikt fokuserer på cybersikkerhed	Fjerde kvartal 2025
Anmode sundhedsorganisationer og andre enheder, der er omfattet af NIS 2-direktivet, om at indberette planer om at betale løsepenge	Fjerde kvartal 2025