Raad van de
Europese Unie

Brussel, 16 januari 2025
(OR. en)

5426/25

CYBER 21
SAN 15

BEGELEIDENDE NOTA

van:	de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur
ingekomen:	15 januari 2025
aan:	mevrouw Thérèse BLANCHET, secretaris-generaal van de Raad van de Europese Unie
nr. Comdoc.:	COM(2025) 10 final
Betreft:	MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S Europees actieplan voor de cyberbeveiliging van ziekenhuizen en zorgaanbieders

Hierbij gaat voor de delegaties document COM(2025) 10 final.

Bijlage: COM(2025) 10 final

EUROPESE
COMMISSIE

Brussel, 15.1.2025
COM(2025) 10 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

Europees actieplan voor de cyberbeveiliging van ziekenhuizen en zorgaanbieders

1. Inleiding

De beveiligingssituatie in de EU verandert snel vanwege een escalatie van hybride en cyberaanvallen met als doel onze samenleving te destabiliseren en te ontwrichten, verdeeldheid te zaaien en profijt te trekken uit cybercriminaliteit. Daarom moet Europa zich in alle sectoren dringend beter voorbereiden op en weerbaarder worden tegen deze nieuwe omstandigheden, en daarvoor een "maatschappijbrede" en "overheidsbrede" benadering volgen. Die oproep is gedaan in het verslag van Sauli Niinistö, de speciale adviseur van de voorzitter van de Europese Commissie.

Veilige en weerbare zorgstelsels vormen een hoeksteen van het sociale model van de EU. Die stelsels en de ziekenhuizen worden echter steeds vaker bedreigd, met name door bendes die ransomware gebruiken om winst te slaan uit de hoge waarde van patiëntengegevens, zoals elektronische patiëntendossiers. De afgelopen vier jaar is geen enkele andere sector in de EU vaker aangevallen dan de gezondheidszorg. Onder meer tijdens de coronapandemie werd de zorginfrastructuur steeds vaker het doelwit van cyberaanvallen. Dergelijke aanvallen op ziekenhuizen en zorgaanbieders berokkenen mensen rechtstreeks schade, vertragen medische procedures, veroorzaken lange wachttijden op de spoedafdeling en kunnen er in extreme gevallen toe leiden dat mensenlevens verloren gaan.

De problematiek wordt nog prangender omdat de sector een belangrijke digitale transformatie doormaakt. Dankzij digitale gezondheid en het gebruik en hergebruik van gezondheidsgegevens kunnen zorgmodellen worden ontwikkeld die beter zijn afgestemd op de behoeften en voorkeuren van de mensen, door ziekten in de kiem te smoren of snellere behandelingen te bieden. De integratie van digitale instrumenten en oplossingen in klinische processen en het gebruik en hergebruik van gezondheidsgegevens kunnen als basis dienen voor betere klinische beslissingen en bijdragen tot snellere, betere en verder geautomatiseerde patiëntenzorg. Digitale instrumenten, gegevensgebruik en medische hulpmiddelen – die vaak verbonden zijn met het internet en worden aangedreven door artificiële intelligentie (AI) – zijn ook cruciaal om uitdagingen zoals het tekort aan zorgaanbieders aan te pakken.

Tegelijkertijd vergroten digitale instrumenten echter ook de potentiële doelwitten van cybercriminelen. Bovendien deinzen bepaalde overheden er niet voor terug om zorginstellingen in het vizier te nemen, zoals blijkt uit de aanhoudende Russische aanvalsoorlog tegen Oekraïne. Dit maakt van de sector een potentieel doelwit voor cyberaanvallen als onderdeel van een bredere hybride campagne. Cyberaanvallen brengen niet alleen de veiligheid van de patiënten in gevaar, maar ondermijnen ook het vertrouwen van het grote publiek in de zorginfrastructuur en brengen aanzienlijke herstelkosten met zich mee. Naast bescherming tegen cyberaanvallen is een weerbare en veilige digitale infrastructuur ook essentieel om de uitvoering en volledige uitrol van de Europese ruimte voor gezondheidsgegevens (EHDS)[1] te ondersteunen.

Daarom moeten de cyberbeveiliging en -weerbaarheid van de Europese ziekenhuizen en zorgaanbieders worden opgewaardeerd en verbeterd, zoals voorzitter Von der Leyen in haar politieke beleidslijnen voor de Commissie 2024-2029[2] heeft benadrukt. Met dit actieplan wordt ingespeeld op

[1] https://www.consilium.europa.eu/nl/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_nl.

de urgentie van de situatie en de specifieke dreigingen voor de sector. Er bestaat geen wondermiddel om de uitdagingen van cyberbeveiliging in de gezondheidszorg op te lossen. In plaats daarvan wordt in het actieplan opgeroepen tot meer preventie, paraatheid en een beter gecoördineerde, solidaire aanpak, waarbij de deskundigheid van de Europese cyberbeveiligingssector wordt benut. Als zodanig weerspiegelt het actieplan de beveiligingsaanpak van de EU die bij de komende Europese strategie voor interne veiligheid verder zal worden ontwikkeld en geformaliseerd, met een alomvattende respons om het hoofd te bieden aan alle bedreigingen voor de interne veiligheid en met de nadruk op het vermogen om op dreigingen te anticiperen, schade te voorkomen en mensen te beschermen. Daarbij wordt op alle niveaus een maatschappijbrede benadering gehanteerd.

De gezondheidszorg beslaat veel instanties en actoren, zoals ziekenhuizen, verzorgingshuizen, revalidatiecentra en diverse zorgaanbieders, naast de farmaceutische, medische en biotechnologische industrie, fabrikanten van medische hulpmiddelen en instellingen voor gezondheidsonderzoek. Dit actieplan is voornamelijk gericht op de cyberbeveiliging van ziekenhuizen en zorgaanbieders. Onder die laatste wordt elke natuurlijke of rechtspersoon of elke andere instantie verstaan die op het grondgebied van een lidstaat op een wettelijke manier gezondheidszorg verstrekt[3]. Ziekenhuizen en zorgaanbieders zijn onderling afhankelijk van andere zorginstanties en staan het dichtst bij de mensen. Tegelijkertijd zouden maatregelen om de cyberbeveiliging van ziekenhuizen en zorgaanbieders te verbeteren ook gericht moeten zijn op risico's voor de bredere toeleveringsketen en het bredere ecosysteem. Die risico's vloeien onder andere voort uit instanties die gezondheidsgegevens gebruiken voor onderzoek en machinaal leren of die medische hulpmiddelen produceren, met name digitale hulpmiddelen die verbinding maken met het internet of andere apparaten (het internet der dingen).

Hoewel de beveiliging van zorgstelsels in de eerste plaats een nationale bevoegdheid is, is gezondheid ook een kritieke sector in het kader van de richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de EU (NIS 2-richtlijn)[4]. Cybercriminelen en andere bedreigende actoren zijn landsgrensoverschrijdend actief en in de lidstaten worden zorgorganisaties geconfronteerd met vergelijkbare uitdagingen voor cyberbeveiliging. Samenwerking op Europees niveau is waardevol om goede werkwijzen op nationaal en EU-niveau te delen en op te schalen. Daarom worden in het actieplan coördinatie en maatregelen op EU-niveau voorgesteld en worden de lidstaten opgeroepen actie te ondernemen om een verschil te maken voor de gezondheidszorg en het gezondheidsecosysteem in ruimere zin.

De nadruk in het actieplan ligt in de eerste plaats op een groter vermogen van de sector om cyberincidenten te **voorkomen**, want dat is altijd beter dan genezen. Ten tweede bevat het actieplan maatregelen voor een betere informatie-uitwisseling over cyberbeveiliging en een beter vermogen om cyberdreigingen **op te sporen**, zodat er sneller op kan worden gereageerd. Ten derde worden er

[3] Artikel 3, punt g), van Richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg, https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32011L0024.

[4] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80), https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:02022L2555-20221227&qid=1737629875209.

maatregelen aangereikt om beter op incidenten te **reageren** en ervan te **herstellen**. Tot slot bevat het actieplan manieren om cybercriminelen te **ontmoedigen** zorgstelsels in Europa aan te vallen.

Het actieplan zal samen met de zorgaanbieders, het ruimere gezondheidsecosysteem, de lidstaten en de cyberbeveiligingsgemeenschap worden uitgevoerd. Deze samenwerking is cruciaal om de doeltreffendste maatregelen te bepalen en verder te verfijnen, zodat alle kritieke zorgaanbieders in Europa daar baat bij hebben. Daarom gaat deze mededeling vergezeld van een uitgebreide raadpleging van belanghebbenden, de sector en de lidstaten. Internationale samenwerking is belangrijk voor cyberbeveiliging vanwege het landsgrensoverschrijdende en onderling verbonden karakter van cyberdreigingen. In de uitbreidings-, nabuurschaps- en andere strategische partnerlanden van de EU zijn ook vergelijkbare dreigingen aanwezig, en uiteindelijk kan dat de beveiliging van de kritieke infrastructuur in de EU ook in gevaar brengen. Het is daarom van belang om rekening te houden met de lessen die uit de uitvoering van het actieplan worden getrokken, ook bij de samenwerking van de EU met uitbreidings- en andere partnerlanden, in het licht van de dreigingsniveaus die zij ondervinden.

2. Cyberbeveiliging van ziekenhuizen en zorgaanbieders

Cyberdreigingen voor de gezondheidszorg

Het aantal cyberaanvallen neemt wereldwijd – en dus ook binnen de EU – toe, en er vormt zich een steeds complexer en dynamischer geheel aan dreigingen. De vooruitgang in AI biedt criminelen en kwaadwilligen krachtige middelen om de nauwkeurigheid en het effect van hun activiteiten te vergroten, maar biedt ook nieuwe mogelijkheden voor cyberbeveiliging doordat er geautomatiseerde, realtime-maatregelen tegen aanvallen kunnen worden ontwikkeld.

Ransomware blijft een essentiële uitdaging voor cyberbeveiliging in de EU en de hele wereld: in een verslag worden de totale jaarlijkse kosten daarvoor tegen 2031 geraamd op meer dan 250 miljard EUR[5]. Als ransomwarecriminelen toeslaan, versleutelen ze niet alleen de gegevens van de slachtoffers voor losgeld, maar lekken ze geleidelijk aan ook meer gevoelige informatie om de druk op te voeren. Een andere grote uitdaging zijn de kwetsbaarheden in software en hardware: volgens het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa)[6] is de gezondheidszorg de sector die de meeste beveiligingsincidenten in verband met dergelijke kwetsbaarheden heeft gemeld[7]. Andere toenemende dreigingen zijn onder meer DDoS-aanvallen (distributed denial-of-service), die zijn ontworpen om

[5] Cybersecurity Ventures (1 juni 2024): "Global Ransomware Damage Costs Predicted to Exceed $265 Billion By 2031". Beschikbaar op https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

[6] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie (de cyberbeveiligingsverordening), https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32019R0881.

[7] Enisa Threat Landscape: Health Sector (juli 2023).

een bepaald systeem met een overvloed aan dataverkeer te overspoelen, waardoor gebruikers er geen toegang meer toe hebben[8].

De gezondheidszorg wordt geconfronteerd met soortgelijke cyberdreigingstrends, met een duidelijke nadruk op ransomware-aanvallen. Volgens Enisa was ransomware in 2021-2023 goed voor 54 % van de onderzochte cyberincidenten in de gezondheidszorg. 83 % van de aanvallen was gebaseerd op financiële overwegingen, namelijk vanwege de grote waarde van gezondheidsgegevens, en 10 % van de aanvallen was afkomstig uit ideologische hoek[9]. Evenzo werd in een verslag van de Commissie in 2024 vastgesteld dat in 71 % van de aanvallen met gevolgen voor de patiëntenzorg (zoals uitgestelde behandelingen, diagnoses en slechtere toegang tot noodhulpdiensten) van ransomware sprake was[10]. Ransomware-aanvallen kunnen de zorgverlening ernstig verstoren, waardoor de veiligheid van patiënten in gevaar komt. Bovendien gaan die aanvallen vaak gepaard met inbreuken op patiëntengegevens[11], die dikwijls gevoelige informatie over hun gezondheid bevatten. Zo wordt het grondrecht op bescherming van de persoonsgegevens geschonden.

Tegelijkertijd ontstaan er door de toenemende digitalisering van de gezondheidszorg meer aanvalsmogelijkheden. Volgens het verslag over de staat van het digitale decennium 2024 heeft gemiddeld 79 % van de EU-burgers toegang tot hun elektronische patiëntendossiers in de eerstelijnszorg[12]. Elektronische patiëntendossiers, klinische informatiesystemen, workflowsystemen van ziekenhuizen, IT-systemen om de vergoeding van behandelingen af te handelen, medische beeldvormingssystemen en medische hulpmiddelen voor diagnostische doeleinden of het toezicht op patiënten zijn allemaal voorbeelden van digitale instrumenten die belangrijk kunnen zijn om de efficiëntie en prestaties van de gezondheidszorg te verbeteren, maar die ook het doelwit van een cyberaanval kunnen worden. Specifieke activiteiten in de gezondheidszorg zoals intensieve zorg en radiologische beeldvorming, of medische vakgebieden zoals oncologie en cardiologie, die sterk afhankelijk zijn van digitale apparaten, lopen extra veel risico op cyberaanvallen. Bovendien kunnen problemen in de toeleveringsketen leiden tot de aanschaf van hulpmiddelen met onvoldoende beveiliging, waardoor de aanwezige risico's nog groter worden.

Zo werden tijdens de coronapandemie grote delen van het Ierse zorgstelsel lamgelegd door een ransomware-aanval, waardoor op de ochtend van het incident van 31 van de 54 acute ziekenhuizen op zijn minst enkele diensten niet werkten[13]. De zorgdiensten moesten terugvallen op papieren

[8] Enisa Threat Landscape 2024.

[9] Enisa Threat Landscape: Health Sector (juli 2023). In het verslag is een analyse gemaakt van zorgaanbieders en andere soorten organisaties, waaronder organisaties die gezondheidsgerelateerd onderzoek verrichten, instanties die bepaalde gezondheidsgerelateerde producten vervaardigen, gezondheidsautoriteiten, ziekteverzekeringsorganisaties, residentiële behandelingsinstellingen en sociale dienstverleners. Beschikbaar op https://www.enisa.europa.eu/publications/health-threat-landscape.

[10] Europese Commissie: Gemeenschappelijk Centrum voor onderzoek, Reina, V., & Griesinger, C., *Cyber security in the health and medicine sector – A study on available evidence of patient health consequences from cyber incident in healthcare settings*, Bureau voor publicaties van de EU, 2024, https://data.europa.eu/doi/10.2760/693487.

[11] Volgens het Enisa Threat Landscape voor de gezondheidszorg is bij 43 % van de onderzochte ransomware-incidenten een data-inbreuk of -diefstal vastgesteld.

[12] Verslag over de staat van het digitale decennium 2024.

[13] Irish Health Service Executive (2021): "Conti cyber attack on the HSE: Independent Post Incident Review".

dossiers, wat de werking vertraagde en de efficiëntie verminderde. De aanval was afkomstig van een phishing-e-mail met een schadelijke bijlage[14]. Het incident toonde aan hoe cyberaanvallen zich over verschillende systemen kunnen verspreiden, en bijgevolg dat het belangrijk is om alle manieren waarop een zorgorganisatie kan worden aangevallen, te beschermen. Het toonde ook het belang aan van een fundamentele cultuur van cyberhygiëne en cyberbeveiliging in alle organisaties.

Maturiteit van cyberbeveiliging van ziekenhuizen en zorgaanbieders

De gezondheidszorg in de EU is zeer divers: eigendom, structuur en omvang van ziekenhuizen en andere zorgaanbieders verschillen sterk per lidstaat. In sommige gevallen is de governance van de gezondheidszorg gecentraliseerd op nationaal niveau, in andere gevallen op regionaal en lokaal niveau. Zorgaanbieders kunnen in publieke of particuliere handen zijn. Bovendien kunnen er ook binnen een land verschillen zijn, bijvoorbeeld als er aanzienlijke sociaal-economische en territoriale ongelijkheden tussen regio's zijn. Dat alles vormt een complex geheel. Dit complexe landschap kan op de proef worden gesteld door grote gezondheidsproblematiek als gevolg van besmettelijke ziekten, zoals de coronapandemie, maar ook door andere gezondheidsrisico's, bijvoorbeeld in verband met de klimaatverandering. Tot slot is er aanzienlijke variabiliteit en versnippering in de mate van digitalisering en het gebruik van technologie door zorgaanbieders. Een voorbeeld van deze complexiteit is dat een onbeschikbare dienst als gevolg van een cyberincident tot ernstige gevaren en letsels voor patiënten kan leiden, zelfs in kleinschalige zorginstellingen zoals klinieken of medische nooddiensten die een essentiële dienst verlenen aan een relatief klein aantal gebruikers.

Volgens het Enisa-verslag over de staat van de cyberbeveiliging in de Unie 2024[15] is de maturiteit van cyberbeveiliging in de gezondheidszorg in de EU van gemiddeld niveau en zijn er grote verschillen tussen zorginstanties in heel Europa. Er zijn tekortkomingen op belangrijke gebieden zoals personele middelen, de kennis van organisaties over hun toeleveringsketens voor informatie- en communicatietechnologie (ICT) en de installatie van actuele beveiligingskenmerken in producten. De sector heeft moeilijkheden op het vlak van elementaire cyberhygiëne en fundamentele cyberbeveiliging. Dat blijkt uit het feit dat bijna alle ondervraagde zorgorganisaties problemen ondervinden om risicobeoordelingen van de cyberbeveiliging uit te voeren en dat bijna de helft zelfs nooit een risicoanalyse heeft uitgevoerd[16].

Een andere belangrijke uitdaging voor de cyberbeveiliging van ziekenhuizen is het raakvlak tussen informatietechnologie (IT) en operationele technologie (OT). Daar komen verschillende beveiligingsprioriteiten voor vertrouwelijkheid, beschikbaarheid en betrouwbaarheid samen en kan een inbreuk op het ene gebied gevolgen hebben voor het andere. In het bovengenoemde Enisa-verslag wordt verder benadrukt dat de gezondheidszorg niet naar behoren presteert om de beveiliging van de

[14] Irish Health Service Executive: "Cyber-attack and HSE response". Beschikbaar op https://www2.hse.ie/services/cyber-attack/what-happened/.
[15] Enisa: Verslag over de staat van de cyberbeveiliging in de Unie 2024 (september 2024). Beschikbaar op https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
[16] Enisa Threat Landscape: Health Sector (juli 2023). Beschikbaar op https://www.enisa.europa.eu/publications/health-threat-landscape.

gebruikte ICT-producten en -processen te waarborgen vanwege de grote verscheidenheid aan zorginstanties, -hulpmiddelen en -producten.

Deze diversiteit, in combinatie met de uiteenlopende niveaus van cyberbewustzijn onder het ziekenhuispersoneel en -bestuur, vormt een complexe uitdaging om de cyberbeveiliging van zorgstelsels te waarborgen. Zo had volgens de Eurobarometer over cybervaardigheden van 2024 slechts 25 % van de ondervraagde ondernemingen in de gezondheids-, onderwijs- en socialezorgsector de afgelopen twaalf maanden opleidingen of bewustmakingsactiviteiten over cyberbeveiliging aangeboden[17]. Er is actie nodig om een cultuur van bewustzijn over cyberbeveiliging onder eerstelijnszorgaanbieders te stimuleren. Personeelsroulatie, gedeelde werkplekken, slecht authenticatiebeheer en verwijderbare media zijn voorbeelden van extra bronnen van kwetsbaarheden die gevolgen kunnen hebben voor de cyberbeveiliging van zorgaanbieders[18].

Vaak worden IT en OT ten minste gedeeltelijk uitbesteed. Uit de Eurobarometer van 2024 bleek dat dat voor 57 % van de ondervraagde ondernemingen in de gezondheid-, onderwijs en socialezorgsector het geval is[19]. Dat aandeel is in geen enkele andere sector hoger. Ook is er een sterke tendens van migratie naar cloudcomputing vanwege de behoefte aan schaalbare gegevensopslag en -beheer, kostenefficiëntie, betere samenwerking en ondersteuning voor geavanceerde technologieën zoals AI en het internet der medische dingen. In 2022 maakte 58 % van de zorgorganisaties gebruik van een digitaal zorgplatform in de cloud[20]. Deze verschuiving kan de efficiëntie aanzienlijk verhogen, maar brengt ook risico's met zich mee waarvoor weloverwogen beslissingen over aanbestedingen en veilige configuratie nodig zijn.

Capaciteitsopbouw en financiering spelen bij al deze uitdagingen een overkoepelende rol. De financiering voor cyberbeveiliging in de gezondheidszorg is beperkt en blijft in de hele EU een uitdaging[21]. Bovendien doen deze financieringsproblemen zich voor in de context van de vergrijzing, die de komende decennia naar verwachting een grote budgettaire druk op de Europese zorgstelsels zal uitoefenen.

Het gebruik van verouderde instrumenten en systemen, de beperkte middelen om incidenten te voorkomen of erop te reageren en lacunes in de maturiteit van cyberbeveiliging zijn vaak het gevolg van financieringstekorten. Ziekenhuizen staan voortdurend voor de uitdaging om een evenwicht te vinden tussen een moderne, veilige en digitale infrastructuur en andere noodzakelijke investeringen om de patiëntenzorg te verbeteren, zoals de aanwerving van artsen en andere zorgaanbieders, de toepassing van nieuwe diagnose- en behandelingsmethoden en de aankoop van hulpmiddelen.

[17] Flash Eurobarometer 547 over cybervaardigheden (mei 2024). Beschikbaar op 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.

[19] Flash Eurobarometer 547 over cybervaardigheden (mei 2024). Beschikbaar op https://europa.eu/eurobarometer/surveys/detail/3176.

[20] Enisa: NIS Investments Report 2022 (november 2022). Beschikbaar op https://www.enisa.europa.eu/publications/nis-investments-2022.

[21] De organisatie en de verstrekking van gezondheidsdiensten en medische zorg is een nationale bevoegdheid krachtens artikel 168 van het Verdrag betreffende de werking van de Europese Unie, en de financiering van de zorgstelsels verschilt per lidstaat.

Volgens Enisa[22] staat de gezondheidszorg slechts op de zevende plaats van de twaalf onderzochte sectoren als het gaat om het aandeel van de totale IT-uitgaven dat naar informatiebeveiliging gaat; in de sector ligt de mediaan op 8,3 %.

3. Europees ondersteuningscentrum voor cyberbeveiliging voor ziekenhuizen en zorgaanbieders

Het EU-kader voor cyberbeveiliging biedt een breed scala aan instrumenten die zouden moeten worden ingezet om de veiligheid en weerbaarheid van ziekenhuizen en zorgaanbieders te verbeteren. Om de talrijke uitdagingen hierboven aan te pakken, moet er een uniforme, strategische benadering op EU-niveau worden ontwikkeld, waarin de nodige middelen, deskundigheid en instrumenten worden samengebracht om cyberdreigingen doeltreffend aan te pakken. Een uitgebreid overzicht en een betere planning en coördinatie zijn essentieel om zorgaanbieders in de hele EU te helpen hun beveiliging te verbeteren. Om dat te bereiken is Enisa het best geplaatst om als onderdeel van zijn mandaat binnen de organisatie een speciaal **Europees ondersteuningscentrum voor cyberbeveiliging voor ziekenhuizen en zorgaanbieders**[23] op te richten[24] om de kritieke infrastructuur van de EU te beschermen en te ondersteunen.

Het centrum zou geleidelijk een **uitgebreide dienstencatalogus moeten ontwikkelen die tegemoetkomt aan de behoeften van ziekenhuizen en zorgaanbieders**, met een overzicht van de beschikbare diensten voor paraatheid, preventie, opsporing en reactie. Samen met de autoriteiten van de lidstaten en op basis van de ervaringen van ziekenhuizen en zorgaanbieders zou het centrum een gebruiksvriendelijk en gemakkelijk toegankelijk register moeten ontwikkelen van alle beschikbare instrumenten op Europees, nationaal en regionaal niveau. Tijdens zijn activiteiten zou het moeten zorgen voor een goede coördinatie met de lidstaten en helpen om voorrang te geven aan acties en die (indien nodig meteen) uit te voeren.

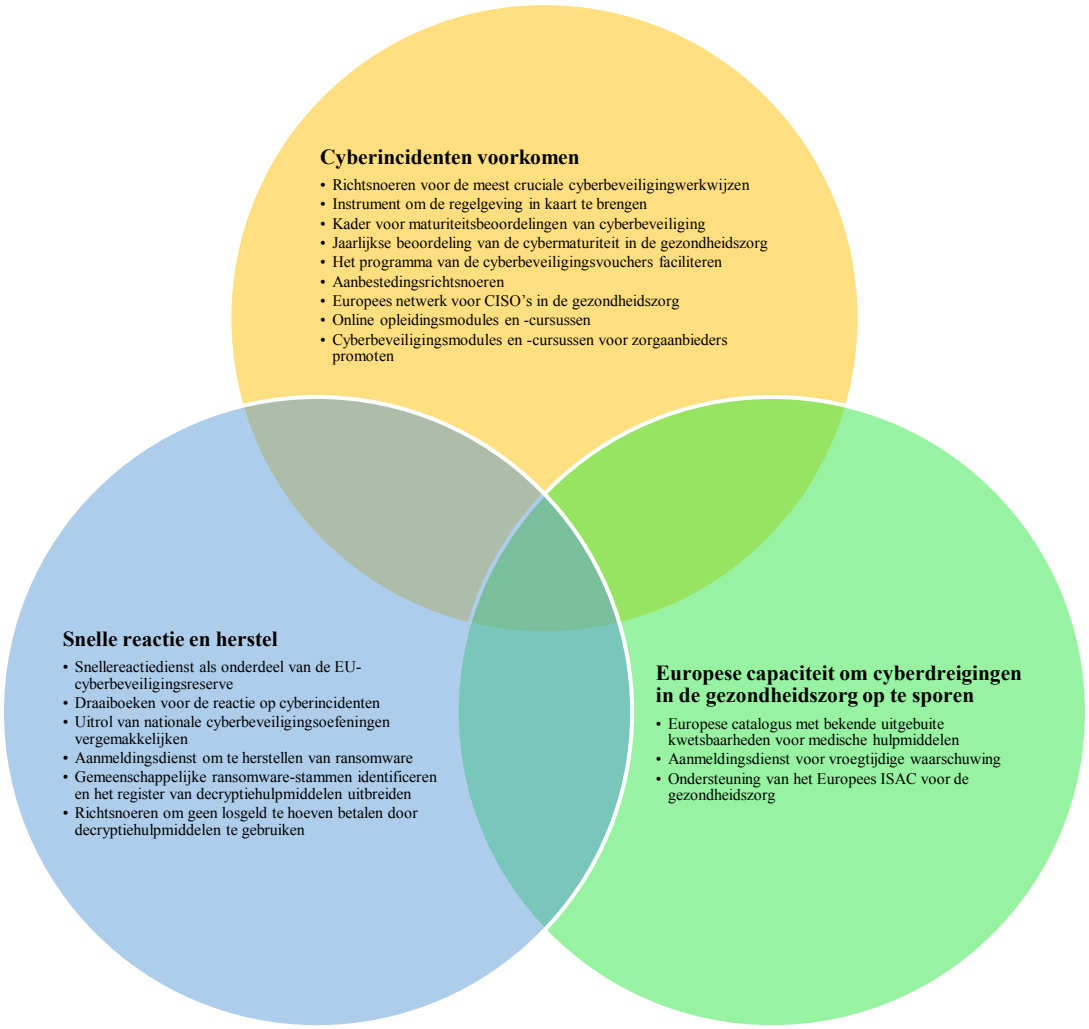
De Commissie zal voorstellen om in de hele EU proefprojecten op te zetten die kunnen dienen als belangrijke bouwsteen voor de ontwikkeling van de dienstencatalogus van het ondersteuningscentrum. Het gaat om projecten om goede werkwijzen op het gebied van cyberhygiëne en beveiligingsrisicobeoordelingen te ontwikkelen, en om de behoefte aan voortdurend cybertoezicht, inlichtingen over dreigingen en reacties op incidenten met geavanceerde cyberbeveiligingsoplossingen aan te pakken. Deze proefprojecten zullen door het programma Digitaal Europa gefinancierd en door het Europees Kenniscentrum voor cyberbeveiliging (ECCC) uitgevoerd worden. De resultaten zullen als input dienen voor verdere acties op EU-niveau, waaronder de werkzaamheden van het centrum.

---

[22] Enisa: NIS Investments Report 2022 (november 2022). Beschikbaar op https://www.enisa.europa.eu/publications/nis-investments-2022.

[23] In dit document ook “ondersteuningscentrum” en “centrum” genoemd.

[24] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15).



Figuur 1: Concepten voor de dienstencatalogus van het ondersteuningscentrum voor ziekenhuizen en zorgaanbieders

3.1. Cyberincidenten voorkomen

Eenvoudige maatregelen die in ons voordeel werken

Basismaatregelen voor cyberbeveiliging, zoals systemen up-to-date houden, backups beheren en multifactorauthenticatie invoeren, kunnen organisaties naar schatting tegen minstens 98 % van de aanvallen beschermen[25]. Veel van de doeltreffendste maatregelen voor cyberhygiëne en risicobeheer

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

zijn vrij eenvoudig in te voeren en dus een laagdrempelige manier om de cyberbeveiliging te verbeteren. Een van de belangrijkste taken van het ondersteuningscentrum zou daarom moeten zijn om **duidelijke, gerichte richtsnoeren te ontwikkelen die de meest cruciale cyberbeveiligingswerkwijzen onder de aandacht brengen en zorgaanbieders helpen die uit te voeren**. Deze steun moet niet alleen gericht zijn op grote ziekenhuizen, maar ook advies op maat omvatten voor kleinere instanties, zoals huisartsenpraktijken en gespecialiseerde klinieken. Die beschikken vaak niet over de middelen voor specifieke cyberbeveiligingsteams, maar blijven even kwetsbaar voor aanvallen. Voorts moet rekening worden gehouden met het regionale belang van specifieke zorginstanties om de patiëntenzorg te waarborgen, bijvoorbeeld in dunbevolkte gebieden. Instanties voor gezondheidsonderzoek die veel gevoelige persoonsgegevens verwerken, kunnen ook baat hebben bij richtsnoeren over basismaatregelen voor cyberbeveiliging om hun weerbaarheid te vergroten.

Zorgorganisaties moeten ook voldoen aan een reeks cyberbeveiligingsverplichtingen die voortvloeien uit de EU-wetgeving[26]. Hoewel de verplichtingen cruciaal zijn om een hoog gemeenschappelijk basisniveau voor cyber- en gegevensbeveiliging te waarborgen, is het essentieel ervoor te zorgen dat de regelgeving niet onnodig moeilijk en omslachtig is. Een sterke nadruk op naleving zou niet mogen indruisen tegen de doelstelling om een sterke cyberbeveiligingscultuur te stimuleren. **Een gemakkelijk toegankelijk instrument om de regelgeving in kaart te brengen kan helpen om de administratieve lasten tot een minimum te beperken voor instanties die aan uiteenlopende regelgeving moeten voldoen.** Naast richtsnoeren en toolkits ontwikkelen, zou het ondersteuningscentrum nauw moeten samenwerken met de Commissie en de lidstaten om een dergelijk instrument zo snel mogelijk te ontwikkelen en te verspreiden. Het centrum zou dan ook een belangrijke rol spelen om de cyberbeveiligingsregels begrijpelijk en gemakkelijk uitvoerbaar te

[26] Zoals de NIS 2-richtlijn; Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen (Verordening cyberweerbaarheid), https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=OJ:L_202402847; Verordening (EU) 2017/745 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen, https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32017R0745; Verordening (EU) 2017/746 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen voor in-vitrodiagnostiek, https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32017R0746; Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32016R0679; Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (verordening artificiële intelligentie), https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=OJ:L_202401689; Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de Europese ruimte voor gezondheidsgegevens (COM(2022) 197 final), https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52022PC0197. De onderhandelingen zijn in het voorjaar van 2024 afgesloten met een politiek akkoord. De bekendmaking in het Publicatieblad wordt na afronding verwacht in het voorjaar van 2025.

maken, bijvoorbeeld door uitvoeringsrichtsnoeren[27] te verstrekken en waar nodig relevante normen te bevorderen.

De komende **Europese portemonnees voor digitale identiteit** zijn een ander instrument om goede cyberhygiëne te vergemakkelijken. Om de risico's van niet toegestane toegang tot gezondheidsgegevens te beperken, is het essentieel minder afhankelijk te worden van zwakke identificatiemechanismen zoals wachtwoorden. Een verschuiving naar veilige aanmeldingsmanieren op basis van betrouwbare identificatie is cruciaal. De Europese portemonnee voor digitale identiteit biedt vanaf eind 2026 een robuuste, uniforme oplossing en een geharmoniseerde aanpak in de hele EU voor elektronische identificatie voor zorgaanbieders. Alle online-gezondheidsinformatiesystemen waarvoor een sterke gebruikersauthenticatie verplicht is, zullen de portemonnee vanaf eind 2027 voor identificatiedoeleinden moeten aanvaarden[28].

Paraatheid en gerichte ondersteuning

Paraatheidstests, met maatregelen zoals penetratietests, zijn een hoeksteen van doeltreffende cyberbeveiliging. De Commissie heeft Enisa al financiering toegewezen voor proefinitiatieven voor paraatheid waaruit is gebleken dat de gezondheidszorg een van de sectoren is die het meest om tests en verdere beoordelingen vragen om lacunes in de maturiteit van cyberbeveiliging vast te stellen. Deze inspanningen zullen aanzienlijk toenemen wanneer de verordening cybersolidariteit in werking treedt; het ECCC zal dan het voortouw nemen. Om aan deze behoefte tegemoet te komen, zal de Commissie, in overleg met de NIS-samenwerkingsgroep, EU-CyCLONe[29] en Enisa, voorstellen om de gezondheidszorg aan te wijzen als een sector waarvoor steun kan worden verleend voor **gecoördineerde paraatheidstests** in het kader van de verordening cybersolidariteit. Voorts zou het ondersteuningscentrum een **kader op maat moeten ontwikkelen voor maturiteitsbeoordelingen van cyberbeveiliging specifiek voor de gezondheidszorg**. Dergelijke beoordelingen zouden instanties bruikbare inzichten bieden in hun kwetsbaarheden en hun de mogelijkheid bieden patiënten en belanghebbenden hun cyberbeveiligingsparaatheid aan te tonen en zo vertrouwen in hun diensten op te bouwen. Op geaggregeerd niveau zou het centrum **jaarlijks een beoordeling van de cybermaturiteit in de gezondheidszorg** moeten uitvoeren, waarin een duidelijk overzicht wordt gegeven van de cyberbeveiliging in de sector op zowel nationaal als EU-niveau.

De gezondheidszorg is voor cyberbeveiligingsdiensten[30] erg afhankelijk van externe contractanten, waardoor er gerichte steun nodig is om de beveiliging te verbeteren. De lidstaten zouden moeten voortbouwen op succesvolle initiatieven zoals de innovatievouchers van de EU en **gerichte maatregelen overwegen, zoals cyberbeveiligingsvouchers voor micro-, kleine en middelgrote**

[27] De ontwikkeling van richtsnoeren voor de interpretatie van de algemene verordening gegevensbescherming (AVG) valt onder de verantwoordelijkheid van het Europees Comité voor gegevensbescherming (EDPB). Bij die ontwikkeling moet Enisa de prerogatieven van het EDPB volledig eerbiedigen.
[28] Artikel 5 septies, leden 1 en 2, van Verordening (EU) 910/2014.
[29] Europees netwerk van verbindingsorganisaties voor cybercrises.
[30] Zie het NIS-investeringsverslag 2023 van Enisa (november 2023), waarin de nadruk wordt gelegd op externe steun voor cyberbeveiligingsaudits en -naleving. Beschikbaar op https://www.enisa.europa.eu/publications/nis-investments-2023.

ziekenhuizen en zorgaanbieders. Deze vouchers zouden goed zijn voor financiële bijstand om specifieke cyberbeveiligingsmaatregelen in te voeren. De voorrang van de toewijzing van vouchers zou gebaseerd moeten zijn op de bevindingen van paraatheidstests en maturiteitsbeoordelingen.

Lokale kennis en context zijn cruciaal voor de doeltreffende uitrol van vouchers en andere steunprogramma's en waarborgen de relevantie en toegankelijkheid. EU-fondsen, zoals het Europees Fonds voor regionale ontwikkeling, worden al gebruikt om initiatieven voor cyberbeveiliging en digitale gezondheid te steunen en kunnen daarom dienen als manier om gerichte regelingen voor cyberbeveiligingsvouchers voor zorgaanbieders te ontwikkelen. Om dat te stimuleren, zou het ondersteuningscentrum moeten samenwerken met de lidstaten en de regionale programma-autoriteiten om te helpen dergelijke regionale regelingen te ontwikkelen, op basis van de lessen die zijn getrokken uit bestaande nationale projecten en maatregelen die in het kader van het programma Digitaal Europa worden gefinancierd, om te zorgen voor een praktische en doeltreffende uitvoering.

Daarnaast hebben de Horizon-programma's sinds 2014 een belangrijke rol gespeeld bij de financiering van een reeks onderzoeksinitiatieven die gericht zijn op een betere weerbaarheid van zorginstellingen (zoals ziekenhuizen) tegen cyberdreigingen en de beperking van de risico's in verband met misbruik van opkomende technologieën. De resultaten omvatten een reeks gespecialiseerde instrumenten, kaders en systemen, zoals risicobeoordelingsinstrumenten, platforms om gegevens te delen en die daarbij de privacy beschermen, cryptografische oplossingen, opleidingsprogramma's voor cyberbewustzijn en realtime-dreigingsdetectiesystemen. Deze oplossingen zijn met name rigoureus gecontroleerd met praktijkproeven in de gezondheidszorg, zodat de doeltreffendheid en toepasbaarheid ervan bij de bescherming tegen cyberdreigingen wordt gewaarborgd.

Toeleveringsketens in de zorg veiligstellen

Een belangrijke uitdaging voor zorgorganisaties is het beheer van complexe ICT-toeleveringsketens, waarbij een scala aan producten betrokken is, zoals met internet verbonden medische hulpmiddelen, systemen voor elektronische patiëntendossiers en kantoorhardware. Ziekenhuizen en zorgaanbieders hebben betrouwbare en veilige ICT-systemen en -diensten nodig voor hun werk. Om cyberbeveiligingsuitdagingen in de gezondheidszorg aan te pakken, zou de NIS-samenwerkingsgroep een **gecoördineerde beveiligingsrisicobeoordeling van technische en strategische risico's in toeleveringsketens voor medische hulpmiddelen moeten uitvoeren en risicobeperkende maatregelen voorstellen**[31]. Indien nodig zou de groep moeten samenwerken met de Coördinatiegroep voor medische hulpmiddelen.

De verordening cyberweerbaarheid is een nieuw, alomvattend kader met cyberbeveiligingseisen voor de planning, het ontwerp, de ontwikkeling, de behandeling, het onderhoud en de rapportage van actief uitgebuite kwetsbaarheden met betrekking tot bijna alle hardware- en softwareproducten, in elke fase

[31] Overeenkomstig artikel 22 van de NIS 2-richtlijn.

van de waardeketen[32]. Medische hulpmiddelen zijn een soort product dat in een van de gevoeligste gebieden van onze samenleving wordt gebruikt. De cyberbeveiligingseisen voor deze producten vloeien voort uit de bestaande verordeningen betreffende medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek[33]. Die verordeningen worden momenteel geëvalueerd, waarbij wordt onderzocht of er meer samenhang en synergie tussen deze kaders mogelijk is om vereenvoudiging en geavanceerde cyberbeveiliging te waarborgen.

Voorts zouden de bevindingen van de risicobeoordeling zorgorganisaties moeten helpen om hun cyberbeveiligingswerkwijzen in de toeleveringsketen te herzien (een bepaling van de NIS 2-richtlijn) en kunnen ze helpen om nieuwe **aanbestedingsrichtsnoeren** te ontwikkelen[34]. Die richtsnoeren, die het ondersteuningscentrum van Enisa zou ontwikkelen, zouden recente tendensen moeten weerspiegelen, zoals het toenemende gebruik van de cloud voor de opslag van patiëntengegevens, waaronder ook de noodzaak van een veilige migratie van elektronische gezondheidsgegevens naar de cloud. Bovendien zouden de nieuwe richtsnoeren organisaties praktische instrumenten moeten bieden om hun toeleveringsketens op te volgen, zoals aanbieders van beheerde beveiligingsdiensten, attestverslagen of risicobeoordelingen van derden.

Voor de cloud zijn meer maatregelen nodig om de specifieke uitdagingen van het beheer van gevoelige gezondheidsgegevens aan te pakken, waaronder grotere veiligheids-, privacy- en operationele risico's. Om de waarborgen te verbeteren, bevelen deskundigen aan om "beveiliging door standaardinstellingen en door ontwerp" in clouddiensten in te bedden. Bij deze benadering krijgen veilige infrastructuur, proactief kwetsbaarheidsbeheer en een mix van publieke en particuliere cloudoplossingen prioriteit. Permanent toezicht en leveranciersspecifieke attesten – zoals certificeringen van beveiligingsaanbieders en nalevingsaudits volgens nationale en internationale normen – zijn ook essentieel om robuuste beveiliging te garanderen.

Voor diensten als IaaS, PaaS en SaaS (respectievelijk infrastructuur, platform en software als een dienst) is de klant vaak verantwoordelijk voor de uitvoering van de beveiliging. Veel zorgorganisaties beschikken echter niet over de middelen om zelfstandig aan deze eisen te voldoen. Daarom zouden **aanbieders van clouddiensten moeten worden aangemoedigd om algemene basisbeveiligingsmaatregelen in te voeren**. Deze maatregelen zouden het risico op verkeerde configuraties verminderen, een consistente bescherming handhaven in alle omgevingen die de klant beheert, en gebruikers meer zekerheid bieden. De bepaling van een algemene basisbeveiliging zou tot doel hebben een evenwicht te vinden tussen robuuste bescherming en uitvoerbaarheid, waarbij wordt gewaarborgd dat die basis bruikbaar is voor een breed scala aan zorgorganisaties. Daarbij wordt dan

[32] In een eerste stap zullen brede categorieën radioapparatuur die niet onder het toepassingsgebied van de verordeningen betreffende medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek vallen vanaf 1 augustus 2025 moeten voldoen aan de essentiële eisen van de richtlijn radioapparatuur die betrekking hebben op cyberbeveiliging wanneer zij in de eengemaakte markt worden gebracht. In een tweede fase, vanaf 11 december 2027, wordt de verordening cyberweerbaarheid van toepassing.

[33] In december 2019 heeft de Coördinatiegroep voor medische hulpmiddelen richtsnoeren voor cyberbeveiliging voor medische hulpmiddelen uitgebracht. Die helpen fabrikanten om aan de eisen van bijlage I bij de twee verordeningen te voldoen: https://ec.europa.eu/docsroom/documents/41863.

[34] Voortbouwend op de aanbestedingsrichtsnoeren van Enisa voor cyberbeveiliging in ziekenhuizen van 2020 (februari 2020). Beschikbaar op https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

nauw samengewerkt tussen cloudaanbieders en de gezondheidszorg en worden de goede werkwijzen van de sector benut om doeltreffende en schaalbare oplossingen te vinden.

Opleiding en ontwikkeling op het vlak van vaardigheden

Voor de duurzame groei en het concurrentievermogen op lange termijn en voor hoogwaardige diensten (waaronder zorgdiensten) in Europa moeten we beschikken over arbeidskrachten met de gezochte vaardigheden. Het tekort aan gekwalificeerde cyberbeveiligingsprofessionals is een grote uitdaging in heel Europa. Naar schatting zijn er in de hele EU 299 000 van dergelijke professionals te weinig[35]. Volgens de Eurobarometer over cybervaardigheden van 2024[36] ondervindt 81 % van de bedrijven moeilijkheden om cyberbeveiligingspersoneel aan te werven zodat ze mogelijke cyberaanvallen tegen kunnen gaan. In de gezondheids-, onderwijs- en socialezorgsector wordt 66 % van de rollen op het gebied van cyberbeveiliging ingevuld door werknemers die afkomstig zijn van niet-cyberbeveiligingsfuncties. Er is dus dringend om- en bijscholing nodig.

Om deze uitdaging aan te pakken, zou het ondersteuningscentrum moeten samenwerken met het toekomstige Europees consortium voor digitale infrastructuur (EDIC) voor cyberbeveiligingsvaardigheden, zoals bepaald in de mededeling van de Commissie over de academie voor cyberbeveiligingsvaardigheden[37]. Het werk zou overleg tussen cyberbeveiligingsprofessionals in de gezondheidszorg, zoals de Chief Information Security Officers (CISO's), moeten vergemakkelijken. Een mogelijke maatregel is de oprichting van een **Europees netwerk voor CISO's in de gezondheidszorg**, te beginnen met een groep deskundigen om goede werkwijzen, strategieën om talent te behouden en oplossingen om cyberbeveiligingsprofessionals naar de gezondheidszorg aan te trekken te delen en te ontwikkelen. Voorts zouden onder de paraplu van de academie voor cyberbeveiligingsvaardigheden – en met steun van het bedrijfsleven en de academische wereld – middelen moeten worden ontwikkeld om de hoeveelheid cyberbeveiligingspersoneel in de gezondheidssector te vergroten. Belanghebbenden uit de sector zouden daarom moeten worden aangemoedigd steun te verlenen om cyberbeveiligingsopleidingen te verbeteren.

Een groot deel van de cyberincidenten in de gezondheidszorg zijn nog steeds te wijten aan menselijke fouten, wat de grote behoefte aan meer cyberbewustzijn en opleidingen van het personeel onderstreept. Aangezien zorgaanbieders vaak digitale hulpmiddelen gebruiken, is het essentieel dat zij de veilige werkwijzen kennen. Gerichte opleidings- en bewustmakingscampagnes kunnen de risico's aanzienlijk verminderen. Om dit aan te pakken, zou het ondersteuningscentrum moeten samenwerken met zorgprofessionals, zorgaanbieders, aanbieders van onderwijs en opleidingen, het

[35] The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study | Digital Skills and Jobs Platform.
[36] Flash Eurobarometer 547 over cybervaardigheden.
[37] Mededeling van de Commissie aan het Europees Parlement en de Raad — Wegwerken van het tekort aan cyberbeveiligingsprofessionals om het concurrentievermogen, de groei en de weerbaarheid van Europa te versterken ("De academie voor cyberbeveiligingsvaardigheden") (COM(2023) 207 final).

bedrijfsleven, het EDIC voor cyberbeveiligingsvaardigheden en de autoriteiten van de lidstaten om **uitgebreide, gemakkelijk toegankelijke online opleidingsmodules en -cursussen** te ontwikkelen en te verspreiden.

Modules over digitale competentie en cyberbeveiliging opnemen in onderwijsprogramma's is cruciaal om een sterke basis voor cyberbeveiliging in de gezondheidszorg op te bouwen. In deze modules zouden sectorspecifieke kwesties moeten worden aangepakt, zoals de bescherming van patiëntengegevens en kwetsbaarheden in de beveiliging van medische hulpmiddelen. Bij de ontwikkeling van deze middelen zou rekening moeten worden gehouden met eerdere maatregelen, zoals het BeWell-[38] en het Panacea-project[39], die worden gefinancierd in het kader van respectievelijk het programma Erasmus+ en Horizon 2020.

3.2.Europese capaciteit om cyberdreigingen in de gezondheidszorg op te sporen

Cyberdreigingen doeltreffend opsporen is essentieel om snel op incidenten te reageren. Cybercriminelen beschikken over technieken om inbreuken moeilijk op te sporen, waardoor ze langere tijd zonder toelating toegang tot een systeem kunnen krijgen[40]. Daarom kan meer capaciteit om bedreigingen op te sporen helpen cyberaanvallen meteen een halt toe te roepen. Een voorbeeld is de ransomware-aanval op Vastaamo, een Finse psychotherapeutische dienstverlener, waarvan de dader vertrouwelijke patiëntendossiers had gestolen en daarmee patiënten afperste. De eerste inbreuk vond plaats in 2018, maar Vastaamo ontdekte dat pas in 2020[41].

Efficiënte informatie-uitwisseling en samenwerking zijn essentieel voor een betere opsporing van bedreigingen en een groter situationeel bewustzijn in de hele EU. Computer Security Incident Response Teams (CSIRT's) spelen een cruciale rol bij de ontvangst van meldingen van incidenten, pogingen tot aanvallen en potentiële dreigingen en bieden richtsnoeren voor risicobeperkende maatregelen op nationaal niveau. **De lidstaten worden echter sterk aangemoedigd om ook alle meldingen van cyberincidenten van ziekenhuizen en zorgaanbieders door te geven aan het ondersteuningscentrum van Enisa om zo het bewustzijn hierover in de EU te vergroten.** Idealiter zou dit vergezeld moeten gaan van een zinvolle karakterisering van verschillende aspecten van de incidenten, waaronder bekende onderliggende kwetsbaarheden en effecten op de zorgdiensten en ongewenste voorvallen bij patiënten. Bovendien worden fabrikanten van medische hulpmiddelen en hulpmiddelen voor in-vitrodiagnostiek aangemoedigd om vrijwillig kwetsbaarheden of ernstige cyberincidenten te melden die gevolgen hebben voor de veiligheid van deze hulpmiddelen, alsook potentieel andere kwetsbaarheden, incidenten, pogingen tot aanvallen en cyberdreigingen die het

[38] BeWell – Blueprint alliance for a future health workforce strategy on digital and green skills. Beschikbaar op 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. Beschikbaar op https://cordis.europa.eu/project/id/826293.
[40] Enisa Threat Landscape 2023.
[41] Besluit 1150/161/2021 van de Finse ombudsman voor gegevensbescherming.

risicoprofiel van die hulpmiddelen kunnen beïnvloeden. Dat moeten ze doen via het centrale meldplatform dat Enisa in het kader van de verordening cyberweerbaarheid zal oprichten en beheren.

Als de informatie in de verslagen niet langer gevoelig is, zou het centrum een door het Enisa gesponsorde Europese catalogus van bekende uitgebuite kwetsbaarheden kunnen opstellen voor medische hulpmiddelen, systemen voor elektronische medische dossiers en aanbieders van ICT-apparatuur en -software voor de gezondheidszorg. Om aanzienlijke uitdagingen voor dreigingsdetectie aan te pakken, zou het ondersteuningscentrum **een abonnementsdienst voor vroegtijdige waarschuwing voor de gezondheidszorg in de hele EU moeten invoeren die vrijwel realtime waarschuwingen geeft**. Deze dienst zou werken op basis van verwerkte gegevens van CSIRT's, zorginstanties en -fabrikanten, inlichtingen uit open bronnen en andere actoren zoals cyberhubs, centra voor informatie-uitwisseling en -analyse (ISAC's) en rechtshandhavingsinstanties. Nauwere samenwerking tussen Enisa en Europol – bijvoorbeeld om patronen in cybercriminaliteit in de gezondheidszorg op te sporen – zou het situationeel bewustzijn verder vergroten.

ISAC's fungeren als centrale middelen voor inlichtingen over cyberdreigingen en bevorderen het vertrouwen en het tweerichtingsverkeer van informatie-uitwisseling tussen de publieke en de particuliere sector. Het ondersteuningscentrum zou de steun voor het **Europese ISAC voor de gezondheidszorg** moeten vergroten met instrumenten, informatie-uitwisseling en verslagen over het situationeel bewustzijn in de sector, en zou een betrouwbare gemeenschap voor tactische en strategische samenwerking moeten bevorderen. De lidstaten zouden de ontwikkeling van nationale ISAC's voor de gezondheidszorg moeten aanmoedigen[42]. De ISAC's zouden ook moeten worden aangemoedigd om zorgaanbieders en fabrikanten bijeen te brengen om tot een gezamenlijk begrip van cyberdreigingen te komen, ook in de toeleveringsketen, en om een dialoog te laten plaatsvinden over veilig productontwerp waarbij echt rekening wordt gehouden met de uitrol ter plaatse.

3.3.Snelle reactie en herstel

Gezien de grote gevoeligheid van patiëntengegevens en de mogelijk verwoestende gevolgen van cyberaanvallen op zorgdiensten, is een snelle en doeltreffende reactie op cyberincidenten cruciaal om de veiligheid van patiënten te waarborgen. Als een ziekenhuis of zorgaanbieder te maken krijgt met een cyberaanval, is het eerste contactpunt het desbetreffende nationale CSIRT[43]. Het CSIRT is verantwoordelijk voor tijdige ondersteuning, idealiter binnen 24 uur, om significante incidenten te helpen beheersen. Als een incident echter de capaciteit van het CSIRT overschrijdt, zou er EU-steun beschikbaar moeten zijn om een snelle en doeltreffende reactie te waarborgen.

[42] Zo heeft Finland een nationaal ISAC voor de gezondheidszorg en de sociale zekerheid. Zie het Finse nationale cyberbeveiligingscentrum: "ISAC information sharing groups", beschikbaar op http://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

[43] In artikel 23, lid 1, van de NIS 2-richtlijn is bepaald dat essentiële en belangrijke entiteiten significante incidenten moeten melden aan het desbetreffende CSIRT of, indien van toepassing, aan de bevoegde autoriteit.

De EU-cyberbeveiligingsreserve, die is opgericht in het kader van de verordening cybersolidariteit, biedt hulp bij de reactie op incidenten van betrouwbare beheerde beveiligingsaanbieders om bijstand te verlenen bij significante of grootschalige cyberincidenten en de eerste herstellingen. Deze reserve is bedoeld als aanvulling op de inspanningen van de CSIRT's van de lidstaten, zodat die extra steun kunnen aanvragen als er kritieke sectoren zoals de gezondheidszorg betrokken zijn. Om dit systeem te verbeteren, **zouden de Commissie en Enisa ervoor moeten zorgen dat de reserve een snellereactiedienst omvat die specifiek voor de gezondheidszorg is bedoeld**. Als aanvulling op andere bestaande kaders zou deze dienst deskundigen inzetten om significante of grootschalige cyberincidenten in de gezondheidszorg onmiddellijk te beheren als de nationale steun ontoereikend is.

Om de reactie en het herstel te verbeteren, zouden het ondersteuningscentrum, de NIS-samenwerkingsgroep, het CSIRT-netwerk en, indien nodig, Europol, **voor de gezondheidszorg draaiboeken op maat voor de reactie op cyberincidenten moeten ontwikkelen**. Deze draaiboeken zouden zowel CSIRT's als zorgorganisaties helpen om te reageren op specifieke cyberdreigingen, waaronder ransomware. Vanwege het belang van de doeltreffende samenwerking tussen CSIRT's en rechtshandhavingsinstanties bij de reactie op en het onderzoek naar criminele cyberincidenten, zouden de draaiboeken onder meer duidelijke richtsnoeren moeten bieden om dergelijke incidenten aan rechtshandhavingsinstanties te melden. Voorts zou het centrum een **grootschalige uitrol van nationale cyberbeveiligingsoefeningen kunnen steunen (voortbouwend op ervaringen met oefeningen zoals die van Cyber Europe 2022 van Enisa) om de draaiboeken te testen en de protocollen voor reacties op incidenten te verbeteren**.

Om het beleid te onderbouwen en de doeltreffendheid van de maatregelen tegen ransomware-aanvallen te beoordelen, moeten meer gegevens worden verzameld. Daartoe zouden de lidstaten instanties die onder de NIS 2-richtlijn vallen (zoals zorgorganisaties), moeten vragen verslag uit te brengen over losgeld dat ze betaald hebben en voornemens zijn te betalen, naast andere informatie die ze verstrekken als ze significante cyberincidenten melden. Dergelijke meldingen helpen bij een doeltreffend onderzoek naar incidenten met ransomware, waaronder de tracering van betalingen op cryptovalutawisselplatforms om de ontvangers te identificeren.

De herstelsnelheid is cruciaal om de weerbaarheid en het vertrouwen van het publiek te behouden – met name in de gezondheidszorg, waar storingen de patiëntenzorg kunnen verstoren. Met het oog op een doeltreffend herstel van ransomware-aanvallen moeten zorgaanbieders veilige, up-to-date en losstaande backups hebben die snel kunnen worden hersteld. Als onderdeel van zijn dienstencatalogus zou het ondersteuningscentrum een **abonnementsdienst voor het herstel van ransomware kunnen aanbieden om ziekenhuizen en zorgaanbieders te helpen op voorhand herstelplannen te maken**. Enisa en Europol zouden moeten samenwerken om de meest voorkomende ransomware-stammen die zorgorganisaties aanvallen, te identificeren en het **register van decryptiehulpmiddelen** die beschikbaar zijn via het No More Ransom-project[44] uit te breiden. Ze zouden ook toegankelijke

[44] https://www.nomoreransom.org/en/index.html.

richtsnoeren moeten ontwikkelen en promoten om zorgaanbieders te helpen geen losgeld te betalen maar decryptiehulpmiddelen te gebruiken.

Het **International Counter Ransomware Initiative**[45] is een belangrijk middel om informatie over specifieke ransomware-incidenten uit te wisselen en de capaciteit van de lidstaten op te bouwen om hun cyberbeveiligingskaders en onderzoekscapaciteiten tegen ransomware-actoren te verbeteren. Samen met de hoge vertegenwoordiger zal de Commissie de samenwerking met het initiatief blijven bevorderen, onder meer voor ransomware-bedreigingen in de gezondheidszorg. Bovendien zal de Commissie streven naar samenwerking in de **G7-werkgroep voor cyberbeveiliging** om de cyberbeveiliging van de gezondheidszorg te verbeteren. De werkgroep zou met name kunnen nadenken over mogelijkheden om de gezondheidszorg te ondersteunen tegen bedreigingen zoals ransomware. Daarbij zou ze voortbouwen op overwegingen zoals de gezamenlijke verklaring over ransomware-aanvallen op faciliteiten voor de gezondheidszorg van 8 november 2024, die in het kader van de VN-Veiligheidsraad is gepresenteerd[46].

4. Nationale maatregelen

Het vermogen van dit actieplan om de cyberbeveiliging in de gezondheidszorg te verbeteren hangt af van de actieve betrokkenheid en inzet van de lidstaten. Om het actieplan met succes uit te voeren, zouden de lidstaten **nationale ondersteuningscentra voor cyberbeveiliging** kunnen aanwijzen, **specifiek voor ziekenhuizen en zorgaanbieders**. Deze centra zouden fungeren als de belangrijkste contactpunten voor de gezondheidszorg op nationaal niveau en nauw samenwerken met het ondersteuningscentrum van Enisa. Indien mogelijk en nuttig zouden de lidstaten bestaande organen, zoals nationale gezondheids-CSIRT's of betrokken autoriteiten, moeten aanwijzen als nationale ondersteuningscentra voor cyberbeveiliging.

De lidstaten worden ook aangemoedigd om **nationale actieplannen op te stellen voor cyberbeveiliging in de gezondheidszorg**. Deze plannen zouden een overzicht geven van de specifieke cyberbeveiligingsrisico's voor zorgstelsels en de nationale maatregelen die worden genomen om ze aan te pakken, en ervoor zorgen dat de middelen en werkwijzen op Europees niveau doeltreffend worden gebruikt. Het ondersteuningscentrum van Enisa kan helpen bij de ontwikkeling van die plannen, waarbij het rekening houdt met bestaande nationale plannen en de inspanningen coördineert om ervoor te zorgen dat de middelen en strategieën van de afzonderlijke lidstaten elkaar aanvullen.

Een ander belangrijk aandachtspunt voor de lidstaten is om het delen van middelen tussen zorgaanbieders te vereenvoudigen, door middel van **gezamenlijke aanbestedingen of gebundelde middelen** op nationaal, regionaal of zelfs Europees niveau. Deze aanpak zou de financiële lasten voor

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

individuele instanties verminderen en tegelijkertijd hun onderhandelingspositie ten opzichte van aanbieders van cyberbeveiligingsdiensten vergroten.

Zo heeft het Franse programma CaRE[47] een aantal maatregelen op nationaal en regionaal niveau ingevoerd om uitdagingen op het gebied van middelen aan te pakken: er is een cybercatalogus met een overzicht van commerciële oplossingen en van cyberoplossingen en -pakketten die beschikbaar zijn voor ziekenhuizen via het nationale agentschap voor cyberbeveiliging, het agentschap voor digitale gezondheid, regionale agentschappen en nationale aankooporganisaties. Deze wordt aangevuld met extra financiering voor regionale agentschappen om gedeelde middelen aan te bieden.

De lidstaten zouden ook de ontoereikende investeringen in cyberbeveiliging in de gezondheidszorg moeten aanpakken. Om voldoende financiering te waarborgen, zouden ze **niet-bindende benchmarks moeten vaststellen en de specifiek op cyberbeveiliging gerichte financieringsdoelstellingen moeten monitoren**, en erop letten dat deze investeringen geen afbreuk doen aan essentiële patiëntenzorg. De doelstellingen zouden ook de integratie van veiligheidsoverwegingen in alle digitale investeringen in de sector ten goede moeten komen. De lidstaten kunnen goede werkwijzen en advies over deze doelstellingen uitwisselen via platforms zoals het e-gezondheidsnetwerk[48].

5. Publiek-private samenwerking

Publiek-private samenwerking en overleg met zorgaanbieders, andere instanties uit de gezondheidszorg en relevante spelers in de cyberbeveiligingssector zijn essentieel om het actieplan met succes uit te voeren. Om verder bij te dragen aan de werkzaamheden van het ondersteuningscentrum, zal de **Commissie, met hulp van Enisa, een gezamenlijke adviesraad voor cyberbeveiliging in de gezondheidszorg oprichten** met hooggeplaatste vertegenwoordigers op beide gebieden. Deze raad kan de Commissie en het ondersteuningscentrum adviseren over doeltreffende acties en de verdere ontwikkeling van publiek-private partnerschappen op dit gebied bespreken. Hij zal voortbouwen op de bestaande inspanningen voor publiek-private partnerschappen, waaronder het Europees ISAC voor de gezondheidszorg.

Daarnaast zal de Commissie cyberbeveiligingsbedrijven, stichtingen, onderwijsinstellingen en belanghebbenden uit de sector **oproepen om tot actie over te gaan en toezeggingen te doen dat ze de uitdagingen in de sector zullen aanpakken**. Voortbouwend op de ervaring van de academie voor cyberbeveiligingsvaardigheden zou een toezegging bijvoorbeeld kunnen zijn om bij de academie opleidingscursussen en -materiaal voor cyberbeveiligingsprofessionals aan te bieden, met bijzondere aandacht voor de gezondheidszorg[49]. Andere toezeggingen zouden betrekking kunnen hebben op bewustmaking of om beheerde beveiligingsdiensten gratis of aan een lagere prijs aan te bieden aan bijzonder kwetsbare instanties, zodat die hun paraatheid en weerbaarheid voor cyberbeveiliging

[47] Frans Agentschap voor digitale gezondheid: Cybersécurité acceleration et Résilience des Établissements (CaRE). Beschikbaar op https://esante.gouv.fr/strategie-nationale/cybersecurite.
[48] Het e-gezondheidsnetwerk is een vrijwillig netwerk van nationale autoriteiten die door de lidstaten zijn aangewezen en verantwoordelijk zijn voor e-gezondheid. Het is opgezet op basis van artikel 14 van Richtlijn 2011/24/EU.
[49] Cyber Skills Academy: Get Involved | Digital Skills and Jobs Platform.

kunnen vergroten. Ook zouden er met het ondersteuningscentrum van Enisa inlichtingen over cyberdreigingen kunnen worden gedeeld. Het ondersteuningscentrum zou een overzicht moeten bijhouden van de toezeggingen die in het kader van de oproep tot actie worden gedaan, om zo de samenhang en complementariteit te waarborgen.

6. Cybercriminelen afschrikken

Het interne en externe cyberbeveiligingsbeleid van de EU zou de doelstelling moeten ondersteunen om cybercriminelen ervan te weerhouden de Europese zorgstelsels aan te vallen. Cyberaanvallen tegen zorgorganisaties zijn een bijzonder onaanvaardbaar soort kwaadwillige cyberactiviteit, omdat die de veiligheid en het leven van mensen in gevaar kunnen brengen. Daarom zou al het afschrikwekkende vermogen van de EU voor cyberbeveiliging en rechtshandhaving moeten worden gebruikt om de algemene werking van cybercriminelen die zich op de gezondheidszorg richten, te ondermijnen en hen de kans te ontnemen gemakkelijk winst te maken. Dit omvat het bevorderen van landsgrensoverschrijdend onderzoek door "indicators of compromise" (inbreukindicatoren) en andere relevante gegevens beter uit te wisselen, en door een grotere nadruk op de belangrijkste doelwitten en belangrijke criminele facilitatoren zoals bulletproof hosting of diensten om cryptovaluta te mengen.

Het **instrumentarium voor cyberdiplomatie** biedt een kader om cyberaanvallen tegen de EU, de lidstaten en partners te voorkomen, tegen te gaan en erop te reageren. De hoge vertegenwoordiger zal het bestaande kader voor cybersancties blijven gebruiken om te reageren op bedreigingen die gericht zijn op de zorgstelsels.

Cybercriminelen ter verantwoording roepen voor hun daden is een belangrijk afschrikwekkend middel. Daarom zouden de lidstaten ervoor moeten zorgen dat de rechtshandhaving volledig wordt geïntegreerd in hun nationale actieplannen. Ze zouden met name ten volle moeten gebruikmaken van de bepalingen van de richtlijn over aanvallen op informatiesystemen[50] en van het Verdrag van Boedapest van de Raad van Europa over cybercriminaliteit[51] om aanvallen tegen te gaan, criminelen voor de rechter te brengen en criminele infrastructuur die aanvallen mogelijk maakt te ontmantelen. Als deze instrumenten met succes worden ingezet, zou dat ertoe moeten leiden dat criminele en kwaadwillige acties tegen de gezondheidszorg worden bestraft.

7. Uitvoering van en toezicht op het actieplan

Dit actieplan bevat een aantal taken voor een ondersteuningscentrum dat binnen Enisa moet worden opgericht. Dit zorgt voor een alomvattende en samenhangende uitvoering van het actieplan en voorkomt de oprichting van nieuwe instanties die tot potentiële overlappingen en overheadkosten

[50] Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad, https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32013L0040.

[51] Het Verdrag over cybercriminaliteit (Verdrag van Boedapest, ETS nr. 185) en de bijbehorende protocollen: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

leiden. De Commissie is van plan te garanderen dat het ondersteuningscentrum over voldoende middelen beschikt.

Zodra het centrum operationeel is, zou Enisa in overleg met de Commissie regelmatig updates van de werkzaamheden van het centrum moeten verstrekken aan de raad van bestuur van Enisa en de betrokken netwerken van de lidstaten, met name de NIS-samenwerkingsgroep, het CSIRT-netwerk, het e-gezondheidsnetwerk en, indien nodig, de Raad voor de EHDS. Voorts zou Enisa voortdurend met de publiek-private adviesraad voor cyberbeveiliging in de gezondheidszorg informatie moeten uitwisselen over de uitvoering van de maatregelen van het ondersteuningscentrum.

De regelmatige verslagen van Enisa, zoals het verslag over de stand van zaken op het gebied van de cyberbeveiliging in de Unie, met daarin een geaggregeerde maturiteitsbeoordeling van de cyberbeveiligingscapaciteiten en -middelen in de hele EU en dus ook in de gezondheidszorg, zouden moeten dienen als gelegenheden om gegevens te publiceren die helpen bij de monitoring van het actieplan. Bovendien kan de EU-cyberbeveiligingsindex van Enisa[52] kwantitatieve en kwalitatieve gegevens verstrekken, die dan als empirische basis dienen om het kritieke karakter en de maturiteit van de gezondheidszorg te beoordelen.

8. Volgende stappen

Deze mededeling bevat een ambitieuze agenda voor betere cyberbeveiliging in de gezondheidszorg in de EU. In het actieplan wordt een weg uitgestippeld om een samenhangende en gedeelde Europese aanpak van de cyberbeveiligingsproblematiek in de sector tot stand te brengen door het voorgestelde ondersteuningscentrum voor cyberbeveiliging voor ziekenhuizen en zorgaanbieders als centraal onderdeel van Enisa te ontwikkelen.

Deze mededeling zou moeten worden beschouwd als de start van een proces om de cyberbeveiliging in de gezondheidszorg te verbeteren. Daarom zal de vaststelling van het actieplan gepaard gaan met de start van uitgebreide raadplegingen van belanghebbenden en zal het overleg met de lidstaten en relevante netwerken worden voortgezet om inzichten te verzamelen. In het vierde kwartaal van 2025 is de Commissie van plan op basis van de resultaten van de raadplegingen aanbevelingen te doen om het actieplan verder te verfijnen.

De Commissie roept de lidstaten en alle belanghebbenden op tot samenwerking om het actieplan te verwezenlijken.

[52] ENISA, EU Cybersecurity Index, Framework and methodological note (2024). Beschikbaar op https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

Bijlage – Overzicht van voorgestelde maatregelen

De Commissie:

Europees ondersteuningscentrum voor cyberbeveiliging voor ziekenhuizen en zorgaanbieders van Enisa	
Zorgen voor passende middelen voor het ondersteuningscentrum Samenwerken met het ECCC om proefprojecten op te starten om goede werkwijzen te ontwikkelen voor de beoordeling van cyberhygiëne en veiligheidsrisico's, en om de behoeften aan continue cybermonitoring, inlichtingen over dreigingen en reacties op incidenten aan te pakken met geavanceerde cyberbeveiligingsoplossingen om de dienstencatalogus van het ondersteuningscentrum te ontwikkelen	2025
Cyberincidenten voorkomen	
In overleg met de NIS-samenwerkingsgroep, EU-CyCLONe en Enisa onderzoeken of de gezondheidszorg moet worden aangewezen als sector waarvoor steun kan worden verleend voor gecoördineerde paraatheidstests in het kader van de verordening cybersolidariteit	Q1 2025
Snelle reactie en herstel	
Samen met Enisa ervoor zorgen dat de EU-cyberbeveiligingsreserve ook een snellereactiedienst omvat, specifiek voor de gezondheidszorg	Q4 2025
Publiek-private samenwerking	
Met steun van Enisa een gezamenlijke adviesraad voor cyberbeveiliging in de gezondheidszorg oprichten	Q1 2025
Cyberbeveiligingsbedrijven, stichtingen, onderwijsinstellingen en belanghebbenden uit de sector oproepen om tot actie over te gaan en toe te zeggen de uitdagingen in de sector aan te pakken	Q2 2025
Cyberdreigingsactoren afschrikken	
Samen met de hoge vertegenwoordiger onderzoeken of het instrumentarium voor cyberdiplomatie kan worden gebruikt om kwaadwillige activiteiten tegen zorgstelsels te voorkomen, te ontmoedigen, tegen te gaan en erop te reageren	2025
Samen met de hoge vertegenwoordiger internationale samenwerking tegen ransomware-actoren stimuleren, met name in het kader van het International Counter Ransomware Initiative	2025-2026
Streven naar samenwerking in de G7-werkgroep voor cyberbeveiliging om de cyberbeveiliging van de gezondheidszorg te verbeteren	2025-2026
Volgende stappen	
Uitgebreide raadplegingen van belanghebbenden starten	Q1 2025
Aanbevelingen vaststellen om het actieplan verder te verfijnen	Q4 2025

Enisa:

Europees ondersteuningscentrum voor cyberbeveiliging voor ziekenhuizen en zorgaanbieders	
Werkzaamheden starten om een Europees ondersteuningscentrum voor cyberbeveiliging voor ziekenhuizen en zorgaanbieders op te richten	Q2 2025
Een uitgebreide dienstencatalogus ontwikkelen en verspreiden	Vanaf Q4 2025
Cyberincidenten voorkomen	
Richtsnoeren uitvaardigen om de meest cruciale cyberbeveiligingswerkwijzen te benadrukken en zorgaanbieders te helpen ze uit te voeren	Q3 2025
In nauwe samenwerking met de Commissie en de lidstaten een instrument ontwikkelen om de regelgeving in kaart te brengen	Q1 2025
Een kader ontwikkelen voor maturiteitsbeoordelingen van cyberbeveiliging, specifiek voor de gezondheidszorg	Q3 2025
Jaarlijks een beoordeling van de cybermaturiteit in de gezondheidszorg uitvoeren	2025-2026
Samenwerken met de lidstaten en regionale programma-autoriteiten om modelprogramma's voor cyberbeveiligingsvouchers op te zetten	2025-2026
Nieuwe aanbestedingsrichtsnoeren ontwikkelen voor de cyberbeveiliging van ziekenhuizen en zorgaanbieders	Q3 2025
Een Europees netwerk voor CISO's in de gezondheidszorg oprichten	Q1 2026
Opleidingsmodules en -cursussen voor zorgaanbieders ontwikkelen en promoten	Q1 2026
Europese capaciteit om cyberdreigingen in de gezondheidszorg op te sporen	
Een Europese catalogus met bekende uitgebuite kwetsbaarheden voor medische hulpmiddelen, systemen voor elektronische medische dossiers en aanbieders van ICT-apparatuur en -software voor gezondheidszorg opstellen	Q4 2025
Een abonnementsdienst voor vroegtijdige waarschuwingen voor de gezondheidszorg in de hele EU invoeren	Vanaf 2026
Het Europees ISAC voor de gezondheidszorg bijstaan met instrumenten en informatie-uitwisseling	2025-2026
Snelle reactie en herstel	
Samen met de Commissie ervoor zorgen dat de EU-cyberbeveiligingsreserve ook een snellereactiedienst omvat, specifiek voor de gezondheidszorg	Q4 2025

Samen met het CSIRT-netwerk draaiboeken voor de reactie op cyberincidenten ontwikkelen die op maat zijn gemaakt voor de gezondheidszorg	Q3 2025
Een grootschalige uitrol van nationale cyberbeveiligingsoefeningen stimuleren om de draaiboeken te testen en de protocollen voor de reactie op incidenten te verbeteren	Vanaf Q4 2025
Een aanmeldingsdienst voor het herstel van ransomware voorzien	Vanaf 2026
Samen met Europol de meest voorkomende ransomware-stammen die zorgorganisaties aanvallen, identificeren en het register van decryptiehulpmiddelen uitbreiden via het No More Ransom-project	Q4 2025
Samen met Europol toegankelijke richtsnoeren ontwikkelen om zorgaanbieders te helpen geen losgeld te betalen	Q3 2025
Nationale maatregelen	
De lidstaten helpen om nationale actieplannen te ontwikkelen	2025
De inspanningen coördineren om ervoor te zorgen dat de middelen en strategieën van de afzonderlijke lidstaten elkaar aanvullen	2025-2026
Uitvoering van en toezicht op het actieplan	
In overleg met de Commissie regelmatig updates verstrekken van de werkzaamheden van het ondersteuningscentrum voor cyberbeveiliging aan relevante netwerken van de lidstaten	2025-2026
Voortdurend informatie uitwisselen met de adviesraad voor cyberbeveiliging in de gezondheidszorg	2025-2026

De lidstaten:

Europese capaciteit om cyberdreigingen in de gezondheidszorg op te sporen	
Meldingen van incidenten van ziekenhuizen en zorgaanbieders in het kader van de NIS 2-richtlijn delen met het ondersteuningscentrum voor cyberbeveiliging	Vanaf Q4 2025
De ontwikkeling van nationale ISAC's voor de gezondheidszorg aanmoedigen	2025-2026
Cyberincidenten voorkomen	
Binnen de NIS-samenwerkingsgroep een gecoördineerde veiligheidsrisicobeoordeling uitvoeren, waarbij zowel technische als strategische risico's in verband met toeleveringsketens voor medische hulpmiddelen worden beoordeeld	Q4 2025
Snelle reactie en herstel	

Nationale cyberbeveiligingsoefeningen uitrollen om de draaiboeken te testen en de protocollen voor de reactie op incidenten te verbeteren	Vanaf 2026
Nationale maatregelen	
Nationale ondersteuningscentra voor cyberbeveiliging voor ziekenhuizen en zorgaanbieders aanduiden	Q2 2025
Nationale actieplannen opstellen voor cyberbeveiliging in de gezondheidszorg	Q4 2025
Het delen van middelen tussen zorgaanbieders vergemakkelijken	2025-2026
Niet-bindende benchmarks vaststellen en financieringsdoelstellingen monitoren die specifiek gericht zijn op cyberbeveiliging	Q4 2025
Zorgorganisaties en andere instanties die onder de NIS 2-richtlijn vallen, vragen verslag uit te brengen over hun voornemen om losgeld te betalen	Q4 2025