Fiche 1: Europees actieplan omtrent de cybersecurity van ziekenhuizen en zorgaanbieders

1. Algemene gegevens

a) Titel voorstel

Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's over het Europees actieplan omtrent de cybersecurity van ziekenhuizen en zorgaanbieders

b) Datum ontvangst Commissiedocument

15 januari 2025

c) Nr. Commissiedocument

COM(2025)10

d) EUR-Lex

EUR-Lex - 52025DC0010 - EN - EUR-Lex

e) Nr. impact assessment Commissie en Opinie

Niet opgesteld

f) Behandelingstraject Raad

Raad voor Vervoer, Telecommunicatie en Energie (Telecomraad)

g) Eerstverantwoordelijk ministerie

Ministerie van Justitie en Veiligheid in nauwe samenwerking met het Ministerie van Volksgezondheid, Welzijn en Sport

2. Essentie voorstel

Op 15 januari 2025 heeft de Europese Commissie (hierna:: "de Commissie") een EU-actieplan gepresenteerd om de cyberbeveiliging van ziekenhuizen en zorgverleners te verbeteren. Deze mededeling was aangemerkt als een topprioriteit binnen de eerste honderd dagen van de nieuwe Commissie. Van alle kritieke sectoren in de EU melden lidstaten in de zorgsector het hoogste aantal cyberincidenten. Bovendien digitaliseert de zorg in toenemende mate en raakt de sector afhankelijker van digitale zorgsystemen en infrastructuren.

Kernpunt van het actieplan is dat er bij het *Europees Agentschap voor Netwerk- en Informatiebeveiliging* (ENISA) een *European Cybersecurity Support Centre for hospitals and healthcare providers* (hierna: "Steuncentrum") wordt opgezet. Dit Steuncentrum zal streven naar een uniforme Europese aanpak voor de uitdagingen op het gebied van cybersecurity in de zorg.
Het plan en de voorgestelde maatregelen zijn onderverdeeld in vijf thema's: preventie, detectie, respons, herstel en afschrikking.

Ten eerste zal er worden gewerkt aan betere preventie: het plan helpt de zorgsector om weerbaarder te zijn tegen cyberincidenten met gerichte maatregelen in de vorm van zogeheten cyberbeveiligingsvouchers (gerichte financiële steun) voor kleinere zorgaanbieders en ondersteuning bij het implementeren van *best practices* op het gebied van cyberbeveiliging. Daarnaast zal het Steuncentrum met hulp van de lidstaten en de Commissie een instrument ontwikkelen dat de administratieve lasten minimaliseert voor entiteiten die aan veel regelgeving onderhevig zijn. De Europese *ID-Wallet* biedt een manier om afhankelijkheid van zwakke identificatiemechanismen te mitigeren. Verder zal worden onderzocht of de zorgsector in aanmerking komt voor gecoördineerde paraatheidstesten onder de Cybersolidariteitsverordening[1] en wordt de ontwikkeling van een raamwerk voor een volwassenheidsbeoordeling specifiek voor cyberveiligheid in de zorgsector voorgesteld. Ook wordt aangeboden een risicoanalyse uit te voeren onder de NIS (Network and Information Security) *Cooperation Group*, om de technische en strategische risico's van medische producten in kaart te brengen. Daarnaast wordt gesproken over de (mogelijke) oprichting van een Europees *Chief Information Security Officer* (CISO-) Netwerk als pool van experts, voor het faciliteren van kennisuitwisseling en het werven van security-experts binnen de zorgsector.

Ten tweede wil de Commissie werken aan de detectie en identificatie van cyberincidenten. Lidstaten worden aangemoedigd om alle cyberincidentnotificaties van ziekenhuizen en zorgaanbieders te delen met het Steuncentrum. Ook zou het Steuncentrum een EU-breed *early-warning* abonnement voor de zorgsector moeten introduceren, om *real time alerts* zodoende te ontvangen. Daarnaast zal het Steuncentrum meer steun aan het *European Health Information Sharing and Analysis Centre* (ISAC) verlenen.

Het derde en vierde thema richten zich op het adequaat reageren op cyberaanvallen en het herstel hiervan, om de gevolgen van cyberaanvallen te beperken. Zo stelt de Commissie voor om binnen de *EU Cybersecurity Reserve*, die al is opgericht met de Cybersolidariteitsverordening, een *Rapid Response Service* op te zetten, specifiek voor de gezondheidszorgsector. Ook wordt voorgesteld om draaiboeken te ontwikkelen om zorgorganisaties te helpen bij een *ransomware*-aanval, en zouden nationale cyberoefeningen moeten worden georganiseerd om deze draaiboeken te testen.

De vijfde prioriteit is vooral gericht op het afschrikken van aanvallen, door de verdere ontwikkeling van een diplomatieke reactie van de EU op kwaadwillige cyberactiviteiten, bijvoorbeeld aan de hand van de reeds bestaande *Cyber Diplomacy Toolbox*.

Het actieplan kondigt ook een uitgebreide publieke consultatie aan. Op basis van de aanbevelingen die uit de consultatie komen, wordt naar verwachting eind 2025 een bijgewerkt actieplan opgeleverd.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

[1] Kamerstuk II 2022-2023, 22112, nr. 3695

De Nederlandse Cybersecuritystrategie (NLCS) zet de vier pijlers uiteen van de kabinetsinzet voor het realiseren van een digitaal veilige en weerbare samenleving.[2] Naast acties en samenwerking op nationaal niveau, benadrukt de NLCS dat internationale samenwerking, zowel in EU- en NAVO-verband als daarbuiten, essentieel is gezien het grensoverschrijdende karakter van cyberdreigingen. Het kabinet zet zich daarom actief in bij de verschillende Europese gremia en samenwerkingsverbanden met als doel de digitale weerbaarheid van de EU te vergroten.

Pijler I van de NLCS ziet op de digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties, waaronder de zorgsector. Hierbij stelt het kabinet het doel om beter zicht te krijgen op mogelijke dreigingen en incidenten en organisaties goed te beschermen tegen digitale risico's, onder meer met de implementatie van de herziene Europese Netwerk- en Informatiebeveiligingsrichtlijn (NIS2-richtlijn) in nationale wetgeving. De NIS2-richtlijn en de aanstaande wetgeving ter implementatie daarvan (Cyberbeveiligingswet), zijn van toepassing op essentiële en belangrijke entiteiten in verschillende belangrijke sectoren in ons land, waaronder (organisaties in) de gezondheidszorg.

Voor de zorgsector zal Z-CERT naar verwachting worden aangewezen als sectoraal *Computer Security Incident Response Team* (CSIRT) onder de aanstaande wetgeving ter implementatie van de NIS2-richtlijn. Op basis van deze aanstaande wetgeving zal Z-CERT de wettelijke taken van het CSIRT ten behoeve van de entiteiten binnen de Nederlandse zorgsector gaan vervullen. Z-CERT vervult reeds de rol van sectoraal computercrisisteam en is daarnaast het expertisecentrum voor cybersecurity in de zorg. Z-CERT voorziet Nederlandse zorginstellingen van advies en dreigingsinformatie, ondersteuning bij cyberaanvallen en kan netwerken monitoren op kwetsbaarheden of verdachte activiteiten.

Daarnaast zet het kabinet in op bewustwording over informatieveiligheid onder zorgmedewerkers. Binnen het project 'informatieveilig gedrag in de zorg' worden initiatieven genomen ter bevordering van veilig online gedrag in de zorgsector. Hierover heeft het kabinet uw Kamer geïnformeerd in de brief 'Voortgang op elektronische gegevensuitwisseling' van 15 december 2022.[3]

In 2023 is op initiatief van Z-CERT de Europese Zorg ISAC opgericht, een samenwerkingsverband door en voor Europese zorgpartijen op het gebied van cybersecurity. Z-CERT vervult op dit moment tevens de voorzittersrol van dit samenwerkingsverband wat haar informatiepositie verder verstevigd en ten goede komt aan de ondersteuning van de Nederlandse zorgsector.

Nationaal beleid richt zich ook op de doorontwikkeling van de verplichte NEN-normen.[4] Deze verplichten zorginstellingen om risico's voor informatiebeveiliging in kaart te brengen en passende maatregelen te nemen. Met deze normen zal ook rekening worden gehouden bij de invulling van

[2] Kamerstukken II 2022-2023, 26643, nr. 925.

[3] Kamerstukken II, 2021-2022, 2752, nr. 268

[4] Normen van Nederlands Normalisatie Insituut (NEN). NEN is verantwoordelijk voor het vaststellen en beheren van NEN-normen. NEN 7510, 7512 en 7512 zijn het meest van belang voor zorginstellingen.

de zorgplicht in de nadere wetgeving op basis van de Cyberbeveiligingswet voor zorginstellingen die onder de toepasselijkheid van die wet komen te vallen. Daarnaast worden praktische hulpmiddelen ontwikkeld om de naleving te vergemakkelijken..

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet verwelkomt de doelstelling van het actieplan om de digitale weerbaarheid van zorginstellingen binnen de EU te vergroten. Aangezien de zorginstellingen dicht bij de burger staan en geavanceerde cyberaanvallen grote consequenties hebben op patiëntveiligheid en de samenleving, is het van belang de digitale weerbaarheid van zorginstellingen te vergroten. Bovendien wordt in de zorg gewerkt met bijzondere persoonsgegevens en worden zorgaanbieders extra kwetsbaar door digitalisering en de daarbij behorende ketenafhankelijkheid. Tegelijkertijd heeft het kabinet vragen over de wenselijkheid van het prioriteren van specifieke sectoren en wijst daarbij op het belang van implementatie van aanstaande cybersecuritywetgeving en het op een generieke manier versterken van cybersecurity, zodat het aan alle (kritieke) sectoren ten goede komt.

Het kabinet verwelkomt de aandacht in het actieplan voor de dreiging van *ransomware* en onderschrijft de intenties van de Commissie. Het kabinet verwelkomt tevens de voorstellen om het zicht op *ransomware* in de Unie te versterken om daarmee een effectieve opsporing te ondersteunen.

Het kabinet hecht groot belang aan de nadruk op het beveiligen van de keten van het zorgveld en kan zich vinden in de voorgestelde acties om de kleinere zorgaanbieders te ondersteunen op gebied van cyberveiligheid. Kleinere zorgaanbieders hebben geen grote IT- of securityteams en hebben een gebrek aan tijd, geld en expertise om cybersecurity succesvol te implementeren binnen de organisatie. In een keten van verbonden zorgsystemen vormen de kleinere zorginstellingen de zwakste schakel. Tevens vallen kleinere zorgaanbieders vaak niet onder de NIS2-richtlijn. Gerichte financiële steun (via cyberbeveiligingsvouchers) en praktische steun op het gebied van basis cyberhygiëne vindt het kabinet daarom nuttig. Het kabinet zal verduidelijking vragen over de financiering en uitvoering van deze vouchers.

Ook de voorgestelde gecoördineerde risicobeoordeling van zowel technische als strategische risico’s van de toeleveringsketen draagt bij aan de cyberweerbaarheid van de gehele zorgsector. Voor middelgrote en grotere zorgaanbieders zal deze risicobeoordeling met inachtneming van het hierover bepaalde in de aanstaande wetgeving ter implementatie van de NIS2-richtlijn plaatsvinden.
Het kabinet ziet de meerwaarde van de inzet op training en bewustwordingsactiviteiten. Online-trainingen en cursussen kunnen zorgen voor een sterke basis van bewustzijn over cybersecurity, en in het bijzonder het herkennen van (cyber)dreigingen. Het is daarom van belang dat de trainingen toegankelijk zijn voor verschillende soorten zorgprofessionals.

Voor de verdere uitwerking en beoordeling van het actieplan streeft het kabinet naar complementariteit, goede samenhang en het voorkomen van duplicatie met bestaande netwerken,

structuren, wetgeving en initiatieven op zowel EU- als nationaal niveau. Ook mogen maatregelen niet conflicteren met de verdragsrechtelijke bepaling over de uitsluitende verantwoordelijkheid van lidstaten op het gebied van bescherming van nationale veiligheid.

In dit kader heeft het kabinet aanmerkingen bij het inrichten van een Steuncentrum voor ziekenhuizen en zorgaanbieders bij ENISA. Allereerst is er de vraag hoe dit Steuncentrum zich zal verhouden tot de taken en verantwoordelijkheden die in de NIS2-richtlijn, en ter implementatie daarvan in nationale wetgeving, nu juist bij instanties van de lidstaten zijn belegd. Zo zijn er vragen over enkele voorgestelde taken omdat deze lijken te overlappen met taken die krachtens de NIS2-richtlijn (en in lijn daarmee de nationale wetgeving ter implementatie daarvan) aan lidstatelijke CSIRTs, waaronder in Nederland naar verwachting Z-CERT voor de zorgsector, zijn toegekend. Het kabinet is voor het gebruiken van datgene wat voortvloeit uit de implementatie van de NIS2-richtlijn en tegen het opzetten van parallelle structuren. Daarbij merkt het kabinet op dat het delen van informatie over cybersecurityincidenten door lidstaten met het Steuncentrum in elk geval niet verder zou moeten gaan dan in de gevallen waarin lidstaten hiertoe krachtens de NIS2-richtlijn gehouden zijn.

Ook is het onduidelijk voor het kabinet uit welke middelen een dergelijk Steuncentrum zal worden bekostigd, aangezien ENISA reeds voor uitdagingen staat als het gaat om de financiering van haar huidige taken. Daarbij heeft ENISA aangegeven over te weinig capaciteit te beschikken om aan haar huidige verplichtingen te kunnen voldoen. Daarnaast vraagt het kabinet zich af of het wenselijk is om middelen onder Digital Europe aan te wenden voor projecten van het Steuncentrum, omdat deze in de eerste plaats bestemd zijn voor het sectoroverstijgend versterken van cybersecurity.

Het kabinet verwelkomt het voorstel van de Commissie om de zorgsector binnen de EU weerbaarder te maken door de ontwikkeling van richtsnoeren, het ontwikkelen van een toegankelijk instrument dat de administratieve last vanwege regelgeving voor entiteiten in de zorg zal helpen minimaliseren en de opstelling van een raamwerk voor cybersecurityvolwassenheidsbeoordeling.
Het kabinet benadrukt echter de noodzaak om na te gaan of er eventueel sprake kan zijn van duplicatie en te kijken naar complementariteit van bestaande initiatieven op nationaal en EU-niveau.

Voor wat betreft de inzet van de in de Cybersolidariteitsverordening voorgestelde *EU Cybersecurity Reserve* in de zorgsector, onderstreept het kabinet het belang dat lidstaten zelf bepalen of zij eventueel gebruik willen maken van de diensten van de *EU Cybersecurity Reserve* een dat die diensten enkel ter ondersteuning van de uitoefening van de taken en bevoegdheden door nationale instanties moeten zijn. Daarnaast heeft het kabinet nadrukkelijk aanmerkingen bij het opzetten van een *Rapid Response Service* voor de zorgsector als onderdeel van de *EU Cybersecurity Reserve* en zal het de Commissie om toelichting vragen over de toegevoegde waarde, haalbaarheid, inrichting en raakvlakken met nationale bevoegdheden van deze dienst.

Ten aanzien van het voorstel om de in de Cybersolidariteitsverordening voorgestelde gecoördineerde paraatheidstesten in te zetten in de zorgsector, ziet het kabinet het testen van (kritieke) entiteiten als één van de maatregelen die een positief effect kunnen hebben op de digitale weerbaarheid van de zorgsector, maar wijst het kabinet ook op het belang van andere paraatheidsacties die hieraan kunnen bijdragen. Daarbij heeft het kabinet vragen over onder meer de selectie van (kritieke) entiteiten binnen de zorgsector voor deze paraatheidstesten en raakvlakken met nationale verantwoordelijkheden.

Het kabinet ontvangt graag een verduidelijking over het nut en de noodzaak van een *Cybersecurity Advisory Board* en een *Chief Information Security Officer* (CISO-) netwerk. Dit vanwege de al bestaande complexiteit binnen het EU-cyberlandschap en (mogelijke) overlap met huidige en aanstaande taken en bevoegdheden van nationale instanties. Zo bestaat het Europese Zorg ISAC primair uit CISO's in de zorgsector uit de verschillende lidstaten. Het kabinet ziet daarom liever een focus op harmonisatie en implementatie van reeds opgerichte instanties.

Tot slot bevat het actieplan nog een aantal elementen dat ingaat op het continueren van bestaand beleid, zoals de inzet van de Europese *ID-Wallet* in de gezondheidszorg en het gebruik van de *Cyber Diplomacy Toolbox*. Het kabinet steunt de voortgang van deze initiatieven en instrumenten.

c) Eerste inschatting van krachtenveld

In algemene zin verwelkomen de andere EU-lidstaten de doelstellingen van het actieplan om de zorgsector weerbaarder te maken. Zij benadrukken echter ook het belang om nationale bevoegdheden in relatie tot crisis-en incidentmanagement in gedachten te houden bij de verdere uitwerking van de maatregelen voortvloeiend uit dit actieplan. Ook zijn er zorgen geuit over de financiering van de voorgestelde initiatieven in het actieplan.

De positie van het Europees Parlement is nog onbekend.

4. Grondhouding ten aanzien van bevoegdheid, subsidiariteit, proportionaliteit, financiële gevolgen en gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

a) Bevoegdheid

De grondhouding van het kabinet is positief. De mededeling heeft betrekking op het verbeteren van de digitale weerbaarheid van de gezondheidszorgsector en dus op de beleidsterreinen van gemeenschappelijke veiligheidsvraagstukken op het gebied van volksgezondheid en de ruimte van vrijheid, veiligheid en recht. Op terreinen van gemeenschappelijke veiligheidsvraagstukken op het gebied van volksgezondheid en de ruimte van vrijheid, veiligheid en recht is sprake van een gedeelde bevoegdheid tussen de EU en de lidstaten op grond van artikel 4, lid 2, sub j en k van het Verdrag betreffende de werking van de Europese Unie (VWEU).

b) Subsidiariteit

De grondhouding van het kabinet is positief. De mededeling heeft tot doel om de cyberweerbaarheid van de zorgsector op Europees niveau te versterken. Gezien het grensoverschrijdende karakter van cyberdreigingen in de zorg, kan dit onvoldoende door de lidstaten op centraal, regionaal of lokaal niveau worden verwezenlijkt. Daarom is een EU-aanpak nodig. Daarnaast is het gelet op het grensoverschrijdend karakter wenselijk om ondersteuning van de Commissie en ENISA te ontvangen om de cyberweerbaarheid van de zorgsector te versterken. Dit geldt met name ook voor veel kleinere zorgaanbieders die niet onder de NIS2-richtlijn vallen. Gelet daarop, is optreden op het niveau van de EU gerechtvaardigd.

Het kabinet plaatst echter een aandachtspunt bij één specifiek aspect van de mededeling. Dit betreft de voorgenomen toewijzing van taken aan het Steuncentrum, die mogelijk overlappen met taken die nu juist nadrukkelijk bij nationale instanties, en meer in het bijzonder CSIRTS van lidstaten, worden of op korte termijn zullen worden belegd. Deze taken kunnen ook voldoende door de CSIRTS worden opgepakt, zonder duidelijke indicaties dat dit beter op Unieniveau zou kan kunnen worden opgepakt. In de uitvoering van deze taken is er dan ook ogenschijnlijk geen gerechtvaardigde reden voor optreden specifiek op het Unieniveau.

c) Proportionaliteit

De grondhouding van het kabinet is positief. De mededeling heeft tot doel om de cyberweerbaarheid van de zorgsector op Europees niveau te versterken. Het voorgestelde optreden is geschikt om deze doelstelling te bereiken. De verscheidene acties inzake preventie, detectie, respons, herstel en afschrikking zullen bijdragen aan het versterken van de cybersecurity van de gezondheidssector. Bovendien gaat het voorgestelde optreden grotendeels niet verder dan noodzakelijk, nu de voorgestelde richtsnoeren en maatregelen voornamelijk ondersteunend van aard zijn.

Wel plaatst het kabinet een aandachtspunt bij de oprichting van een *Rapid Response Service* bij het *EU Cybersecurity Reserve*. Dit lijkt verder te gaan dan noodzakelijk voor het bereiken van het doel. Lidstaten kunnen al goed terecht bij de *EU Cybersecurity Reserve* voor hulp bij incidentrespons. In dat kader heeft een dergelijke dienst op Europees niveau naar oordeel van het kabinet weinig toegevoegde waarde. Het kabinet pleit ervoor om de huidige structuur van hulp bij incidentrespons te behouden.

d) Financiële gevolgen

De gevolgen voor de EU-begroting zijn nog lastig in te schatten. Het kabinet zal de Commissie vragen aan te geven wat het financieel beslag van de toekomstige voorstellen zal zijn en wie aan deze financiële verantwoordelijkheden moet voldoen. Daarnaast zal het kabinet verduidelijking vragen over de financiering van (huidige) taken in relatie tot het gegeven budget gezien ENISA reeds heeft aangegeven over onvoldoende budget te beschikken om deze taken te kunnen uitvoeren en over de wenselijkheid van het reserveren van gelden binnen het Digital Europe programma voor projecten van het Steuncentrum. Daarnaast moet de ontwikkeling van de administratieve uitgaven in lijn zijn met de Europese Raadsconclusies van juli 2020 over het Meerjarig Financieel Kader (MFK) akkoord. Wanneer er sprake is van een stijging van het aantal werknemers zal het kabinet hier nauwkeurig op toe zien. Het kabinet is van mening dat de benodigde EU-middelen dienen te worden gevonden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2021-2027 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting. Het kabinet wil niet vooruit lopen op de integrale afweging van middelen na 2027.

Het kabinet ziet graag een specificering van de verdere financiële gevolgen voor lidstaten. Eventuele budgettaire gevolgen worden ingepast op de begroting van de beleidsverantwoordelijke departementen, conform de regels van de budgetdiscipline.

Het kabinet ontvangt graag een verdere specificering over het bekostigen van de in het actieplan voorgestelde uitrol van cyberbeveilingsvouchers voor kleinere ziekenhuizen en zorgaanbieders.

e) Gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

De gevolgen voor de regeldruk die moeten blijken uit het actieplan zijn nog moeilijk te duiden. Het is namelijk onduidelijk of de initiatieven omschreven in het actieplan voortbouwen op bestaande of aanstaande implementatie van de NIS2-richtlijn, of dat het om nieuwe initiatieven zal gaan. Het kabinet zal hierover verduidelijking vragen en inzetten op zo min mogelijk regeldruk. Er kan sprake zijn van additionele administratieve lasten voor de lidstaten en medeoverheden.

Er zijn geen gevolgen voor de concurrentiekracht van de EU. Het actieplan draagt bij aan de weerbaarheid van de EU en Nederland door de paraatheid en de responscapaciteiten van entiteiten in het zorgdomein te versterken.