Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 4056

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 12 mei 2025

De vaste commissie voor Volksgezondheid, Welzijn en Sport heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Volksgezondheid, Welzijn en Sport over de brief van 21 februari 2025 over het Fiche: Europees actieplan omtrent de cybersecurity van ziekenhuizen en zorgaanbieders (Kamerstuk 22 112, nr. 4000).

De vragen en opmerkingen zijn op 3 april 2025 aan de Minister van Volksgezondheid, Welzijn en Sport voorgelegd. Bij brief van 12 mei 2025 zijn de vragen beantwoord.

De voorzitter van de commissie,
Mohandis

Adjunct-griffier van de commissie,
Meijer

kst-22112-4056
ISSN 0921 - 7371
's-Gravenhage 2025

Inhoudsopgave

I. Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de PVV-fractie

De leden van de PVV-fractie hebben kennisgenomen van de brief van de Minister inzake het BNC-Fiche: Europees actieplan omtrent de cybersecurity van ziekenhuizen en zorgaanbieders. De leden van de PVV-fractie willen hierover een aantal vragen stellen.

In de brief wordt onder nummer twee (essentie voorstel) gesteld dat er hoge urgentie is voor het actieplan cybersecurity gezondheidssector door onder andere aanvallen van kwaadaardige software die bestanden blokkeert. In welke frequentie komen deze aanvallen voor en is bekend wat de oorsprong hiervan is? Ook zijn de leden van de PVV-fractie benieuwd hoe lang deze aanvallen al plaatsvinden en waarom er nu actie wordt ondernomen. De urgentie is blijkbaar hoog, maar was de urgentie daarvoor niet hoog genoeg of was er überhaupt geen dreiging waarneembaar?

Ook worden onder nummer twee vijf prioriteiten behandeld. In het tweede punt daarvan wordt gesteld dat er een steuncentrum komt voor ziekenhuizen en zorgaanbieders voor een betere informatie-uitwisseling. Waarom zou dit op dit gebied een goede maatregel/oplossing zijn en is er ook naar andere maatregelen/oplossingen gekeken? Zo ja, welke zijn dat geweest en waarom is daar niet voor gekozen? Onder het laatste punt (vijf) wordt beschouwd het ontmoedigen van de cyberaanvallen op Europese zorgstelsels. De EU zet hierbij in op cyberdiplomatie. Is dit niet een te slappe maatregel en hoe denkt het kabinet dat dit daadwerkelijk de cyberaanvallen zal doen afnemen? Kan het kabinet op dit punt hardere maatregelen voorstellen? Zo nee, waarom niet?

In de brief wordt aangegeven dat de gezondheidszorgsector zelf betrokken is bij het actieplan. Met welke organisaties uit deze sector is hierover gesproken, is onderzocht en/of zijn deze organisaties meegenomen in de terugkoppeling(en) op het actieplan? Is het kabinet van mening dat dit een representatief beeld geeft van hoe de gezondheidssector naar dit actieplan kijkt?

Onder punt vier (grondhouding ten aanzien van bevoegdheid, subsidiariteit, proportionaliteit, financiële gevolgen en gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten) hebben de leden van de PVV-fractie een vraag over punt B (subsidiariteit). Het kabinet heeft een kabinetsreactie gegeven over het actieplan en plaatst een aantal vraagtekens bij onder andere subsidiariteit en financiering. Welke verschillen ziet het kabinet in dit verschil van «enthousiasme» voor het actieplan en hoe kunnen het kabinet en de gezondheidssector nader tot elkaar komen hierbij? Tenslotte wordt uit de brief niet duidelijk hoe het kabinet verwacht dat het actieplan de implementatie van de EHDS moet ondersteunen. Kan

het kabinet duidelijkheid verschaffen over hoe dit nu verder gaat en hoe onze nationale bevoegdheid niet in het geding komt?

De leden van de PVV-fractie zien de meerwaarde van de inzet op training en bewustwordingsactiviteiten van zorgprofessionals. Zoals benoemd kunnen online trainingen en cursussen zorgen voor een sterke basis van bewustzijn over cybersecurity en in het bijzonder het herkennen van (cyber)dreigingen. Hoe gaat het kabinet ervoor zorgen dat de administratieve lasten hierdoor niet juist weer toenemen? Hoe wordt er geborgd dat dit niet ten koste gaat van «de handen aan het bed?»

De leden van de PVV-fractie kijken uit naar de verduidelijking over het nut en de noodzaak van een Cybersecurity Advisory Board en een Chief Information Security Officer (CISO-) netwerk. Vanwege de al bestaande complexiteit binnen het EU-cyberlandschap en (mogelijke) overlap met huidige en aanstaande taken en bevoegdheden van nationale instanties. Tevens ontvangen genoemde leden graag de verdere specificering over het bekostigen van de in het actieplan voorgestelde uitrol van cyberbeveiligingsvouchers voor kleinere ziekenhuizen en zorgaanbieders en de verdere financiële gevolgen voor lidstaten.

Vragen en opmerkingen van de GroenLinks-PvdA-fractie

De leden van de GroenLinks-PvdA-fractie hebben met interesse kennisgenomen van de voorliggende stukken over het actieplan van de Europese Commissie om cyberbeveiliging van ziekenhuizen en zorgverleners in Europa te verbeteren.

Deze leden achten het van groot belang dat de digitale veiligheid in de zorg op orde is, zeker in het licht van de toenemende dreiging van buiten de Europese Unie. Bovendien onderstrepen diverse ICT-storingen in Nederlandse ziekenhuizen van de afgelopen jaren en de storing bij het Amerikaanse CrowdStrike, waardoor vier Nederlandse ziekenhuizen operaties moesten schrappen, hun poliklinieken moesten sluiten en geen toegang meer hadden tot patiëntendossiers, de urgentie van een sterk beveiligde digitale infrastructuur in de zorg. Daarvoor is het van belang dat de sectorcapaciteit om cybersecurity-incidenten te voorkomen wordt versterkt, de informatie-uitwisseling en detectie van cyberdreigingen op orde komt en er sneller wordt gereageerd op incidenten.

De leden van de GroenLinks-PvdA-fractie zijn dan ook positief gestemd wanneer zij lezen dat het kabinet de intenties van de Commissie onderschrijft en de aandacht in het actieplan voor onder andere de dreiging van ransomware verwelkomt. Wel plaatsen de betreffende leden vraagtekens bij de wijze van financiering van de plannen. Zo staat het kabinet positief tegenover de voorgestelde acties om de kleinere zorgaanbieders te ondersteunen op het gebied van cyberveiligheid en vindt het kabinet gerichte financiële steun (via cyberbeveiligingsvouchers) en praktische steun via bijvoorbeeld trainingen en cursussen «nuttig». Het kabinet schrijft dat het verduidelijking zal vragen over de financiering en uitvoering van deze vouchers. Doordat op dit moment financiële toezeggingen echter nog ontbreken, is het voor deze leden niet duidelijk hoe de voorstellen worden gefinancierd en waar de verantwoordelijkheid daarvoor ligt: bij de EU via Europese fondsen of bij individuele lidstaten. Als het kabinet het actieplan daadwerkelijk onderschrijft en de noodzaak ervan onderkent, is het kabinet dan ook bereid hier structurele middelen voor vrij te maken wanneer dit niet of slechts deels wordt gefinancierd via Europese fondsen? Heeft het kabinet inzicht in de mogelijke kosten voor Nederland wanneer de maatregelen uit het actieplan volledig door de

lidstaten zelf betaald zouden moeten worden? Kan hier op zijn minst een schatting van gemaakt worden?

Ook hebben de leden van de GroenLinks-PvdA-fractie enkele vragen over hoe het actieplan van de EU zich verhoudt tot nationale plannen en projecten, zoals stichting Z-CERT. Hoe kunnen dergelijke initiatieven elkaar versterken? Hoe kan voorkomen worden dat er dubbelingen plaatsvinden of het zelfs leidt tot meer regeldruk?

Daarnaast hebben deze leden vragen over de verwachte reikwijdte en effectiviteit van het actieplan. In hoeverre verwacht het kabinet dat het zal bijdragen aan bijvoorbeeld het voorkomen van grote ICT-storingen of ransomware-aanvallen gericht op zorgverleners en ziekenhuizen? Wat is volgens het kabinet de balans tussen preventieve maatregelen in het actieplan enerzijds en maatregelen die pas in gang worden gezet wanneer er een storing of aanval plaatsvindt anderzijds? Is de verwachting dat met het actieplan sneller kan worden geacteerd bij grote storingen of aanvallen? En op welke termijn kan het actieplan naar verwachting geïmplementeerd worden wanneer eind 2025 een bijgewerkt actieplan wordt opgeleverd?

Tot slot vragen de leden van de GroenLinks-PvdA-fractie in hoeverre het actieplan bijdraagt aan een grotere Europese onafhankelijkheid van onze digitale zorginfrastructuur. Is het actieplan ook bedoeld om hierop te acteren? Wordt bijvoorbeeld verkend hoe Europese zorgverleners minder afhankelijk kunnen worden van niet-Europese clouddiensten en andere digitale systemen, of hoe digitale infrastructuur van zorgverleners en ziekenhuizen kan worden beschermd tegen overnames van bedrijven buiten de EU? Is het kabinet bereid zich ervoor in te zetten dat dit onderdeel wordt van het actieplan?

Vragen en opmerkingen van de VVD-fractie

De leden van de VVD-fractie hebben met interesse kennisgenomen van het fiche over een Europees actieplan omtrent de cybersecurity van ziekenhuizen en zorgaanbieders. Zij maken zich al langer zorgen over de toename van cybercrime en cyberincidenten in de zorg en hebben daar regelmatig vragen over gesteld.[1] De leden zien dat een urgente aanpak nodig is en zijn positief over een gezamenlijke aanpak op Europees niveau en hebben hierbij enkele vragen.

Dat het hoogste aantal cyberincidenten gemeld wordt in de zorgsector baart de leden van de VVD-fractie grote zorgen. Hoeveel cyberincidenten zijn er gemeld in de jaren 2023 en 2024? En is bij incidenten sprake geweest van risico's met betrekking tot patiëntgegevens of continuïteit van zorg, wat voor type risico's waren dat en hoe zijn die geminimaliseerd of opgelost?

In de financiële sector is de cyberveiligheid onder andere verstevigd door het zogenoemde TIBER-programma waarbij (grote) financiële instellingen door middel van ethische hacks – uiteraard binnen geldende regels – cyberaanvallen naspelen om zo eventuele kwetsbaarheden te vinden en weg te nemen. Hierover dienen zij periodiek te rapporteren aan de Nederlandsche Bank (DNB), opdat de veiligheid van gegevens optimaal wordt beschermd. De leden van de VVD-fractie vinden het een interessante gedachte om een dergelijke maatregel ook in de zorgsector toe te passen. Zij vragen naar de norm die geldt voor financiële instellingen en

[1] Aanhangsel Handelingen II 2021/22, nr. 1981, Aanhangsel Handelingen II 2022/23, nrs. 1883 en 2246

in welke mate deze ook voor zorginstellingen kan worden ingesteld. Kan een overzicht worden gegeven van type gegevens die financiële instellingen moeten aanleveren bij de DNB en welke andere stappen zij moeten zetten voor deelname aan dit programma?

De leden van de VVD-fractie lezen dat het kabinet over het algemeen positief is over het actieplan, maar ook nog vragen en aanmerkingen heeft. Welke aanbevelingen zou het kabinet willen zien om het actieplan te verbeteren?

Met betrekking tot de financiering van het actieplan, vinden de leden van de VVD-fractie dit te summier en erg onduidelijk. Zij lezen dat het kabinet gerichte financiële steun nuttig vindt, maar lezen niet hoe het kabinet dit gerealiseerd ziet worden. Kan de Minister een financiële paragraaf toevoegen met daarin duidelijker inzicht.

Tot slot lezen de leden van de VVD-fractie dat het kabinet inzet op bewustwording over informatieveiligheid onder zorgmedewerkers. Hier wordt verwezen naar een brief uit december 2022. Welke stappen zijn sindsdien gezet om bewustwording te vergroten en hebben deze stappen geleid tot daadwerkelijk resultaat?

Vragen en opmerkingen van de NSC-fractie

De leden van de Nieuw Sociaal Contract-fractie hebben met interesse het fiche gelezen over het Europees actieplan omtrent de cybersecurity van ziekenhuizen en zorgaanbieders. De leden zijn er positief over dat de EU zich ook gaat bezighouden met de cybersecurity van zorgaanbieders. Wel hebben wij daarover een aantal vragen.

De leden van de NSC-fractie willen graag van de Minister weten in hoeverre de Nederlandse zorgaanbieders reeds aansluiten bij de systemen die in de EU worden gebruikt voor de preventie, detectie en identificatie van cyberaanvallen.

De leden van de NSC-fractie maken zich zorgen over de huidige cyberveiligheid van zorginstellingen, aangezien een groot deel nog niet voldoet aan de NEN-normen. Wat gaat de Minister doen om ervoor te zorgen dat alle zorginstellingen binnen twee jaar aan deze normen voldoen en wat wordt de rol van Z-CERT hierin?

Nederland kent zowel kleine als grote zorgaanbieders. De leden van de NSC-fractie willen graag weten hoe de implementatie en de eventuele prioritering van de cyberveiligheidsmaatregelen voor zorgaanbieders verloopt, en hoe de NIS2-richtlijn hierin wordt meegenomen.

De leden van de NSC-fractie lezen dat Z-CERT een belangrijke rol zal spelen bij de implementatie van de cybersecuritymaatregelen. Hoe wordt gegarandeerd dat Z-CERT medewerkers screent op betrouwbaarheid?

De leden van de NSC-fractie vragen de Minister op welke manier aanbieders van digitale systemen betrokken worden door Z-CERT en ENISA bij de implementatie van de cybersecuritymaatregelen. Welke eisen worden aan aanbieders van digitale systemen gesteld om ervoor te zorgen dat zij voldoen aan de EU-normen?

De leden van de NSC-fractie willen graag weten op welke manier het actieplan zich richt op het secundaire gebruik van zorgdata (door onderzoekers).

De leden van de NSC-fractie willen graag weten op welke wijze cyberincidentnotificaties van ziekenhuizen en zorgaanbieders momenteel worden verzameld en verwerkt.

De leden van de NSC-fractie vragen hoe het kabinet zich zal inzetten om ervoor te zorgen dat online trainingen en cursussen voor bewustwording van cybersecurity toegankelijk zijn voor verschillende soorten zorgprofessionals.

De leden van de NSC-fractie willen graag weten op welke wijze het kabinet zich inzet om te onderzoeken of er sprake is van duplicatie van initiatieven en hoe de complementariteit van bestaande initiatieven op nationaal en EU-niveau wordt gewaarborgd.

De leden van de NSC-fractie vragen hoe het kabinet ervoor zorgt dat er geen overlap van taken ontstaat tussen ENISA en Nederlandse instanties.

De leden van de NSC-fractie willen graag weten wat de financiële consequenties voor Nederland zijn om deze plannen uit te voeren, en of deze al zijn opgenomen in de huidige begroting.

Vragen en opmerkingen van de BBB-fractie

De leden van de BBB-fractie hebben kennisgenomen van het Fiche: Europees actieplan omtrent de cybersecurity van ziekenhuizen en zorgaanbieders. De leden hebben geen vragen aan de Minister.

II. Reactie van de Minister

De leden van de PVV-fractie hebben kennisgenomen van de brief van de Minister inzake het BNC-Fiche: Europees actieplan omtrent de cybersecurity van ziekenhuizen en zorgaanbieders. De leden van de PVV-fractie willen hierover een aantal vragen stellen.

In de brief wordt onder nummer twee (essentie voorstel) gesteld dat er hoge urgentie is voor het actieplan cybersecurity gezondheidssector door onder andere aanvallen van kwaadaardige software die bestanden blokkeert. In welke frequentie komen deze aanvallen voor en is bekend wat de oorsprong hiervan is? Ook zijn de leden van de PVV-fractie benieuwd hoe lang deze aanvallen al plaatsvinden en waarom er nu actie wordt ondernomen. De urgentie is blijkbaar hoog, maar was de urgentie daarvoor niet hoog genoeg of was er überhaupt geen dreiging waarneembaar?

Digitale systemen vormen «het zenuwstelsel» van onze maatschappij (inclusief de zorg) en we worden hiervan in toenemende mate afhankelijk. Met een sterk gewijzigde geopolitieke situatie én door het breder beschikbaar komen van nieuwe technologieen zoals AI, moet de zorg weerbaarder worden tegen cyberaanvallen. De afgelopen jaren zijn meer ziekenhuizen en zorginstellingen in Europa slachtoffer geweest van ransomware-aanvallen. Dit blijkt onder andere uit het jaarlijkse dreigingsbeeld dat sinds 2020 gepubliceerd wordt door Z-CERT, expertisecentrum voor cybersecurity in de zorg. Nederland doet het in verhouding tot andere Europese landen relatief goed. De kwaad willenden zijn in de meeste gevallen criminele hackers die gevoelige data stelen om instellingen losgeld te vragen en af te persen. Er is bij Z-CERT geen geval bekend van een aanval van een statelijke actor[2]. Echter, in het kader van de huidige geopolitieke ontwikkelingen is niet uit te sluiten dat een

[2] Cybersecurity Dreigingsbeeld voor de zorg 2024

dergelijke aanval in de toekomst plaats zal vinden. In het meest recente cybersecuritybeeld komt namelijk naar voren dat statelijke actoren hun capaciteiten verbreden en hun activiteiten intensiveren. Bovendien kunnen nieuwe technologieën, zoals generatieve AI, van invloed zijn op de digitale veiligheid. AI kan bijvoorbeeld ingezet worden om cyberaanvallen op een snellere, automatischere en laagdrempeligere manier uit te voeren. Met bovenstaande ontwikkelingen op de achtergrond onderschrijf ik de doelstelling van het actieplan om de cyberweerbaarheid van de zorgsector te verhogen.

Ook worden onder nummer twee vijf prioriteiten behandeld. In het tweede punt daarvan wordt gesteld dat er een steuncentrum komt voor ziekenhuizen en zorgaanbieders voor een betere informatie-uitwisseling. Waarom zou dit op dit gebied een goede maatregel/oplossing zijn en is er ook naar andere maatregelen/oplossingen gekeken? Zo ja, welke zijn dat geweest en waarom is daar niet voor gekozen?

Het steuncentrum heeft onder andere als doelstelling om (vroegtijdig) notificaties van cyberincidenten uit te wisselen en een instrument te ontwikkelen dat administratieve lasten verlicht voor entiteiten die aan wetgeving onderhevig zijn. Het is mij niet bekend of de Commissie in dit kader gekeken heeft naar andere instrumenten dan het inrichten van een steuncentrum. Zoals beschreven in het fiche heeft het kabinet bedenkingen bij het instellen van een steuncentrum, vanwege de verhouding met de taken en verantwoordelijkheden op nationaal niveau. Ook is niet duidelijk uit welke middelen het steuncentrum zou moeten worden bekostigd. Deze bedenkingen worden meegegeven in de onderhandelingen in de werkgroep waar de lidstaten voorstellen van de Europese Commissie op gebied van cyberbeleid bespreken, de Horizontale groep Cybervraagstukken. In dit gremium zal worden ingezet op zo min mogelijk regeldruk en overlap of duplicatie van bestaande taken. Aangezien dit voorstel een nieuwe sectorspecifieke aanpak behelst, moet er nog veel duidelijk worden en blijft het een lopend gesprek tussen lidstaten over de toegevoegde waarde van de voorgestelde acties in het actieplan.

Onder het laatste punt (vijf) wordt beschouwd het ontmoedigen van de cyberaanvallen op Europese zorgstelsels. De EU zet hierbij in op cyberdiplomatie. Is dit niet een te slappe maatregel en hoe denkt het kabinet dat dit daadwerkelijk de cyberaanvallen zal doen afnemen? Kan het kabinet op dit punt hardere maatregelen voorstellen? Zo nee, waarom niet?

De inzet van cyberdiplomatie is één instrument, naast vele andere. Zoals beschreven onder Pijler III van de Nationale Cybersecurity Strategie (NLCS) is de inzet van diplomatieke middelen wenselijk om zicht te krijgen op snelgroeiende digitale dreigingen van staten en criminelen[3]. Dit kan bijvoorbeeld via gerichte diplomatieke rapportages, consultaties en coalitievorming met gelijkgezinden en dialogen met niet-gezinde partijen. Naast het versterken van de informatiepositie over digitale ontwikkelingen kunnen door diplomatieke samenwerking ook nieuwe en effectievere opties voor respons op cyberdreigingen worden ontwikkeld. Een voorbeeld hiervan is de EU *Cyber Diplomacy Toolbox.* Onderdeel van het Europese actieplan is om te verkennen hoe de *Toolbox* ingezet kan worden om kwaadwillende activiteiten tegen digitale zorgsystemen tegen te gaan. Complementair hieraan worden er meer tastbare acties voorgesteld zoals bijvoorbeeld publiek-private samenwerking en het inrichten van bewustwordingstrainingen voor zorgprofessionals. Daarnaast is het actieplan een aanvulling op wet- en regelgeving, zoals de NIS2, welke

[3] Nederlandse Cybersecuritystrategie 2022-2028

ervoor zorgt dat organisaties en entiteiten hun digitale veiligheid en cyberweerbaarheid moeten verhogen.

In de brief wordt aangegeven dat de gezondheidszorgsector zelf betrokken is bij het actieplan. Met welke organisaties uit deze sector is hierover gesproken, is onderzocht en/of zijn deze organisaties meegenomen in de terugkoppeling(en) op het actieplan? Is het kabinet van mening dat dit een representatief beeld geeft van hoe de gezondheidssector naar dit actieplan kijkt?

Onder punt vier (grondhouding ten aanzien van bevoegdheid, subsidiariteit, proportionaliteit, financiële gevolgen en gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten) hebben de leden van de PVV-fractie een vraag over punt B (subsidiariteit). Het kabinet heeft een kabinetsreactie gegeven over het actieplan en plaatst een aantal vraagtekens bij onder andere subsidiariteit en financiering. Welke verschillen ziet het kabinet in dit verschil van «enthousiasme» voor het actieplan en hoe kunnen het kabinet en de gezondheidssector nader tot elkaar komen hierbij?

Het kabinet erkent dat cyberdreigingen per definitie grensoverschrijdend zijn en wil leren van bewezen goede praktijken in Europese landen om de zorg in Nederland nog weerbaarder te krijgen. Tegelijkertijd is nog veel onhelder over een eventuele Europese aanpak. De commissie heeft via verschillende wegen, waaronder van Z-CERT, input verzameld vanuit de lidstaten om het Health Action Plan op te stellen. Zoals beschreven in het actieplan is na publicatie van het actieplan een publieke consultatie uitgezet bij stakeholders binnen de zorgsector zoals zorgaanbieders, maar ook bij patiënten en overheden. Het doel hiervan is het ophalen van ideeën voor effectieve implementatie van de voorgestelde acties in het plan. De digitale consultatie is recent open gezet en kan tot eind juni worden ingevuld door bijvoorbeeld zorgprofessionals, cybersecurity specialisten en patiënten. Ik zal de consultatie breed onder de aandacht brengen onder verschillende koepels en brancheorganisaties in de Nederlandse zorg om te zorgen dat er een volledig beeld wordt geschetst.

Tenslotte wordt uit de brief niet duidelijk hoe het kabinet verwacht dat het actieplan de implementatie van de EHDS moet ondersteunen. Kan het kabinet duidelijkheid verschaffen over hoe dit nu verder gaat en hoe onze nationale bevoegdheid niet in het geding komt?

De EHDS legt vereisten neer voor beveiliging, bijvoorbeeld voor EPD-systemen die door ziekenhuizen worden gebruikt voor de verwerking en uitwisseling van gezondheidsgegevens. Het actieplan en de EHDS vullen elkaar zodanig aan dat gezondheidsgegevens beschikbaar zijn voor geautoriseerde personen en zorgaanbieders weerbaarder worden voor cyberincidenten. Daarmee wordt de continuïteit van de zorg geborgd en zijn gezondheidsgegevens veilig bij ziekenhuizen en zorginstellingen. Het actieplan bevat geen bindende vereisten en is bedoeld om de cyberveiligheid van het zorgveld te versterken door een gecoördineerde Europese aanpak.

De leden van de PVV-fractie zien de meerwaarde van de inzet op training en bewustwordingsactiviteiten van zorgprofessionals. Zoals benoemd kunnen online trainingen en cursussen zorgen voor een sterke basis van bewustzijn over cybersecurity en in het bijzonder het herkennen van (cyber)dreigingen. Hoe gaat het kabinet ervoor zorgen dat de administratieve lasten hierdoor niet juist weer toenemen? Hoe wordt er geborgd dat dit niet ten koste gaat van «de handen aan het bed?»

Ik onderschrijf de noodzaak om te voorkomen dat de administratieve lasten met dit actieplan onnodig toenemen. In de zorg is het een permanent balanceren tussen gebruikersgemak (inclusief administratieve lasten voor zorgprofessionals) en de patiënt- en dataveiligheid van de patiënt. Zorgprofessionals spelen een cruciale rol in het bewaken van die veiligheid. Bronnen vermelden dat circa 75% van de cyberincidenten in de zorg gedrag gerelateerd is; we moeten daarom permanent werken aan het cyberbewustzijn onder zorgprofessionals. Dat kan met laagdrempelige en online training modules en cursussen, zoals het actieplan voorstelt. Ten tweede wordt met het actieplan juist beoogd om de administratieve lasten te verlichten voor entiteiten die aan verschillende complexe soorten wetgeving in het zorgveld en cybersecurity domein onderhevig zijn. Een van de voorgestelde acties is om een hulpmiddel te ontwerpen om beter inzicht te krijgen in het veelal complexe netwerk van verschillende wet- en regelgeving. Dit moet zorgaanbieders juist helpen in het navigeren naar de juiste naleving van wettelijke vereisten.

De leden van de PVV-fractie kijken uit naar de verduidelijking over het nut en de noodzaak van een Cybersecurity Advisory Board en een Chief Information Security Officer (CISO-) netwerk. Vanwege de al bestaande complexiteit binnen het EU-cyberlandschap en (mogelijke) overlap met huidige en aanstaande taken en bevoegdheden van nationale instanties. Tevens ontvangen genoemde leden graag de verdere specificering over het bekostigen van de in het actieplan voorgestelde uitrol van cyberbeveiligingsvouchers voor kleinere ziekenhuizen en zorgaanbieders en de verdere financiële gevolgen voor lidstaten.
Er is op dit moment nog weinig meer bekend over de denkbeelden achter een Advisory Board of een CISO-netwerk. Z-CERT participeert nu reeds in een netwerk van like-minded organisaties. Juist de korte lijnen en het informele karakter maakt dat informatie ten tijde van incidenten snel gedeeld wordt. Onderling vertrouwen is hierin minstens zo belangrijk als institutionele arrangementen.
Ook over het idee van vouchers hoop ik de komende tijd meer te leren in de Brusselse werkgroepen. Wanneer de Europese Commissie verduidelijking gegeven heeft, zal ik nadere informatie hierover met u delen in een door mij toegezegde Kamerbrief over cybersecurity en weerbaarheid in het zorgveld in Q3 van 2025.

De leden van de GroenLinks-PvdA-fractie zijn dan ook positief gestemd wanneer zij lezen dat het kabinet de intenties van de Commissie onderschrijft en de aandacht in het actieplan voor onder andere de dreiging van ransomware verwelkomt. Wel plaatsen de betreffende leden vraagtekens bij de wijze van financiering van de plannen. Zo staat het kabinet positief tegenover de voorgestelde acties om de kleinere zorgaanbieders te ondersteunen op het gebied van cyberveiligheid en vindt het kabinet gerichte financiële steun (via cyberbeveiligingsvouchers) en praktische steun via bijvoorbeeld trainingen en cursussen «nuttig». Het kabinet schrijft dat het verduidelijking zal vragen over de financiering en uitvoering van deze vouchers. Doordat op dit moment financiële toezeggingen echter nog ontbreken, is het voor deze leden niet duidelijk hoe de voorstellen worden gefinancierd en waar de verantwoordelijkheid daarvoor ligt: bij de EU via Europese fondsen of bij individuele lidstaten. Als het kabinet het actieplan daadwerkelijk onderschrijft en de noodzaak ervan onderkent, is het kabinet dan ook bereid hier structurele middelen voor vrij te maken wanneer dit niet of slechts deels wordt gefinancierd via Europese fondsen?

Over het idee van vouchers en hun financiering hoop ik de komende tijd meer te leren in de Brusselse werkgroepen. Nadere informatie hierover zal ik met u delen in een door mij toegezegde Kamerbrief over cybersecurity

en weerbaarheid in het zorgveld. Ik wil nu alvast wel twee kanttekeningen maken. Een systeem van Europese vouchers mag niet leiden tot uitgebreide bureaucratische processen. Daarnaast doen eventuele EU-vouchers niet af aan de primaire verantwoordelijkheid van zorgaanbieders voor hun informatieveiligheid. Zorginstellingen nemen maatregelen om cyberincidenten te voorkomen, de gevolgen van cyberaanvallen te beperken, en waar nodig zo spoedig mogelijk te mitigeren. Deze maatregelen vloeien voort uit hun verantwoordelijkheden inzake het beroepsgeheim en goed hulpverlenerschap en zijn uitgewerkt in specifieke wettelijke verplicht gestelde normen voor informatiebeveiliging in de zorg. Dit betreft de NEN7510, 7512 en 7513. Kern hierbij is de NEN 7510 norm, die met name voorschrijft dat zorginstellingen de risico's voor informatiebeveiliging in kaart brengen en hiervoor passende maatregelen nemen. De norm vereist ook beheersmaatregelen voor de bescherming van netwerken, bedrijfscontinuïteit en bereikbaarheid. De aanvullende normen NEN 7512 en 7513 zien er daarnaast op toe dat er wordt voldaan aan eisen voor veilige gegevensuitwisseling en logging. De zorg voor cybersecurity is een integraal deel van de bedrijfsvoering en dient net zo vanzelfsprekend te zijn als de zorg voor bijvoorbeeld een brandverzekering.

Heeft het kabinet inzicht in de mogelijke kosten voor Nederland wanneer de maatregelen uit het actieplan volledig door de lidstaten zelf betaald zouden moeten worden? Kan hier op zijn minst een schatting van gemaakt worden?

Het is op dit moment niet mogelijk inzicht te geven in eventuele financiële gevolgen van het actieplan voor Nederland. Vele ideeën in het Actieplan zijn namelijk nog vaag of onbestemd en we kunnen in Nederland de weging over toegevoegde waarde (nog) niet maken.

Ook hebben de leden van de GroenLinks-PvdA-fractie enkele vragen over hoe het actieplan van de EU zich verhoudt tot nationale plannen en projecten, zoals stichting Z-CERT. Hoe kunnen dergelijke initiatieven elkaar versterken? Hoe kan voorkomen worden dat er dubbelingen plaatsvinden of het zelfs leidt tot meer regeldruk?

Zoals beschreven, ondersteun ik het zorgveld op verschillende manieren bij het bewerkstelligen van informatieveiligheid. Ik zet bijvoorbeeld in op het breed beschikbaar stellen van de diensten van expertisecentrum voor cybersecurity in de zorg Z-CERT. Z-CERT helpt zorginstellingen onder andere bij preventie, detectie, respons en herstel van cyber incidenten. Deze lopende taken en acties van Z-CERT hebben op verschillende manieren toegevoegde waarde in de Europese context. Zo werkt Z-CERT internationaal samen als oprichter en voorzitter van *het European Health Information Sharing & Analyses Center* (EH- ISAC). Dit is een samenwerkingsverband door en voor Europese zorgpartijen op het gebied van cybersecurity. Het verstevigen van dit samenwerkingsverband is onderdeel van het actieplan en hiermee kan ook de informatiepositie van Z-CERT verbeterd worden. Dit zal het Nederlandse zorgveld ten goede komen. Tevens kunnen Nederlandse initiatieven van Z-CERT zoals het Zorg Detectie Netwerk, waarmee dreigingsinformatie sneller gedeeld kan worden, en de cybersecurity volwassenheidstoetsen als *best practices* gedeeld worden met andere lidstaten. Omgekeerd staat Z-CERT open om te leren van bewezen goede praktijken uit andere EU-landen. Cyberdreigingen hebben namelijk per definitie een grensoverschrijdend karakter en van een betere bescherming van zorginstellingen in de gehele EU zal ook de Nederlandse zorg profiteren.

Op dit moment zijn de gevolgen voor de regeldruk die moeten blijken uit het actieplan nog moeilijk te duiden. Het is namelijk niet duidelijk of de voorgestelde acties in het actieplan voortbouwen op bestaande of aanstaande acties in het kader van implementatie van de NIS2-richtlijn, of dat het om nieuwe initiatieven zal gaan.

Daarnaast hebben deze leden vragen over de verwachte reikwijdte en effectiviteit van het actieplan. In hoeverre verwacht het kabinet dat het zal bijdragen aan bijvoorbeeld het voorkomen van grote ICT-storingen of ransomware-aanvallen gericht op zorgverleners en ziekenhuizen? Wat is volgens het kabinet de balans tussen preventieve maatregelen in het actieplan enerzijds en maatregelen die pas in gang worden gezet wanneer er een storing of aanval plaatsvindt anderzijds? Is de verwachting dat met het actieplan sneller kan worden geacteerd bij grote storingen of aanvallen?

Omdat nog veel onhelder is over de uitwerking van deze eerste ideeën in dit Actieplan, is het moeilijk uitspraken te doen over een meetbaar effect van instrumenten uit dit Actieplan. Aangezien cyberdreigingen een grensoverschrijdend karakter hebben, kan een Europese aanpak meerwaarde hebben. Het leren van andere landen hoe preventie effectiever in te richten, voegt al snel waarde toe. Het snel geïnformeerd raken over aard en achtergrond van een incident in één land kan leiden tot preventieve of mitigerende maatregelen in een ander land. Preventie en incident-response gaan daarbij hand in hand. De nadruk in het actieplan ligt op de preventieve maatregelen zoals het voorkomen en detecteren van cyberincidenten of dreigingen. Er staan in mindere mate acties in het plan die gericht zijn op herstel en respons.

En op welke termijn kan het actieplan naar verwachting geïmplementeerd worden wanneer eind 2025 een bijgewerkt actieplan wordt opgeleverd?

Enkele acties die gebaseerd zijn op reeds bestaande initiatieven zijn al gestart, zoals een hulpmiddel waarmee de verschillende wetgevingstrajecten in beeld worden gebracht, het oprichten van een cybersecurity adviesraad binnen ENISA gericht op de zorg en het publiceren van een publieke consultatie over het actieplan. Daarnaast zijn er nieuw voorgestelde acties waarover onderhandeld wordt in de werkgroep waar de lidstaten voorstellen van de Europese Commissie op gebied van cyberbeleid bespreken. In deze onderhandelingen worden ook de resultaten van de publieke consultatie bij stakeholders meegenomen. Naar aanleiding van de inbreng van de lidstaten en de publieke consultatie zal eind 2025 een bijgewerkt plan worden opgeleverd en zal naar verwachting in de loop van 2026 gestart worden met het uitvoeren van acties.

Tot slot vragen de leden van de GroenLinks-PvdA-fractie in hoeverre het actieplan bijdraagt aan een grotere Europese onafhankelijkheid van onze digitale zorginfrastructuur. Is het actieplan ook bedoeld om hierop te acteren? Wordt bijvoorbeeld verkend hoe Europese zorgverleners minder afhankelijk kunnen worden van niet-Europese clouddiensten en andere digitale systemen, of hoe digitale infrastructuur van zorgverleners en ziekenhuizen kan worden beschermd tegen overnames van bedrijven buiten de EU? Is het kabinet bereid zich ervoor in te zetten dat dit onderdeel wordt van het actieplan?

De Europese onafhankelijkheid van digitale zorginfrastructuur is geen onderdeel van dit actieplan. Ik onderschrijf de noodzaak om door de huidige geopolitieke spanningen kritisch te kijken naar afhankelijkheid van zorgaanbieders. De ontwikkeling van het gezondheidsinformatiestelsel, gericht op data beschikbaarheid, biedt kansen om bij de ontwikkeling van

het stelsel maatregelen te nemen om afhankelijkheid van specifieke leveranciers te voorkomen. Zo heeft bijvoorbeeld Stichting Cumuluz Zorgdata in de uitwerking van een zorg data-integratielaag, zich gecommitteerd om dit vendor neutraal en volgens de normen van het Rijk in te richten. Dit geldt ook voor cloud-oplossingen. Tevens wordt de Wet veiligheidstoets investeringen, fusies en overnames (Vifo) herzien door het Ministerie van Economische Zaken. Deze wet is gericht op het voorkomen van vijandige investeringen, fusies en overnames. Ik zoek momenteel uit of het mogelijk is om partijen binnen de digitale infrastructuur van de zorg onder deze wet te laten vallen. Daarnaast werk ik samen met het Ministerie van Justitie en Veiligheid aan de nieuwe Cyberbeveiligingswet, die partijen in de zorg verplicht om maatregelen te treffen om hun digitale veiligheid en weerbaarheid te vergroten.

De leden van de VVD-fractie hebben met interesse kennisgenomen van het fiche over een Europees actieplan omtrent de cybersecurity van ziekenhuizen en zorgaanbieders. Zij maken zich al langer zorgen over de toename van cybercrime en cyberincidenten in de zorg en hebben daar regelmatig vragen over gesteld.[4] De leden zien dat een urgente aanpak nodig is en zijn positief over een gezamenlijke aanpak op Europees niveau en hebben hierbij enkele vragen.

Dat het hoogste aantal cyberincidenten gemeld wordt in de zorgsector baart de leden van de VVD-fractie grote zorgen. Hoeveel cyberincidenten zijn er gemeld in de jaren 2023 en 2024? En is bij incidenten sprake geweest van risico's met betrekking tot patiëntgegevens of continuïteit van zorg, wat voor type risico's waren dat en hoe zijn die geminimaliseerd of opgelost?

Z-CERT brengt jaarlijks een dreigingsbeeld cybersecurity in de zorg uit. Uit het dreigingsbeeld van 2023 blijkt dat Z-CERT 29 incidenten bij zorgaanbieders in Europa registreerde, met impact op 101 locaties[5]. In 2024 waren er 37 getroffen zorgorganisaties, met (in)directe impact op 91 zorglocaties[6]. Z-CERT heeft geen inzicht of er sprake is geweest van risico's met betrekking tot patiëntgegevens of continuïteit van zorg. De manier waarop risico's geclassificeerd en behandeld worden, verschilt per zorginstelling. Zorginstellingen wordt geadviseerd basisprincipes toe te kennen die door het Nationaal Cybersecurity Centrum (NCSC) onder de aandacht zijn gebracht[7]. Door het toepassen van deze principes kunnen veel risico's verkleind worden.

In de financiële sector is de cyberveiligheid onder andere verstevigd door het zogenoemde TIBER-programma waarbij (grote) financiële instellingen door middel van ethische hacks – uiteraard binnen geldende regels – cyberaanvallen naspelen om zo eventuele kwetsbaarheden te vinden en weg te nemen. Hierover dienen zij periodiek te rapporteren aan de Nederlandsche Bank (DNB), opdat de veiligheid van gegevens optimaal wordt beschermd. De leden van de VVD-fractie vinden het een interessante gedachte om een dergelijke maatregel ook in de zorgsector toe te passen. Zij vragen naar de norm die geldt voor financiële instellingen en in welke mate deze ook voor zorginstellingen kan worden ingesteld. Kan een overzicht worden gegeven van type gegevens die financiële instellingen moeten aanleveren bij de DNB en welke andere stappen zij moeten zetten voor deelname aan dit programma?

---

[4] Aanhangsel Handelingen II 2021/22, nr. 1981, Aanhangsel Handelingen II 2022/23, nrs. 1883 en 2246

[5] Cybersecurity dreigingsbeeld voor de zorg 2023

[6] Cybersecurity dreigingsbeeld voor de zorg 2024

[7] 5 basisprincipes van digitale weerbaarheid

De norm voor informatiebeveiliging in de zorg, NEN-7510, is net als de normen voor informatiebeveiliging in de financiële sector gebaseerd op de mondiale norm voor informatiebeveiliging, de ISO27001. De basis voor gegevensbeveiliging is daarmee voor deze twee sectoren vergelijkbaar. De verdere uitwerking en invulling in de zorg verschilt echter van de bancaire wereld. Het aantal en vooral de diversiteit aan zorgaanbieders vraagt om proportionele en realistische verplichtingen, vandaar dat de NEN7510 vanuit een op te stellen risico-analyse verder normeert. Het toezicht op naleving is daarmee ook fundamenteel anders ingericht. Ik onderschrijf het belang van ethische hacks om te onderzoeken of cybersecurity maatregelen in de praktijk werken. Via het Zorg *Redteaming Resilience* Oefeningen (ZORRO) raamwerk ondersteunt Z-CERT bij het doen van ethische hacktesten bij een beperkt aantal zorgaanbieders[8]. Als basis voor ZORRO wordt het *Advanced Red Teaming* raamwerk (ART) gebruikt en deze is ontwikkeld in samenwerking met CIO-Rijk en de Nederlandsche Bank. Dit raamwerk is ontwikkeld als lichtere variant van het TIBER raamwerk en is daardoor geschikter om ook door kleinere organisaties gebruikt te worden. Met de testen kan toegezien worden of preventieve maatregelen werken, maar ook of detectie van een aanval plaatsvindt en welke reactie hierop wordt gegeven. Daarnaast worden de resultaten van de geanonimiseerde testen gedeeld met de community van Z-CERT zodat andere zorginstellingen hier ook van kunnen leren.

De leden van de VVD-fractie lezen dat het kabinet over het algemeen positief is over het actieplan, maar ook nog vragen en aanmerkingen heeft. Welke aanbevelingen zou het kabinet willen zien om het actieplan te verbeteren?

Zoals beschreven in het BNC-fiche heeft het Kabinet aanmerkingen bij een aantal van de voorgestelde acties in het Actieplan. Reden hiervoor is dat deze acties beperkt uitgewerkt zijn of beperkte toegevoegde waarde lijken te hebben voor Nederland. Daarom is het op dit moment niet mogelijk om meer verbeterpunten te noemen dan die in het BNC-fiche beschreven zijn. Er zal daarom verduidelijking gevraagd worden bij de Commissie over de specifieke invulling van deze acties.

Met betrekking tot de financiering van het actieplan, vinden de leden van de VVD-fractie dit te summier en erg onduidelijk. Zij lezen dat het kabinet gerichte financiële steun nuttig vindt, maar lezen niet hoe het kabinet dit gerealiseerd ziet worden. Kan de Minister een financiële paragraaf toevoegen met daarin duidelijker inzicht.

Het is op dit moment niet mogelijk inzicht te geven in de financiële gevolgen van het actieplan aangezien nog niet gecommuniceerd is door de Europese Commissie hoe de precieze financiering van de acties in het actieplan eruit gaat zien. Zoals beschreven in de aan uw Kamer aangeboden Kabinetsreactie op het actieplan wordt aan de Commissie gevraagd om verheldering te geven over de financiële gevolgen voor de EU begroting en de lidstaten. Wanneer de commissie deze verduidelijking gegeven heeft, zal ik deze met u delen in een door mij toegezegde Kamerbrief over cybersecurity in het zorgveld in Q3 van 2025.

Tot slot lezen de leden van de VVD-fractie dat het kabinet inzet op bewustwording over informatieveiligheid onder zorgmedewerkers. Hier wordt verwezen naar een brief uit december 2022. Welke stappen zijn sindsdien gezet om bewustwording te vergroten en hebben deze stappen geleid tot daadwerkelijk resultaat?

[8] ZORRO-raamwerk Z-CERT

Ik heb ingezet op de verdere uitbreiding van het programma informatieveilig gedrag in de zorg. Zo zijn er naast de Wegwijzer, waarin de methode voor gedragsverandering op het gebied van informatieveilig gedrag in de zorg wordt toegelicht, diverse hulpmiddelen ontwikkeld. Ten eerste zijn *Toolkits* ontwikkeld met praktische tips over bijvoorbeeld veilig communiceren in de zorg, het melden van een datalek, veilig omgaan met patiëntgegevens en veilig gebruik van AI chatbots. Ten tweede worden trainingen en masterclasses georganiseerd over bijvoorbeeld het implementeren van de NEN7510 en veilig omgaan met AI in de zorg. In 2024 hebben er ruim 340 partijen deelgenomen aan de trainingsactiviteiten. Deelnemers komen uit de volgende subsectoren: gehandicaptenzorg, GGZ, Huisartsenzorg/eerstelijnszorg, Jeugdzorg, Verpleeghuizen & thuiszorg en ziekenhuizen. De website van het programma heeft gemiddeld enkele duizenden bezoekers per maand. De diverse praktische hulpmiddelen, zoals *infographics* en *toolkits*, zijn in totaal ruim duizend keer gedownload. De zorgorganisaties die aan de slag gaan binnen het programma Informatieveilig gedrag geven hiermee een concrete invulling aan verschillende paragrafen uit de NEN7510.

De leden van de Nieuw Sociaal Contract-fractie hebben met interesse het fiche gelezen over het Europees actieplan omtrent de cybersecurity van ziekenhuizen en zorgaanbieders. De leden zijn er positief over dat de EU zich ook gaat bezighouden met de cybersecurity van zorgaanbieders. Wel hebben wij daarover een aantal vragen.

De leden van de NSC-fractie willen graag van de Minister weten in hoeverre de Nederlandse zorgaanbieders reeds aansluiten bij de systemen die in de EU worden gebruikt voor de preventie, detectie en identificatie van cyberaanvallen.

Het is mij niet bekend in hoeverre zorgaanbieders in Nederland aansluiten op systemen aangeboden door de Europese Unie. Steeds meer zorgaanbieders hebben of maken gebruik van een uitbesteed Security Operations Center (SOC). Dit is een team dat digitale systemen monitort, controleert en eventueel bewaakt. Een SOC beschermt een zorginstelling tegen cyberaanvallen. Deze teams werken vrijwel allemaal internationaal samen en ontvangen signalen uit netwerken over landsgrenzen heen. Daarnaast kunnen zorginstellingen via Z-CERT aangesloten zijn op het Zorg Detectie Netwerk. In dit netwerk kunnen zorginstellingen informatie over incidenten met elkaar delen. Ook wordt informatie over aanvallen automatisch gedeeld, zodat aangesloten zorginstellingen zich daartegen kunnen beschermen. Het actieplan biedt een kans om dit netwerk Europees door te ontwikkelen.

De leden van de NSC-fractie maken zich zorgen over de huidige cyberveiligheid van zorginstellingen, aangezien een groot deel nog niet voldoet aan de Nen-normen. Wat gaat de Minister doen om ervoor te zorgen dat alle zorginstellingen binnen twee jaar aan deze normen voldoen en wat wordt de rol van Z-CERT hierin?

Zorgaanbieders zijn zelf verantwoordelijk voor het op orde hebben van de informatieveiligheid, onderdeel hiervan is voldoen aan de wettelijk verplicht gestelde normen voor informatiebeveiliging in de zorg NEN7510, 7512 en 7513. De IGJ houdt hier toezicht op de naleving van deze normen. Bij gebrekkige naleving worden eerst informele interventies ingezet. Denk hierbij aan het aanspreken van de raad van bestuur op tekortkomingen en het opvragen van verbeterplannen met termijnen. Door middel van informele interventies probeert de IGJ te bereiken dat zorgaanbieders zelf actie ondernemen. Bij het blijvend niet-naleven van (bijvoorbeeld) informatiebeveiligingsnormen, kan de IGJ grijpen naar formele instru-

menten zoals schriftelijke aanwijzing, schriftelijk bevel en last onder dwangsom.

Het is zorgelijk dat nog niet alle zorginstellingen aan de NEN7510 voldoen. Om die reden heb ik verschillende initiatieven genomen. Ik heb middelen verstrekt aan het programma informatieveilig gedrag in de zorg, uitgevoerd door ECP, Platform voor de InformatieSamenleving. Het programma realiseert toolkits, podcasts, webinars en masterclasses ter bevordering van bewustzijn over informatieveilig gedrag binnen zorginstellingen. Met een stevige communicatiestrategie heeft het programma de afgelopen jaren een groeiende doelgroep weten te bereiken. Daarnaast heb ik voor kleinere zorginstellingen, voor wie naleving van de NEN7510 een uitdaging kan zijn, een quick scan beschikbaar gesteld. Dit is een eenvoudig instrument om te bepalen welke maatregelen voor informatieveiligheid (nog) genomen dienen te worden. Tot slot heb ik aan het Nederlands Normalisatie Instituut (NEN) middelen verstrekt om opleidingen te verzorgen, implementatiehandvatten te ontwikkelen en een community te faciliteren waarin zorgmedewerkers van elkaar kunnen leren. NEN kijkt hierbij in het bijzonder naar tools die de kleinere zorgaanbieders ondersteunen.

Nederland kent zowel kleine als grote zorgaanbieders. De leden van de NSC-fractie willen graag weten hoe de implementatie en de eventuele prioritering van de cyberveiligheidsmaatregelen voor zorgaanbieders verloopt, en hoe de NIS2-richtlijn hierin wordt meegenomen.

De NIS2-richtlijn wordt nationaal omgezet in de Cyberbeveiligingswet, dit doe ik samen met mijn collega van Justitie en Veiligheid die dit coördineert. Deze wet schrijft voor dat onder andere de sector zorg en de subsectoren die eronder vallen (zorgaanbieders, EUREF laboratoria, entiteiten die onderzoek doen naar geneesmiddelen, entiteiten die farmaceutische basisproducten bereiden en vervaardigen, en entiteiten die medische hulpmiddelen vervaardigen in noodsituaties) gehouden zullen worden aan cyberbeveiligingsnormen zoals de NEN7510 en de mondiale erkende norm voor informatiebeveiliging ISO270001. De organisaties die vallen onder de Cyberbeveiligingswet worden bepaald op basis van bepaalde grootte en omvang.
Het actieplan is een communicatie van de Europese Commissie dat als specifieke aanvulling dient op het horizontale karakter van de NIS2-richtlijn. De Europese Commissie erkent dat de zorg een kwetsbare schakel is in het cyberlandschap. Om ervoor te zorgen dat organisaties binnen de zorg bewuster worden van de gevaren van cyberdreigingen en hier weerstand tegen kunnen bieden, is het actieplan opgesteld. Een deel van de organisaties binnen de zorg vallen met hun grootte en omvang al onder de Cyberbeveiligingswet (aldus NIS2), maar de kleinere organisaties die hierbuiten vallen kunnen aanvullende kennis en expertise halen uit het actieplan om alsnog hun cyberveiligheidsmaatregelen goed op orde te hebben.
De leden van de NSC-fractie lezen dat Z-CERT een belangrijke rol zal spelen bij de implementatie van de cybersecuritymaatregelen. Hoe wordt gegarandeerd dat Z-CERT medewerkers screent op betrouwbaarheid?

Voordat nieuwe medewerkers bij Z-CERT in dienst komen worden zij gescreend door een externe partij. Onderdeel hiervan is een referentiecheck, een vragenlijst en gesprek over integriteit en een Verklaring Omtrent Gedrag (VOG). Daarnaast wordt momenteel verkend of voor vertrouwensfuncties een Veiligheidsonderzoek nodig is.

De leden van de NSC-fractie vragen de Minister op welke manier aanbieders van digitale systemen betrokken worden door Z-CERT en ENISA bij de implementatie van de cybersecuritymaatregelen. Welke eisen worden aan aanbieders van digitale systemen gesteld om ervoor te zorgen dat zij voldoen aan de EU-normen?

Z-CERT geeft beveiligingsadviezen en organiseert kennissessies om zorgaanbieders handvatten te geven om hun informatiebeveiliging beter op orde te krijgen. Het daadwerkelijk implementeren van cybersecurity-maatregelen is aan de zorginstelling zelf. Zij bepalen zelf de eisen die zij aan hun leveranciers stellen. Een beperkt aantal leveranciers uit de eerstelijnszorg is als deelnemer aangesloten bij Z-CERT, net als bijvoorbeeld een partij die zorgt voor uitwisseling van administratieve gegevens in de zorg. Met de komst van de Cyberbeveiligingswet (Cbw) zal dit mogelijk veranderen omdat ICT leveranciers niet onder de sector gezondheidszorg vallen. De samenwerking met Z-CERT met de leveranciers blijft van groot belang gezien ook de meldingen over kwetsbaarheden in hun systemen relevant zijn voor de gehele keten in de zorg.

Het *European Agency for Network and Information Security* (ENISA) ondersteunt de Europese lidstaten bij het versterken van hun digitale weerbaarheid. ENISA doet dit onder andere door het bieden van ondersteuning bij beleidsontwikkeling en de implementatie van de NIS2, het organiseren van cybercrisisoefeningen, en het publiceren van dreigingsinformatie, *best practices* en technische richtlijnen. Nederland is actief lid van de Management Board van ENISA, waarin de prioriteiten voor het agentschap worden bepaald. Daarnaast geeft het Nationaal Cybersecurity Center (NCSC) invulling aan de functie National Liaison Officer, het eerste contactpunt voor ENISA in Nederland.

Aanbieders van digitale systemen vallen (als zij aan bepaalde voorwaarden voldoen) onder de Cyberbeveiligingswet (NIS2-richtlijn). Het Ministerie van Justitie en Veiligheid (JenV) coördineert de omzetting van NIS2 in de Cyberbeveiligingswet (Cbw). JenV werkt daarbij nauw samen met de betrokken vakdepartementen die verantwoordelijk zijn voor de sectoren waarop de Cbw van toepassing zal zijn. De richtlijn draagt bij aan een hoger niveau van informatiebeveiliging bij bedrijven en organisaties in diverse sectoren in de gehele EU. De komst van de Cbw is bedoeld om de kans op een cyberincident, en de gevolgen hiervan, te beperken of te voorkomen. Zo bevat de wet een zorgplicht waarbij organisaties weerbaarheidsverhogende maatregelen dienen te treffen en vindt hier toezicht op plaats. Bij het nemen van deze maatregelen dienen organisaties rekening te houden met Europese en internationale normen.[9] Daarnaast moeten significante cyberincidenten binnen 24 uur worden gemeld zodat cyberaanvallen e.a. beter kunnen worden gemonitord door de NCSC en in de EU door ENISA.

Daarnaast worden in de verordening cyberweerbaarheid ofwel de Cyber Resilience Act (CRA) essentiële eisen gesteld aan de cybersecurity van producten met digitale elementen die op de EU-markt worden aangeboden. Verplichtingen in de CRA worden gesteld aan marktdeelnemers zoals fabrikanten, importeurs en distributeurs. De Rijksinspectie Digitale Infrastructuur (RDI) houdt toezicht op de NIS2 voor digitale aanbieders en de CRA. Aangezien voor medische apparatuur sectorspecifieke cybersecurity eisen worden gesteld in de Europese verordeningen voor medische hulpmiddelen en in-vitro diagnostica (MDR en IVDR), zijn deze producten uitgezonderd van de CRA. De Inspectie, Gezondheid en Jeugd (IGJ) houdt toezicht op deze sectorspecifieke richtlijn.

[9] Zie artikel 21, tweede lid, van de Cbw.

De leden van de NSC-fractie willen graag weten op welke manier het actieplan zich richt op het secundaire gebruik van zorgdata (door onderzoekers).

Wat betreft het primaire en secundaire gebruik van zorgdata gebruik ik een integrale benadering waarbij veiligheid centraal staat. Dit actieplan richt zich op het verbeteren van de cybersecurity van zorginstellingen en ziekenhuizen, waarmee onder andere geborgd wordt dat zorgvuldig wordt omgegaan met zorgdata door zorgprofessionals door bijvoorbeeld het inrichten van online cursussen ter bevordering van bewustzijn over cyberveiligheid. Het plan richt zich niet specifiek op het secundaire gebruik van zorgdata door bijvoorbeeld onderzoekers.

De leden van de NSC-fractie willen graag weten op welke wijze cyberincidentnotificaties van ziekenhuizen en zorgaanbieders momenteel worden verzameld en verwerkt.

Ziekenhuizen en zorginstellingen hebben op dit moment geen verplichting om cyberincidenten bij Z-CERT te melden. Z-CERT kan 24 uur per dag digitaal en telefonisch reageren op incidentmeldingen en adviseert getroffen organisaties over het oplossen van een incident. Daarnaast probeert Z-CERT technische informatie over het incident te verzamelen waarmee de rest van de zorgsector (anoniem) gewaarschuwd kan worden. Dit waarschuwen gebeurt via het Zorg Detectie Netwerk en via een berichtensysteem en gebeurt zowel binnen als buiten kantooruren. Incidentnotificaties vanuit andere bronnen worden op dezelfde wijze verwerkt.
De deelnemende organisaties aan Z-CERT vormen een netwerk om gezamenlijk uitdagingen als ransomware, phishing, datalekken of hacken aan te pakken. Het netwerk bestaat behalve de deelnemers uit brancheorganisaties, leveranciers, andere CERT's, internationale contacten en (hackers)communities. Zo verzamelt Z-CERT de informatie die nodig is om risico's of dreigingen snel te signaleren en de deelnemers te adviseren hoe ze daarmee om kunnen gaan.
De leden van de NSC-fractie vragen hoe het kabinet zich zal inzetten om ervoor te zorgen dat online trainingen en cursussen voor bewustwording van cybersecurity toegankelijk zijn voor verschillende soorten zorgprofessionals.

Bewustwording van risico's is essentieel voor goede informatieveiligheid. Daarom zet ik in op het stimuleren van informatieveilig gedrag bij zorgprofessionals. Via dit project worden cursussen, masterclasses en webinars aangeboden gericht op het verhogen van bewustzijn over informatieveiligheid. Tijdens deze trainingen wordt bijvoorbeeld ingegaan op het veilig omgaan met AI in de zorg en het implementeren van de NEN7510. Daarnaast zijn hulpmiddelen ontwikkeld met praktische tips over bijvoorbeeld veilig communiceren in de zorg, het melden van een datalek, veilig omgaan met patiëntgegevens en veilig gebruik van AI chatbots. Op dit moment is nog niet uitgewerkt hoe de online trainingen en cursussen van het actieplan eruit gaan zien en wanneer deze beschikbaar zullen worden gesteld door de Europese Commissie. De voorgestelde actie in het actieplan stelt dat deze begin 2026 zullen worden ontworpen en vervolgens verspreid. Wanneer de trainingen en cursussen beschikbaar worden gesteld door
de Europese Commissie zal ik deze verspreiden onder de koepels en branche organisaties van de subsectoren binnen de zorg zodat deze voor zowel kleine als grote zorgaanbieders beschikbaar zijn.

De leden van de NSC-fractie willen graag weten op welke wijze het kabinet zich inzet om te onderzoeken of er sprake is van duplicatie van initiatieven en hoe de complementariteit van bestaande initiatieven op nationaal en EU-niveau wordt gewaarborgd.

Het actieplan wordt behandeld in de Horizontale Groep cybervraagstukken. Lidstaten komen in deze werkgroep bijeen om de werkzaamheden van de Raad op het gebied van cybervraagstukken te coördineren. Op basis van het BNC-fiche zal in dit gremium worden toegezien op de besluitvorming rondom de voorgestelde acties en zal worden ingezet op het voorkomen van duplicatie. Daarnaast worden in de werkgroep *best practices* uit Nederland gedeeld, zoals het programma Informatieveilig gedrag in de zorg en de volwassenheidstest van Z-CERT. Hiermee wordt de specifieke context van de Nederlandse cybersecurity geschetst aangezien deze per lidstaat verschillend is.

De leden van de NSC-fractie vragen hoe het kabinet ervoor zorgt dat er geen overlap van taken ontstaat tussen ENISA en Nederlandse instanties.

Het actieplan wordt behandeld in de Horizontale Werkgroep cybervraagstukken. Lidstaten komen in deze werkgroep bijeen om de werkzaamheden van de Raad op het gebied van cybervraagstukken te coördineren. Daarnaast is Nederland actief lid van de Management Board van ENISA, waarin de prioriteiten voor het agentschap worden bepaald. In zowel de Horizontale Werkgroep als de Management Board wordt, zoals beschreven in het BNC-fiche, benadrukt dat overlap tussen Europese en nationale acties niet wenselijk is. Een voorbeeld hiervan is dat enkele voorgestelde acties overlap lijken te hebben met taken die krachtens de NIS-2 richtlijn (en in lijn daarmee de nationale wetgeving ter implementatie daarvan) aan lidstatelijke CSIRTS zijn toegekend. In Nederland is dit naar verwachting Z-CERT. Het is belangrijk om dergelijke overlap in de daarvoor bestemde gremia te voorkomen.

De leden van de NSC-fractie willen graag weten wat de financiële consequenties voor Nederland zijn om deze plannen uit te voeren, en of deze al zijn opgenomen in de huidige begroting.

Het is op dit moment niet mogelijk inzicht te geven in de financiële gevolgen van het actieplan voor Nederland aangezien de Europese Commissie nog niet gecommuniceerd heeft over hoe de acties in het actieplan gefinancierd gaan worden. Zoals beschreven in de aan uw Kamer aangeboden Kabinetsreactie op het actieplan wordt aan de Commissie gevraagd om specificering van de verdere financiële gevolgen. Wanneer de commissie deze verduidelijking gegeven heeft, zal ik deze met u delen in een door mij toegezegde Kamerbrief over cybersecurity in het zorgveld in Q3 van 2025.