2025D14571

00 000 Dossiertitel

INBRENG VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

In de vaste commissie voor Volksgezondheid, Welzijn en Sport bestond bij enkele fracties behoefte een aantal vragen en opmerkingen voor te leggen aan het kabinet over de brief van de Minister van Buitenlandse Zaken betreffende het BNC-fiche: Europees actieplan omtrent de cybersecurity van ziekenhuizen en zorgaanbieders d.d. 21 februari 2025 (Kamerstuk 22 112 nr. 4000).

De voorzitter van de commissie,
Mohandis

Adjunct-griffier van de commissie,
Meijerink

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 in welke mate deze ook voor zorginstellingen kan worden ingesteld. Kan

[1] Kamerstukken 2022D08707, 2023D10550 en 2023D15533.

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.