Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

27 529 Informatie- en Communicatietechnologie (ICT) in de Zorg

Nr. 353 **BRIEF VAN DE MINISTER VAN VOLKSGEZONDHEID, WELZIJN EN SPORT**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 4 december 2025

In deze brief leest u over de ontwikkelingen op het gebied van informatieveiligheid van de zorgsector. Ik duid het dreigingsbeeld, recente incidenten en de voortgang van de implementatie van de Cyberbeveiligingswet (NIS2-richtlijn) in het zorgveld[1]. Ook ga ik in op de maatregelen die ik neem om het zorgveld te ondersteunen. Het is van groot belang het niveau van informatieveiligheid in het zorgveld te verhogen en hiermee ga ik samen met de zorgsector aan de slag

Ik doe drie toezeggingen af en reageer op drie moties:
- De toezegging dat ik uw Kamer zou informeren over mijn visie op quantumveiligheid voor de zorg[2].
- De toezegging over verduidelijking van de financiële gevolgen van het EU-actieplan cybersecurity voor ziekenhuizen en zorgaanbieders[3].
- De toezegging om een vervolg te geven aan het toepassen van *end-to-end-beveiliging* bij de geprioriteerde gegevensuitwisselingen onder de Wet elektronische gegevensuitwisseling in de zorg (Wegiz)[4].
- De motie van Kamerlid Hertzberger over het steviger inzetten op de naleving van de NEN7510 en de stappen die hiervoor gezet worden[5].
- De motie van Kamerlid De Korte over de inzet van ethische hackers[6].

[1] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIB-richtlijn).
[2] Toezegging TZ202504-086
[3] Toegezegd in Kamerstukken II 2024/25, 22 112, nr. 4056
[4] Toegezegd in Kamerstukken II 2023/24, 36 410 XVI, nr. 160 en Handelingen II 2023/24, nr. 95, item 8.
[5] Kamerstuk 32 793, nr. 863
[6] Kamerstuk 27 529, nr. 341

kst-27529-353
ISSN 0921 - 7371
's-Gravenhage 2025

- De motie van Kamerlid De Korte over de opslag en benadering van BSN-gegevens en gevoelige informatie[7]

Zonder veiligheid geen vertrouwen, zonder vertrouwen geen databeschikbaarheid

Om de zorg voor iedereen goed, toegankelijk en betaalbaar te houden, is de beweging ingezet naar passende (hybride) zorg, gezondheid en preventie. Cruciaal voor die beweging is digitalisering, gegevensuitwisseling en databeschikbaarheid: de juiste gegevens, op het juiste moment, op de juiste plek. Met de Nationale visie en strategie voor het gezondheidsinformatiestelsel (NVS) werkt het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) daarom aan databeschikbaarheid voor burgers, zorgverleners en de wetenschap.[8]

Om databeschikbaarheid te bereiken, is onder andere vertrouwen nodig van burgers, patiënten en zorgverleners in de veiligheid van gezondheidsgegevens. Voor dit vertrouwen moet de infrastructuur en techniek voor het uitwisselen en beschikbaar maken van gezondheidsgegevens betrouwbaar worden ingericht en veilig worden gebruikt.

1. Dreigingen voor de zorgsector

De dreiging van cyberaanvallen in de zorg neemt al jaren toe. Volgens de Europese Commissie is de zorgsector een van de meest aangevallen sectoren.[9] Ook Z-CERT, expertisecentrum op het gebied van cyberbeveiliging in de zorg, ziet een toename van digitale aanvallen gericht op zorgaanbieders in Nederland in 2024. Steeds vaker zijn hierbij niet alleen zorgaanbieders zelf het doelwit, maar ook andere actoren in de zorgketen, zoals ICT-leveranciers. De bedreigingen in de zorgsector zijn divers. Ze variëren van dreigingen met *malware*, schadelijke software die systemen kan platleggen, tot *social engineering*, waarbij mensen gemanipuleerd worden tot het vrijgeven van gevoelige gegevens. Het dreigingslandschap is ook in ontwikkeling. De technologie waarmee aanvallen worden uitgevoerd, is steeds geavanceerder. En er zijn verschillende kwaadwillende groepen die de aanvallen uitvoeren.

Tot nu toe zijn kwaadwillenden vooral uit op geld. De Autoriteit Persoonsgegevens (AP) meldt in haar jaarlijkse datalekkenreportage een verdubbeling aan datadiefstallen door cybercriminelen.[10] De buitgemaakte data worden vaak verkocht aan derden. Daarnaast blijft het gebruik van *ransomware* een van de grootste dreigingen in de zorgsector.[11] Hierbij worden systemen of gegevens versleuteld tot er wordt betaald.

Door geopolitieke ontwikkelingen zijn aanvallen door statelijke actoren niet uit te sluiten. In het «Cybersecuritybeeld Nederland» staat dat deze actoren hun activiteiten intensiveren en hun capaciteiten verbreden.[12] Ook

---

[7] Kamerstuk 24 170, nr. 374

[8] *Kamerstukken II* 2022/23, 27 529, nr. 292 en Nationale strategie voor het gezondheidsinformatiestelsel, oktober 2024.

[9] «European Action Plan on the Cybersecurity of Hospitals and Healthcare Providers», Europese Commissie, https://ec.europa.eu/newsroom/dae/redirection/document/111664 (15 januari 2025)

[10] Rapportage datalekken 2024, Autoriteit Persoonsgegevens, https://www.autoriteitpersoonsgegevens.nl/documenten/rapportage-datalekken-2024 (3 juli 2025)

[11] Cybersecurity Dreigingsbeeld voor de zorg 2024, Z-CERT, https://z-cert.nl/assets/uploads/Actueel/DEF_Z-CERT_CyberDreigingsbeeldvoordezorg-LR.pdf. (12 februari 2025)

[12] Cybersecuritybeeld Nederland 2024, Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), https://www.nctv.nl/documenten/2024/10/28/cybersecuritybeeld-nederland-2024, (28 oktober 2024) https://www.nctv.nl/documenten/2025/07/23/dreigingslandschap-vitale-infrastructuur

de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) stelt dat statelijke actoren en hacktivisten met cyberaanvallen een dreiging vormen voor de vitale infrastructuur van Nederland.[13] Digitalisering van de zorgsector biedt veel kansen, maar vergroot ook het risico op cyberincidenten – dat benadrukt onder andere de Europese Commissie.

Twee ontwikkelingen: kansen én risico's

Het gebruik van de *cloud* - het opslaan en gebruiken van data en toepassingen via externe servers – kan zorgen voor betere toegankelijkheid, schaalbaarheid en kostenefficiëntie. Steeds vaker worden bijvoorbeeld zorgaanbieder-informatiesystemen (XIS'en) of elektronische patiëntendossiers (EPD's) in de cloud ondergebracht. Tegelijkertijd neemt de afhankelijkheid van de aanbieders van clouddiensten toe. Bovendien is de cloud steeds vaker het doelwit van cyberaanvallen.

Ook kunstmatige intelligentie (AI) kan – als het juist wordt ingezet – bijdragen aan maatschappelijke vraagstukken die spelen in zorg en welzijn. Maar kwaadwillenden kunnen het ook gebruiken om bijvoorbeeld gerichte en moeilijk te filteren phishingmails te maken – waarbij oplichters zich voordoen als betrouwbare organisaties of personen om gegevens los te krijgen. Daarnaast maakt AI het mogelijk om snel nieuwe en geavanceerde *malware* te ontwikkelen, waar criminele organisaties en vijandige staten dankbaar gebruik van maken.

De dreiging is reëel

Cyberaanvallen hebben gevolgen voor de vertrouwelijkheid, beschikbaarheid en juistheid van gezondheidsgegevens. Daardoor kan een cyberaanval de continuïteit van zorgverlening in gevaar brengen. Dit heeft direct impact op de burger. Een recent voorbeeld is de hack bij het lab Clinical Diagnostics in juli dit jaar. Dat hierbij gezondheidsgegevens bemachtigd zijn van deelnemers aan het bevolkingsonderzoek het bevolkingsonderzoek baarmoederhalskanker betreur ik ten zeerste. In deze brief wil ik nogmaals benadrukken dat er nog verschillende onderzoeken lopen naar de hack en het datalek dat daarop volgde en dat ik daarom nog geen nadere uitspraken kan doen over de oorzaak en omvang. Uw Kamer wordt wel doorlopend op de hoogte gehouden over deze situatie en de maatregelen die zijn, en mogelijk nog, worden getroffen.

Dit voorbeeld, boven op de benoemde technologieën en dreigingen uit voorgaande alinea's, laat zien dat de vraag niet is óf er weer een incident komt, maar wanneer. Een continue en vooral geïntensiveerde inspanning vanuit de zorgsector om de informatiebeveiliging op orde te hebben, is nodig om op deze dreigingen in te spelen.

2. Huidig beleid

2.1 Stelselverantwoordelijkheid

Zorgaanbieders zijn in de eerste plaats zelf verantwoordelijk voor hun informatiebeveiliging. Dit is onderdeel van de bedrijfsvoering, en zou net zo vanzelfsprekend moeten zijn als andere onderdelen, zoals veiligheid van het gebouw en personeel. ICT-uitgaven of investeringen zouden dit belang moeten reflecteren. Zorgaanbieders bepalen welke maatregelen genomen moeten worden om de risico's op het gebied van informatiebe-

[13] Dreigingslandschap Vitale Infrastructuur (2025), Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), https://www.nctv.nl/documenten/2025/07/23/dreigingslandschap-vitale-infrastructuur, (24 juli 2025)

veiliging te beheersen – al dan niet met hulp van hun koepel of brancheorganisatie. De van toepassing zijnde NEN-normen verplichten zorginstellingen om deze risico's in kaart te brengen en om passende maatregelen te nemen[14]. Een belangrijke factor zijn hierbij de IT-leveranciers, die de naleving van de verplichtingen grotendeels moeten faciliteren. Zorgaanbieders en samenwerkingsverbanden moeten zorgen dat ze de juiste eisen stellen aan hun leveranciers. Ik vraag hier in een brief aan koepels en zorgbestuurders die in november gestuurd zal worden aandacht voor.

Verplichte NEN normen voor de zorgsector:
- NEN 7510 – De Nederlandse norm voor informatiebeveiliging in de zorg.
- NEN 7512 – Beschrijft hoe zorgverleners veilig gegevens uitwisselen.
- NEN 7513 – Beschrijft hoe acties in elektronische zorginformatievoorzieningen vastgelegd moeten worden (logging)

De Inspectie Gezondheidszorg en Jeugd (IGJ) constateert dat de naleving van de verplichte NEN-normen te wensen overlaat. In reactie op de motie van Kamerlid Hertzberger[15] over het steviger inzetten op de naleving van de NEN7510 norm benadruk ik dat ik als stelselverantwoordelijke regie neem om het zorgveld te ondersteunen. Dit doe ik door me in het huidige beleid te richten op het stimuleren van bewustwording, passende hulp te bieden, toezicht te versterken en te ondersteunen bij incidenten. In onderdeel 3 van deze brief zet ik uiteen hoe ik deze ondersteuning wil intensiveren.

2.2 Normeren

2.2.1 Cyberbeveiligingswet (Cbw)

Vanwege de eerder beschreven geopolitieke ontwikkelingen en de toenemende afhankelijkheden binnen Europa, werkt Europa gezamenlijk aan het versterken van de digitale weerbaarheid in vitale sectoren, zoals de gezondheidszorg.

Om organisaties te helpen hun digitale weerbaarheid planmatig op orde te krijgen en te houden is er de Europese *Network and Information Security directive* (NIS2-richtlijn). Die richtlijn wordt nu in Nederland omgezet in de Cyberbeveiligingswet (Cbw).[16] De coördinatie hiervan ligt bij het Ministerie van Justitie en Veiligheid (JenV). De vakdepartementen (zoals VWS) zorgen voor de sectorafhankelijke inhoudelijke invulling.

Terzijde: er is ook wetgeving in de maak voor *fysieke* weerbaarheid. Om de lidstaten ook weerbaar te maken tegen fysieke dreigingen – zoals terrorisme en natuurrampen – is er de *Critical Entities Resilience* directive (CER). Deze Europese richtlijn wordt, tegelijk met de NIS2-richtlijn, omgezet in de nationale Wet weerbaarheid kritieke entiteiten (Wwke).[17]

---

[14] De NEN 7510 geldt voor elke zorgaanbieder die gegevens van personen verwerkt in een zorginformatiesysteem en een elektronisch uitwisselingssysteem. Dit is bepaald in het Besluit elektronische gegevensverwerking door zorgaanbieders (Begz). Er dient aangetoond te kunnen worden dat gewerkt wordt volgens de NEN 7510.

[15] Motienummer 32 793, nr. 863

[16] Regels ter implementatie van Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (PbEU 2022, L 333) (Wet weerbaarheid kritieke entiteiten) | Tweede Kamer der Staten-Generaal

[17] Regels ter implementatie van Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (PbEU 2022, L 333) (Wet weerbaarheid kritieke entiteiten) | Tweede Kamer der Staten-Generaal

Ook bij deze wetgeving zorgt VWS – in samenwerking met JenV – voor de inhoudelijke invulling voor de zorg.

Plichten

De Cbw gaat gelden voor een breed segment aan organisaties binnen de zorg – van zorgaanbieders tot geneesmiddelenfabrikanten en vervaardigers van medische hulpmiddelen. De wet gaat organisaties verplichten om risico's op cyberincidenten in kaart te brengen en passende en evenredige maatregelen hiertegen te treffen.

Rechten

De hierboven beschreven verplichtingen gaan pas gelden na implementatie van de NIS2-richtlijn in de Cbw. Maar de rechten uit de NIS2-richtlijn hebben directe werking en gelden daarom al sinds 17 oktober 2024. Dit betekent dat organisaties die onder de Cbw gaan vallen vanaf die datum al recht hebben op ondersteuning door het sectorale Computer Security Incident Response Team (CSIRT). Voor de zorg gaat Z-CERT die rol op zich nemen.

Toezicht

Het toezicht op de naleving van de Cbw komt te liggen bij de Inspectie Gezondheidszorg en Jeugd (IGJ). Nu al voldoen aan NEN 7510 en ISO 27001 is een stap in de goede richting om straks aan de Cbw te voldoen.

Bestuurlijke aansprakelijkheid

Onder de Cbw worden bestuurders van de raden van bestuur van organisaties die onder de wet vallen verplicht om training in cyberbeveiliging te volgen. Ook kunnen zij persoonlijk aansprakelijk worden gesteld indien zij niet aan deze trainingseisen voldoen.

Lagere regelgeving

Eerder dit jaar stuurde ik uw Kamer de concepttekst van de Cbw.[18] Met die conceptwet stuurde ik ook het concept-Cyberbeveiligingsbesluit (Cbb) mee. Dat is de algemene maatregel van bestuur (AMvB) waarin onderdelen van de wet nader worden uitgewerkt. Op dit moment werk ik verder aan een ministeriële regeling voor de zorg, momenteel in internetconsulatie, waarin onder andere de zorgplicht en de meldplicht voor significante incidenten uit de Cbw verder worden uitgewerkt.

Inwerkingtreding Cbw naar verwachting Q2 2026

Zoals eerder aan uw Kamer medegedeeld door de Minister van JenV kost de implementatie van de NIS2-richtlijn in de Cbw meer tijd dan oorspronkelijk gepland. Dat komt doordat de complexiteit en de omvang van het traject om een zorgvuldige aanpak vragen. Naar verwachting treden de wet en de lagere regelgeving voor onder meer de zorg in het tweede kwartaal van 2026 in werking. Uiterlijk in het tweede kwartaal van 2026 ontvangt uw Kamer een uitgebreidere brief, met een toelichting over de concrete inzet op en vervolgstappen richting de implementatie van de Cbw.

[18] Wetsvoorstel nr. 36 764, Cyberbeveiligingswet, ingediend 2 juni 2025, Tweede Kamer

2.2.2 NEN-normen

Ik zet in op de doorontwikkeling van de verplichte NEN-normen voor informatiebeveiliging in de zorg: NEN 7510, 7512 en 7513. Daarnaast werk ik aan een geactualiseerde NEN 7616-norm, om wanneer dat nodig is zo veilig mogelijk gezondheidsgegevens te mailen of via een chatdienst te delen.

Achterblijvende naleving NEN-normen zorgelijk

De constatering van de IGJ dat de naleving van de NEN-normen voor informatieveiligheid achter blijft, vind ik zeer zorgelijk.[19] Daarom onderneem ik verschillende activiteiten om zorgaanbieders te ondersteunen:

- Ik verstrek middelen aan het programma Informatieveilig gedrag in de zorg. In alinea 2.5 over het stimuleren van bewustwording ga ik verder in op de doelen, de resultaten en het belang van dit programma.
- Voor kleinere zorginstellingen, voor wie naleving van NEN 7510 een uitdaging kan zijn, heb ik een quickscan beschikbaar gesteld: een eenvoudig instrument om te bepalen welke maatregelen (nog) genomen moeten worden voor informatieveiligheid.
- Tot slot heb ik aan het Nederlands Normalisatie Instituut (NEN) middelen verstrekt voor het verzorgen van opleidingen, het ontwikkelen van implementatiehandvatten en het oprichten van een community waarin zorgmedewerkers van elkaar kunnen leren. De hulpmiddelen zijn kosteloos ter beschikking gesteld en ontwikkeld voor zowel organisaties die voor het eerst NEN 7510 implementeren als voor organisaties die NEN 7510 al geïmplementeerd hebben en moeten overstappen op de nieuwe versie van de norm.

2.3 Ondersteuning bij incidenten

Z-CERT

Ik zet ook in op het breder beschikbaar stellen van de diensten van Z-CERT, het expertisecentrum voor cybersecurity in de zorg. Z-CERT helpt zorginstellingen onder andere bij preventie, detectie, respons en herstel van cyberincidenten. Z-CERT voorziet deelnemers van advies en dreigingsinformatie. En bij een cyberaanval kan het een zorginstelling ondersteunen bij het beperken van de gevolgen. Verder heeft Z-CERT een kennisbank waarop kennisproducten gepubliceerd worden over bijvoorbeeld NEN 7510 en het voorkomen en herkennen van malware.

Voorbereiding is cruciaal

Uit de dreigingsbeelden blijkt dat er altijd incidenten zullen zijn, ondanks preventieve maatregelen. Het is daarom belangrijk om daarop voorbereid te zijn. De praktijk heeft laten zien dat het cruciaal is om te oefenen met

---

[19] Professionele digitale zorg vraagt van ziekenhuizen steeds opnieuw evalueren en verbeteren, Inspectie Gezondheidszorg en Jeugd (IGJ), https://www.igj.nl/site/binaries/site-content/collections/documents/2021/12/21/professionele-digitale-zorg-vraagt-van-ziekenhuizen-steeds-opnieuw-evalueren-en-verbeteren/73298_IGJ_Factsheet_TG.pdf (21 december 2021)
Gehandicaptenzorg worstelt met digitale vormen van zorg, Inspectie Gezondheidszorg en Jeugd (IGJ), https://www.igj.nl/site/binaries/site-content/collections/documents/2023/06/16/publicatie-gehandicaptenzorg-worstelt-met-digitale-vormen-van-zorg/Gehandicaptenzorg+worstelt+met+digitale+vormen+van+zorg.pdf (16 juni 2023)
Zeer grote zorgaanbieders ouderenzorg hebben digitale zorg op orde, informatiebeveiliging moet beter (IGJ), Zeer grote zorgaanbieders ouderenzorg hebben digitale zorg op orde, informatiebeveiliging moet beter | Inspectie Gezondheidszorg en J https://www.igj.nl/documenten/2025/06/05/digitale-zorg-bij-zeer-grote-zorgaanbieders (5 juni 2025)

cyberincidenten. En om continuïteitsplannen te testen met simulaties en instrumenten als *red-teaming* – een gesimuleerde aanvalstest door ethische hackers. In reactie op de motie van Kamerlid De Korte over de inzet van ethische hackers[20] wordt u geïnformeerd dat ik er bij zorginstellingen op aandring om voldoende aandacht te besteden aan crisisvoorbereiding. Z-CERT biedt op dit moment aanvullend optionele cybersecuritydiensten aan, zoals geavanceerde ethische hacktesten onder de naam ZORRO[21].

Wettelijke taken Z-CERT

Z-CERT krijgt onder de Cbw wettelijke taken. Z-CERT wordt het CSIRT van de zorgsector en krijgt als zodanig een aantal wettelijke taken, zoals het monitoren op en analyseren van kwetsbaarheden en dreigingen, het leveren van ondersteuning bij incidenten en het uitgeven van vroegtijdige waarschuwingen. Organisaties die onder de Cbw gaan vallen hebben zowel rechten als plichten, waarbij zij een beroep kunnen doen op de ondersteuning door Z-CERT.

2.4 Toezicht

IGJ houdt risico gebaseerd, steekproefsgewijs en op basis van NEN 7510 toezicht op informatiebeveiliging in de zorg. Uit inspectiebezoeken in voorgaande jaren blijkt dat de naleving van deze norm in diverse zorgsectoren ondermaats is.[22] Recent constateerde de IGJ dat naleving bijvoorbeeld niet op orde is in de huisartsenspoedzorg.[23] In 2022 constateerde de IGJ dat bij het merendeel van de ziekenhuizen de naleving niet op niveau was, ondanks aandacht voor dit thema en wettelijke verplichting. De IGJ heeft daarom verbeteracties gevraagd en na meerdere rondes waren de meeste ziekenhuizen in het najaar van 2023 op niveau. Na de ziekenhuizen worden ook andere zorgsectoren op deze manier opgevolgd, zoals de gehandicaptenzorg en de ouderenzorg. Het doel hiervan is een cyclische verbetering van de naleving van de NEN 7510-norm. We zien dat deze op leren gerichte kritische benadering enerzijds tijd vraagt, maar anderzijds wel resultaten oplevert. De bezochte sectoren laten substantiële verbeteringen zien.

Extra aandacht IGJ door Incident bij Clinical Diagnostics

De hack en het datalek bij Clinical Diagnostics zijn voor de IGJ een extra aanleiding om laboratoria in het vizier te krijgen en op te nemen in haar werkplan. Als uit de lopende onderzoeken naar het incident blijkt dat er specifieke risico's waren bij Clinical Diagnostics worden deze ook als aandachtspunt meegenomen in het toezicht bij andere zorgaanbieders en andere zorgsectoren.

Meer financiële middelen naar IGJ

Omdat ik het zorgelijk vind dat naleving van de verplichte norm achterblijft, zet ik naast de aanvullende middelen voor het toezicht op de Cbw, vanaf 2024 voor de komende jaren gericht en structureel middelen in om het toezicht op informatiebeveiliging te intensiveren. Deze middelen gebruikt de IGJ onder andere voor het versterken van kennis van

---

[20] Kamerstuk 27 529, nr. 341
[21] ZORRO – Z-CERT
[22] Zie voetnoot 13.
[23] Huisartsenspoedzorg moet zo snel mogelijk voldoen aan de norm voor informatiebeveiliging (IGJ), https://www.igj.nl/documenten/2025/10/13/huisartsenspoedzorg-moet-zo-snel-mogelijk-voldoen-aan-de-norm-voor-informatiebeveiliging (13 oktober 2025)

inspecteurs, samenwerken met verwante toezichthouders zoals de Rijksinspectie Digitale Infrastructuur (RDI) en onderzoek in het veld naar de stand van zaken op het gebied van informatiebeveiliging, gericht op een beter inzicht in de risico's die de IGJ in haar toezicht moet betrekken. Tevens zal de IGJ zich met deze middelen richten op het ontwikkelen van een effectieve toezichtstrategie op de kleinere zorgaanbieders. Het doel hiervan is de naleving van de NEN7510 en de informatieveiligheid bij kleine zorgaanbieders te verhogen. Ik ga hier in deze brief verder op in bij onderdeel 3.1.

2.5 Bewustwording stimuleren

Programma Informatieveilig gedrag in de zorg

Ik zet in op het stimuleren van bewustwording met de verdere uitbreiding van het programma Informatieveilig gedrag in de zorg. Met dit project werkt VWS aan een gestructureerde methode voor gedragsverandering op het gebied van informatieveiligheid. De methode is uitgewerkt in een Wegwijzer, met manieren om informatieveilig gedrag in de zorg te bevorderen en is kosteloos beschikbaar.[24]

Naast de Wegwijzer worden binnen het programma diverse hulpmiddelen ontwikkeld zoals toolkits met praktische tips over bijvoorbeeld het melden van een datalek, veilig omgaan met patiëntgegevens en veilig gebruik van AI-chatbots. Deze toolkits zijn direct toepasbare en laagdrempelig te gebruiken hulpmiddelen gericht op veelvoorkomende problemen en risico's voor informatieveiligheid. Hierdoor zijn ze nuttig en efficiënt voor (kleinere) zorgaanbieders die capaciteit missen om de hele wegwijzer te doorlopen. De toolkits worden veel gedownload en gebruikt. Verder organiseert het programma trainingen, webinars en masterclasses over bijvoorbeeld het implementeren van NEN 7510 en veilig omgaan met AI in de zorg. Met een stevige communicatiestrategie heeft het programma Informatieveilig gedrag in de zorg de afgelopen jaren een groeiende doelgroep weten te bereiken. Het programma is een effectieve en toekomstbestendige methode gebleken waarin informatiebeveiligingsexperts van verschillende zorgorganisaties aan elkaar worden verbonden in een community. Bovendien geven zorgorganisaties met het programma een concrete invulling aan verschillende paragrafen uit de NEN 7510.

Kickstart Informatiebeveiliging en Privacy

Sinds juli 2023 loopt ook het programma *Kickstart Informatiebeveiliging en Privacy* (Kickstart IB&P)[25]. Met dit programma, uitgevoerd door ICTU, worden zorgorganisaties – van klein tot groot – ondersteund in het versterken van hun informatiebeveiliging en het waarborgen van privacy. De Kickstart IB&P biedt ondersteuning, afgestemd op de dagelijkse praktijk van zorgaanbieders. Met behulp van een modulaire aanpak kunnen zorgorganisaties aansluiten, passend bij hun eigen ontwikkelfase en specifieke vraagstukken. De volgende modules zijn ontwikkeld: voorbereiding, risicoanalyse, maatregelen, effectiviteit van de maatregelen, bewustwording en informatieveilig gedrag. De modules zijn kosteloos beschikbaar voor de zorg.

[24] https://www.informatieveiliggedragindezorg.nl/wegwijzer.
[25] https://www.samenwerkenaaneoverdracht.nl/kickstart-ibp-voor-organisaties-in-de-langdurige-zorg/

2.6 Bouwen aan een veilig gezondheidsinformatiestelsel (GIS)

In het kader van het gezondheidsinformatiestelsel zijn er verschillende lopende trajecten en initiatieven die bijdragen aan de digitale weerbaarheid van de zorg.

European Health Data Space

De European Health Data Space-verordening (EHDS) – die gaat zorgen voor betere databeschikbaarheid en regulering van de zorg-ICT-markt in Nederland en Europa – gaat vereisen dat EPD-systemen aan de kaders rondom cyberveiligheid moeten gaan voldoen conform de Cyberweerbaarheidsverordening[26]. De EHDS is daarmee een aanjager van wetgeving waarmee de nationale kaders versterkt worden.

Generieke functies

Generieke functies zijn sets van afspraken, standaarden en voorzieningen om bijvoorbeeld vast te stellen: Wie logt er in? (Identificatie) Ben je wie je zeg dat je bent? (Authenticatie) Is de patiënt akkoord met het delen van medische gegevens? (Toestemming).

Ook een aantal generieke functies die in het kader van het gezondheidsinformatiestelsel worden ontwikkeld, dragen bij aan informatieveiligheid. Denk aan het nieuwe stelsel voor identificatie en authenticatie voor zorgprofessionals: *dé nieuwe zorgidentiteit*, afgekort *Dezi*[27]. Hiermee kunnen zorgprofessionals straks kiezen tussen verschillende inlogmiddelen op het hoogste betrouwbaarheidsniveau. Dit betekent betere bescherming van cliëntgegevens. Inloggen via Dezi wordt de uniforme standaard voor het raadplegen en uitwisselen van cliëntgegevens in het hele zorgveld. Verder horen hier ook afspraken over autorisatie bij: wie mag welke gegevens gebruiken? Dit maakt de toegang tot deze gegevens veiliger.

Landelijk dekkend netwerk (LDN)

Vertrouwen is een van de uitgangspunten van het *landelijk dekkend netwerk (LDN)* – waaraan VWS werkt om de huidige versnippering van het zorginformatielandschap tegen te gaan. Het LDN is een overkoepelende term waarover mijn voorganger uw Kamer heeft geïnformeerd[28]. Om dat vertrouwen te borgen worden er technische, organisatorische en juridische afspraken gemaakt. Die afspraken moeten burgers en zorgverleners vertrouwen geven in het veilige en verantwoorde gebruik van gezondheidsgegevens. In alle stappen die richting een landelijk dekkend netwerk worden gezet, geldt daarom onder andere het uitgangspunt van *privacy en security by design*. Dit houdt in dat privacy en gegevensbeveiliging al bij de ontwikkeling van een functionaliteit worden meegenomen in het ontwerp.

3. Ambities voor informatiebeveiliging in het zorgveld

Gezien het benoemde dreigingsbeeld, de veranderde geopolitieke situatie en de naleving van NEN 7510 die te wensen overlaat, vind ik het noodzakelijk het cybersecuritybeleid voor de zorgsector te intensiveren.

---

[26] Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen

[27] https://www.dezi.nl/

[28] Kamerstukken II 2024/25, 27 529, nr. 331

3.1 Gedragsverandering bij zorgveld

3.1.1 Focus op informatiebeveiliging kleine zorgaanbieder

Het netwerk van verbonden systemen, dat er met het landelijk dekkend netwerk (LDN) moet komen, is zo sterk als de zwakste schakel. Daarbij speelt mee dat kleinere zorgaanbieders vaker moeite hebben met het voldoen aan de NEN normen dan bij de meeste grotere zorgaanbieders. Met name de omvang van de norm en het gebrek aan capaciteit spelen hier een rol. Dit neemt echter niet weg dat de informatieveiligheid ook bij de kleinere zorgaanbieder omhoog moet.

De IGJ ontwikkelt nieuwe toezichtsmethoden waarin ook rekening wordt gehouden met belemmerende factoren. Ik zal de IGJ hierin ondersteunen en in 2026 meer focussen op de informatiebeveiliging van de kleine zorgaanbieders. Ik ga onder andere een verkenning doen naar het centraal en uniform beschikbaar maken van hulpmiddelen voor informatiebeveiliging, zodat deze makkelijker vindbaar zijn voor de sector. Daarnaast stimuleer ik samenwerking tussen de verschillende stakeholders zoals koepels, branches, veiligheidsregio's en (lokale) samenwerkingsverbanden. Hierbij is het belangrijk dat verschillende zorgsectoren van elkaar leren en dat *best practices* uitgewisseld worden.

Tot slot voer ik een pilot uit met een periodieke monitor die de volwassenheid van zorginstellingen meet en zo inzicht geeft in de stand van de informatiebeveiliging in de sector. Ik verwacht hierdoor duidelijk te krijgen welke onderdelen achterblijven, zodat ik mijn beleid daarop kan aanpassen.

3.1.2 EU Health Action Plan Cybersecurity

Afgelopen januari heeft de Europese Commissie een EU-actieplan gepresenteerd om de cyberveiligheid van ziekenhuizen en (kleine) zorginstellingen te verbeteren.[29] De zorg heeft hoge prioriteit omdat in geen andere kritieke sector in de EU zoveel incidenten worden gemeld.

De financiële gevolgen

Na de publicatie van het actieplan is een Kabinetsbrede reactie opgesteld.[30] In mei gaf mijn voorganger antwoord op de vragen over dit BNC-fiche[31, 32]. In deze antwoorden zegde zij toe terug te komen op de financiële gevolgen van het actieplan.

Het NCC-NL (Nederlands Cybersecurity Coördinatiecentrum) liet mij weten dat de financiering van het actieplan uit verschillende financieringsstromen zal komen:

- € 30 miljoen via Digital Europe aan subsidies voor EU-projecten die cybersecurity in de zorg versterken. Deze subsidie kan aangevraagd worden door regionale of nationale clusters van ziekenhuizen en zorgaanbieders bestaande uit kleine, middelgrote of grote organisaties.

---

[29] European Action Plan on the Cybersecurity Hospitals and Health providers (Europese Commissie), https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers (15 januari 2025)

[30] Kamerstukken II 2024/25, 22 112, nr. 4000

[31] De afkorting BNC staat voor Beoordeling Nieuwe Commissievoorstellen. In de BNC-fiches geeft de regering een eerste oordeel over de voorstellen van de Europese Commissie.

[32] Kamerstukken II 2024/25, 22 112, nr. 4056

- € 6 miljoen vanuit het Digital Europe programma voor het Cybersecurity Agentschap ENISA via een bijdrageovereenkomst.
- Prioritaire inzet van paraatheidsacties en de cyber reserve via de Cyber Solidarity Act voor de zorgsector. Dit gaat om € 36 miljoen en is niet uitsluitend beschikbaar ten behoeve van de sector zorg.

Tot midden juli 2025 konden stakeholders uit het zorgveld tijdens een door de Europese Commissie georganiseerde publieke consultatie reageren op het actieplan. Het doel hiervan was het ophalen van ideeën voor effectieve implementatie van de voorgestelde acties in het plan. Een cijfermatig overzicht van de resultaten is door de Europese Commissie gedeeld.[33] Op basis van deze resultaten wordt eind 2025 een bijgewerkt actieplan opgeleverd. Ik zal het Nederlandse zorgveld via de koepels informeren over de voortgang en mogelijkheden van het actieplan.

3.2 Inspelen op gewijzigd dreigingsbeeld en technologische ontwikkelingen

3.2.1 Digitale autonomie

Gezien de huidige geopolitieke situatie roep ik de sector op om in hun risicoafwegingen de afhankelijkheid van leveranciers mee te nemen. Afhankelijkheid van leveranciers, binnen en buiten Europa kan risico's met zich meebrengen. De continuïteit van zorg moet altijd zeker gesteld zijn. Zorgverlening is vaak kritieke dienstverlening, die niet een paar weken kan wachten. Het is dan ook belangrijk om na te denken over een exit-strategie. Ik ben mij ervan bewust dat zorgaanbieders niet gemakkelijk kunnen overstappen naar een andere leverancier, maar de complexiteit kan geen argument zijn hier niet expliciet bij stil te staan.

Ketenverantwoordelijkheid al in wetgeving vastgelegd

In onze nationale wettelijke norm voor informatiebeveiliging in de zorg, NEN 7510, is al benoemd dat het verplicht is om een risicobeoordeling[34] uit te voeren, en digitale afhankelijkheden moeten daar een onderdeel van zijn.Daarnaast verplicht de Cyberbeveiligingswet (Cbw) organisaties om hun leveranciersketen in kaart te brengen, en om aan de leveranciers in die keten informatiebeveiligingsnormen te stellen.

Geen dwingend kader voor inzet specifieke technologie

De Cbw, en NEN 7510, 7512 en 7513 zijn (dwingende) wet- en regelgeving, maar voor de inzet van specifieke technologie kan en wil ik geen dwingend kader aan de sector voorschrijven. Aangezien de zorgaanbieder in de eerste plaats zelf verantwoordelijk is voor zijn informatieveiligheid, zal die ook zelf de afwegingen moeten maken, passend bij de eigen context.

Bijzondere aandacht in het kader van digitale autonomie verdient de risicoanalyse bij de inzet van cloud-toepassingen, omdat die vaak zorgt voor een grotere afhankelijkheid van leveranciers.

---

[33] Factual summary report: Targeted consultation on the Action Plan on the cybersecurity of hospitals and healthcare providers, (Europese Commissie), https://digital-strategy.ec.europa.eu/en/library/factual-summary-report-targeted-consultation-action-plan-cybersecurity-hospitals-and-healthcare, 12 september 2025

[34] NEN 7510:2024, Informatiebeveiliging in de zorg, artikel 6.1.2.

3.2.2 De cloud

Mijn collega's van Economische Zaken (EZ) en Binnenlandse Zaken en Koningsrelaties (BZK) hebben recent in een Kamerbrief een reactie gegeven op de initiatiefnota «Wolken aan de Horizon» van Tweede Kamerleden Six Dijkstra en Kathmann.[35] De risico's van toenemende afhankelijkheid van clouddiensten worden herkend. In de brief is toegezegd het cloudbeleid te herzien en daarbij ook de uitkomsten van onderzoeken van de Auditdienst Rijk (ADR) en de Algemene Rekenkamer (AR) mee te nemen. De Rijksoverheid is van plan om het Rijkscloudbeleid aan te passen aan de recente geopolitieke ontwikkelingen. Het onderwerp «de cloud» is ook meegenomen in de Nederlandse Digitaliseringsstrategie.[36] Ook in Europees verband wordt er nagedacht over een Europees antwoord op de afhankelijkheid van niet Europese aanbieders van cloudtoepassingen.

Ook voor de zorgsector herken ik naast de voordelen en kansen, de risico's van cloudgebruik. Het is essentieel dat zorgaanbieders de voor- en nadelen van cloudoplossingen afwegen en de juiste maatregelen nemen. Waar cloudtoepassingen in worden gezet of al ingezet zijn, adviseer ik om daarvoor het Implementatiekader risicoafweging cloudgebruik[37] voor de Rijksoverheid te gebruiken. Dit kader is zo generiek dat dit ook voor de zorgsector bruikbaar is. Ik zal de komende maanden met de sector bespreken of dit instrument voldoende bruikbaar is voor de zorg en zo nodig een zorg specifiek afwegingskader ontwikkelen.

3.2.3 Postquantumcryptografie

Cryptografie is een veelgebruikte wiskundige versleuteling van data die alleen ontsleuteld kan worden door iemand de sleutel heeft. Deze manier van beveiliging zorgt ervoor dat bij een hack de data onleesbaar is.

Op dit moment wordt wereldwijd gewerkt aan de ontwikkeling van quantumcomputers, die op een volledig andere manier tot hun rekenkracht komen dan de computers die we nu kennen. Ondanks dat nog niet zeker is wanneer de eerste quantumcomputers in de praktijk gebruikt kunnen worden, moet de zorgsector zich voorbereiden op postquantumcryptografie.

Voorsorteren op toekomstige risico's

Zodra quantumcomputers hun enorme rekenkracht kunnen inzetten, zijn bestaande versleutelingstechnieken te kraken. Daarom is het belangrijk oog te hebben voor:

- Het risico's van «nu stelen, straks ontsleutelen». Dit houdt in dat aanvallers data nu al kunnen stelen en bewaren, om die later te ontsleutelen als quantumcomputers de huidige encryptie kunnen kraken. Dit risico maakt het belangrijk om nu al vast te stellen welke informatie over een aantal jaar nog vertrouwelijk moet zijn en welke aanvullende maatregelen nu nodig zijn om die informatie te beschermen.
- De aanwezigheid van medische apparatuur met een lange levensduur, die gebruikmaakt van encryptie die tijdens de levensduur misschien ontcijferbaar wordt. Bij de aankoop van zulke apparatuur moet

[35] Kamerstukken II 2024/25, 36 574, nr. 3
[36] https://www.digitaleoverheid.nl/nederlandse-digitaliseringsstrategie-nds/
[37] Implementatiekader risicoafweging cloudgebruik, versie 1.1, (CIO Rijk – Interdepartementale Commissie Bedrijfsvoering Rijksdienst), https://open.overheid.nl/documenten/ronl-734f947ec6465e4f75a56bed82fe64a1135f71a8/pdf (5 januari 2023)

rekening worden gehouden met de mogelijkheid om de encryptie op die apparatuur te zijner tijd aan te passen.

Om goed en op tijd met de risico's van quantumcomputers om te gaan, zijn er al hulpmiddelen beschikbaar vanuit de Rijksoverheid.[38] Omdat het (voorlopig) om generieke problematiek gaat, zijn er geen zorg specifieke hulpmiddelen nodig.

3.2.4 End-to-end encryptie

Mijn voorganger heeft uw Kamer toegezegd terug te komen op het onderwerp end-to-end-encryptie (E2E-encryptie) – waarbij alleen de zender en de ontvanger van een bericht dat bericht kunnen inzien.

Uit onderzoek[39] blijkt dat dit om technische, organisatorische en financiële redenen voor zorgaanbieders niet makkelijk te implementeren is. De eisen van de NEN-normen voor de zorgsector op grond van de Wet elektronische gegevensuitwisseling in de zorg (Wegiz) zijn hier van toepassing. Om aan de eisen van de NEN normen te voldoen is E2E-encryptie noodzakelijk. De noodzakelijke vertrouwelijkheid van gezondheidsgegevens en continuïteit van zorg maken dat hier geen concessies aan gedaan kunnen worden. Dit is ook in lijn met de richtlijnen van de Autoriteit Persoonsgegevens.

Bij de ontwikkeling van het landelijk dekkend netwerk werk ik daarom aan de implementatie van E2E-encryptie. In combinatie met generieke functies wordt technisch afgedwongen dat data alleen versleuteld verstuurd kunnen worden en dat middels certificaten er zekerheid is over de afzender én ontvanger.

In het traject om tot een geactualiseerde NEN 7516-norm voor veilig mailen en chatten te komen is dit ook het geldende kader.
Daar waar de eis van E2E-encryptie wijzigingen vraagt in de IT van de zorgaanbieders, dring ik erop aan dat zij die zo spoedig mogelijk implementeren en hier een plan van aanpak voor opstellen. Zorginstellingen moeten deze eisen ook stellen aan hun leveranciers.

3.2.5 Privacy Enhancing Technologies en Multi Party Computation (MPC)

Privacy Enhancing Technologies (PET) zijn verschillende technieken in informatiesystemen om de bescherming van persoonsgegevens te ondersteunen. Multi Party Computation (MPC), Polymorfe encryptie (PEP), *Zero-knowledge proofs* en pseudonimiseren zijn hier voorbeelden van. Daar waar nuttig, doelmatig en mogelijk pas ik deze technieken toe bij het ontwerp van het gezondheidsinformatiestelsel. Ik roep zorginstellingen op om bij gegevensverwerkingen te beoordelen wat de toegevoegde waarde van deze technieken is in een specifieke situatie. In reactie op de motie van Kamerlid De Korte over de opslag en benadering van BSN-gegevens en gevoelige informatie[40] informeer ik u dan ook dat dit niet aan mij is, maar aan het zorgveld. Het is belangrijk om mee te wegen dat een aantal PET's nog geen erkende (open) industriestandaard zijn.

---

[38] Digitale Overheid, Quantumveilige cryptografie, https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/quantumveilige-cryptografie/

[39] Rapportage onderzoek naar de gevolgen van een verplichting tot E2E-beveiliging (PwC in opdracht van VWS) https://www.tweedekamer.nl/downloads/document?id=2023D40039. (30 juni 2023)

[40] Kamerstuk 24 170, nr. 374

3.2.6 OpenKAT

Binnen mijn ministerie is de afgelopen jaren een opensource-tool ontwikkeld die kwetsbaarheden in IT-systemen scant, analyseert en monitort: OpenKAT. Omdat de broncode openbaar is, kan de tool ook door andere (overheids-)organisaties worden gebruikt. Z-CERT was nauw betrokken bij de ontwikkeling van de tool.
Ik ben nu bezig om OpenKAT vanaf eind 2025 op zo'n manier los te laten dat het product duurzaam en structureel kan worden voorgezet, in een uitbreidend gebruikersveld. Door de opensource-licentie kunnen alle huidige en nieuwe gebruikers OpenKAT blijven gebruiken.

Tot slot

Voor burgers en zorgverleners is het cruciaal dat de juiste medische gegevens op tijd en volledig beschikbaar zijn, zodat burgers optimale zorg kunnen krijgen. Een goede beveiliging en zorgvuldig gebruik van data is voorwaardelijk voor het vertrouwen van burgers en zorgverleners in deze technologieën. Burgers zijn daardoor eerder geneigd hun gegevens beschikbaar te stellen aan hun eigen zorgverleners en bijvoorbeeld voor wetenschappelijk onderzoek.

In deze brief heb ik uiteengezet wat ik doe om de informatiebeveiliging op een niveau te brengen waarop de zorgsector voldoende weerbaar is tegen de huidige dreigingen. Ik kan dat niet alleen, maar doe dit samen met de zorgsector.

Zorgaanbieders moeten nu de handschoen oppakken – ze moeten ervoor zorgen dat ze voldoen aan de wettelijke kaders en actief sturen op informatieveilig gedrag van medewerkers. De veranderende omgeving vraagt om intensivering. Verder is het essentieel dat zij afspraken maken met hun leveranciers en dat die leveranciers voldoen aan de aan hen gestelde normen.

De Minister van Volksgezondheid, Welzijn en Sport,
J.A. Bruijn