Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1684

Vragen van de leden **Vervuurt** en **El Boujdaini** (beiden D66) aan de Minister van Volksgezondheid, Welzijn en Sport en de Staatssecretaris van Economische Zaken en Klimaat over *de hack bij ChipSoft dat software levert voor Nederlandse zorginstellingen* (ingezonden 9 april 2026).

Antwoord van Minister **Sterk** (Langdurige Zorg, Jeugd en Sport) (ontvangen 21 april 2026).

Vraag 1
Bent u bekend met de berichtgeving over de cyberaanval op ChipSoft, leverancier van elektronische patiëntendossiers voor een groot deel van de Nederlandse zorginstellingen?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u een actueel beeld geven van de aard, omvang en impact van deze aanval, en welke patiënten hierdoor zijn geraakt?

Antwoord 2
Het Ministerie van VWS onderhoudt geen klantrelatie met Chipsoft en is daarmee geen onderdeel van de informatievoorziening van Chipsoft naar zijn klanten. Uit informele contacten heb ik begrepen dat Chipsoft momenteel samen met een extern team van cybersecurity-experts forensisch onderzoek uitvoert om de oorzaak, omvang en bron van het incident vast te stellen. Naar ik begrepen heb zijn uit voorzorg de verbindingen sinds 8 april 20:00 uur met patiëntportalen die door ChipSoft worden gehost, verbroken. Dit betreft Zorgportaal, HiX Mobile[2] en het Zorgplatform. Deze zijn hierdoor tijdelijk niet beschikbaar. Op donderdag 16 april heeft ChipSoft gecommuniceerd met haar klanten dat er bij de hack ook gegevens zijn gestolen. Hierover heb ik de Kamer, mede namens de Staatssecretaris van Justitie en Veiligheid, in een Kamerbrief op 21 april 2026 geïnformeerd. De resultaten

[1] NOS, 7 april 2026, «Bedrijf dat software levert voor patiëntendossiers aangevallen door hackers», https://nos.nl/artikel/2609548-bedrijf-dat-software-levert-voor-patientendossiers-aangevallen-door-hackers.

[2] HiX mobile is het mobiele platform van ChipSoft dat zorgprofessionals via smartphones of tablets *realtime* toegang geeft tot het elektronisch patiëntendossier (EPD)

ah-tk-20252026-1684
ISSN 0921 - 7398
's-Gravenhage 2026

van het forensisch onderzoek, die van belang zijn voor de hersteloperatie bij zorginstellingen, zullen, zo heeft ChipSoft ons doen laten weten, zo snel mogelijk worden gecommuniceerd. In de tussentijd ondersteunt Z-CERT, als expertisecentrum cybersecurity in de zorg, en biedt hulp aan ChipSoft voor analyse, communicatie en incidentmanagement. Z-CERT informeert en adviseert haar deelnemers over deze situatie.

Vraag 3
In hoeverre heeft deze aanval gevolgen (gehad) voor de continuïteit van zorg, bijvoorbeeld door verminderde toegang tot patiëntgegevens, vertragingen in zorgverlening of het moeten overschakelen op noodprocedures?

Antwoord 3
Ik heb van de betrokken zorginstellingen begrepen dat de zorgprocessen doorlopen en zorgverleners bij de gegevens van patiënten kunnen. Patiënten kunnen echter wel hinder ondervinden bij het online maken van afspraken, dit gaat nu telefonisch. Daarnaast kunnen patiënten momenteel niet zelf hun dossier inzien Ook is er met name impact op de uitwisseling van gegevens. Tussen zorgverleners, zoals huisarts en ziekenhuizen, kunnen verwijzingen niet goed plaatsvinden. Echter, ziekenhuizen zijn voorbereid op dit soort incidenten en zij hebben hiervoor noodprotocollen die ook in werking zijn getreden. Hierdoor kunnen veel zorgprocessen doorlopen, maar vaak met een noodzakelijke extra inzet van personeel. Deze situatie kan daarmee maar voor een beperkte periode bestaan. Inmiddels zo begreep ik is er sinds vrijdag 17 april weer sprake van het opstarten van functionaliteiten, nadat deze veilig zijn bevonden.

Vraag 4
Zijn er aanwijzingen dat patiëntgegevens zijn ingezien, buitgemaakt of anderszins gecompromitteerd? Hoe wordt dit onderzocht en wanneer verwacht u hierover duidelijkheid te kunnen geven?

Antwoord 4
Op donderdag 16 april heeft ChipSoft gecommuniceerd met haar klanten dat er bij de hack patiëntgegevens zijn gestolen. Hierover heb ik de Kamer, mede namens de Staatssecretaris van Justitie en Veiligheid, in een Kamerbrief op 21 april geïnformeerd. Ik vind dit een zeer ernstige zaak. ChipSoft moet alles uit de kast halen en de volle verantwoordelijkheid nemen om snel en zorgvuldig te onderzoeken en duidelijkheid te creëren voor patiënten en zorgverleners, zodat mensen weten of hun data gestolen is en om welke data het gaat.

Vraag 5
Hoe beoordeelt u de sterke afhankelijkheid van een beperkt aantal commerciële leveranciers voor cruciale zorg-IT, en hoe worden de risico's daarvan beperkt?

Antwoord 5
Op verzoek van de toenmalige Minister van VWS heeft de Nederlandse Zorgautoriteit (NZa) in januari 2025 een rapport uitgebracht: «Sturing op kwaliteit en betaalbaarheid zorg-ICT». Daarin staat dat onder andere in de ziekenhuiszorg een paar grote leveranciers de markt domineren. Deze concentratie van marktmacht zorgt ervoor dat er minder concurrentie is, wat de prijzen op kan drijven en innovatie kan vertragen. Ook in de Definitieve leidraad goedwerkende markten voor zorg-ICT van de ACM[3] staat dat het voor nieuwe, innovatieve spelers moeilijk is om voet aan de grond te krijgen, omdat zorginstellingen huiverig zijn om risico's te nemen door met kleine of nieuwe partijen in zee te gaan. Bovendien wordt toetreding tot de Neder-

[3] Bij de beoordeling van mogelijke economische machtsposities kijkt de ACM naar verschillende factoren: het marktaandeel van de onderneming op de relevante markt, de marktpositie en uitbreidingsmogelijkheden van bestaande concurrenten, toetredingsmogelijkheden van nieuwe aanbieders, overstapmogelijkheden tussen aanbieders en de onderhandelingspositie van afnemers. Een hoog marktaandeel is een indicatie voor een economische machtspositie. Echter, ook ondernemingen met een beperkt marktaandeel kunnen een economische machtspositie hebben.

landse markt van nieuwe buitenlandse leveranciers bemoeilijkt door de complexe, internationaal niet te vergelijken bekostigingssystematiek in de zorgsector. Een te grote eenzijdige afhankelijkheid kan risico's met zich brengen voor de continuïteit van zorg. Zorginstellingen zijn zelf verantwoordelijk om deze risico's in kaart te brengen en keuzes te maken om invulling te geven aan hun digitale autonomie.
Ik ben echter ook van mening dat de ontwikkeling naar een European Health Data Space (EHDS) bij kan dragen om de markt toegankelijker te maken voor EPD-leveranciers. Om dat te bereiken worden er bijvoorbeeld op Europees niveau harmoniserende regels gesteld aan interoperabiliteit tussen de EPD-systemen en het verplicht maken van een loggingsmechanisme voor gebruik van gegevens door zorgverleners. Ook wordt gekeken hoe het toezicht versterkt kan worden. In de brief Voortgang agenda databeschikbaarheid van 20 januari 2026[4] is de stand van zaken over de zorg-ICT-markt uiteengezet. Om de risico's te beperken ga ik de komende tijd aan de slag om te bezien hoe de bewustwording en kennis en expertise bij bestuurders over zorg-ICT vergroot kan worden. Daarnaast wordt samen met partijen onderzocht hoe het inkoopproces verbeterd kan worden en zal er samen met overheidspartijen met een regulerende of toezichthoudende rol in het zorgveld een zogenoemde signaleringstafel worden opgezet waar signalen aangaande zorg-IT kunnen worden gedeeld en vanuit bestaand instrumentarium kan worden bekeken of en zo ja welke (gezamenlijke) interventie gewenst is.

Vraag 6
Welke eisen worden momenteel gesteld aan leveranciers van zorg-IT op het gebied van cybersecurity, weerbaarheid en continuïteit, en in hoeverre zijn deze eisen voldoende gezien de kritieke rol van deze partijen voor ons zorgsysteem?

Antwoord 6
Nederlandse zorgaanbieders zijn momenteel wettelijk verplicht om te voldoen aan de norm voor informatiebeveiliging in de zorg, de NEN 7510. De NEN 7510 geeft richtlijnen voor controlemaatregelen en stelt eisen aan het informatiebeveiligingssystemen. De norm vereist ook beheersmaatregelen voor bedrijfscontinuïteit en bereikbaarheid. Bij de inzet van ICT-producten die medische gegevens verwerken, eisen zorgaanbieders van de softwareleveranciers van deze ICT-producten dat ook zij voldoen aan de NEN 7510. Softwareleveranciers dienen dit aan te tonen met een certificaat. Daarnaast zullen aanvullende eisen voor cyberweerbaarheid worden gesteld in de NIS2 richtlijn die wordt omgezet in de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit. Ik ga hier verder op in bij vraag 8. De EHDS draagt bij aan toegankelijkheid van de zorg-ICT-markt in Nederland en Europa en betere databeschikbaarheid. Deze verordening gaat de nieuwe eis stellen dat EPD-systemen aan de kaders rondom cyberveiligheid moeten gaan voldoen conform de Cyberweerbaarheidsverordening[5].

Vraag 7
In hoeverre zijn zorginstellingen verplicht of gestimuleerd om scenario's uit te werken voor uitval van essentiële IT-systemen, en hoe wordt geborgd dat zorgverlening doorgang kan vinden bij langdurige verstoringen?

Antwoord 7
Het doen van een risicoanalyse is onderdeel van de norm voor informatieveiligheid in de zorg (NEN7510). Aan deze norm dienen zorgaanbieders aantoonbaar te voldoen. Bij het werken volgens de norm hoort ook het nemen van maatregelen om uitval (door bijvoorbeeld een cyberincident) te voorkomen en de impact te beperken. Een belangrijk onderdeel van de norm is bovendien dat er plannen worden gemaakt voor bedrijfscontinuïteit bij onverwachte verstoringen of uitval en dat deze periodiek getest, geëvalueerd en verbeterd worden.

---

[4] *Kamerstukken II*, 2025/2026, 27 529, nr. 355
[5] Verordening (EU) 2024/2847 van het Europees parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen

Vraag 8
Hoe wordt binnen het beleid rond de implementatie van de NIS2-richtlijn specifiek rekening gehouden met de afhankelijkheid van de zorgsector van externe IT-leveranciers?

Antwoord 8
De NIS2 richtlijn wordt omgezet in de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit. In de Cyberbeveiligingswet is in artikel 10 opgenomen dat de organisaties die onder deze wet vallen verplicht zijn om beleid vast te stellen over de beveiliging van de toeleveringsketen. Dit betekent dat de zorgaanbieders die onder de reikwijdte vallen niet alleen hun eigen netwerken informatiesystemen op orde hebben, maar ook die van hun rechtstreekse leveranciers periodiek toetsen. Daarnaast zullen IT-leveranciers ook rechtstreeks onder de reikwijdte van de wet vallen, onder de sector digitale infrastructuur.

Vraag 9
Ziet u aanleiding om aanvullende eisen te stellen aan leveranciers van kritieke zorg-IT, bijvoorbeeld op het gebied van redundantie, interoperabiliteit of exit-strategieën, zodat zorginstellingen minder kwetsbaar zijn bij uitval of incidenten?

Antwoord 9
Zorgaanbieders zijn verantwoordelijk voor de afspraken die gemaakt worden met hun ICT-leveranciers. Uit deze verantwoordelijkheid volgt dat zij handelingsperspectieven moeten opstellen op basis van de individuele risicoafwegingen en passend bij de eigen context. In de NEN7510 is de verplichting opgenomen een risicobeoordeling uit te voeren en digitale afhankelijkheden in kaart te brengen. Daarnaast verplicht de Cyberbeveiligingswet (Cbw) organisaties, waaronder zorgaanbieders, om hun leveranciersketen in kaart te brengen en om aan de leveranciers in die keten informatiebeveiligingsnormen te stellen.

Vraag 10
In hoeverre wordt gewerkt aan het verminderen van single points of failure in de digitale infrastructuur van de zorg, en welke concrete stappen worden gezet om diversificatie en alternatieven te stimuleren?

Antwoord 10
Er wordt vanuit verschillende projecten en programma's gewerkt aan het realiseren van een duurzaam en veilig gezondheidsinformatiestelsel. Bij de totstandkoming van dit stelsel is het uitgangspunt dat er sprake is van een federatief stelsel waarbij data aan de bron blijft. Voor vertrouwen in het gebruik van gezondheidsgegevens zijn enkele (centrale) vertrouwenscomponenten noodzakelijk. Om te waarborgen dat deze voorzieningen geen centrale point-of-failure worden, is bij de realisatie van de techniek rekening gehouden met de mogelijkheden om de data te kunnen repliceren zonder dat daarmee de betrouwbaarheid van data in het geding komt. Zo wordt het Landelijk Register Zorgaanbieders (LRZa) ingericht om adresseerbare punten per zorgaanbieder op te kunnen vragen zodat de decentrale punten direct met elkaar kunnen uitwisselen. Om te voorkomen dat dit een single-point-of-failure wordt, is er synchronisatie van gegevens mogelijk zodat de adresseerbare punten periodiek kunnen worden geharmoniseerd zonder dat dit de betrouwbaarheid van de gegevens in het geding brengt.
Zoals beschreven bij vraag 5 worden er bij de European Health Data Space-verordening regels opgelegd aan leveranciers om de EPD-markt beter te laten functioneren en concurrentie en innovatie te bevorderden. Daarmee wordt het voor nieuwe toetreders aantrekkelijker om toe te treden tot de Nederlandse markt. Ook wordt ingezet op een betere vraagbundeling en vraagarticulatie en het verbeteren van het inkoopproces.

Vraag 11
Welke andere lessen trekt u uit dit incident voor de bredere digitalisering van de zorg, met name op het gebied van digitale autonomie, en hoe worden deze lessen vertaald naar concreet beleid?

Antwoord 11
Digitale veiligheid is nooit voor honderd procent te garanderen en dit soort aanvallen zijn nooit helemaal te voorkomen. Wat we wel gezamenlijk kunnen doen, is de risico's zoveel mogelijk beperken en ervoor zorgen dat eventueel misbruik snel wordt gesignaleerd en doeltreffend wordt aangepakt. Ik vind het belangrijk dat zorgaanbieders regie nemen over hun digitale autonomie. Bij digitale autonomie hoort een inzicht én keuzes jegens kwetsbaarheden in veiligheid, maar ook in eenzijdige afhankelijkheden van dominante marktpartijen. Dit vraagstuk is niet specifiek voor de zorg. Hier kan de zorg dus inspiratie putten uit stappen die in andere sectoren gezet worden. Zonder in contractuele verplichtingen te willen treden, zie ik het als mijn taak de zorgsector in deze bredere maatschappelijke beweging mee te krijgen.

Vraag 12
Kunt u de Kamer op korte termijn informeren over de uitkomsten van het onderzoek naar deze aanval, inclusief de implicaties voor het beleid rondom digitale weerbaarheid in de zorg?

Antwoord 12
In eerste instantie is ChipSoft zelf verantwoordelijk om te communiceren over de bevindingen van het forensisch onderzoek dat zij momenteel, in samenwerking met cybersecurity-experts, laten uitvoeren. Ik volg de zaak uiteraard nauwlettend. Mocht de rapportage van ChipSoft aanleiding zijn voor mij om vanuit mijn systeemverantwoordelijkheid aanvullende acties te ondernemen dan zal ik uw Kamer hierover informeren.