Ministerie van Volksgezondheid,
Welzijn en Sport

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
F 070 340 78 34
www.rijksoverheid.nl

Ons kenmerk
4375579-1097269-DICIO

Bijlagen
1

Datum document
10 april 2026

Correspondentie uitsluitend richten aan het retouradres met vermelding van de datum en het kenmerk van deze brief.

> Retouradres Postbus 20350 2500 EJ Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Datum 24 april 2026
Betreft Kamervragen

Geachte voorzitter,

De leden Bushoff en Kathmann (beiden GroenLinks-PvdA) hebben vragen gesteld aan de minister van Volksgezondheid, Welzijn en Sport en de staatssecretaris Digitale Economie en Soevereiniteit (2026Z07622). Omdat deze vragen gaan over een datahack in de zorgsector verzend ik u de beantwoording op deze vragen.

Hoogachtend,

de minister van Langdurige Zorg,
Jeugd en Sport,

Mirjam Sterk

Antwoorden op Kamervragen van Bushoff en Kathmann (beiden GroenLinks-PvdA) over de hack bij software voor patiëntendossiers aan de minister van Volksgezondheid, Welzijn en Sport en de staatssecretaris Digitale Economie en Soevereiniteit (2026Z07622) (ingezonden 10 april 2026)

Vraag 1
Bent u op de hoogte van de hack bij ChipSoft, het bedrijf dat software voor patiëntendossiers en andere digitale systemen voor ziekenhuizen levert?

Antwoord vraag 1
Ja.

Vraag 2
Kunt u toelichten wat de ernst is van de hack en hoeveel ziekenhuizen, huisartsenpraktijken en eventuele andere zorgverleners zijn geraakt door de hack?

Antwoord vraag 2
Patiënten moeten erop kunnen vertrouwen dat hun gegevens veilig zijn. Chipsoft voert momenteel samen met een extern team van cybersecurity-experts forensisch onderzoek uit om de oorzaak, omvang en bron van het incident vast te stellen. ChipSoft levert software aan ongeveer 70% van de Nederlandse ziekenhuizen. Uit voorzorg zijn sinds 8 april 20:00 uur de verbindingen met patiëntportalen die door ChipSoft worden gehost, verbroken. Dit betreft Zorgportaal, HiX Mobile[1] en het Zorgplatform. Deze zijn hierdoor tijdelijk niet beschikbaar geweest. Inmiddels is er sinds vrijdag 17 april weer sprake van het gefaseerd opstarten van functionaliteiten, nadat deze veilig zijn bevonden. Op donderdag 16 april heeft ChipSoft gecommuniceerd met de klanten die dat betrof 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[2]. ChipSoft heeft geen gedetailleerde inzage gegeven in welke klanten op welke wijze getroffen zijn. In de zojuist genoemde Kamerbrief heb ik ons inzicht met u gedeeld. De resultaten van het forensisch onderzoek, die van belang zijn voor de hersteloperatie bij zorginstellingen, zullen, zo heeft ChipSoft ons 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
Wat zijn de gevolgen van de hack voor zorgverleners en hun patiënten, bijvoorbeeld doordat zorginstellingen hun systemen offline hebben moeten halen?

Antwoord vraag 3
Navraag bij de betrokken zorginstellingen leert 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

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

[2] Kamerbrief over hack ChipSoft, verstuurd 21 april (dossiernummer en stuknummer zijn op moment van schrijven nog niet bekend).

impact op de uitwisseling van gegevens. Tussen zorgverleners, zoals huisarts en ziekenhuizen, kunnen digitale verwijzingen niet goed plaatsvinden.

Ziekenhuizen zijn hier echter op dit soort incidenten voorbereid 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.

Vraag 4
Is bepaalde zorg uitgesteld vanwege de hack en zo ja, op welke schaal?

Antwoord vraag 4
Nee, de zorgprocessen lopen door.

Vraag 5
Is er gevoelige data, zoals patiëntgegevens, in handen gekomen van criminelen?

Antwoord vraag 5
Patiënten moeten erop kunnen vertrouwen dat hun gegevens veilig zijn. Op donderdag 16 april heeft ChipSoft gecommuniceerd met haar klanten dat er bij de hack patiëntgegevens zijn gestolen. Welke exacte patiëntgegevens hierbij zijn buitgemaakt is nog in onderzoek. Ik heb de Kamer, mede namens de staatssecretaris van Justitie en Veiligheid, in een Kamerbrief op 21 april hierover geïnformeerd.[3] 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 6
Hoe verklaart u de verschillende aanpak van ziekenhuizen na de hack, bijvoorbeeld in het wel of niet offline halen van systemen?

Antwoord vraag 6
Ziekenhuizen die klant zijn bij ChipSoft hebben op advies van Z-CERT, het expertisecentrum cybersecurity in de zorg, preventieve maatregelen genomen en hebben monitoring op hun lopende systemen geïntensiveerd. De keuzes die gemaakt worden, zijn door de ziekenhuizen of organisaties zelf gemaakt op basis van eigen specifieke situatie en risico inschatting.

Vraag 7
Verschilt de impact van de hack tussen ziekenhuizen die hun gegevens lokaal, hybride of juist in een cloudomgeving opslaan? Kunt u uitleggen welke keuze de meeste weerbaarheid biedt?

Antwoord vraag 7
De gegevens van de zorgaanbieders die gebruikmaken van de cloudomgeving van ChipSoft zijn gestolen. Van instellingen die de software van ChipSoft in eigen beheer uitvoeren of door derden laten beheren, zijn geen gegevens gestolen. Hierover heb ik de

[3] Kamerbrief over hack ChipSoft, verstuurd 21 april (dossiernummer en stuknummer zijn op moment van schrijven nog niet bekend).

Kamer, mede namens de staatssecretaris van Justitie en Veiligheid, in een Kamerbrief op 21 april geïnformeerd[4]

Er valt niet in z'n algemeenheid te zeggen welke keuze de meeste weerbaarheid biedt. Dit hangt af van de lokale context van de zorgaanbieder en de risicoafweging die gedaan is en de beheersmaatregelen die daarbij genomen zijn.

Vraag 8
Welke rol speelt de overheid in de afwikkeling van de hack?

Antwoord vraag 8
Wat betreft de afwikkeling van de hack en opsporing en/of vervolging ligt de verantwoordelijkheid bij de politie en het Openbaar Ministerie (OM). Diverse toezichthouders doen onderzoek naar de hack. Vanuit onze stelselverantwoordelijkheid ondersteunen we de koepelorganisaties die in het Informatieberaad Zorg zitten met informatie over de digitale aanval en een woordvoeringslijn die zij kunnen gebruiken naar hun leden.
Ook worden bijvoorbeeld handelingsperspectieven uitgewisseld. VWS en organisaties die gesubsidieerd worden door VWS ondersteunen de getroffen zorginstellingen zoveel als mogelijk. Zo financiert de overheid Z-CERT, het expertise centrum cybersecurity in de zorg. Z-CERT, biedt hulp aan ChipSoft voor analyse, communicatie en incidentmanagement. Z-CERT informeert en adviseert haar deelnemers over deze situatie. Vanuit het ministerie volgen we de ontwikkelingen zeer nauw, adviseren we koepels en zorgaanbieders en duiden we de rollen en bevoegdheden, waar nodig.

Vraag 9
Zijn er alternatieven voorhanden bij een hack als deze, bijvoorbeeld alternatieve software waar ziekenhuizen en andere zorgverleners op kunnen terugvallen?

Antwoord vraag 9
Ziekenhuizen hebben draaiboeken en protocollen voor als systemen niet werken om te zorgen dat het zorgproces door kan blijven gaan. Dit volgt uit de verplichte risico analyse die zij moeten doen. Zo gaan bijvoorbeeld verwijzingen van huisartsen naar Chipsoft-ziekenhuizen niet meer digitaal, maar per mail of telefonisch. Zie ook het antwoord op vraag 3. Het is aan zorgverleners zelf om deze protocollen, gegeven de specifieke situatie van de betreffende zorgverlener, in te richten. De ingebruikname van een ander elektronisch patiëntendossier of andere alternatieve software is niet iets wat in enkele dagen of weken geregeld kan worden. Dit is technisch zeer complex en kent een lange doorlooptijd. Bovendien brengt het hoge kosten en andere risico's met zich mee.

Vraag 10
Welke eisen gelden er voor leveranciers van cruciale zorg-ICT?

Antwoord vraag 10
Nederlandse zorgaanbieders zijn 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

[4] Idem.

softwareleveranciers van deze ICT-producten dat ook zij voldoen aan de NEN 7510. Softwareleveranciers dienen dit aan te tonen met een certificaat.

In de nabije toekomst zullen aanvullende eisen voor cyberweerbaarheid worden gesteld in de NIS2-richtlijn die wordt omgezet in de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit. De European Health Data Space-verordening (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 11

Is de ketenweerbaarheid op het gebied van ICT in de zorg wat u betreft op orde, onder andere in de domeinen hosting, beheer, en koppelingen? Waarom wel of niet?

Antwoord vraag 11

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 gaat de Cyberbeveiligingswet (Cbw) organisaties, waaronder zorgaanbieders, verplichten om hun leveranciersketen in kaart te brengen, en om aan de leveranciers in die keten informatiebeveiligingsnormen te stellen. De Cbw is voorzien medio 2026 in te gaan.

Vraag 12

Deelt u de opvatting dat dit geen incident is, maar een symptoom van te grote afhankelijkheid van een paar dominante leveranciers in de zorg, waarbij een incident bij één leverancier meteen een nationale zorgvraag wordt?

Antwoord vraag 12

Nee, ik deel die opvatting niet. Zorgaanbieders dienen afspraken te maken met zorg-ICT-leveranciers en hierbij risico's af te wegen. Het is wel zo dat de omvang van een hack groter kan zijn wanneer een leverancier met een groot marktaandeel wordt getroffen waarbij ook nog eens patiëntgegevens zijn opgeslagen.

Vraag 13

Deelt u de zorgen over de risico's wanneer één dominante marktpartij de infrastructuur levert voor zorginstellingen of andere essentiële publieke voorzieningen?

Antwoord vraag 13

Het is belangrijk dat er sprake is van een gezonde marktwerking op de zorg-ICT-markt. 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 marktconcentratie zorgt voor minder concurrentie, wat de prijzen op kan drijven en innovatie kan vertragen. Ook is er een definitieve leidraad goedwerkende markten voor zorg-ICT van de ACM[6] gepubliceerd. Het ministerie van VWS maakt hieruit op dat het voor nieuwe innovatieve spelers moeilijk is voet aan de

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

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 Nederlandse markt van nieuwe buitenlandse leveranciers bemoeilijkt door de complexe, internationaal niet te vergelijken bekostigingssystematiek in onze 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 overwegingen van digitale autonomie.

In de brief Voortgang agenda databeschikbaarheid van 20 januari 2026 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 de bewustwording en kennis en expertise bij bestuurders over zorg-ICT te vergroten. Ook wordt samen met partijen onderzocht hoe het inkoopproces verbeterd kan worden. Daarnaast wordt er samen met overheidspartijen met een regulerende of toezichthoudende rol in het zorgveld een zogenoemde signaleringstafel opgezet. Daar kunnen signalen over zorg-ICT worden gedeeld en kan vanuit bestaand instrumentarium bekeken worden of en zo ja welke (gezamenlijke) interventie gewenst is. Naast de hierboven genoemde acties zet ik in op de European Health Data Space (EHDS) om de markt toegankelijker te maken voor EPD-leveranciers. Om dat te bereiken worden er op Europees niveau harmoniserende regels gesteld aan interoperabiliteit tussen de EPD-systemen en aan een verplicht loggingsmechanisme voor gebruik van gegevens door zorgverleners. Ook wordt gekeken hoe het toezicht versterkt kan worden op zorg-ICT.

Vraag 14
Zijn er maatregelen die u neemt om dergelijke marktdominantie tegen te gaan, bijvoorbeeld door afspraken te maken over het inkoop- en aanbestedingsbeleid in de zorgsector? Waarom wel of niet?

Antwoord vraag 14
In de eerste plaats zijn zorgaanbieders zelf verantwoordelijk voor de inkoop, aanbesteding en contractering van zorg-ICT. Wel blijkt uit het NZa rapport 'Sturing op kwaliteit en betaalbaarheid zorg-ICT' januari 2025 dat de bewustwording en kennis en expertise bij bestuurders over zorg-ICT vergroot kan worden. Daarom wordt samen met partijen onderzocht hoe het inkoopproces verbeterd kan worden, bijvoorbeeld door de inzet van externe expertise om gezamenlijke inkoop van een kernapplicatie te laten slagen. Dit zorgt voor schaalvoordelen en vergroot de kans op samenwerking. Over dit soort onderwerpen heeft mijn ministerie ook regelmatig overleg met de ICT-gebruikersverenigingen van de ziekenhuizen.

Vraag 15
Hoe zorgt u voor voldoende diversificatie tussen ICT-leveranciers bij zorginstellingen? Is het uw verantwoordelijkheid om monopolievorming in de zorg-ICT tegen te gaan?

Antwoord vraag 15

[6] Autoriteit Consument & Markt.Definitieve Leidraad 'Goedwerkende markten voor zorg-ICT'. (gepubliceerd 22 november 2022).

De Autoriteit Consument en Markt (ACM) houdt toezicht op eerlijke concurrentie en marktwerking, zo ook op de zorg-ICT markt. In eerste instantie is zij de toezichthouder op basis van de Mededingingswet die toezicht houdt op de markt en ook concentraties (fusies/overnames) beoordeelt. Zij heeft in haar brief op 28 januari 2025[7] aangegeven dat de zorg-ict markt niet goed werkt omdat ICT-systemen gesloten zijn. De ACM geeft aan dat zij op dit moment onvoldoende instrumenten heeft om eerlijke concurrentie en marktwerking structureel af te dwingen en adviseert het ministerie van VWS om openheid van digitale informatiesystemen via wetgeving te verplichten.

Ik vind het belangrijk dat de zorg-ICT-markt toegankelijk is, zodat concurrentie en innovatie worden gestimuleerd. Met de EHDS wordt ook ingezet op een zo open mogelijke markt voor onder andere EPD-leveranciers. Ik onderzoek de mogelijkheden om als randvoorwaardelijk onderdeel van de EHDS, te komen tot additionele regulerende instrumenten.

Vraag 16
Is het wenselijk dat zorginstellingen individueel ICT-diensten inkopen en hierover onderhandelen? Welke voor- en nadelen ziet u bij een meer gezamenlijke vorm van inkoop?

Antwoord vraag 16
In de eerste plaats zijn zorgaanbieders zelf verantwoordelijk voor de inkoop, aanbesteding en contractering. Gezamenlijke inkoop kan schaalvoordelen opleveren, vergroot de kans op samenwerking en versterkt de positie van de zorgaanbieders. Een nadeel kan zijn dat er minder maatwerk wordt geleverd.

Vraag 17
Wat is de status van de uitvoering van de motie-Bushoff/Bevers om bij de evaluatie van de Wet vifo te bezien of bij fusies en overnames vanuit het buitenland van digitale zorginfrastructuur vergelijkbare voorwaarden gesteld kunnen worden als bij andere cruciale sectoren, zoals de chip-, energie- en telecomsector?

Antwoord vraag 17
Sinds juni 2023 is de Wet Veiligheidstoets investeringen, fusies en overnames (vifo) van kracht. De Wet vifo introduceerde een mechanisme voor investeringstoetsing in Nederland. Recent is de wet, conform de toezegging aan de Tweede Kamer, geëvalueerd.

Tevens is in december 2025 de herziene Foreign Direct Investment (FDI)-screeningsverordening vastgesteld. Met de wijziging van de Verordening worden de reikwijdte en procedures van de nationale investeringstoetsingsregimes in de Europese Unie gestroomlijnd om economische veiligheidsrisico's van investeringen op een meer coherente manier aan te pakken. Nadat de herziene FDI verordening formeel is vastgesteld, start de termijn voor omzetting van de Verordening in nationale wetgeving. In Nederland wordt deze Verordening geïmplementeerd in de Wet vifo. Ik koers aan op een verwijzing in de wet vifo naar de (terminologie van de) Wet weerbaarheid kritieke entiteiten (Wwke). Hiermee zullen kritieke entiteiten in de zorg in het geval van vijandige investeringen, fusies of overnames kunnen worden getoetst.

[7] Autoriteit Consument & Markt (ACM), Advies aan het Ministerie van Volksgezondheid, Welzijn en Sport: verplicht openheid van zorginformatiesystemen om innovatie te bevorderen, ACM.nl (gepubliceerd 28 januari 2025).

Vraag 18
Deelt u de zorgen van de Autoriteit Consument & Markt (ACM) over gesloten datastandaarden bij ICT-aanbieders in de zorg, aangezien systemen daardoor niet goed met elkaar communiceren en zorgaanbieders minder keuze hebben in hun leveranciers, met monopolievorming tot gevolg?

Antwoord vraag 18
Ja ik deel deze zorgen. Het niet gebruiken van open standaarden en de geslotenheid van ICT-systemen bevordert niet de door de Nationale, Visie en Strategie[8] gewenste interoperabiliteit op weg naar databeschikbaarheid. Om dat te veranderen zal een mix van Europese verplichtingen en nationale keuzes nodig zijn. Met de European Health Data Space (EHDS) verordening wordt ingezet op een zo open mogelijke markt voor EPD-leveranciers. Om dat te bereiken worden er op Europees niveau harmoniserende regels gesteld aan interoperabiliteit tussen de EPD-systemen. Vanuit de NVS-ambitie stuur ik op openstelling van systemen via open gestandaardiseerde koppelvlakken: publiek beschikbare koppelvlakken,

zodat data veilig, herbruikbaar en leverancier-onafhankelijk kan stromen door het hele stelsel. De specificaties van deze open koppelvlakken zijn een publieke verantwoordelijkheid. Zo nodig zal ik deze koppelvlakken ook als open source laten ontwikkelen en beschikbaar stellen aan marktpartijen.

Vraag 19
Wat is de status van de uitvoering van de motie-Bushoff/Kathmann over een routekaart waarlangs ICT-leveranciers in de zorg de komende jaren verplicht worden gebruik te maken van open datastandaarden?

Antwoord vraag 19
In mijn brief ‘stand van zaken landelijk dekkend netwerk’ die ik voor het commissiedebat digitale zorg (gepland op 21 mei) naar uw Kamer zal sturen, zal ik dieper ingaan op dit vraagstuk.

Vraag 20
Welke structurele problemen in de zorg-ICT legt deze hack bloot? Wie is er aan zet om deze op te lossen?

Antwoord vraag 20
Het onderzoek naar deze hack is nog in volle gang. Het is daarmee te vroeg om een verband te leggen tussen deze hack en structurele problemen in de zorg-ICT.

Vraag 21
Welke maatregelen neemt u om de cyberveiligheid en weerbaarheid van zorginstellingen structureel te vergroten?

Antwoord vraag 21
In het versterken van de cyberweerbaarheid van de zorg neem ik een kader stellende, toezichthoudende, stimulerende en faciliterende rol in. In de brief over informatieveiligheid in de zorg van 4 december 2025 heeft mijn voorganger uw Kamer

[8] Kamerstukken II 2022/23, 27 529, nr. 292

geïnformeerd over de maatregelen die mijn ministerie neemt[9]. Ik ondersteun zorginstellingen bij het voorkomen van incidenten door het verhogen van bewustzijn van zorgmedewerkers in het programma Informatieveilig gedrag in de zorg. Een groot deel van cyberincidenten zijn mede veroorzaakt door menselijk handelen. Daarnaast bied ik hulpmiddelen aan om te voldoen aan de NEN7510, de norm voor informatiebeveiliging in de zorg. Deze norm schrijft organisatorische, mensgerichte, fysieke en technologische beheersmaatregelen voor die de digitale weerbaarheid van een organisatie concreet verhogen. Dit met het doel om dreigingen te voorkomen, detecteren of erop te reageren. Tot slot helpt het expertisecentrum cybersecurity in de zorg (Z-CERT) zorginstellingen in het voorkomen van incidenten door te monitoren en eventuele dreigingsinformatie te delen. Daarnaast biedt Z-CERT ondersteuning bij het beperken van de gevolgen wanneer er onverhoopt een incident heeft plaatsgevonden.

Vraag 22
Wat wordt de rol van de Cyberbeveiligingswet, zodra deze is aangenomen, om dergelijke hacks te voorkomen en sneller af te wikkelen? Wat gaat er concreet veranderen in een casus zoals deze?

Antwoord vraag 22
Voor alle zorgaanbieders is de NEN 7510, de norm voor informatiebeveiliging in de zorg, nu al wettelijk verplicht. De Cyberbeveiligingswet (Cbw) gaat bredere eisen stellen aan netwerk- en informatiebeveiliging voor diverse sectoren waaronder de sector zorg. Zodra de Cbw van kracht is (voorzien medio 2026), hebben organisaties die onder de wet vallen een meldplicht. Dit houdt in dat een significante cyberincident[10] binnen 24 uur wordt gemeld bij het portaal van het Nationaal Cyber Security Centrum (NCSC). Het NSCS werkt nauw samen met Z-CERT, het expertisecentrum op het gebied van het cybersecurity in de zorg. Deze meldplicht zorgt ervoor dat alle significante meldingen worden gemonitord en er tijdig wordt gewaarschuwd tegen cyberdreigingen. Daarnaast stelt de Cbw een zorgplicht voor organisaties verplicht. Dit houdt in dat organisaties vallend onder Cbw maatregelen moeten nemen om hun netwerk- en informatiesystemen te beschermen tegen significante incidenten. De Cbw zal cyberincidenten niet voorkomen, maar de cyberweerbaarheid in Nederland en daarmee ook in de sector zorg wordt verhoogd doordat significante cyberincidenten worden gemonitord en vervolgens snel wordt gehandeld om de beveiliging van informatiesystemen en bedrijfscontinuïteit te waarborgen.

Vraag 23
Kunt u deze vragen afzonderlijk van elkaar en nog vóór het commissiedebat over digitale ontwikkelingen in de zorg van 21 mei 2026 beantwoorden?

Antwoord vraag 23
Ja.

[9] Kamerstukken II, 2025/26, 27529, nr. 353

[10] Significante incidenten zijn gebeurtenissen die ernstige verstoringen in de dienstverlening veroorzaken of aanzienlijke schade, zowel materieel als immaterieel, tot gevolg hebben zoals een cyberaanval.

1) NOS, 8 april 2026, 'Bedrijf dat software levert voor patiëntendossiers aangevallen door hackers' (Bedrijf dat software levert voor patiëntendossiers aangevallen door hackers)

2) Kamerstuk 27529, nr. 349

3) Kamerstuk 27529, nr. 348