2026Z07622

(ingezonden 10 april 2026)

Vragen van de leden Bushoff en Kathmann (beiden GroenLinks-PvdA) aan de minister van Langdurige Zorg, Jeugd en Sport en de staatssecretaris van Economische Zaken en Klimaat over de hack bij software voor patiëntendossiers aan de minister van Volksgezondheid, Welzijn en Sport en de staatssecretaris Digitale Economie en Soevereiniteit.

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

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

Wat zijn de gevolgen van de hack voor zorgverleners en hun patiënten, bijvoorbeeld doordat zorginstellingen hun systemen offline hebben moeten halen?

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

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

Hoe verklaart u de verschillende aanpak van ziekenhuizen na de hack, bijvoorbeeld in het wel of niet offline halen van systemen?

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?

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

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

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

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?

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?

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

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?

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

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?

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? 2)

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?

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? 3)

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

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

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?

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

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