2026Z24112

(ingezonden 5 november 2026)

Vragen van de leden Zwinkels en Poortman (beiden CDA) aan de minister van Volksgezondheid, Welzijn en Sport en de staatssecretaris van Economische Zaken en Klimaat over het artikel ‘Vriezers van Franse bloedbank gehackt, temperatuur verhoogd’

Bent u bekend met het artikel ‘Vriezers van Franse bloedbank gehackt, temperatuur verhoogd’ en deelt u de zorgen over de risico's van dergelijke cyberaanvallen voor de volksgezondheid en de weerbaarheid van Nederland? 1)

Op welke manier worden bloedbanken en andere kritieke organisaties in de gezondheidszorg proactief ondersteund bij het versterken van hun digitale weerbaarheid en het effectief inregelen van hun cybersecurity om zo cyberaanvallen te voorkomen?

In hoeverre verplicht de Cyberbeveiligingswet bloedbanken en andere kritieke zorginstellingen om cybersecurityrisico's, waaronder die van digitaal aangestuurde apparatuur en externe leveranciers, proactief te beheersen? Welke concrete maatregelen vloeien hieruit voort?

Op welke manier werken organisaties binnen dezelfde branche of keten samen om cyberincidenten te voorkomen en informatie over kwetsbaarheden en dreigingen uit te wisselen?

Wordt er gecoördineerd gewerkt aan noodplannen en fysieke terugvalopties wanneer kritieke apparatuur of infrastructuur door een cyberaanval uitvalt of wordt gemanipuleerd? Hoe wordt hierop toegezien in het kader van de Wet weerbaarheid kritieke entiteiten (Wwke)?

Hoe wordt de samenwerking tussen organisaties binnen dezelfde keten of branche gecoördineerd wanneer zich een ernstig cyberincident voordoet, bijvoorbeeld wanneer meerdere organisaties afhankelijk zijn van dezelfde leverancier of wanneer een verstoring bij één organisatie gevolgen heeft voor andere organisaties in de keten?

Valt digitaal aangestuurde koelapparatuur, zoals de installaties bij bloedbanken, onder de Cyber Resilience Act (CRA)? Zo ja, welke cybersecurityvereisten en eventuele risicoclassificaties zijn hierop van toepassing?

Welke verantwoordelijkheden hebben fabrikanten van dergelijke apparatuur op grond van de CRA met betrekking tot cybersecurity en het tijdig verhelpen van kwetsbaarheden?

Hoe is de juridische verantwoordelijkheid verdeeld tussen fabrikanten, leveranciers en gebruikers wanneer apparatuur, zoals koelinstallaties, door een cyberaanval wordt getroffen?

Wat is er inmiddels bekend over de daders en achtergronden van de recente cyberaanval op de Franse bloedbank en andere cyberaanvallen op koelapparatuur? Zijn er aanwijzingen voor mogelijke betrokkenheid van statelijke actoren?

1) RTL, 4 november, 'Vriezers van Franse bloedbank gehackt: 'Temperatuur naar 110 graden' (https://www.rtl.nl/nieuws/economie/artikel/5662920/hackpoging-bij-franse-bloedbank)