Ministerie van Volksgezondheid,
Welzijn en Sport

> Retouradres Postbus 20350 2500 EJ Den Haag

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

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

Ons kenmerk
4573467-1106629-GMT

Bijlagen
1

Datum document
5 november 2026

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

Datum 27 november 2026
Betreft Kamervragen

Geachte voorzitter,

Hierbij zend ik u mede namens de staatssecretaris van Economische Zaken en Klimaat-Digitale Economie en Soevereiniteit en de minister van Langdurige Zorg, Jeugd en Sport, de antwoorden op de vragen van de leden Zwinkels en Poortman (beiden CDA) over het artikel 'Vriezers van Franse bloedbank gehackt, temperatuur verhoogd' (2026Z24112).

Hoogachtend,

de minister van Volksgezondheid,
Welzijn en Sport,

Sophie Hermans

Antwoorden op Kamervragen van de leden Zwinkels en Poortman (beiden CDA) over het artikel ‘Vriezers van Franse bloedbank gehackt, temperatuur verhoogd’ (2026Z24112) (ingezonden d.d. 5 november 2026).

1.
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.
Ja, daarmee ben ik bekend. Het toenemende aantal cyberaanvallen op de zorg, in dit geval op de Franse bloedvoorziening, is een zorgelijke ontwikkeling. Een continue en vooral geïntensiveerde inspanning vanuit de zorgsector om de informatiebeveiliging op orde te hebben, is noodzakelijk om tijdig op de cyberdreigingen in te spelen en de risico’s te beperken.

2.
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?

2.
Organisaties die onder de Cyberbeveiligingswet (Cbw) vallen, moeten risico’s voor hun netwerk- en informatiesystemen in kaart brengen en hier passende en evenredige maatregelen voor nemen. Hierbij valt te denken aan incidentprocedures, continuïteits- en herstelplannen en de beveiliging van de toeleveringsketen. Om deze risico’s in kaart te brengen kunnen bestaande kaders zoals NEN 7510 en ISO 27001 als uitgangspunt dienen. Online kan iedere organisatie in de zorgsector nagaan of zij voldoet aan de wettelijk verplichte NEN 7510-norm. Dit vormt een goede basis om aan de zorgplicht van de Cbw te voldoen.

De ondersteuning voor deze organisaties bestaat onder meer uit dreigingsinformatie en expertise van Z-CERT (het Cyber Emergency Response Team voor het zorgveld). Z-CERT monitort cyberincidenten om organisaties tijdig te informeren en te waarschuwen, en verleent tijdens een significant incident hulp bij het afhandelen en afronden daarvan.

3.
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?

3.
De Cbw is sinds 15 augustus 2026 van kracht. Een organisatie die onder de Cbw valt, is wettelijk verplicht haar informatiebeveiliging op orde te hebben. Hieronder valt ook de verantwoordelijkheid om de cyberveiligheid van rechtstreekse ICT-toeleveranciers en

dienstverleners te toetsen. Denk hierbij aan leveranciers van software, netwerkdiensten en andere digitale oplossingen die de organisatie
afneemt om te kunnen functioneren. Dit betekent dat organisaties die onder de Cbw vallen, hun toeleveranciers kunnen verplichten om extra beveiligingsmaatregelen te nemen om zo de gehele keten te versterken.

De bloedbank werkt samen met publieke en private partijen om de digitale weerbaarheid van de organisatie en de continuïteit van de bloedvoorziening te versterken. Daarbij wordt gebruikgemaakt van dreigingsinformatie en veiligheidsadviezen van onder meer het Nationaal Cyber Security Centrum (NCSC), Z-CERT en andere relevante sectorale en internationale netwerken (zoals Fox-IT). Daarnaast vindt afstemming plaats met leveranciers, ketenpartners en overheidsinstanties over actuele dreigingen, kwetsbaarheden en passende beheersmaatregelen.

4.
Op welke manier werken organisaties binnen dezelfde branche of keten samen om cyberincidenten te voorkomen en informatie over kwetsbaarheden en dreigingen uit te wisselen?

4.
Het is aan de zorgorganisaties zelf om voorbereid te zijn op eventuele cyberincidenten, aangezien zij in de eerste plaats zelf verantwoordelijk zijn voor hun informatieveiligheid. Zo beschikt Sanquin over generieke crisis- en continuïteitsplannen voor de beleidsmatige reactie op een crisis, en over specifieke bedrijfsnoodplannen voor kritieke processen die noodzakelijk zijn voor de bloedvoorziening. Binnen deze plannen wordt rekening gehouden met scenario's waarbij digitale systemen, technische installaties of andere kritieke voorzieningen geheel of gedeeltelijk uitvallen. Afhankelijk van het betreffende proces worden redundante voorzieningen, alternatieve werkwijzen en fysieke terugvalmogelijkheden ingezet om de continuïteit van de dienstverlening zoveel mogelijk te waarborgen. Sanquin is bezig met het verder versterken van de weerbaarheid door het integraal benaderen van (informatie)beveiliging, continuïteit en weerbaarheid.

Z-CERT wisselt informatie uit over dreigingen en kwetsbaarheden. Daarnaast faciliteert Z-CERT de samenwerking door bijvoorbeeld bekende kwetsbaarheden bij één organisatie breed te verspreiden in de zorgsector, zodat andere organisaties zich hiertegen kunnen beschermen.

5.
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)?

5.
De minister van VWS heeft kritieke entiteiten vertrouwelijk aangewezen op basis van de essentiële diensten die zij verrichten voor de maatschappij of de volksgezondheid. Gezien de geopolitieke ontwikkelingen is ervoor gekozen om de kritieke entiteiten niet met naam en toenaam te noemen. De Inspectie Gezondheidszorg en Jeugd (IGJ) is de

toezichthouder op de kritieke entiteiten in de zorgsector en ziet erop toe of er door de kritieke entiteiten voldoende maatregelen zijn genomen in het kader van hun vertrouwelijke risicobeoordeling.

De kritieke entiteiten moeten op grond van de Wwke maatregelen treffen, onder andere om te voorkomen dat incidenten zich voordoen, de gevolgen van incidenten te bestrijden en te herstellen van incidenten. De entiteiten hebben echter na aanwijzing 10 maanden de tijd om zich hierop voor te bereiden alvorens de verplichtingen uit de wet voor hen van kracht worden. Deze periode is nog niet verstreken.

6.
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?

6.
Organisaties die onder de reikwijdte van de Cbw vallen, blijven zelf verantwoordelijk voor de beveiliging van hun netwerk- en informatiesystemen en voor het beheersen van de gevolgen van incidenten. Bij een ernstig cyberincident vindt afstemming plaats via de vastgestelde crisis- en incidentstructuren. Afhankelijk van de aard van het incident worden hierbij ook leveranciers, ketenpartners, sectorale samenwerkingsverbanden en bevoegde autoriteiten geinformeerd. Wanneer sprake is van een gedeelde kwetsbaarheid of een incident met mogelijke keteneffecten, wordt relevante informatie uitgewisseld om de impact voor andere organisaties te beperken en passende maatregelen te coördineren.

Bij een significant incident moeten organisaties die onder de Cbw vallen dit melden volgens de wettelijke meldprocedure. De wettelijke meldingen vinden plaats in het NCSC-portaal en meldingen in de sector zorg worden doorgestuurd naar Z-CERT en de IGJ. Z-CERT kan vervolgens ondersteuning bieden bij de afhandeling en dreigingsinformatie delen.

Wanneer een significant incident gevolgen heeft voor de ontvangers van haar diensten (zoals ketenpartners), moeten zij de afnemers van haar diensten informeren over significante incidenten die een nadelige invloed kunnen hebben op de verlening van die diensten. De verantwoordelijkheid voor de eigen cyberbeveiliging en eventuele meldingen blijft bij iedere organisatie afzonderlijk.

7.
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?

7.
Ja, digitaal aangestuurde koelapparatuur valt onder de Cyber Resilience Act (CRA). Voor het op de markt brengen van digitale producten die onder de CRA vallen, gelden vanaf 11 december 2027 verplichtingen ten aanzien van het ontwerp van het product (zoals

zorgen voor bescherming tegen ongeoorloofde toegang en het beschermen van de vertrouwelijkheid van opgeslagen gegevens) en ten aanzien van de omgang met kwetsbaarheden (zoals kwetsbaarheden documenteren en beleid voeren voor het gecoördineerd openbaar maken van kwetsbaarheden). Daarnaast zijn fabrikanten verplicht om gedurende de gehele

redelijk te verwachten levensduur van het product veiligheidsupdates aan te bieden. Koelapparatuur is onder de CRA niet opgenomen als belangrijk of kritiek product. Dat betekent dat conformiteitsbeoordeling kan plaatsvinden op basis van zelfevaluatie door de fabrikant.

Sommige koelinstallaties voor specifieke medische doeleinden, waaronder sommige installaties bij bloedbanken, vallen onder de Medical Device Regulation (MDR). Daarmee zijn ze uitgezonderd van de CRA. Dit betekent niet dat er geen digitale veiligheidseisen gelden. De invulling van de cybersecurityeisen voor medische hulpmiddelen en in-vitrodiagnostica is onderwerp van de huidige onderhandelingen over de wetgeving voor medische hulpmiddelen (MDR-IVDR). In overeenstemming met het BNC-fiche hieromtrent zet het kabinet in op het creëren van betere samenhang tussen de MDR-IVDR en de Cyberbeveiligingswet.

8.
Welke verantwoordelijkheden hebben fabrikanten van dergelijke apparatuur op grond van de CRA met betrekking tot cybersecurity en het tijdig verhelpen van kwetsbaarheden?

8.
Fabrikanten moeten zoals onder vorige vraag beschreven vanaf 11 december 2027 op grond van de CRA zorgen dat hun producten digitaal veilig op de markt worden gebracht en gedurende de redelijk te verwachten levensduur veiligheidsupdates verstrekken. Daarnaast moeten fabrikanten al sinds 11 september 2026 geëxploiteerde kwetsbaarheden en incidenten melden. Als er een kwetsbaarheid wordt ontdekt, moet daarvoor zo snel mogelijk een gratis veiligheidsupdate worden verstrekt (bij zakelijke overeenkomsten mag contractueel worden afgesproken dat hiervoor kosten in rekening worden gebracht). Fabrikanten moeten zorgen dat hun producten worden aangeboden met de instelling dat updates in beginsel automatisch worden geïnstalleerd (met een opt-out en een uitzondering voor producten voor industriële omgevingen).

9.
Hoe is de juridische verantwoordelijkheid verdeeld tussen fabrikanten, leveranciers en gebruikers wanneer apparatuur, zoals koelinstallaties, door een cyberaanval wordt getroffen?

9.
Vanuit de CRA gelden verplichtingen voor fabrikanten, zoals beschreven onder vraag 7 en 8. Voor de MDR geldt dat de verdeling van verantwoordelijkheid momenteel onderwerp is van lopende onderhandelingen.

Fabrikanten en leveranciers van apparatuur, zoals koelinstallaties, vallen niet automatisch onder de reikwijdte van de Cyberbeveiligingswet (Cbw). Een gebruiker van de apparatuur, bijvoorbeeld een zorgaanbieder die onder de Cbw valt, moet een incident

melden wanneer dit voldoet aan de criteria voor een significant incident. Dat kan bijvoorbeeld het geval zijn als sectorspecifieke drempelwaarden worden geraakt.

10.
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?

10.
De aanvallen die plaatsvonden in de nacht van 11 op 12 oktober 2026 tegen koelapparatuur in Franse supermarkten zijn door de Franse autoriteiten toegeschreven aan de Iraanse statelijke hackersgroep Shahid Kaveh, die deel uitmaakt van de Islamitische Revolutionaire Garde. Overige aanvallen, zoals de aanval die aanleiding was voor deze Kamervragen, zijn voor zover bekend nog niet geattribueerd.

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)