

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
www.rijksoverheid.nl

Kenmerk
1671841-204015-DICIO

Bijlage(n)
-

Uw brief
204015

Datum 14 april 2020
Betreft Beleidsreactie OVV op het onderzoeksrapport Patiëntveiligheid bij ICT-
uitval in ziekenhuizen

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

Geachte voorzitter,

Op 18 februari jl. heb ik uw Kamer het rapport van de Onderzoeksraad voor Veiligheid (hierna OVV) 'Patiëntveiligheid bij ICT-uitval in ziekenhuizen' gezonden¹. Daarbij heb ik aangegeven het rapport van de OVV te bestuderen en binnen acht weken met een beleidsreactie te komen. Ik onderschrijf volledig de aanvullende aandacht die de OVV vraagt voor informatieveiligheid in de zorg.

Conclusie OVV: Ziekenhuizen niet goed voorbereid

Het rapport van de OVV richt zich op de risico's van de toenemende ICT-afhankelijkheid in ziekenhuizen. Op basis van eigen onderzoek concludeert de OVV dat ziekenhuizen niet goed voorbereid zijn op ICT-storingen. De kwaliteit en veiligheid van de zorg voor patiënten kan daardoor in het geding komen. Volgens de OVV zijn ziekenhuizen zo gedigitaliseerd dat het leveren van goede zorg zonder ICT bijna niet meer mogelijk is. "Een defect onderdeel of verkeerde netwerkinstelling kan de primaire zorgprocessen in een ziekenhuis uren- of zelfs dagenlang stilleggen met eventueel enorme gevolgen voor patiëntveiligheid", aldus de OVV. Het rapport beschrijft dat er tijdens een ICT-storing of een cyberaanval veel aandacht voor de patiënt is, maar er na afloop nauwelijks aandacht is voor wat de gevolgen van de storing hadden kunnen zijn voor de patiënt en de schade voor de continuïteit van de zorg als geheel.

Waardering voor de conclusies van het OVV

Ik onderschrijf de aanbeveling dat ziekenhuizen meer aandacht moeten besteden aan risicovolle situaties als gevolg van een ICT-storing of cyberaanval. De OVV wijst ons er terecht op dat ICT een belangrijk instrument is om de kwaliteit van zorg en de patiëntveiligheid te ondersteunen. Uitgangspunt in ons zorgstelsel is hierbij dat alle zorginstellingen primair zelf verantwoordelijk zijn voor hun informatieveiligheid. Dat betekent ook het treffen van de nodige maatregelen ter verhoging van digitale weerbaarheid om de continuïteit van de zorg te waarborgen.

De IGJ is verantwoordelijk voor het toezicht op deze zorgcontinuïteit. De IGJ heeft

¹ TK 2019-2020, 31 016 nr. 281

in haar toezicht op de ziekenhuizen aandacht voor dit onderwerp. Zo focust het toetsingskader E-Health² van de IGJ op het aanwezig zijn van de juiste randvoorwaarden voor de inzet van ICT door zorgaanbieders. Bij inspecties komt aan de orde welke voorzieningen en plannen bij ziekenhuizen aanwezig zijn om op storingen te kunnen reageren. De IGJ herkent zich in het beeld dat de OVV schetst. Er is nog te weinig bewustzijn van de risico's van afhankelijkheid van ICT voor de continuïteit van de zorg en de hiervoor te treffen noodzakelijke maatregelen. Dit geldt ook op het gebied van informatiebeveiliging in de ziekenhuizen. Naar aanleiding van de aanbevelingen van de OVV zal de IGJ dit onderwerp nog uitgebreider meenemen in de gesprekken met het veld en het toezicht verder invulling geven.

Kenmerk
1671841-204015-DICIO

Digitale weerbaarheid van de Nederlandse zorgsector verhogen

Ondersteunen verhoging bewustwording

Goede zorg kan niet zonder goede informatievoorziening. Sinds medio 2019 is de vereniging Brancheorganisaties Zorg (BOZ) met het breed gedragen project 'Informatieveilig gedrag' actief bezig om zorgverleners bewuster en veiliger om te laten gaan met informatie in de dagelijkse praktijk. Het doel is de beschikbaarheid, juistheid en vertrouwelijkheid van informatie te blijven borgen. De verandering die dit project uiteindelijk wil bewerkstelligen, is dat zorgorganisaties effectieve interventies voor gedragsverandering kennen en gebruiken voor hun belangrijkste informatieveiligheidsproblemen. Dit project sluit aan bij de ontwikkelingen van veilige en betrouwbare elektronische gegevensuitwisseling binnen de zorg. Ik ondersteun financieel dit initiatief vanuit de zorgsector.

Versterken van Z-CERT

Ik vind het van het grootste belang dat de gegevens van patiënten en zorginstellingen veilig zijn en daarom hecht ik eraan dat de zorginstellingen bij het treffen van maatregelen worden ondersteund door Z-CERT, het cybersecuritycentrum voor de zorg. Z-CERT heeft als cyberinformatieknoppunt voor de Nederlandse zorgsector een unieke positie weten op te bouwen, waarbij vertrouwen, onafhankelijkheid en professioneel handelen centraal staan. Inmiddels zijn alle ziekenhuizen (al dan niet via de koepelorganisatie) aangesloten bij Z-CERT. Daarnaast zijn ook de categorale instellingen zoals revalidatiecentra en diagnostische centra aangesloten voor zover ze lid zijn van de NVZ, evenals een aantal instellingen voor geestelijke gezondheidszorg (GGZ) en een aantal care- en jeugdhulpinstellingen. Los van de uitdagingen zoals geschetst in het OVV-rapport heeft het belang van Z-CERT zich voor de Nederlandse zorgsector bewezen, zoals recent met het ondersteunen van aangesloten en de niet aangesloten instellingen rondom de Citrix kwetsbaarheid en de huidige coronacrisis. In nauwe samenwerking met het Nationaal Cyber Security Center (NCSC) werkt Z-CERT momenteel hard aan het verhogen van de digitale weerbaarheid. Hiertoe worden de ziekenhuizen opgenomen in het Nationaal Detectie Netwerk (NDN) van het NCSC waarmee actuele dreigingsinformatie kan worden uitgewisseld en in een platform waarmee mogelijke cyberkwetsbaarheden van de ziekenhuizen in kaart wordt gebracht.

² www.igj.nl/documenten/toetsingskaders/2019/10/18/toetsingskader-inzet-van-e-health-door-zorgaanbieders

Ik vind het erg belangrijk dat meer zorginstellingen zich aansluiten bij Z-CERT. De motie van het Kamerlid Ellemet³ vraagt mij of deelname aan Z-CERT verplicht kan worden gesteld. In mijn brief *Informatieveiligheid in zorg* in september van dit jaar zal ik de voortgang van mijn onderzoek met uw Kamer delen.

Kenmerk
1671841-204015-DJIC/O

Herbeoordelen van de zorg als vitale sector

De OVV staat in haar rapport stil bij het besluit van VWS om de zorgsector niet als 'vitaal'⁴ te verklaren. Zij stelt dat VWS een aantal jaar geleden besloten heeft om de ziekenhuizen en andere zorgaanbieders niet als vitaal te identificeren en dat VWS dit besluit momenteel heroverweegt, wat ertoe kan leiden dat delen van de zorg (al dan niet voor specifieke processen/onderdelen) in 2020 als vitaal zouden worden aangewezen. In mijn eerste brief *Informatieveiligheid en Privacy in de zorg* en tijdens het *AO Gegevensuitwisseling van 9 oktober jl.*⁵ heb ik uw Kamer toegezegd een herbeoordeling van (delen van) de zorg als vitaal proces te willen verkennen. Ik kan u zeggen dat deze verkenning loopt. Daarin wordt ook meegenomen of het aanwijzen van bepaalde delen van de zorgsector als vitaal tot betere informatiebeveiliging in ziekenhuizen leidt. In de eerste helft van volgend jaar zal ik in een aparte brief de voortgang van de herbeoordeling met uw Kamer delen.

Waarborgen van zorgcontinuïteit in tijden van digitale storingen

Het 'ononderbroken functioneren van digitale systemen', is cruciaal en is tegelijk een vraagstuk dat continue aandacht van de zorgsector behoeft om de zorgcontinuïteit te kunnen waarborgen. Meer inzicht en bewustzijn in de risico's en gevolgen van ICT-storingen, draagt bij aan een meer adequate sturing van dit vraagstuk. De OVV doet hiervoor al goede aanbevelingen. Ik onderschrijf daarbij de aanbeveling van de OVV het vraagstuk gezamenlijk met de sector te benaderen. Ik zal hiertoe verkennen of en op welke wijze de (bestaande) regionale ketenverbanden en structuren hieraan vorm kunnen geven.

Voorts wil ik onderzoeken welke aanvullende maatregelen kunnen bijdragen om de zorgsector te stimuleren meer aandacht te geven aan dit vraagstuk en daarmee zich beter voor te bereiden op het beheersen van de gevolgen van ICT-storingen. Daarbij wil ik bijvoorbeeld kijken naar de mogelijkheden om in bestaande stimuleringsregelingen nadrukkelijker aandacht hieraan te geven.

Tot slot

³ TK 2018-2019, 27 529 nr. 177

⁴ Voor de implementatie van de Europese NIB-richtlijn (Netwerk & Informatiebeveiliging richtlijn) worden Rijksbreed de criteria voor vitale Infrastructuur gebruikt om te bepalen of een sector als vitaal kan aangemerkt worden. In Nederland is de NIB-richtlijn geïmplementeerd in de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni). Er is onderscheid gemaakt tussen de categorie A en de categorie B om recht te doen aan de diversiteit binnen de vitale infrastructuur, om te kunnen prioriteren bij onder andere incidenten en om maatwerk bij weerbaarheid verhogende maatregelen mogelijk te maken. Voor de vitaliteitsbeoordeling hanteren we Categorie B. In deze categorie staat de infrastructuur die bij verstoring, aantasting of uitval de ondergrenzen van minstens één van de drie impactcriteria voor categorie B raakt:

Economische gevolgen: > ca. 5 miljard euro schade of ca. 1.0 % daling reëel inkomen
Fysieke gevolgen: meer dan 1.000 personen dood, ernstig gewond of chronisch ziek
Sociaal maatschappelijke gevolgen: meer dan 100.000 personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen

⁵ TK 2018-2019, 27 529 nr. 193

Samen met het veld wil ik graag werk maken van de adviezen van de OVV. De OVV wijst ons er terecht op dat ICT een belangrijk instrument is om de kwaliteit van zorg en de patiëntveiligheid te ondersteunen. Tegelijkertijd brengt het gebruik van ICT ook risico's met zich mee. Door de versnelling van de ontwikkelingen qua dreiging, technologie en afhankelijkheden in de zorg worden deze vraagstukken de komende jaren alleen maar urgenter. Het OVV-rapport helpt om hiermee gericht aan de slag te gaan.

Kenmerk
1671841-204015-DJGLO

Hoogachtend,

de minister van Volksgezondheid,
Welzijn en Sport,

Let op: vul A.U.B. de naam van de ondertekenaar NIET handmatig in. Dit tekstvak mag ALLEEN worden verwijderd op het moment dat het stuk in "Printen en Verzenden" zit en de ondertekening volledig is. De naam van de ondertekenaar wordt automatisch door Marjolein ingevuld, vlak voordat het stuk ter ondertekening wordt aangeboden.