Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1981

Vragen van de leden **Rajkowski** en **Tielen** (beiden VVD) aan de Minister van Volksgezondheid, Welzijn en Sport over *het bericht «Ziekenhuizen kwetsbaar voor cyberaanval: Wachten totdat het misgaat»* (ingezonden 15 februari 2022).

Antwoord van Minister **Kuipers** (Volksgezondheid, Welzijn en Sport) (ontvangen 8 maart 2022).

Vraag 1
Bent u bekend met het bericht «Ziekenhuizen kwetsbaar voor cyberaanval: Wachten totdat het misgaat» van 26 januari jongstleden?[1]

Antwoord 1
Ja.

Vraag 2
Deelt u de zorgen bij het lezen van de constatering van beveiligingsexperts dat Nederlandse ziekenhuizen nog altijd kwetsbaar zijn voor cyberaanvallen? Zo nee, wat is dan uw oordeel over deze constatering?

Antwoord 2
Ik deel de zorgen dat er een toename is aan veiligheidsdreigingen voor zorginstellingen door een toename van cyberaanvallen. Tegelijkertijd kunnen cyberaanvallen nooit helemaal worden voorkomen. Informatiebeveiliging vraagt daarmee continue aandacht om de beschikbaarheid, integriteit en vertrouwelijkheid van (patiënt)informatie te waarborgen. Zorgaanbieders, zoals ziekenhuizen, moeten daar alert op zijn. Zij zijn verantwoordelijk voor het op orde hebben en houden van hun informatiebeveiliging. Onderdeel daarvan is het voldoen aan de wettelijk verplichte NEN 7510-norm die de kaders stelt om beschikbaarheid, integriteit en vertrouwelijkheid van medische gegevens te borgen. Daarnaast worden ziekenhuizen ondersteund door Z-CERT (het Computer Emergency Response Team voor de zorg) bij (dreigende) cyberincidenten en bij het vergroten van hun digitale weerbaarheid. Er zijn de laatste jaren door de ziekenhuizen al grote stappen gezet op het gebied van informatiebeveiliging, waaronder ook het aantoonbaar

[1] Nu.nl, 26 januari 2022, «Ziekenhuizen kwetsbaar voor cyberaanval: Wachten totdat het misgaat» (www.nu.nl/tech/6178900/ziekenhuizen-kwetsbaar-voor-cyberaanval-wachten-totdat-het-misgaat.html).

ah-tk-20212022-1981
ISSN 0921 - 7398
's-Gravenhage 2022

voldoen aan de NEN 7510. Dit komt ook naar voren in het recent gepubliceerd inspectierapport van de Inspectie Gezondheidzorg en Jeugd (IGJ) bij ziekenhuizen[2]. Ziekenhuizen die op het moment van het inspectiebezoek hun informatiebeveiliging niet op orde hadden, hebben na het inspectiebezoek beveiligingsmaatregelen genomen waaronder het aantoonbaar voldoen aan de NEN7510 norm.

Vraag 3
Hoeveel Nederlandse ziekenhuizen en andere zorginstellingen zijn in 2021 geraakt door cyberaanvallen, en hoeveel in 2020 en 2019? Om welk type cyberaanvallen ging het in die gevallen? In hoeveel gevallen is de continuïteit van zorg in gevaar gekomen als gevolg van een cyberaanval?

Antwoord 3
Cybercrime en het aantal cyberincidenten nemen in rap tempo toe. Het is niet bekend hoeveel zorginstellingen in 2021, 2020 en 2019 precies geraakt zijn door cyberaanvallen. Daarvan is geen meldingsplicht. Wel heeft Z-CERT op mijn verzoek gemeld dat er in de afgelopen drie jaar ruim 1300 hulpverzoeken en (cyber)incidenten zijn gemeld bij Z-CERT. Met name in 2021 is het aantal meldingen fors gestegen. Dit komt mede omdat er in 2021 een grote groep nieuwe deelnemers is aangesloten. Onder andere meldden in 2021 vijf zorginstellingen te zijn geraakt door een ransomware-aanval, vier meer dan in 2020 aldus Z-CERT in haar recent *gepubliceerde «Cyber Dreigingsbeeld in de zorg 2021»*[3]. In 2019 werden 176 en in 2020 182 hulpverzoeken gemeld bij Z-CERT.

Vraag 4
Deelt u de mening dat het zorgelijk is dat beveiligingsexperts constateren dat de zorgsector qua digitale beveiliging achterloopt op andere sectoren? Hoe beoordeelt u dit in het licht van het vitale karakter van zorgprocessen?

Antwoord 4
De beveiliging en beschikbaarheid van ICT in de zorg verdienen blijvend aandacht. Mijn beleid focust zich op het verhogen van bewustwording van de noodzaak tot beveiliging van de gevoelige persoonsgegevens die juist in de gezondheidszorg zo'n grote rol spelen. Ik herken mij niet in het beeld dat de zorgsector achter zou lopen op andere sectoren als het gaat om digitale weerbaarheid. Er zijn de laatste jaren door de ziekenhuizen en andere zorginstellingen grote stappen gezet op het gebied van informatiebeveiliging, waaronder het verhogen van cyberbewustwording, het (collectief) aansluiten bij Z-CERT en ook het aantoonbaar voldoen aan de wettelijk verplichte NEN 7510.

Vraag 5
Klopt het dat de Inspectie Gezondheidszorg en Jeugd (IGJ) in 2021 al concludeerde dat de informatiebeveiliging van de meeste ziekenhuizen niet voldoet aan de gestelde eisen? Zo ja, welke consequenties zijn er voor ziekenhuizen die hier niet aan voldoen? Zijn sinds de conclusie van de Inspectie stappen gezet om de informatiebeveiliging van deze ziekenhuizen op het juiste niveau te krijgen? Zo ja, welke? Zo nee, waarom niet?

Antwoord 5
Het artikel van Nu.nl refereert aan een publicatie van de IGJ van december 2021 over het toezicht op e-health bij 22 ziekenhuizen («Professionele digitale zorg vraagt van ziekenhuizen steeds opnieuw evalueren en verbeteren»). De inspectiebezoeken vonden plaats in de periode tussen september 2017 en oktober 2021. Hierbij keek de inspectie onder andere naar het thema informatiebeveiliging: ziekenhuizen moeten een managementsysteem voor informatiebeveiliging hebben dat voldoet aan de wettelijk verplichte norm NEN 7510. Een onderdeel van deze norm is dat een onafhankelijke beoordeling van het managementsysteem voor informatiebeveiliging aanwezig moet

[2] 73298_IGJ_Factsheet.pdf (Professionele digitale zorg vraagt van ziekenhuizen steeds opnieuw evalueren en verbeteren)
[3] Z-CERT_RapportDreigingsbeeld_2021.pdf

zijn. Bij meer dan de helft van de bezochte ziekenhuizen bleek dit op het moment van het inspectiebezoek niet het geval. De ziekenhuizen die onvoldoende konden aantonen dat zij voldeden aan de norm, kregen de opdracht van de inspectie om dit alsnog aan te tonen. Dit betekende in de praktijk dat de meeste van deze ziekenhuizen alsnog een onafhankelijke beoordeling moesten laten uitvoeren en zo nodig naar aanleiding van de uitkomsten een verbeterplan moesten doorvoeren.
De desbetreffende ziekenhuizen gaven hieraan gehoor. Bij acht ziekenhuizen heeft dit er vervolgens toe geleid dat zij een (niet wettelijk verplicht) certificaat hebben behaald voor NEN 7510. Uit de publicatie van de IGJ van december 2021 kunnen geen conclusies worden getrokken over de ziekenhuizen die niet zijn bezocht. In de publicatie van de inspectie roept de inspectie alle ziekenhuizen op om hun informatiebeveiliging snel aantoonbaar op orde te krijgen voor zover dat nu nog niet het geval is. De inspectie zal ook andere ziekenhuizen hierop in de toekomst aanspreken als bij een thematisch bezoek blijkt dat de informatiebeveiliging niet aantoonbaar voldoet aan de norm.

Vraag 6
Welke maatregelen nemen ziekenhuizen al dan niet in samenwerking met Z-CERT, om cyberaanvallen te voorkomen? In hoeverre wordt bijvoorbeeld geoefend met Z-CERT op cyberincidenten? In hoeverre wordt de Kwetsbaarheden Analyse Tool (KAT) al ingezet binnen de zorgsector om doorlopend te scannen op kwetsbaarheden?

Antwoord 6
In de afgelopen jaren hebben ziekenhuizen extra beveiligingsmaatregelen getroffen om de toenemende cyberdreiging het hoofd te bieden. De wettelijk verplichte NEN 7510 norm biedt hiervoor een goed kader. Ook zien we dat steeds meer ziekenhuizen zich laten certificeren tegen deze NEN norm. Met onder meer de publicatie van richtlijnen ter voorkoming van ransomware en met het organiseren van webinars draagt Z-CERT bij aan het vergroten van het bewustzijn en het treffen van adequate maatregelen. Z-CERT informeert en adviseert ziekenhuizen dagelijks over dreigingen en incidenten met betrekking tot hun zorginformatiesystemen. Ook helpt Z-CERT-ziekenhuizen zich voor te bereiden op (en om te gaan met) ernstige ICT-incidenten of ICT-crises. Deze inspanningen dragen bij aan het voorkomen van cyberincidenten. In samenwerking met een aantal ziekenhuizen voert Z-CERT op beperkte schaal al cyberoefeningen uit. Het voornemens is om in de komende jaren verder te investeren in het organiseren van cyberoefeningen bij ziekenhuizen en andere deelnemers van Z-CERT. Dat ondersteun ik.
De Kwetsbaarheden Analyse Tool (KAT) wordt op dit moment specifiek toegepast in het zorgdomein. Thans loopt er een project bij Z-CERT om deze dienst in te richten en te operationaliseren en deze beschikbaar te stellen aan zorginstellingen. Dit in aanvulling op andere middelen die worden ingezet om deelnemers van Z-CERT te controleren op kwetsbaarheden en proactief te waarschuwen.

Vraag 7
Deelt u de mening dat het van groot en urgent belang is dat ziekenhuizen maatregelen treffen, zeker gezien de COVID-19-crisis, om cyberaanvallen te voorkomen? Zo ja, bent u bereid om op korte termijn mét de sector en Z-CERT te werken aan maatregelen om zorginstellingen, zoals ziekenhuizen, digitaal weerbaar te maken? Op welke termijn verwacht u de Kamer hierover te kunnen informeren? Zo nee, waarom niet?

Antwoord 7
Ik vind het van belang dat zorginstellingen de aan hun toevertrouwde informatie beveiligen en beschermen. Tegelijkertijd zullen er in de digitale wereld altijd cyberrisico's blijven. Het is zaak die te onderkennen, zoveel mogelijk te mitigeren, voortdurend te bewaken en in te grijpen bij (dreigende) verstoringen. Zorginstellingen moeten daar alert op zijn aangezien zij zelf verantwoordelijk zijn voor het op orde hebben en houden van hun informatiebeveiliging. Ik werk momenteel al samen met de sector en Z-CERT om de zorg weerbaarder te maken.
Ik ondersteun Z-CERT met het risicogestuurd uitbreiden van het aantal deelnemers. Z-CERT heeft nu ruim 200 zorginstellingen aangesloten. Dit is

een verdubbeling ten opzichte van een jaar eerder. Daarnaast werk ik samen met Z-CERT om openbare diensten en producten te ontwikkelen zoals de reeds verschenen *«handreiking verlopen domeinnamen» Z-CERT_Handreiking2021.pdf*. Deze handreiking helpt bij het proactief en continu monitoren op kwetsbaarheden van verlopen zorgdomeinnamen.
Om bewustwording over informatiebeveiliging in de zorg te verhogen heb ik in samenwerking met Brancheorganisaties Zorg de wegwijzer «*Aan de slag met Informatieveilig gedrag»* ontwikkeld en deze medio 2021 beschikbaar gesteld aan het veld[4]. De wegwijzer helpt zorginstellingen om de informatieveiligheid te verbeteren en helpt hen ook concreet bij het voldoen aan de wettelijk verplichte NEN 7510. In mijn volgende Kamerbrief over elektronische gegevensuitwisseling in de zorg zal ik uw Kamer nader informeren over de vorderingen op het gebied van informatieveiligheid in de zorg.

[4] Focus op gedrag voor meer informatieveiligheid – Brancheorganisaties Zorg