Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

Aanhangsel van de Handelingen

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

1880

Vragen van de leden **Van den Berg** en **Slootweg** (beiden CDA) aan de Minister van Volksgezondheid, Welzijn en Sport en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *recente berichten over ict-storingen en cyberaanvallen in onder andere het Maastricht UMC en het UMC Groningen* (ingezonden 22 februari 2023).

Antwoord van Minister **Kuipers** (Volksgezondheid, Welzijn en Sport), mede namens de Minister van Justitie en Veiligheid (ontvangen 16 maart 2023).

Vraag 1
Bent u bekend met de recente berichten over ict-storingen en cyberaanvallen in onder andere het Maastricht UMC en het UMC Groningen?[1, 2, 3]

Antwoord 1
Ja.

Vraag 2 en 3
Kunt u toelichten om wat voor soort ict-storing het in deze gevallen precies gaat? Gaat het om ondersteunende processen of zijn ook vitale processen geraakt?
Welke gevolgen heeft de ict-storing bij het Maastricht UMC gehad voor operaties, behandelingen en afspraken van patiënten?

Antwoord 2 en 3
Op 28 januari kregen aan aantal Nederlandse ziekenhuizen te maken met DDoS aanvallen. Tijdens de DDoS-aanvallen waar de artikelen naar verwijzen is de zorgcontinuïteit niet in het geding geweest. De aanvallen hebben vooral geleid tot het beperkt beschikbaar zijn van de websites van ziekenhuizen. Ziekenhuizen zijn via andere kanalen wel bereikbaar gebleven.
Op 14 februari was er in het Maastricht UMC+ een ICT-storing. Er was een technische storing in het EPD waardoor niet naar behoren met het systeem

[1] NOS, 14 februari 2023, «Ict-storing: nauwelijks operaties en poli in Maastricht UMC» (Ict-storing: nauwelijks operaties en poli in Maastricht UMC (nos.nl))
[2] Telegraaf, 11 februari 2023, «Dokters bibberen voor cyberaanval: «Grote hack is een kwestie van tijd»» (Dokters bibberen voor cyberaanval: «Grote hack is een kwestie van tijd» | Financieel | Telegraaf.nl)
[3] Skipr, 30 januari 2023, «UMCG getroffen door Russische cyberaanval, meer ziekenhuizen onder vuur» (UMCG getroffen door Russische cyberaanval, meer ziekenhuizen onder vuur – Skipr)

ah-tk-20222023-1880
ISSN 0921 - 7398
's-Gravenhage 2023

gewerkt kon worden. Hierbij was geen sprake van een cybersecurity incident. Er is naar aanleiding van de storing besloten in de ochtend het merendeel van de poli's en operaties af te zeggen. De reden hiervoor was het waarborgen van de patiëntveiligheid. Ook het afnemen van bloed is tijdelijk niet mogelijk geweest. Spoedeisende zorg en overige zorgprocessen zijn niet verstoord.

Vraag 4
Wordt informatie over de (evaluatie van een) storing bij een bepaald ziekenhuis standaard gedeeld met andere ziekenhuizen, zodat zij hiervan kunnen leren? Zo nee, waarom niet?

Antwoord 4
Het Computer Emergency Response Team voor de zorg (Z-CERT) deelt dreigings- en incidentinformatie onder hun leden, waar het gaat om IT-beveiliging. Alle Nederlandse ziekenhuizen die lid zijn van de Nederlandse Federatie van Universitair Medische Centra (NFU) of de Nederlandse Vereniging van Ziekenhuizen (NVZ) zijn aangesloten bij Z-CERT. Door gebruik te maken van de diensten van Z-CERT zoals het Zorgdetectienetwerk, kunnen ziekenhuizen informatie over incidenten met elkaar en andere zorginstellingen delen. Z-CERT deelt geen incidentinformatie onder hun leden wanneer het gaat om generieke ICT-storingen.

Vraag 5
Ben u mening dat deze storing en de eerdere cyberaanvallen incidenten zijn of is er sprake van structurele en toenemende risico's voor ziekenhuizen op het gebied van ict-veiligheid?

Antwoord 5
Z-CERT, het Nationaal Cyber Security Center (NCSC) of hun (internationale) partners hebben niet eerder kennisgenomen dat Nederlandse ziekenhuizen doelwit waren van een DDoS-aanval. Uit het dreigingsbeeld dat Z-CERT jaarlijks publiceert blijkt echter wel dat het risico van cyberaanvallen op zorgorganisaties toeneemt[4]. Zorginstellingen zijn daarnaast in toenemende mate afhankelijk van ICT-middelen. Versterking van de digitale weerbaarheid van het zorgveld is daarom des te belangrijker. Mijn beleid is daar ook op gericht. Ik ga hier verder op in bij de beantwoording van vraag 13.

Vraag 6
Kunt u een update geven van de status van de maatregelen die ziekenhuizen moeten nemen om de deadline van de Inspectie Gezondheidszorg en Jeugd (IGJ) te halen om eind 2023 aan de wettelijke norm voor informatiebeveiliging (NEN 7510) te voldoen? Zijn alle ziekenhuizen goed op weg om deze deadline te halen?

Antwoord 6
Om aan de wettelijke norm voor informatiebeveiliging (NEN 7510) te voldoen moeten ziekenhuizen een managementsysteem voor informatiebeveiliging inrichten. Dit houdt in dat zij op basis van een risicoanalyse vaststellen welke beheersmaatregelen voor informatiebeveiliging zij gaan inrichten. Na het inrichten van deze beheersmaatregelen moeten zij geregeld controleren of de maatregelen werken zoals bedoeld en zo nodig nadere maatregelen nemen. Dit heet ook wel een kwaliteitscyclus of plan-do-check-act cyclus. De NEN 7510 vereist dat een ziekenhuis beschikt over een onafhankelijke beoordeling van de informatiebeveiliging.
De Inspectie Gezondheidszorg en Jeugd (IGJ) besteed al geruime tijd aandacht aan de status van informatiebeveiliging bij ziekenhuizen. Zie hiervoor ook de eerder gepubliceerde factsheets Professionele digitale zorg vraagt van ziekenhuizen steeds opnieuw evalueren en verbeteren[5] en

[4] Z-CERT presenteert tweede Cybersecurity Dreigingsbeeld voor de zorg – Z-CERT
[5] Professionele digitale zorg vraagt van ziekenhuizen steeds opnieuw evalueren en verbeteren | Rapport | Inspectie Gezondheidszorg en Jeugd (igj.nl)

ICT-storingen in ziekenhuizen: lessen voor bestuurders en ICT-managers[6]. In juni 2022 heeft de IGJ van alle ziekenhuizen in kaart gebracht of zij aantoonbaar voldeden aan de norm.
Het voortgangsbeeld is nog in beweging. Inmiddels heeft een groot deel van de ziekenhuizen een onafhankelijke beoordeling uitgevoerd. Waar dat nodig is gebleken, zijn de ziekenhuizen bezig om de daaruit voortgekomen noodzakelijke verbetermaatregelingen door te voeren. De IGJ heeft lopende afspraken over de voortgang met alle ziekenhuizen die nog niet aantoonbaar aan de norm voldoen. Waar nodig zal de IGJ te zijner tijd handhavingsmaatregelen overwegen bij ziekenhuizen waar de informatiebeveiliging onvoldoende is.

Vraag 7 en 8
Het klopt toch dat alle grote zorgorganisaties zoals ziekenhuizen en ggz-instellingen al jaren verplicht aangesloten zijn bij Z-Cert?
Is intussen voor kleinere zorgaanbieders, zoals wijkverpleging, huisartsen, apothekers, ook aansluiting bij Z-Cert verplicht, aangezien daar ook veel gevoelige informatie is opgeslagen? Zo nee, waarom niet en wanneer gaat dit dan wel gebeuren?

Antwoord 7 en 8
Er bestaat geen wettelijke verplichting voor zorgorganisaties om zich aan te sluiten bij Z-CERT. Echter, alle Nederlandse ziekenhuizen die lid zijn van de Nederlandse Federatie van Universitair Medische Centra (NFU) of de Nederlandse Vereniging van Ziekenhuizen (VVZ) zijn deelnemer van Z-CERT. Het zelfde geldt voor de Nederlandse GGZ instellingen. Daarnaast worden steeds meer zorgaanbieders uit andere (sub-)sectoren lid. Het Ministerie van VWS beleid is erop gericht de dienstverlening van Z-CERT zo breed mogelijk beschikbaar te stellen binnen de gehele zorgsector. Het Ministerie van VWS kiest er daarbij voor om de aansluiting van aanbieders en sectoren te organiseren op basis van een risico-gebaseerde aansluitstrategie. Dit is in oktober 2021 aan uw Kamer gecommuniceerd in een Kamerbrief.[7] Deze strategie houdt in dat (sub-)sectoren met de grootste risico's op cyberaanvallen – en de daarbij behorende impact – geprioriteerd worden aangesloten bij Z-CERT. Daarbij wordt rekening gehouden met het absorptievermogen van Z-CERT. Op dit moment zijn bijna 300 instellingen uit verschillende (sub-)sectoren aangesloten bij Z-CERT.

Vraag 9
Begrijpen wij correct dat Z-CERT ook gehackt is, terwijl Z-Cert juist degene is die zorgorganisaties moet attenderen op potentiële bedreigingen?

Antwoord 9
Nee, dat is niet correct. Z-CERT is niet gehackt. De website van Z-CERT heeft kortdurend hinder ondervonden van een DDoS-aanval. Dit heeft geen invloed gehad op de dienstverlening van Z-CERT.

Vraag 10
Controleert Z-Cert ook bij zorgorganisaties of men de updates heeft geïnstalleerd? Zo nee, waarom niet en hoe wordt in dat geval toezicht gehouden?

Antwoord 10
Het zorgdragen voor de implementatie van de juiste ICT-producten, inclusief daarbij horende latere aanpassingen, is een eigen verantwoordelijkheid van zorgaanbieders. Z-CERT ziet niet toe op welke aanpassingen wel of niet worden geïnstalleerd, maar ondersteunt aangesloten zorginstellingen bij het zelf zorgdragen voor een afdoende veiligheidsniveau, en biedt hulp bij incidenten. Het toezicht op informatieveiligheid van zorgaanbieders is belegd bij de Inspectie Gezondheidszorg en Jeugd (IGJ). De toetsingseisen die IGJ hanteert staan beschreven in het E-health toetsingskader en zijn onder andere gebaseerd op de wettelijke verplichte NEN-normen voor informatieveiligheid in de zorg, waaronder de NEN-7510. Onderdeel van de NEN norm 7510 is dat

[6] ICT-storingen in ziekenhuizen: lessen voor bestuurders en ICT-managers | Publicatie | Inspectie Gezondheidszorg en Jeugd (igj.nl)
[7] Kamerstuk 27 529, nr. 268

zorginstellingen kwetsbaarheden in hun software, bv. door middel van patches, moeten mitigeren.

Vraag 11
In hoeverre heeft de NCTV nu ook zorgorganisaties toegevoegd indien bedreigingen worden vastgesteld?

Antwoord 11
De NCTV heeft een coördinerende rol bij de ontwikkeling van het beleid rond de bescherming van de Nederlandse vitale infrastructuur. Hierbij zijn de verschillende vakdepartementen, waaronder het Ministerie van Volksgezondheid, Welzijn en Sport, verantwoordelijk voor de sectoren die binnen hun beleidsdomein vallen. Ik zal u uiterlijk voor de zomer per Kamerbrief informeren over de stand van zaken van het aanwijzen van de zorgsector als vitale sector. In deze brief wordt u ook geïnformeerd over de implementatie van de herziene richtlijn voor Netwerk- en Informatiebeveiliging (NIB2) en de richtlijn Veerkracht van Kritieke Entiteiten (CER) in het zorgveld.

Vraag 12
Gaat u minimumeisen stellen aan programma's zodat slecht beveiligde programma's uitgebannen worden? Zo nee, waarom niet?

Antwoord 12
De Europese Commissie heeft in september 2022 een voorstel gedaan voor een *Cyber Resilience Act* (CRA). In deze verordening worden fabrikanten, importeurs en distributeurs van hard- en software die in de EU in de handel wordt gebracht verplicht er zorg voor te dragen dat deze voldoen aan de daar gestelde cybersecurityvereisten. Deze beveiligingseisen zullen ook gelden voor software in de zorg. Het Kabinet is positief over het voorstel. Over de inhoud van de CRA wordt momenteel nog onderhandeld. Naast de CRA zijn er reeds Europese verordeningen over medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek (2017/745 en 2017/746) van kracht. Deze verordeningen stellen ook eisen aan de software die gebruikt wordt in medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek.

Vraag 13
Zijn er wat u betreft andere aanvullende structurele maatregelen nodig om de ict-veiligheid en cyberweerbaarheid van Nederlandse ziekenhuizen en andere zorgorganisaties te versterken? Zo ja, welke en welke stappen neemt u samen met de ziekenhuizen en zorgorganisaties om hieraan te werken?

Antwoord 13
Er wordt op verschillende manieren gewerkt aan de informatieveiligheid van het Nederlandse Zorgveld. Bewustwording van risico's en het belang van zorgvuldig handelen door eigen medewerkers is essentieel voor goede informatieveiligheid, ook in de zorg. Ik zet daarom ten eerste in op het stimuleren van informatieveilig gedrag van zorgprofessionals. Daarvoor is het Ministerie van VWS in 2019 het project informatieveilig gedrag gestart. Via dit project werk ik aan een gestructureerde methode voor gedragsverandering op het gebied van informatieveiligheid, toegespitst op de Nederlandse zorgsector. In mijn brief «Voortgang op elektronische gegevensuitwisseling» van 15 december 2022 heb ik uw Kamer hier nader over geïnformeerd.[8]
Zoals beschreven in het antwoord op vraag 7 en 8 is VWS-beleid er daarnaast op gericht om de dienstverlening van Z-CERT zo breed mogelijk beschikbaar te stellen binnen het zorgveld, middels een risicogestuurde aansluitstrategie. Er wordt ook actief ingezet op een uitbreiding van de diensten van Z-CERT. Daarnaast zorg ik er samen met het zorgveld voor dat we de eerder genoemde NEN-normen voor informatiebeveiliging blijven ontwikkelen, en breng ik deze normen actief onder de aandacht bij zorgaanbieders. Zo heb ik NEN in 2022 de opdracht gegeven om een herziening van de NEN-7510 te coördineren, en daarbij ook *implementatietools* te ontwikkelen.
Eveneens heeft het Ministerie van VWS in januari 2023 samen met ROAZ Zuidwest-Nederland en GHOR Zuid-Holland Zuid een grootschalige oefening

[8] Kamerstuk 27 529, nr. 288

georganiseerd. Hierbij is gezamenlijk geoefend met een scenario waarin sprake was van digitale verstoring van onder andere de ziekenhuiszorg. De lessen die hieruit zijn getrokken zullen de komende tijd worden gebruikt om de voorbereiding op dergelijke incidenten te verbeteren.
Tot slot wordt de komende tijd gewerkt aan de implementatie van nieuwe Europese richtlijnen met betrekking tot informatieveiligheid (NIB2) en algemene weerbaarheid (CER). Over de deze implementatie zal ik uw Kamer binnenkort nader informeren.