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

2246

Vragen van de leden **Hermans**, **Rajkowski** en **Rahimi** (allen VVD) aan de Ministers van Volksgezondheid, Welzijn en Sport en van Justitie en Veiligheid over *de berichten «Naaktbeelden borstkankerpatiënten VS gepubliceerd om ziekenhuis af te persen» en «Paspoorten van dokters op straat na hack bij oudereninstelling Gelderland»* (ingezonden 8 maart 2023).

Antwoord van Minister **Kuipers** (Volksgezondheid, Welzijn en Sport), mede namens de Minister van Justitie en Veiligheid en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 13 april 2023).

Vraag 1
Bent u bekend met de berichten: «Naaktbeelden borstkankerpatiënten VS gepubliceerd om ziekenhuis af te persen», en «Paspoorten van dokters op straat na hack bij oudereninstelling Gelderland»?[1, 2]

Antwoord 1
Ja.

Vraag 2
Is bekend of meer Nederlandse ziekenhuizen of zorginstellingen slachtoffer zijn (geweest), of doelwit zijn van ransomware-aanvallen waarbij patiëntgegevens en gegevens van (zorg)medewerkers zoals foto's en persoonsinformatie buit zijn gemaakt? Om hoeveel gevallen gaat het? Welke stappen zijn gezet om de schade voor patiënten zo veel mogelijk te beperken?

Antwoord 2
De afgelopen jaren zijn meerdere ziekenhuizen en zorginstellingen slachtoffer geweest van ransomware-aanvallen. Uit het dreigingsbeeld cybersecurity van het Computer Emergency Response Team voor de zorg (Z-CERT) blijkt dat er in 2022 vijf ransomware-incidenten bij Nederlandse zorginstellingen zijn

[1] RTLnieuws, 6 maart 2023, «Naaktbeelden borstkankerpatiënten VS gepubliceerd om ziekenhuis af te persen» (https://www.rtlnieuws.nl/nieuws/buitenland/artikel/5369862/cybercrimelen-publiceren-naaktbeelden-borstkankerpatienten).
[2] RTL Nieuws, 7 maart 2023, «Paspoorten van dokters op straat na hack bij oudereninstelling Gelderland» (https://www.rtlnieuws.nl/nieuws/nederland/artikel/5370082/attent-zorg-behandeling-hack-ransomware-paspoorten-datalek)

ah-tk-20222023-2246
ISSN 0921 - 7398
's-Gravenhage 2023

geregistreerd door Z-CERT.[3] In het jaar 2021 betrof dit ook vijf geregistreerde ransomware incidenten. In 2023 is er voorlopig sprake van twee genoteerde incidenten.[4] Het is mij niet bekend bij hoeveel van deze incidenten er gegevens van patiënten of (zorg-)medewerkers zijn ontvreemd. Zorgaanbieders die geraakt worden door ransomware kunnen (technische) experts inzetten om de gevolgen van het incident te beperken. Zorgaanbieders die zijn aangesloten bij Z-CERT kunnen hierbij rekenen op ondersteuning door Z-CERT. Het is daarnaast van belang dat zorginstellingen contact opnemen met de betrokken patiënten of medewerkers om hen te informeren over de gevolgen die het incident voor hen heeft, en in overleg met de ICT-leverancier maatregelen treffen ten behoeve van de informatieveiligheid.

Vraag 3
Welke veiligheidsmaatregelen worden getroffen door Nederlandse ziekenhuizen en zorginstellingen om patiëntgegevens, gegevens van (zorg)medewerkers en andere gevoelige data zo goed mogelijk te beschermen, de continuïteit van zorgprocessen te borgen en om cybercriminelen buiten de deur te houden? In hoeverre wordt de zorgsector hierbij ondersteund door Z-CERT? In hoeverre wordt Z-CERT ook actief benaderd en betrokken door de zorgsector zelf wanneer het gaat om bijstand bij cyberaanvallen? Is Z-CERT ook in het verleden betrokken geweest bij cyberaanvallen op Nederlandse ziekenhuizen en andere zorginstellingen? Zo ja, wat was hun rol?

Antwoord 3
Zorginstellingen nemen maatregelen om de gevolgen van cyberaanvallen te beperken en zo spoedig mogelijk te mitigeren. Deze maatregelen vloeien voort uit hun verantwoordelijkheden en zijn uitgewerkt in wettelijk verplicht gestelde normen voor informatiebeveiliging in de zorg. Dit betreft de NEN7510, 7512 en 7513. Kern hierbij is de NEN 7510 norm, die met name voorschrijft dat zorginstellingen de risico's voor informatiebeveiliging in kaart brengen en hiervoor passende maatregelen nemen. De norm vereist ook beheersmaatregelen voor de bescherming van netwerken, bedrijfscontinuïteit en bereikbaarheid. De aanvullende normen NEN 7512 en 7513 zien er daarnaast op toe dat er wordt voldaan aan eisen voor veilige gegevensuitwisseling en *logging*.
Op dit moment zijn meer dan 300 instellingen uit verschillende sub-sectoren aangesloten bij Z-CERT. Z-CERT voorziet hun deelnemers van advies en dreigingsinformatie, en in het geval van een incident kan Z-CERT een zorginstellingen ondersteunen bij het mitigeren van de gevolgen van een cyberaanval. Z-CERT heeft dit in het verleden ook gedaan, bijvoorbeeld tijdens de recente DDoS-aanvallen op Nederlandse ziekenhuizen. Door gebruik te maken van de diensten van Z-CERT zoals het Zorgdetectienetwerk, kunnen zorginstellingen informatie over incidenten met elkaar delen. Z-CERT monitort daarnaast actief op signalen van incidenten bij haar deelnemers. Ook scant Z-CERT op internet naar kwetsbare systemen bij de deelnemers en informeert deze daarover om zo mogelijke incidenten te voorkomen.
Het Ministerie van VWS ondersteunt het gefaseerd aansluiten van de gehele zorgsector op basis van een risicogebaseerde aansluitstrategie, zodat steeds meer zorginstellingen deelnemer worden van Z-CERT. Het Ministerie van VWS blijft zich inzetten om de dienstverlening van Z-CERT zo breed mogelijk beschikbaar te stellen binnen de gehele zorgsector.

Vraag 4
Welke maatregelen worden genomen om te voorkomen dat een klik op een verkeerde link door een (zorg)medewerker cybercriminelen toegang geeft tot de meest gevoelige en kwetsbare informatie van patiënten?

Antwoord 4
Bewustwording van risico's en het belang van zorgvuldig handelen door eigen medewerkers is essentieel voor goede informatieveiligheid, ook in de zorg. Het Ministerie van VWS zet daarom ten eerste in op het stimuleren van informatieveilig gedrag van zorgprofessionals. In de brief «Voortgang op

[3] Z-CERT_RapportDreigingsbeeld2022.pdf
[4] Home – Z-CERT

elektronische gegevensuitwisseling» van 15 december 2022 heb ik u hier nader over geïnformeerd.[5] In 2019 is het Ministerie van VWS het project informatieveilig gedrag gestart. Via dit project werkt het ministerie aan een gestructureerde methode voor gedragsverandering op het gebied van informatieveiligheid, toegespitst op de Nederlandse zorgsector. De methode is uitgewerkt in een Wegwijzer, waarin manieren zijn opgenomen om informatie veilig gedrag in de zorg te bevorderen. Hierin wordt onder andere ingegaan op welke interventies mogelijk zijn om te voorkomen dat (zorg)medewerkers slachtoffer worden van *phishing*.
Daarnaast heeft Z-CERT een publicatie over *phishing* gemaakt waarin maatregelen en een handelingsperspectief beschreven worden.[6] Deze publicatie is terug te vinden op website van Z-CERT en is door Z-CERT verspreid onder haar deelnemers. Hierin staan naast bewustwordingsmaatregelen ook technische maatregelen die zorginstellingen kunnen toepassen om beter beschermd te zijn tegen *phishing*.

Vraag 5
Welke maatregelen neemt Z-CERT om de cyberbewustwording en weerbaarheid bij Nederlandse ziekenhuizen en zorginstellingen te verhogen?

Antwoord 5
Z-CERT biedt hun deelnemers een breed pakket aan diensten om hun cybersecurity bewustwording en weerbaarheid te verhogen. Zoals ik in mijn antwoord op vraag 3 heb aangegeven gaat het hierbij onder andere om het verspreiden van dreigingsinformatie, adviseren over preventieve maatregelen en het ondersteunen bij het mitigeren van de impact van een cyberaanval. Concreet gaat het bijvoorbeeld om adviezen over hoe te reageren op een ransomwareaanval, en hoe e-mailstandaarden en monitoring te implementeren.[7] Z-CERT helpt hun deelnemers daarnaast bij het organiseren van cybercrisisoefeningen, en Z-CERT informeert deelnemers geregeld over cyberbewustwordingsonderwerpen. Op de website van Z-CERT is eveneens een kennisbank te vinden met daarin documentatie die informatie bevat over verschillende thema's. Het doel van deze publicaties is om het zorgveld cyberweerbaar en cyberbewust te maken. Deze informatie is voor iedereen toegankelijk.

Vraag 6
Hoe hoog wordt het dreigingsniveau van eventuele aanvallen door cybercriminelen op Nederlandse ziekenhuizen en zorginstellingen, maar ook breder dan deze sector, geschat? Hoe beoordeelt u de digitale weerbaarheid van Nederlandse sectoren in vergelijking met de huidige toenemende digitale dreiging waar Nederland nu mee te maken heeft? Welke maatregelen worden op dit moment in Nederland genomen om weerstand te bieden aan deze toenemende dreiging, ook in aanloop naar de implementatie van de NIS2?

Antwoord 6
In het dreigingsbeeld cybersecurity 2022 geeft Z-CERT per type cyberdreiging voor het zorgveld een risico-inschatting. Zo wordt het dreigingsniveau met betrekking tot de impact van ransomware-aanvallen op Nederlandse ziekenhuizen en zorginstellingen aangemerkt als «hoog».[8]
In het meest recente Cybersecuritybeeld Nederland staat genoteerd dat er sprake is van een scheefgroei tussen de toenemende dreiging en de ontwikkeling van de weerbaarheid.[9] Omdat digitale systemen het «zenuwstelsel» van onze maatschappij vormen, maakt het kabinet zich daarom hard voor de versterking van onze digitale weerbaarheid via de verschillende ambities die omschreven staan in de Nederlandse Cybersecuritystrategie (NLCS), zodat deze scheefgroei geadresseerd wordt.[10] In het actieplan van de NLCS staan de maatregelen waarmee deze ambities worden gerealiseerd en wie daarvoor verantwoordelijk is.

---

[5] Kamerstuk 27 529, nr. 288
[6] TLPWHITE-Pak-phishing-aan-Maatregelen-voor-effectieve-preventie-1.0.pdf (z-cert.nl)
[7] Cybermaand 2021: Tien tips tegen ransomware – Z-CERT
[8] Z-CERT_RapportDreigingsbeeld2022.pdf
[9] Kamerstuk 26 643, nr. 891
[10] NLCS (Kamerstuk 26 643, nr. 925)

Vraag 7
Hoe staat het met de toezegging dat Nederland zich inzet om de zwaarste cybercriminelen op Europese sanctielijsten te krijgen? Deelt u de mening dat de cybercriminelen van onder andere Black Cat en Qilin hier ook op thuishoren? Zo nee, waarom niet? Zo ja, wat gaat u doen om dit te bereiken?

Antwoord 7
Als internationaal recht en in VN-verband overeengekomen normen geschonden worden door cyberaanvallen, kunnen diplomatieke maatregelen in coalitieverband worden genomen. In EU-verband hebben we hiertoe de Cyber Diplomacy Toolbox, die mede door Nederland tot stand is gekomen. Het EU Cyber Sanctie Regime is onderdeel van deze Toolbox. Inmiddels zijn acht personen en vier entiteiten die verantwoordelijk zijn voor de meest schadelijke cyberaanvallen op de sanctielijst van de EU geplaatst. Op de sanctielijst staan onder andere de verantwoordelijken voor de verstoorde Russische cyberoperatie tegen de Organisatie voor het Verbod op Chemische Wapens (OPCW). Daarnaast kregen personen en entiteiten uit China en Noord-Korea sancties opgelegd. Op dit moment wordt de Cyber Diplomacy Toolbox herzien, met als doel daadkrachtiger op te kunnen treden tegen ontwrichtende cyberoperaties, hier speelt Nederland wederom een actieve rol in. Welke respons opportuun is, zal afhankelijk zijn van de ernst en impact van het incident. Voor inzet van het sanctiemiddel is bovendien unanimiteit vereist in de EU-besluitvorming.

Vraag 8
Hoe gaat u er zorg voor dragen dat de KopielD-app van de rijksoverheid, waarmee identiteitsbewijzen veilig gekopieerd, verstuurd en getraceerd kunnen worden, meer bekendheid en gebruikers krijgt, zodat in geval van diefstal en lekken locaties sneller te achterhalen zijn?

Antwoord 8
Vanaf juni dit jaar wordt de KopielD-app extra onder de aandacht gebracht. Dat zal gebeuren via social media, advertorials en bij bibliotheken waar de Informatiepunten Digitale Overheid zijn. De KopielD-app zelf zal in juni ook gebruiksvriendelijker zijn dan de huidige app. Zo is de app straks in meer talen te gebruiken en kunnen documenten automatisch worden herkend zodat men niet meer zelf met de vinger onderdelen onzichtbaar hoeft te maken te maken. De app herkent dan ook documenten als de Sédula, de identiteitskaarten die gebruikt worden in het Caribisch deel van het Koninkrijk.

Vraag 9
Hoe kan er zorg voor gedragen worden dat «vervuilde data», zoals verlopen paspoorten, sneller opgeruimd worden, zodat deze niet meer onderdeel kunnen worden van een cyberaanval? Hoe groot is het probleem van vervuilde data in Nederland?

Antwoord 9
De kopieën van de identiteitsbewijzen in het artikel en «Paspoorten van dokters op straat na hack bij oudereninstelling Gelderland» waren van werknemers. Die kopieën worden gemaakt als iemand in dienst treedt bij een werkgever. Werkgevers zijn verplicht om deze kopieën, zonder doorgestreepte elementen, te bewaren. Dat moet tot vijf jaar nadat een werknemer weg is bij deze werkgever. Het komt dus voor dat er terecht kopieën worden bewaard van identiteitsbewijzen die inmiddels zijn verlopen. Werkgevers dienen kopieën van oud-werknemers niet onnodig lang te bewaren. Of en hoeveel kopieën onnodig worden bewaard, is onbekend.[11]

Vraag 10
Ziet u mogelijkheden om, in het kader van de toenemende internationale cyberdreiging, aanvullende maatregelen te nemen op de korte termijn om de digitale weerbaarheid van de zorgsector en andere sectoren te vergroten? Zo ja, welke concrete maatregelen bent u bereid te treffen? Zo nee, waarom niet?

[11] Wat moet ik als werkgever doen om te voldoen aan de identificatieplicht? | Rijksoverheid.nl

Antwoord 10
Zoals in het antwoord op vraag 6 is aangegeven staan in het actieplan van de NLCS alle acties die het kabinet uit zal voeren om de algehele digitale weerbaarheid van de maatschappij te versterken. Hierin vindt u dus ook welke concrete maatregelen op korte termijn getroffen (zullen) worden. Een voorbeeld van belangrijke maatregelen die de digitale weerbaarheid op korte termijn zullen vergroten is het bieden van meer zicht op cyberincidenten, -dreigingen en -risico's aan organisaties door meer en efficiëntere informatie-uitwisseling. Daarnaast wordt er dit jaar geoefend met het Landelijk Crisisplan Digitaal middels de nationale oefening ISIDOOR.
Het actieplan 2022–2023 van de NLCS is het startpunt. Het actieplan wordt jaarlijks geactualiseerd, waardoor adequaat ingespeeld kan worden op de snelle ontwikkeling van het cybersecurity domein en bijgestuurd kan worden als hier aanleiding toe is. De komende jaren geeft het kabinet samen met medeoverheden, bedrijfsleven en wetenschap invulling aan de noodzakelijke vervolgstappen richting een digitaal veilig Nederland.

Vraag 11
Herinnert u zich de eerdere schriftelijke vragen over de Pro-Russische DDoS-aanval op Nederlandse ziekenhuizen? Kunt u toezeggen deze en bovenstaande schriftelijke vragen te beantwoorden vóór het aanstaande commissiedebat Cybercrime d.d. 30 maart 2023?[12]

Antwoord 11
Ja.

[12] Vragen van de leden Tielen en Rajkowski (beiden VVD) aan de Ministers van Volksgezondheid, Welzijn en Sport en van Justitie en Veiligheid over het bericht «Pro-Russische DDoS-aanvallers vallen Nederlandse ziekenhuizen aan» (ingezonden 2 februari 2023).