Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

Aanhangsel van de Handelingen

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

1662

Vragen van het lid **Hijink** (SP) aan de Minister voor Medische Zorg over *het bericht «Stilleggen van het dataverkeer door het Medisch Centrum Leeuwarden naar aanleiding van een hackpoging»* (ingezonden 16 januari 2020).

Antwoord van Minister **Bruins** (Medische Zorg) (ontvangen 10 februari 2020).

Vraag 1
Wat is uw reactie op het bericht dat hackers erin zijn geslaagd binnen te dringen in de systemen van het Medisch Centrum Leeuwarden (MCL)? Welke schade is hierdoor aangericht? Zijn er patiëntgegevens of andere belangrijke data in handen van onbevoegden gekomen?[1]

Antwoord 1
Zorgaanbieders zijn zelf verantwoordelijk voor hun eigen ICT en de informatieveiligheid. Daarbij moeten zij zich onder meer houden aan de Nederlandse normen voor informatieveiligheid in de zorg (NEN 7510). De IGJ ziet hierop toe. 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.
Het MCL meldt op haar website dat uit het onderzoek naar de poging tot inbraak op de systemen van het MCL is gebleken dat de aanval niet is doorgedrongen tot de interne systemen of patiëntgegevens. Het MCL heeft mij laten weten dat de patiëntveiligheid geen enkel moment in gevaar is geweest

Vraag 2
Zijn er berichten van andere organisaties in de zorg die hierdoor zijn getroffen? Welke schade hebben zij ondervonden?

[1] NOS.nl, 15 januari 2020, «Hackpoging ziekenhuis Leeuwarden, NCSC vreest aanvallers in meer systemen» (https://nos.nl/artikel/2318734-hackpoging-ziekenhuis-leeuwarden-ncsc-vreest-aanvallers-in-meer-systemen.html).

ah-tk-20192020-1662
ISSN 0921 - 7398
's-Gravenhage 2020

Antwoord 2
Het College Beoordeling Geneesmiddelen heeft laten weten gecompromitteerd te zijn. Hiervan is een melding gemaakt bij NCSC. Forensisch onderzoek loopt nog, maar het huidige beeld is dat er geen indicatoren zijn dat er data is gelekt.

Vraag 3 en 4
Waarom heeft het ziekenhuis niet tijdig ingegrepen nadat Citrix al in december waarschuwde voor de mogelijke risico's?
Hoe kan het dat zelfs nadat het Nationaal Cyber Security Centrum (NCSC) op 9 januari jl. waarschuwde dat hackers actief op zoek zijn naar kwetsbaarheden, er niet is gehandeld door het ziekenhuis?

Antwoord 3 en 4
Zoals reeds gemeld zijn zorginstellingen zijn zelf primair verantwoordelijk voor hun eigen ICT en de informatieveiligheid onder alle omstandigheden. Daarbij moeten zij zich onder meer houden aan de Nederlandse normen voor informatieveiligheid in de zorg (NEN 7510). De IGJ ziet hierop toe. Hierbij hoort ook het direct nemen van maatregelen om de risico's te verkleinen. Het MCL heeft mij laten weten de workaround van medio december 2019 niet tijdig te hebben uitgevoerd. Het MCL heeft mij daarbij gemeld daar onderzoek naar te doen.

Vraag 5
Wat was de rol van Z-Cert, expertisecentrum op het gebied van cybersecurity in de zorg, in deze? Waarom is op de website van Z-Cert sinds december geen bericht te lezen over de risico's voor organisaties die werken met Citrix?

Antwoord 5
Z-CERT heeft vanaf het bekend worden van de kwetsbaarheid in december 2019 haar deelnemers actief geïnformeerd en voorzien van handelingsadvies. Z-CERT gebruikt een speciaal platform om met de deelnemers te communiceren. Ook wordt per e-mail gecommuniceerd. Gezien de omvang van de Citrix-kwetsbaarheid, is in dit geval gekozen om ook een advies op de website te plaatsen.

Vraag 6
Kunt u aangeven welke contacten er zijn geweest tussen het NCSC en Z-Cert om zorgaanbieders te informeren en aan te sporen actie te ondernemen?

Antwoord 6
NCSC en Z-CERT staan in nauw contact met elkaar om informatie uit te wisselen over onder andere kwetsbaarheden in IT-systemen van hun onderscheidenlijke doelgroepen.

Vraag 7
Klopt de analyse van experts dat de samenwerking rondom databescherming tekortschiet?

Antwoord 7
Deze vraag kan ik niet beantwoorden omdat ik deze analyse niet ken.

Vraag 8
Welke maatregelen gaat u nemen om ervoor te zorgen dat zorginstellingen eerder, actiever en indringender worden bijgestaan bij het nemen van maatregelen om hun data te beschermen tegen hackers?

Antwoord 8
Zoals reeds gemeld zijn zorgaanbieders zelf verantwoordelijk voor hun eigen ICT en de informatieveiligheid. De IGJ ziet hierop toe. In reactie op de motie van het Kamerlid Ellemeet[2] verken ik of deelname aan Z-CERT verplicht kan worden gesteld. Voor de zomer van 2020 zal ik de resultaten hiervan met uw Kamer delen.

[2] Kamerstuk 27 529, nr. 177

Het kabinet werkt aan een landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden waarbinnen informatie over dreigingen, incidenten en kwetsbaarheden breder, efficiënter en effectiever tussen publieke en private partijen wordt gedeeld. In dit verband is Z-CERT eerder deze maand door de Minister van JenV[3] aangewezen als computercrisisteam, waaraan op grond van de Wet beveiliging netwerk- en informatiesystemen bepaalde informatie (bv. namen van bedrijven in relatie tot dreigingen) kan worden verstrekt. Dit maakt het mogelijk voor het NCSC om zoveel mogelijk informatie en handelingsperspectieven te delen met Z-CERT.

[3] https://zoek.officielebekendmakingen.nl/stcrt-2020–4410.html