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

1843

Vragen van het lid **Veldman** (VVD) aan de ministers voor Medische Zorg en van Justitie en Veiligheid over *het bericht «Hackpoging ziekenhuis Leeuwarden, NCSC vreest aanvallers in meer systemen»* (ingezonden 17 januari 2020).

Antwoord van Minister **Bruins** (Medische Zorg), mede namens de Minister van Justitie en Veiligheid (ontvangen 21 februari 2020). Zie ook Aanhangsel Handelingen, vergaderjaar 2019–2020, nr. 1657.

Vraag 1
Bent u bekend met het bericht «Hackpoging ziekenhuis Leeuwarden, NCSC vreest aanvallers in meer systemen»?[1]

Antwoord 1
Ja.

Vraag 2
Bent u van mening dat het ziekenhuis direct actie had moeten ondernemen toen het Nationaal Cyber Security Centrum (NCSC) van het Ministerie van Justitie en Veiligheid Citrix-gebruikers waarschuwde voor de kwetsbaarheid van deze servers voor aanvallen van hackers?

Antwoord 2
Zorgaanbieders zijn zelf primair verantwoordelijk voor hun eigen ICT en de informatieveiligheid. Zij worden hierin ondersteund door Z-CERT, het cybersecuritycentrum voor de zorg. Het NCSC en Z-CERT staan in nauw contact met elkaar om zo veel als mogelijk voor elkaar relevante informatie uit te wisselen. Z-CERT heeft vanaf het bekend worden van de kwetsbaarheid in december 2019 haar deelnemers actief geïnformeerd en voorzien van handelingsadvies. Het MCL heeft mij laten weten de tussentijdse mitigerende maatregelen van Citrix van medio december niet tijdig te hebben uitgevoerd. Het MCL heeft mij daarbij gemeld daar onderzoek naar te doen.

[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-20192020-1843
ISSN 0921 - 7398
's-Gravenhage 2020

Vraag 3
Kunt u toelichten in hoeverre kwetsbaarheden in servers waar ziekenhuizen gebruik van maken meegenomen worden in de nieuwe wetgeving rondom gegevensuitwisseling in de zorg?

Antwoord 3
De nieuwe wet elektronische gegevensuitwisseling in de zorg waar ik aan werk, zal bepalingen bevatten die het mogelijk maken dat eisen kunnen worden gesteld aan, onder meer, informatieveiligheid en privacy. Ook worden er bepalingen in opgenomen die certificering van ICT-producten mogelijk maken. Kwetsbaarheden in producten zullen overigens aan het licht blijven komen. Daarom is het van belang dat zorgaanbieders blijvend aandacht besteden aan informatiebeveiliging.

Vraag 4
In hoeverre kunt u toelichten of er meer ziekenhuizen in Nederland gebruikmaken van servers van Citrix of andere servers waar kwetsbaarheden zijn ontstaan? Zo ja, hoeveel zijn dit er dan?

Antwoord 4
Ik heb hier geen inzicht in. Zorginstellingen zijn zelf verantwoordelijk voor hun eigen ICT en welke systemen en/of servers zij gebruiken.

Vraag 5
Kunt u toelichten in hoeverre het dataverkeer tussen overige ziekenhuizen ook stilgelegd is na ontdekking van de hackpoging?

Antwoord 5
Het is mij niet bekend in hoeverre het dataverkeer tussen overige ziekenhuizen is stilgelegd na ontdekking van de hackpoging bij het Medisch Centrum Leeuwarden (MCL).

Vraag 6
Hoe ziet u de uitspraak van oktober 2019 over het harder aanpakken van bedrijven die hun ICT niet op orde hebben in het licht van de situatie bij het Medisch Centrum Leeuwarden?[2]

Antwoord 6
Ik deel met mijn ambtsgenoot Minister Grapperhaus dat informatieveiligheid een prioriteit dient te zijn, zo ook op alle bestuurslagen van de zorgsector. Zoals reeds gemeld zijn zorginstellingen zelf primair verantwoordelijk voor hun eigen ICT en de informatieveiligheid onder alle omstandigheden. Zorginstellingen als het MCL worden hierin ondersteund door Z-CERT. Zorginstellingen moeten zich meer in het algemeen onder meer houden aan de Nederlandse normen voor informatieveiligheid in de zorg (NEN-norm 7510). De Inspectie Gezondheidszorg en Jeugd (IGJ) ziet hierop toe. Verder werk ik momenteel aan een herbeoordeling om te bezien of bepaalde organisaties binnen de zorgsector als vitale aanbieders zouden moeten worden aangewezen.

[2] NOS.nl, 1 oktober 2019, «Grapperhaus wil harde aanpak bedrijven met slechte digitale beveiliging» (https://nos.nl/artikel/2304164-grapperhaus-wil-harde-aanpak-bedrijven-met-slechte-digitale-beveiliging.html).