Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017 **Aanhangsel van de Handelingen**

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

2342

Vragen van het lid **Gerbrands** (PVV) aan de Minister van Volksgezondheid, Welzijn en Sport over *het bericht dat ziekenhuizen getroffen zijn door ransomware-aanvallen* (ingezonden 29 juni 2017).

Antwoord van Minister **Schippers** (Volksgezondheid, Welzijn en Sport) (ontvangen 14 juli 2017).

Vraag 1
Wat is uw reactie op het bericht «Ransomware treft zeker 15 ziekenhuizen»?[1]

Antwoord 1
Ransomware aanvallen komen voor in alle sectoren. Ik vind het zorgelijk dat ook zorginstellingen worden getroffen door ransomware aanvallen. Patiënten moeten er op kunnen vertrouwen dat de bescherming van hun medische informatie is gewaarborgd.
Ik blijf me samen met de sector inspannen om aanvallen of andere manieren om de ICT systemen in de zorg te ontregelen te voorkomen, of als ze zich toch voordoen de schade zo veel mogelijk te beperken. (zie ook het antwoord op vraag 6).

Vraag 2, 3
Hoeveel en welke gegevens zijn hierdoor verloren gegaan?
Is er losgeld betaald aan criminelen? Zo ja, hoeveel?

Antwoord 2, 3
Het Nationaal Cyber Security Centrum (NCSC) heeft mij laten weten dat zij sinds 1 januari 2014 vijf meldingen hebben geregistreerd van ransomware op infrastructuur van een ziekenhuis. Er is niet bekend of er losgeld is betaald. Evenmin is bekend of er bestanden onherstelbaar verloren zijn gegaan. Ook Z-CERT (Computer Emergency Response Team voor de zorg) heeft geen informatie over eventueel losgeld of verloren informatie. De Inspectie voor de Gezondheidszorg (IGZ) heeft geen meldingen ontvangen van situaties met ransomware.

[1] Telegraaf, 25-06-2017
http://www.telegraaf.nl/binnenland/28469696/__Ransomware_treft_ziekenhuizen__.html

ah-tk-20162017-2342
ISSN 0921 - 7398
's-Gravenhage 2017

Vraag 4, 5
Hoeveel ziekenhuizen werken nog met verouderde medische apparatuur of verouderde besturingssystemen?
Wie is er verantwoordelijk voor de beveiliging van medische apparatuur, de ziekenhuizen of de leveranciers?

Antwoord 4, 5
Ziekenhuizen zijn in eerste plaats zelf verantwoordelijk voor de beveiliging van medische apparatuur. Ziekenhuizen moeten passende maatregelen nemen op het gebied van informatiebeveiliging, dit geldt ook voor apparaten die nog niet zijn afgeschreven met verouderde software. De eisen voor informatiebeveiliging van ziekenhuizen zijn te vinden in de NEN-normen. Ook moeten ziekenhuizen voldoen aan het convenant veilige toepassing van medische technologie in de medisch specialistische zorg.

Vraag 6
Wat gaat u doen om ervoor te zorgen dat Nederlandse ziekenhuizen niet langer kwetsbaar zijn voor gijzelsoftware?

Antwoord 6
Naar aanleiding van de wereldwijde ransomware aanval van 12 mei jl. heb ik 19 mei jl. een brief gestuurd naar de leden van het Informatieberaad Zorg waarin ik verzoek om adequate maatregelen te treffen en aandacht heb gevraagd voor informatiebeveiliging. Ik ga er vanuit dat zorginstellingen de noodzakelijke prioriteit geven aan dit onderwerp.
Samen met de sector heb ik de afgelopen periode diverse initiatieven genomen om de beveiliging van systemen te versterken:
Met brancheorganisaties in de medisch-specialistische zorg en geestelijke gezondheidszorg heb ik een «Actieplan (informatie)beveiliging patiëntgegevens» opgesteld dat 20 juni jl. naar de Tweede Kamer is verzonden[2]. In het Informatieberaad van 26 juni 2017 is aangekondigd dat ik dit actieplan wil uitbreiden tot het hele zorgveld. Activiteiten uit het plan moeten leiden tot een structurele verbeteringen in de dagelijkse werkpraktijk bij ziekenhuizen op het gebied van privacybescherming en informatiebeveiliging.
Om weerbaarder te zijn voor informatiebeveiligingsincidenten en de mogelijke gevolgen te beperken is begin dit jaar de sectorale CERT (Computer Emergency Response Team) voor de zorg opgericht, de stichting Z-CERT. De Z-CERT is een voorziening die bij cyberincidenten snel in actie te komt, om detectie te versnellen en kennisdeling over informatiebeveiligingsincidenten te vergroten. Hiermee wordt de impact van dergelijke incidenten beperkt. Ik ondersteun dit initiatief met een opstartsubsidie.
Daarnaast heeft het NCSC een samenwerkingsverband ontwikkeld in de vorm van een sector Information Sharing and Analysis Centre (ISAC). Een ISAC is een publiek-private sectoraal samenwerkingsverband, waarbinnen op tactisch niveau deelnemers van de zorgsector, waaronder ziekenhuizen om de sector als geheel weerbaarder te maken tegen cyber incidenten. Door het delen van (incident) informatie en het opbouwen van een netwerk kunnen ziekenhuizen hun eigen informatiebeveiliging verbeteren.

[2] https://www.rijksoverheid.nl/documenten/rapporten/2017/06/20/actieplan