

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

1663

Vragen van het lid **Van den Berg** (CDA) aan de Minister voor Medische Zorg over *het bericht «MCL legt dataverkeer stil na cyberaanval»* (ingezonden 16 januari 2020).

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

Vraag 1

Kent u het bericht «MCL legt dataverkeer stil na cyberaanval»?¹

Antwoord 1

Ja.

Vraag 2

Welke invloed heeft het feit dat het Medisch Centrum Leeuwarden (MCL) uit voorzorg al het dataverkeer met de buitenwereld (zoals communicatie met andere ziekenhuizen) heeft stilgelegd voor patiënten die met spoed geholpen moeten worden?

Antwoord 2

Op 15 januari heeft het MCL gemeld dat er een poging tot digitale inbraak in de systemen is geweest. Daarbij werd gemeld dat uit voorzorg alle dataverkeer met de buitenwereld werd afgesloten. Door deze maatregel konden patiënten niet bij hun elektronische dossier en ook is de elektronische communicatie met andere ziekenhuizen gehinderd. Het MCL heeft laten weten dat de patiëntveiligheid geen enkel moment in gevaar is geweest. Het MCL heeft op 21 januari via hun website laten weten dat alle systemen weer werken en dat uit onderzoek naar de poging tot inbraak is gebleken dat de aanval niet is doorgedrongen tot de interne systemen van het MCL of patiëntgegevens.

Vraag 3

Welke andere ziekenhuizen werken ook met Citrix-servers?

¹ Omrop Fryslân, 15 januari 2020, «MCL legt dataverkeer stil na cyberaanval» (<https://www.omropfryslan.nl/nieuws/930034-mcl-legt-dataverkeer-stil-na-cyberaanval>).

Antwoord 3

Dit is mij niet bekend. Zorginstellingen zijn zelf verantwoordelijk voor hun eigen ICT en welke systemen en/of servers zij gebruiken.

Vraag 4

Zijn er bij andere ziekenhuizen ook pogingen gedaan om de Citrix-servers te hacken? Zo ja, hebben hackers kans gezien om in de systemen te komen?

Antwoord 4

Op dit moment heb ik geen aanwijzingen dat bij andere ziekenhuizen pogingen zijn gedaan.

Vraag 5

Heeft het MCL de «workaround» uitgevoerd, waarmee Citrix medio december 2019 bedrijven adviseerde zich te beschermen omdat er tot op heden nog geen updates zijn die tegen het lek in de Citrix-servers beschermen?²

Antwoord 5

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 om uit te zoeken wat precies de redenen waren om niet al in december in te grijpen.

Vraag 6 en 7

Kunt u een update geven voor alle ziekenhuizen? Hebben zij voldoende maatregelen getroffen?

Wordt met de «workaround» van Citrix de kans op een cyberaanval en het hiermee hacken van gegevens voldoende beperkt? Zo nee, welke maatregelen dienen ziekenhuizen nog meer te nemen?

Antwoord 6 en 7

Of alle ziekenhuizen workarounds hebben uitgevoerd naar aanleiding van de poging tot hackpoging bij het MCL is mij onbekend. Z-CERT heeft haar deelnemers gewaarschuwd voor de kwetsbaarheid in Citrix en heeft handelingsadvies gegeven en aangeraden om alle stappen te doorlopen uit het beveiligingsadvies van het NCSC.

Citrix heeft inmiddels patches beschikbaar gesteld om de kwetsbaarheid te herstellen. Op basis van zijn informatie adviseert het NCSC op hun website om deze patches te vertrouwen en te installeren, tenzij uit eigen risicoanalyse blijkt dat de systemen waarschijnlijk gecompromitteerd zijn. Het NCSC adviseert ook om na de installatie van de patches te blijven monitoren en detectie toe te passen op misbruik van de kwetsbaarheden.

Vraag 8 en 9

Welke ziekenhuizen zijn nog niet aangesloten bij Z-Cert, het expertisecentrum op het gebied van cybersecurity in de zorg?

Wat gaat u doen om te bevorderen dat zo spoedig mogelijk alle ziekenhuizen zijn aangesloten bij Z-Cert?

Antwoord 8 en 9

Alle ziekenhuizen (academisch, topklinisch en algemeen) zijn via de koepel van Nederlandse Vereniging van Ziekenhuizen (NVZ) en de koepel van Nederlandse Federatie van Universitair Medische Centra (NFU) aangesloten. Onderzocht wordt, conform de motie van het Kamerlid Ellemeest, of deelname aan Z-Cert verplicht kan worden. Na het zomerreces zal ik de voortgang van mijn onderzoek met uw kamer delen.

² Het Financieele Dagblad, 14 januari 2020, «Honderden Nederlandse bedrijven met Citrix-servers vatbaar voor hack» (<https://fd.nl/ondernemen/1330985/honderden-nederlandse-bedrijven-met-citrix-servers-vatbaar-voor-hack>).