Ministerie van Onderwijs, Cultuur en Wetenschap

>Retouradres Postbus 16375 2500 BJ Den Haag

De voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Hoger Onderwijs en Studiefinanciering
Rijnstraat 50
Den Haag
Postbus 16375
2500 BJ Den Haag
www.rijksoverheid.nl

Onze referentie
21447964

Bijlagen
1

Datum 14 februari 2020

Betreft Antwoord op schriftelijke vragen van de leden Wiersma en Nijkerken-de Haan (beiden VVD) aan de minister van Onderwijs, Cultuur en Wetenschap over het bericht 'Cyberaanval Universiteit Maastricht duurt mogelijk tot na de kerstvakantie'.

Hierbij zend ik u het antwoord op de vragen van de leden Wiersma en Nijkerken-de Haan (beiden VVD) van uw Kamer inzake het bericht 'Cyberaanval Universiteit Maastricht duurt mogelijk tot na de kerstvakantie'. De vragen werden mij toegezonden bij uw bovenaangehaalde brief met kenmerk 2019Z26211.

Vandaag heb ik uw Kamer tevens nader geïnformeerd over de ransomware-aanval op de Universiteit Maastricht zoals door uw Kamer verzocht tijdens de Regeling van Werkzaamheden van 14 januari jl. In deze brief ga ik ook in op het verzoek van de vaste commissie Onderwijs, Wetenschap en Cultuur, om een beeld te schetsen van de cyberveiligheid in het onderwijs.

De minister van Onderwijs, Cultuur en Wetenschap,

Ingrid van Engelshoven

Antwoorden op de schriftelijke vragen van de leden Wiersma en Nijkerken-de Haan (beiden VVD) van de Tweede Kamer der Staten-Generaal inzake het bericht 'Cyberaanval Universiteit Maastricht duurt mogelijk tot na de kerstvakantie' (ingezonden d.d. 30 december 2019).

Vraag 1
Bent u bekend met het bericht 'Cyberaanval Universiteit Maastricht duurt mogelijk tot na de kerstvakantie' ? 1)

Ja.

Vraag 2
Wat is er precies op kerstavond gebeurd tijdens de cyberaanval op Universiteit Maastricht?

Na de cyberaanval heeft de Universiteit Maastricht gespecialiseerd bureau Fox-IT in de arm genomen om onderzoek te doen naar wat er is gebeurd. Uit het rapport van Fox-IT[1] blijkt dat de aanvaller halverwege oktober via phishing e-mails eerste toegang heeft gekregen tot het netwerk van de Universiteit Maastricht. Vervolgens heeft de aanvaller in een periode van ruim twee maanden zichzelf toegang verschaft tot de rest van het netwerk van de Universiteit Maastricht. Dit heeft er uiteindelijk toe geleid dat aan het begin van de avond van 23 december de zogenaamde ransomware is uitgerold in het systeem, waarmee op 267 servers alle bestanden zijn versleuteld. Onder de getroffen systemen bevonden zich zeer kritieke systemen voor de bedrijfsvoering en zijn enkele back-upservers getroffen. Vervolgens is door de hackers losgeld geëist om de versleuteling van de databestanden op te heffen.

Vraag 3
Wat zijn de gevolgen van de cyberaanval op Universiteit Maastricht voor haar studenten? Welke systemen zijn niet meer bereikbaar? Welke back-upsystemen heeft de Universiteit Maastricht? Zouden goede back-upsystemen niet onderdeel moeten zijn van de reguliere beveiligingsprocessen? Hoe groot is de kans dat de data überhaupt niet meer beschikbaar wordt?

In de kerstvakantie is een groot deel van de data niet beschikbaar geweest voor studenten en zijn systemen niet toegankelijk geweest. Op 6 januari is het onderwijs en onderzoek hervat. De centrale systemen zijn snel weer beschikbaar gesteld en ook de decentrale systemen waren in de loop van januari weer te gebruiken. Een beperkte segmentatie binnen het netwerk was één van de redenen dat dit incident kon ontstaan. De Universiteit Maastricht heeft aangekondigd de aanbevelingen van Fox-IT op dit vlak op te zullen volgen. De Universiteit Maastricht geeft bovendien aan dat er voor elk cruciaal systeem inmiddels beter afgeschermde back-ups zijn gemaakt. Er zijn vooralsnog geen aanwijzingen over verminderde beschikbaarheid van data.

Vraag 4
Welke stappen worden er gezet om de documenten van en voor studenten veilig te stellen? In hoeverre heeft de Universiteit Maastricht haar studenten hierover geïnformeerd?

en

[1] Spoedondersteuning Project Fontana, 5 februari 2020, Fox-IT.

Vraag 5
In hoeverre kan Universiteit Maastricht garanderen dat wetenschappelijke data beschermd is? Hoe gaat u dit waarborgen?

In het door Fox-IT uitgevoerde onderzoek is uitdrukkelijk aandacht besteed aan eventuele data-extractie. Fox-IT concludeert: "Tijdens het onderzoek zijn sporen aangetroffen die aantonen dat de aanvaller data heeft verzameld aangaande de topologie van het netwerk, gebruikersnamen en wachtwoorden van meerdere accounts, en andere netwerkarchitectuur-informatie. Fox-IT heeft binnen de scope van het onderzoek geen sporen aangetroffen die wijzen op het verzamelen van andersoortige data. Additioneel forensisch onderzoek op kritieke systemen, ook wel aangeduid als kroonjuwelen, zou hier meer inzicht in kunnen bieden." De Universiteit Maastricht heeft aangekondigd vervolgonderzoek te (laten) doen. De Universiteit Maastricht heeft studenten en andere betrokken nagenoeg dagelijks op de hoogte gesteld via de website en sociale media. Studenten hebben hier volgens de Universiteit Maastricht in algemene zin waardering voor geuit.

Vraag 6
Hoe gaat Universiteit Maastricht er zo snel mogelijk voor zorgen dat de gijzeling van haar computersystemen wordt beëindigd? Heeft u aanwijzingen dat de universiteit hiervoor losgeld gaat betalen? Kunt u het betalen van losgeld uitsluiten?

en

Vraag 7
In hoeverre bent u het met het Expertisecentrum Cyberweerbaarheid Limburg eens, dat het moeilijk te verkopen is dat overheidsinstellingen criminelen gaan betalen om een einde te maken aan de cyberhack van Universiteit Maastricht? In hoeverre bent u betrokken bij het besluit om wel of niet losgeld te betalen aan deze criminelen? Deelt u de mening dat het betalen van deze criminelen ervoor zorgt dat hun verdienmodel in stand wordt gehouden?

Door de Universiteit Maastricht ben ik op de hoogte gesteld van het feit dat er losgeld is betaald aan de criminele organisatie, inclusief de hoogte van het bedrag. Voordat de Universiteit Maastricht hiertoe over is gegaan, heb ik de universiteit kenbaar gemaakt dat de regering van mening is dat er geen geld naar criminelen toe moet vloeien. Het is de eigen afweging van het college van bestuur van de Universiteit Maastricht geweest om het losgeld te betalen. De universiteit heeft mij te kennen gegeven dat de betaling van het losgeld, inclusief alle overige kosten die samenhangen met de ransomware-aanval, bekostigd zijn uit de verkoop van een deelneming van de holding Universiteit Maastricht.

Vraag 8
Kan Universiteit Maastricht er zeker van zijn dat het betalen van de criminelen er ook daadwerkelijk voor zorgt dat de cyberaanval stopt? 2) Zo nee, hoe gaat u er dan voor zorgen dat dit niet gebeurt?

Na het betalen van het losgeld zijn alle versleutelde gegevens van de Universiteit Maastricht ontsleuteld. Daarvoor en daarna heeft de Universiteit Maastricht mitigerende maatregelen getroffen zodat de criminelen geen toegang meer hadden tot het netwerk.

Vraag 9
Op welke manier biedt het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) op dit moment hulp aan Universiteit Maastricht?

Kort na de cyberaanval heeft de UM contact opgenomen met het ministerie van

OCW en gedurende de aanval is er nauw contact onderhouden tussen de Universiteit Maastricht, het ministerie van OCW, de Inspectie, de NCTV, het NCSC en SURF om een volledig beeld te verkrijgen en te adviseren.

Universiteiten en Hogescholen hebben met ondersteuning van OCW in 2018 een Platform Integrale Veiligheid Hoger Onderwijs (Platform IV-HO) opgericht om expertise te bundelen en grip te krijgen op incidenten en veiligheidsrisico's in het hoger onderwijs waaronder in het cyberdomein. Daarnaast heeft onderwijs-ICT-organisatie SURF veel expertise op het gebied van digitale veiligheid. SURF en het Platform IV-HO staan met elkaar in nauw contact en bundelen zo hun kracht om universiteiten en hogescholen zo goed mogelijk bij te staan en voor te bereiden op dergelijke situaties. Ook in deze situatie hebben het Platform IV-HO en SURF hun expertise beschikbaar gesteld.

Vraag 10
Hoeveel andere universiteiten in Nederland hebben te maken met dergelijke cyberaanvallen of pogingen daartoe? Heeft u aanwijzingen dat naast Universiteit Maastricht ook andere Nederlandse universiteiten aan de beurt zijn?

Cyberaanvallen op grote instellingen in de private en publieke sector zijn aan de orde van de dag. Zo ook bij universiteiten. De universiteiten hebben mij aangegeven dat zij maatregelen hebben aangescherpt om aanvallen af te slaan of de gevolgen van aanvallen te beperken. Daarbij is het goed te realiseren dat 100% veiligheid niet bestaat, zo concludeert ook de Wetenschappelijke Raad voor Regeringsbeleid in het rapport "Voorbereiden op digitale ontwrichting".[2] De WRR stelt daarin dat het volledig voorkomen van digitale incidenten een illusie is.

Vraag 11
Deelt u de mening dat informatieveiligheid een belangrijk onderdeel is van de organisatie van onderwijsinstellingen? In hoeverre wordt hierop toegezien binnen de reguliere inspectie?

Het instellingstoezicht door de Inspectie van het Onderwijs (hierna: Inspectie) vindt in het hoger onderwijs plaats naar aanleiding van incidenten of signalen van niet-naleving. De Wet op het hoger onderwijs en wetenschappelijk onderzoek geeft geen specifieke voorschriften voor informatieveiligheid. Van het bestuur mag worden verwacht dat zij zorgdraagt voor de goede voortgang van het onderwijs en daartoe verantwoorde beslissingen neemt over alle aspecten die dat mogelijk maken. Daaronder valt ook de verantwoordelijkheid voor informatieveiligheid. In dat kader heeft de Inspectie een onderzoek ingesteld.

Vraag 12
Zijn er al aanwijzingen waar de cyberaanval op Universiteit Maastricht vandaan komt en met welk doel deze cyberaanval is uitgevoerd? Is de aanval vergelijkbaar met de aanval op Universiteit Antwerpen van afgelopen oktober?

Fox-IT geeft aan dat de werkwijze van de aanvaller overeenkomt met een bij hen bekende criminele groepering, publiek bekend als 'TA505', die –volgens hun informatie- al meer dan 150 slachtoffers heeft gemaakt in 2019. De werkwijze is vergelijkbaar met die van de aanval op de Universiteit Antwerpen.

Vraag 13
Welke stappen gaat u zetten om dergelijke cyberaanvallen in de toekomst te voorkomen? 3)

In de Kamerbrief 'Cyberveiligheid in het onderwijs' heb ik aangekondigd dat in het

[2] Wetenschappelijke Raad voor het Regeringsbeleid (2019) Voorbereiden op digitale ontwrichting, wrr-Rapport 101, Den Haag: wrr.

mbo en hoger onderwijs aanvullende acties worden gepleegd om de cyberveiligheid te versterken. In de acties is aandacht voor de lessen die zijn getrokken uit de aanval op Universiteit Maastricht, de toetsing van digitale veiligheid in het onderwijs, de monitoring en scanfunctie en voor vergroten van awareness. Vanuit mijn rol als verantwoordelijke voor de continuïteit van het gehele stelsel, zal ik mij ervan vergewissen dat de continuïteit ook in dit geval geborgd is en mij met enige regelmaat laten informeren over de voortgang van de aangekondigde acties.

1) https://nos.nl/artikel/2316373-cyberaanval-universiteit-maastricht-duurt-mogelijk-tot-na-kerstvakantie.html
2) https://www.1limburg.nl/cyberaanval-universiteit-maastricht-kan-nog-weken-duren?context=default
3) https://www.nieuwsblad.be/cnt/dmf20191028_04690427