Ministerie van Economische Zaken
en Klimaat

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Binnenhof 4
2513 AA DEN HAAG

Directoraat-generaal
Bedrijfsleven & Innovatie
Directie Innovatie en Kennis

Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag

Postadres
Postbus 20401
2500 EK Den Haag

Overheidsidentificatienr
00000001003214369000

T 070 379 8911 (algemeen)
F 070 378 6100 (algemeen)
www.rijksoverheid.nl/ezk

Datum 30 juni 2020
Betreft Beantwoording vragen over het bericht 'Onderzoeksinstituut Wetsus in Leeuwarden gehackt, hacker betaald in bitcoins'

Ons kenmerk
DGBI-I&K / 20175174

Uw kenmerk
2020Z03095

Geachte Voorzitter,

Hierbij stuur ik u, mede namens de Minister van Onderwijs, Cultuur en Wetenschappen, de antwoorden op de vragen van de leden Wiersma en Aukje de Vries (beiden VVD) over het bericht "Onderzoeksinstituut Wetsus in Leeuwarden gehackt, hacker betaald in bitcoins" (ingezonden 17 februari 2020, met kenmerk 2020Z03095).

Hoogachtend,

mr. drs. M.C.G. Keijzer
Staatssecretaris van Economische Zaken en Klimaat

Directoraat-generaal
Bedrijfsleven & Innovatie
Directie Innovatie en Kennis

Ons kenmerk
DGBI-I&K / 20175174

2020Z03095

1
Ben u bekend met het bericht 'Onderzoeksinstituut Wetsus in Leeuwarden gehackt, hacker betaald in bitcoins'?

Antwoord
Ja.

2
Wat heeft er precies plaatsgevonden bij het onderzoeksinstituut Wetsus met betrekking tot de ransomeware-aanval?

Antwoord
Op maandag 3 februari heeft een niet geïdentificeerde hacker een ransomeware-aanval uitgevoerd op Wetsus. Door de cyberaanval was tot en met 11 februari het netwerk en de e-mailserver van Wetsus niet toegankelijk. Wetsus heeft op 3 februari direct actie ondernomen en het incident gemeld bij de aangewezen instanties: de politie, de Autoriteit Persoonsgegevens en het Nationaal Cyber Security Center. Na overleg met cybersecurity experts heeft Wetsus de afweging gemaakt om losgeld te betalen.

3
Worden er minimale veiligheidseisen gesteld op het gebied van cyberveiligheid bij onderzoeksinstituten die een financiering vanuit de overheid ontvangen? Zo ja, wat zijn die eisen? Zo nee, waarom niet?

Antwoord
Het borgen van de (cyber)veiligheid is primair een verantwoordelijkheid van onderzoeksinstituten zelf, uiteraard met inachtneming van de relevante wet- en regelgeving. Afhankelijk van het onderzoeksinstituut kunnen er specifieke aanvullende eisen aan de (cyber)veiligheid gesteld worden. Zo zijn de onderzoeksinstituten die onderzoek doen voor het ministerie van Defensie onderworpen aan de Algemene Beveiligingseisen Defensieopdrachten 2019 (ABDO 2019), waarin een heel hoofdstuk is gewijd aan cyberveiligheid. Deze eisen gelden bijvoorbeeld voor de TO2-instellingen TNO, Marin en NLR.

4
Ziet u aanleiding om voortaan minimale cyberveiligheidseisen te stellen aan onderzoeksinstituten die financiering ontvangen vanuit nationale of Europese instellingen? Zo nee, waarom niet?

Antwoord
Nee. Cyberveiligheid is een verantwoordelijkheid van de onderzoeksinstituten zelf en dient binnen de eigen bedrijfsvoering geregeld te worden. Defensie-gerelateerd onderzoek vormt hierop een uitzondering. Via de Algemene Beveiligingseisen Defensieopdrachten (ABDO) bestaat er een minimale set van eisen voor kennisinstellingen die onderzoek doen voor het ministerie van Defensie. Mijn ministerie is naar aanleiding van de incidenten bij de Universiteit Maastricht en

Wetsus in gesprek gegaan met de TO2-federatie en andere onderzoeksinstituten om het veiligheidsbewustzijn te vergroten en de samenwerking op het gebied van cyberveiligheid te verbeteren. Daarnaast zijn de gesprekken bedoeld om verder te bezien hoe de Rijksoverheid kan faciliteren dat onderzoeksinstellingen ook in de toekomst beschermd blijven tegen cyberaanvallen en cybercriminaliteit.

5
Heeft de ransomeware-aanval gevolgen voor de gelden die ontvangen worden uit Europese programma's, zoals Horizon 2020? Kennen deze programma's minimale eisen van cyberveiligheid die gevraagd worden aan ontvangers?

Antwoord
Horizon 2020 kent geen specifieke eisen met betrekking tot cyberveiligheid. Wel kent het Kaderprogramma bepalingen rondom data-management (zoals de bescherming van persoonsgegevens) en ethiek. Subsidieontvangers zijn verplicht persoonlijke data te verwerken onder de geldende EU- en nationale databeschermingswetgeving. Een cyberaanval zelf heeft geen directe gevolgen voor de bijdragen verkregen uit Horizon 2020-projecten. In de projectrapportage zal de begunstigde moeten aangeven hoe is voldaan aan de geldende voorwaarden en bepalingen. Er wordt van begunstigden verwacht dat zij in de rapportage aan de Europese Commissie aangeven hoe zij met de gevolgen van een dergelijk incident zijn omgegaan, met name in de context van bescherming van persoonlijke data. Wanneer een beneficiant gebleken nalatigheid is te verwijten, heeft de Europese Commissie de mogelijkheid over te gaan tot vermindering van de subsidie en/of beëindiging van de *Grant Agreement* van de betrokken deelnemer.

6
Wanneer en op welke manier bent u op de hoogte gesteld van de ransomeware-aanval van onderzoeksinstituut Wetsus?

Antwoord
Op woensdag 5 februari heeft de directie van Wetsus telefonisch contact gelegd met het ministerie van Economische Zaken en Klimaat. Gedurende de cyberaanval is er regelmatig contact geweest.

7
Op welke manier heeft u het onderzoeksinstituut Wetsus ondersteuning geboden bij het verhelpen van de ransomeware-aanval?

Antwoord
Mijn ministerie heeft de directie van Wetsus direct geïnformeerd over de instanties die kunnen adviseren in het geval van een cyberaanval. Wetsus heeft in dit gesprek aangegeven de verantwoordelijke instanties benaderd te hebben en met politie en cybersecurity experts reeds te werken aan een oplossing.

8
Op welke manier heeft de ransomware-aanval van het onderzoeksinstituut Wetsus overeenkomsten met die van de Universiteit Maastricht eind vorig jaar?

Antwoord
In beide gevallen is het netwerk ontoegankelijk gemaakt door een onbekende hacker die het netwerk pas vrij gaf na betaling van losgeld.

9
Hoeveel losgeld is er uiteindelijk aan de criminelen betaald? Hoe beoordeelt u de keuze dat dit heeft plaatsgevonden? Van welke geld wordt dit betaald? Komt dit geld direct uit de verstrekte subsidies?

Antwoord
Het kabinet is van mening dat er geen geld naar (cyber)criminelen toe moet vloeien. Het is echter een eigen afweging van Wetsus geweest om losgeld te betalen. In overleg met de politie heeft Wetsus verder geen details gegeven over de hoogte van het betaalde bedrag. Wetsus heeft het ministerie van Economische Zaken en Klimaat geïnformeerd dat het losgeld is gefinancierd uit het eigen vermogen en niet uit ontvangen subsidies.

10
Deelt u de mening dat het betalen van criminelen alleen maar hun businessmodel van ransomeware steunt en dat overheidsgeld niet gebruikt moet worden om criminelen te financieren? Zo ja, welke maatregelen gaat u nemen om herhaling te voorkomen? Hoe wordt hierbij rekening gehouden bij een eventuele aanvraag voor financiering van onderzoeksinstituut Wetsus voor het jaar 2021? Zo nee, welke maatregelen gaat u desondanks nemen om herhaling te voorkomen?

Antwoord
Het kabinet is van mening dat er geen losgeld aan (cyber)criminelen zou moeten vloeien. Het borgen van de cyberveiligheid is echter een verantwoordelijkheid van kennisinstellingen zelf. Desondanks zien we dat kennisinstellingen in toenemende mate worden geconfronteerd met geavanceerde cyberdreigingen. Na het incident bij de Universiteit Maastricht heeft het ministerie van Onderwijs, Cultuur en Wetenschappen aangegeven te verwachten dat hoger onderwijsinstellingen zich bewust zijn van kwetsbaarheden en zo veel mogelijk kennis delen, periodiek hun eigen systemen door experts laten controleren en bij een effectieve aanpak van de digitale veiligheid rekenschap geven van de risico's van hun aanpak, zoals de risico's bij een vergaande decentralisatie van de ICT-systemen.

Hogeronderwijsinstellingen zijn momenteel concreet bezig met maatregelen om dit te realiseren. Naar aanleiding van de incidenten bij de Universiteit Maastricht en Wetsus is mijn ministerie in gesprek gegaan met de TO2-federatie en andere kennisinstellingen om te bezien hoe de samenwerking tussen kennisinstellingen kan worden verbeterd en of er een rol ligt voor het ministerie om te faciliteren dat kennisinstellingen in de toekomst beter beschermd zijn tegen cyberaanvallen en cybercriminaliteit.

11
In hoeverre kan de hack van het onderzoeksinstituut Wetsus worden gelieerd aan de waarschuwing van de AIVD dat het veiligheidsbewustzijn en de weerbaarheid

van Nederlandse kennisinstellingen onvoldoende zijn tegen risico's van diefstal van onderzoeksbevindingen vanuit landen zoals China?

Antwoord
Nederlandse kennisinstellingen zijn zich er van bewust dat naast de voordelen van internationale samenwerking er ook risico's bestaan op ongewilde kennisoverdracht en de negatieve gevolgen hiervan. Het veiligheidsbewustzijn en de weerbaarheid van Nederlandse universiteiten en hogescholen wordt gestimuleerd in het platform Integraal Veilig Hoger Onderwijs. Dit platform is met steun van het ministerie van Onderwijs, Cultuur en Wetenschappen ingericht door de Vereniging van Nederlandse Universiteiten en de Vereniging Hogescholen. Hierin werken bestuurders en veiligheidsexperts van hoger onderwijsinstellingen samen aan het stimuleren van veiligheidsbewustzijn door het uitwisselen van kennis en kunde en het ontwikkelen van tools en handreikingen.

Op verzoek van de ministeries van Onderwijs, Cultuur en Wetenschappen en Buitenlandse Zaken ontwikkelde het *The Hague Centre for Strategic Studies* de 'Checklist voor Samenwerking met Chinese Academische en Kennisinstellingen'. Daarnaast is het ministerie van Buitenlandse Zaken een traject gestart om te onderzoeken in hoeverre aanvullende maatregelen gewenst zijn om ongewenste kennis- en technologieoverdracht in brede zin via academisch onderwijs en onderzoek te voorkomen. In dit traject wordt onder andere onderzocht of en zo ja op welke manier een brede kennisregeling kan worden opgezet. Verder is mijn ministerie in gesprek gegaan met de TO2-federatie en andere kennisinstellingen om te kijken hoe het veiligheidsbewustzijn en de samenwerking tussen kennisinstellingen kan worden verbeterd en of er een rol ligt voor het ministerie om te faciliteren dat kennisinstellingen in de toekomst beter beschermd zijn tegen cyberaanvallen en cybercriminaliteit.

12
Is er volgens u binnen kennisinstituten voldoende bewustzijn over het plaatsvinden van spionage door China? Zo nee, wat gaat u doen om dit bewustzijn te vergroten? Zo ja, welke maatregelen worden binnen deze instituten genomen?

Antwoord
De TO2- en NWO-instituten zijn zich er van bewust dat naast de voordelen van internationale samenwerking er ook risico's bestaan op ongewilde kennisoverdracht en de negatieve gevolgen hiervan. Zowel de TO2-instituten als NWO (en KNAW) volgen daarom actief de ontwikkelingen en de informatie van de Rijksoverheid ten aanzien van kennisveiligheid. NWO-I, de institutenorganisatie van NWO, neemt bijvoorbeeld deel aan het overleg van het Ministerie van Onderwijs, Cultuur en Wetenschappen met het kennisveld over de kennisveiligheid en mogelijke maatregelen. De door het Ministerie van Buitenlandse Zaken en het *The Hague Centre for Strategic Studies* ontwikkelde Checklist voor Samenwerking met Chinese Academische en Kennisinstellingen is hierbij zeer behulpzaam.

13
Hoe helpt de Nederlandse regering kennisinstituten met het beschermen van hun kennis, patenten, octrooien etc.? Wordt hier voorlichting over gegeven aan

kennisinstituten? Bestaan er, net zoals hij het MKB, subsidies voor cyberweerbaarheid voor onderzoeksinstituten? Zo nee, waarom niet?

Antwoord
Kennisinstituten kunnen gebruik maken van het juridisch instrumentarium om kennis te beschermen en doen dat in de praktijk ook. Daarbij kan gedacht worden aan de octrooiwetgeving en de wetgeving voor de bescherming van bedrijfsgeheimen. Bij gelegenheid van het van kracht worden van de Wet bescherming bedrijfsgeheimen (2018) heeft ook een voorlichtingscampagne over het belang van een adequate bescherming van bedrijfsvertrouwelijke informatie plaatsgevonden. Momenteel worden er geen subsidies voor cyberweerbaarheid verstrekt aan kennisinstellingen. Uit de gesprekken met de kennisinstellingen zal moeten blijken of deze meerwaarde zouden kunnen hebben.

14
Op welke manier ontvangt het onderzoeksinstituut Wetsus financiering van de lokale, nationale en Europese overheid? Hoe hoog zijn deze bedragen? Klopt het ook dat onderzoeksinstituut Wetsus nog opzoek is naar financiering voor het jaar 2021? Wat gaat u (daarmee) doen?

Antwoord
In de periode 2016-2020 ontving Wetsus financiering vanuit het bedrijfsleven (3,5 miljoen per jaar), universiteiten (3 miljoen per jaar), NWO (0,5 miljoen per jaar) en subsidies vanuit de rijkoverheid en de regio (6,5 miljoen per jaar, waarvan 4,75 uit de Zuiderzeelijnmiddelen). Daarnaast wordt jaarlijks ongeveer 1,5 miljoen aan Europese middelen ingezet.

Het klopt dat Wetsus op zoek is naar financiering vanaf 2021, omdat de financiering vanuit de zogenaamde Zuiderzeelijnmiddelen in 2021 ophoudt. Voor het bedrijfsleven, de universiteiten, de regio en het Rijk is Wetsus een belangrijk kennisinstituut dat toonaangevend onderzoek verricht op het gebied van watertechnologie en een belangrijke bijdrage kan leveren aan het missiegedreven innovatiebeleid, met name binnen het maatschappelijke thema Landbouw, Water Voedsel. In de in januari 2019 door NWO uitgevoerde evaluatie van Wetsus wordt dit bevestigd. Vanwege het belang van Wetsus heb ik een groep van experts en stakeholders ingesteld. Over hun advies heb ik uw Kamer op 4 juni jl. geïnformeerd.[1] Ik heb hierin aangekondigd dat met de bij dit advies betrokken stakeholders afspraken zijn gemaakt over een overbruggingsfinanciering voor de jaren 2021 en 2022. Voor de jaren na 2021 wordt door de expertgroep een aantal kansrijke routes geschetst die de komende tijd door Wetsus verder uitgewerkt zullen worden.

15
Klopt het dat uit onderzoek, dat is uitgevoerd in opdracht van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), is gebleken dat het financieringsmodel van onderzoeksinstituut Wetsus niet duurzaam is en dat een onafhankelijke commissie heeft geadviseerd om het financieringsmodel minder

[1] Kamerstuk 33 009, nr.90

afhankelijk te maken overheidsfinanciën? Welke oplossing ziet u daarvoor, aangezien Wetsus is een belangrijk kennisinstituut is?

Antwoord
Zie antwoord op vraag 14.

16
Kunt u deze vragen afzonderlijk beantwoorden?

Antwoord
Ja. Enkel de beantwoording van vragen 14 en 15 is samengenomen.