Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

Aanhangsel van de Handelingen

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

3779

Vragen van de leden **Van der Woude** (VVD) en **Peters** (CDA) aan de Minister van Onderwijs, Cultuur en Wetenschap over *het bericht «AIVD: hoger onderwijs is zich totaal niet bewust van digitale dreiging»* (ingezonden 14 juni 2021).

Antwoord van Minister **Van Engelshoven** (Onderwijs, Cultuur en Wetenschap) (ontvangen 25 augustus 2021). Zie ook Aanhangsel Handelingen, vergaderjaar 2020–2021, nr. 3387.

Vraag 1
Bent u bekend met het artikel in ScienceGuide «AIVD: hoger onderwijs is zich totaal niet bewust van digitale dreiging»[1] over uitspraken van de heer Akerboom tijdens de technische briefing van de AIVD aan de Vaste Commissie voor Binnenlandse Zaken ten aanzien van het gebrek aan bestuurlijke aandacht voor digitale veiligheid bij hogescholen en universiteiten?

Antwoord 1
Ja

Vraag 2
Hoe kijkt u aan tegen de uitspraak van de heer Akerboom dat kennisinstellingen in het hoger beroepsonderwijs en wetenschappelijk onderwijs niet zijn doordrongen van de dreiging van cyberaanvallen van statelijke actoren? Bent u het eens met de heer Akerboom dat het bewustzijn hierover bij universiteiten en hogescholen nog te laag is? Zo ja, wat gaat u hieraan doen? Zo nee, waarom niet?

Antwoord 2
Ik ben op het gebied van kennisveiligheid en cyberveiligheid in gesprek met kennisinstellingen, de koepels en ook met het Nationaal Cyber Security Centrum (NCSC). Deze instellingen heb ik ook betrokken bij de laatste Kamerbrief over cyberveiligheid, die ik op 19 mei 2021[2] naar uw Kamer heb gestuurd.

[1] ScienceGuide, 9 juni 2021, AIVD: hoger onderwijs is zich totaal niet bewust van digitale dreiging, www.scienceguide.nl/2021/06/aivd-hoger-onderwijs-is-zich-totaal-niet-bewust-van-digitale-dreiging/

[2] Kamerbrief «Cyberveiligheid in het hoger onderwijsveld en onderzoeksveld», 19 mei 2021

ah-tk-20202021-3779
ISSN 0921 - 7398
's-Gravenhage 2021

Mijn indruk is dat de instellingen zich bewust zijn van de dreiging van cyberaanvallen, of deze dreiging nu van statelijke actoren of van hackersgroepen afkomstig is. Ik ben het met de heer Akerboom eens dat de veiligheid van onze instellingen verder moet worden verhoogd. Het is duidelijk dat deze bewustwording nodig is in alle lagen van de organisaties en vertaald dient te worden in maatregelen gericht op het tegengaan van dreigingen. De hoger onderwijsinstellingen zijn hier dan ook actief mee bezig en ik zal de voortgang van de instellingen blijven volgen, zoals ik in de Kamerbrief heb aangekondigd. Daarbij realiseer ik mij dat cyberveiligheid een gezamenlijke verantwoordelijkheid is van zowel de instellingen als de overheid. Belangrijk hierbij is dat de cyberveiligheid van instellingen expliciet wordt meegenomen in de reguliere bestuurlijke gesprekken die mijn ministerie met de instellingen en de koepels voert. Deze periodieke gesprekken over cyberveiligheid bevorderen het internaliseren van cyberveiligheidsmaatregelen in de bedrijfsvoering van de gehele sector.
In die Kamerbrief heb ik ook beschreven welke concrete maatregelen de hoger onderwijs- en kennisinstellingen nemen om hun digitale veiligheid te verhogen. Dit doen zij bijvoorbeeld door monitoringssystemen, maar ook door het vergroten van bewustwording en trainingen. Een knooppunt in de aanpak van cyberdreigingen is het SURF Computer Emergency Response Team (SURFcert), dat 24/7 ondersteuning biedt bij cyberincidenten en in direct contact staat met het NCSC. Daarnaast is er, op initiatief van de hoger onderwijsinstellingen, een Security Operations Center (SURFsoc) gerealiseerd bij SURF. Een belangrijk onderdeel van het SOC is de 24/7 monitoring van netwerken en de signalering van dreigingen bij deelnemende instellingen. De continue monitoring helpt instellingen enorm met het versterken van de informatiebeveiliging, omdat er constant informatie wordt verzameld die bij mogelijke dreigingen snel sector breed wordt gedeeld. De toetreding van instellingen tot de SURFsoc zal nu gefaseerd plaatsvinden, door de technische en contractuele voorbereidingen die per instelling moeten worden getroffen.

Vraag 3
Hoe verhouden de uitspraken van de heer Akerboom zich met uw uitspraken in de kamerbrief[3] van 19 mei 2021 waarin u stelt dat «cyberveiligheid bij de hoger onderwijs- en onderzoekinstellingen hoog op de agenda staat»? Baseert u deze veronderstelling enkel op gesprekken met kennis- en onderzoeksinstellingen of heeft u hier zelf ook actief onderzoek naar gedaan? Hoe verklaart u de uitspraak van de heer Akerboom dat er bij hogescholen en universiteiten onvoldoende bestuurlijke aandacht is voor digitale veiligheid?

Antwoord 3
De directeur-generaal van de AIVD, heeft in de technische briefing over de WIV d.d. 2 juni 2021 gepleit voor een breed cyberoffensief, te beginnen met een betere awareness en actie in eigen huis. Zijn uitspraken in de technische briefing over cyberveiligheid betroffen kennisinstellingen, het bedrijfsleven en de overheid.Zowel bij kennisinstellingen, overheden als bedrijfsleven bestaat aandacht voor (cyber)veiligheid, maar actie en bewustzijn is volgens de directeur-generaal nodig in alle lagen van de betrokken organisaties. Zoals ik ook bij vraag 2 meldde, ben ik het met hem eens dat de digitale veiligheid van de instellingen verder kan worden vergroot. Ik heb daarom de instellingen eerder al opgeroepen om hun veiligheidsbeleid in hun jaarverslagen op te nemen wanneer dit nog niet het geval is, dit onderwerp structureel met hun Raden van Toezicht te bespreken en een meerjarenvisie op dit terrein te presenteren. De genomen maatregelen (zie vraag 2 en de Kamerbrief) laten wat mij betreft zien dat de instellingen de cyberveiligheid serieus nemen. Het bereiken van 100% veiligheid is helaas onmogelijk, er zal altijd een risico op cyber- en kennisveiligheidsincidenten blijven bestaan.

Vraag 4
In hoeverre hebben kennisinstellingen oog voor ogenschijnlijk «onschuldige» incidenten, zoals de cyberaanvallen bij de Universiteit van Amsterdam en de Hogeschool van Amsterdam van afgelopen februari, die mogelijkerwijs

[3] Kamerstuk 31 288, nr. 910

grotere gevolgen kunnen hebben? Zoals een opmaat tot cyberaanvallen met meer impact?

Antwoord 4
Ik denk dat, wanneer het gaat om de preventie van cyberaanvallen, er niet gesproken kan worden over «ogenschijnlijk onschuldige incidenten». Uiteindelijk kan de aangerichte schade wel verschillen, maar de preventiebenadering is dezelfde. De schade van deze «onschuldige» incidenten is juist beperkt gebleven doordat de kennisinstellingen goed samenwerken en kennis over de cyberaanvallen binnen hun netwerk snel met elkaar delen. Dat doen zij zowel bij zwaardere als bij lichtere incidenten, want er wordt door SURF 24/7 gemonitord en ondersteuning geboden. Bij dit incident speelde ook de vroege detectie door het Security Operations Centre (SOC) en ingrijpen door het Computer Emergency Response Team (CERT) een belangrijke rol in het inperken van de impact.

Vraag 5
Erkent u, naast de dreiging van ransomware aanvallen, de dreiging vanuit statelijke actoren als het gaat om spionage, met name gericht op het verkrijgen van hightech kennis en informatie, en sabotage? Zo ja, welke gerichte stappen gaat u nemen naar aanleiding van dit signaal van de AIVD om de bestuurlijke aandacht voor digitale veiligheid te vergroten? Zo nee, waarom niet?

Antwoord 5
In een eerdere brief[4] over kennisveiligheid schreef ik dat het verwerven van (hoogwaardige) kennis voor diverse statelijke actoren tot hun strategische doelstellingen behoort. Ik heb in die brief ook verschillende maatregelen benoemd om de kennisveiligheid in het hoger onderwijs en de (toegepaste) wetenschap beter te borgen, welke momenteel worden uitgevoerd. Zo komt er dit jaar nog een specifieke «leidraad» voor kennisveiligheid beschikbaar, die de rijksoverheid samen met de kennissector ontwikkelt. Ook worden er bestuurlijke afspraken gemaakt met de kennisinstellingen waarin de aandacht ook naar digitale veiligheid zal uitgaan. Bovendien wordt een Expertise- en adviesloket Kennisveiligheid opgezet om kennisinstellingen te ondersteunen bij de afwegingen die zij vanuit hun verantwoordelijkheid maken. In dit kader hebben de Nederlandse universiteiten al een belangrijke stap gezet door op 8 juli het Kader Kennisveiligheid te presenteren. Door dit kader kunnen wetenschappers en universiteiten nog scherper de afweging maken tussen de openheid van wetenschap en het voorkomen van ongewenste kennisoverdracht.
Naast de eerder genoemde maatregelen die instellingen nemen om hun digitale veiligheid te vergroten, heb ik zoals ik ook aangaf in het antwoord op vraag 4 en de Kamerbrief «Cyberveiligheid in het hoger onderwijsveld en onderzoeksveld», de instellingen opgeroepen om hun veiligheidsbeleid in hun jaarverslagen op te nemen, dit onderwerp structureel met hun Raden van Toezicht te bespreken en een meerjarenvisie op dit terrein te presenteren. De rol van bestuurders hierbij is evident, zo ook het belang van een integrale veiligheidsaanpak in het onderwijs-en onderzoeksveld.

Vraag 6
Bent u het ermee eens dat de activiteiten van statelijke actoren een hogere prioriteit moeten krijgen als het gaat om de (digitale) beveiliging van onze kennisinstellingen? Zo ja, hoe gaat u dit concreet oppakken in samenwerking met universiteiten, hogescholen en de AIVD? Zo nee, waarom niet?

Antwoord 6
De maatregelen die ik heb benoemd bij het antwoord op vraag 5 laten zien dat de rijksoverheid en de kennisinstellingen momenteel al intensief samenwerken om kennisveiligheid in het hoger onderwijs en bij de kennisinstellingen te verhogen. Ik zal uw Kamer in het najaar van 2021 opnieuw

[4] Kamerbrief «Maatregelen Kennisveiligheid voor Hoger Onderwijs en Wetenschap» van 27 november 2020.

informeren over de voortgang die er op het gebied van kennisveiligheid wordt geboekt.