Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

31 288 Hoger Onderwijs-, Onderzoek- en Wetenschapsbeleid

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 910

BRIEF VAN DE MINISTER VAN ONDERWIJS, CULTUUR EN WETENSCHAP

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 19 mei 2021

Op 25 februari jl. heb ik uw Kamer geïnformeerd dat de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) slachtoffer is geworden van een ransomware-aanval.[1] Ik heb toegezegd dat ik uw Kamer nader zou informeren over dit incident.

Helaas komt cybercriminaliteit steeds vaker voor, waarbij ook hoger onderwijs- en onderzoeksinstellingen worden getroffen. In deze brief zal ik kort ingaan op de stappen die er, op het gebied van cyberveiligheid, sinds juli 2020[2] in deze sector zijn gezet. Daarna ga ik kort in op de incidenten die plaatsvonden bij NWO, de Universiteit van Amsterdam (UvA), de hogeschool van Amsterdam (HvA) en Inholland. Tot slot wil ik stilstaan bij het belang van een integrale veiligheidsaanpak in het hoger onderwijs- en onderzoeksveld.

Belangrijke stappen gezet in de sector

Sinds de aanval op de Universiteit Maastricht, eind 2019, heeft de sector op het gebied van cyberveiligheid en in haar aanpak van cyberdreigingen belangrijke stappen gezet. Deze benoemde ik eerder in de Kamerbrief *«Onderzoek naar cyberaanval Universiteit Maastricht en maatregelen cyberveiligheid»*[3]. In die brief ging ik in op het belang van het vergroten van cyberbewustzijn bij medewerkers en studenten, risicomanagement en het belang van een ketenbrede samenwerking in onderwijs en onderzoek. Ook kondigde ik aan dat ik de Kamer begin dit jaar zou informeren over het onderzoek van de Inspectie naar de cyberveiligheid op stelselniveau. De resultaten van dit onderzoek worden dit kwartaal verwacht. Ik zal uw Kamer hierover informeren.

[1] Kamerstukken 26 643 en 29 338, nr. 744.
[2] Kamerstukken 31 288 en 26 643, nr. 872.
[3] Zie ook voetnoot 2.

kst-31288-910
ISSN 0921 - 7371
's-Gravenhage 2021

Uit de gesprekken die ik met de instellingen heb gevoerd blijkt dat cyberveiligheid bij de hoger onderwijs- en onderzoeksinstellingen hoog op de agenda staat. Er wordt goed samengewerkt tussen instellingen, informatie over cyberaanvallen wordt snel en open met elkaar gedeeld en de instellingen zijn transparant over de ontstane situatie wanneer een incident zich voordoet. Deze samenwerking is cruciaal om crises snel het hoofd te bieden, de gevraagde capaciteit zo snel mogelijk beschikbaar te hebben en om eventuele vergelijkbare aanvallen bij andere instellingen vroegtijdig af te wenden. Door deze sectorbrede aanpak zijn de gevolgen van een aantal recente incidenten beperkt gebleven, zoals die bij de UvA, HvA en Inholland.

Zoals ik eerder aangaf[4] ligt de verantwoordelijkheid van een goede bedrijfsvoering, conform de WHW, bij de instelling zelf. De instelling is dus in beginsel ook zelf verantwoordelijk om de eigen kwetsbaarheden in de cyberveiligheid te mitigeren en de beveiliging op orde te hebben. Toch blijkt uit de gesprekken met het veld dat goede samenwerking tussen instellingen en de overheid nodig is om dit vraagstuk aan te kunnen gaan. Daarbij realiseer ik me dat ook instellingen die zeer goed zijn voorbereid kunnen worden getroffen en dat 100% veiligheid in geen enkele sector realistisch is.

Risicomanagement

Voor hoger onderwijs- en onderzoeksinstellingen is het SURF Computer Emergency Response Team (SURFcert) een belangrijk knooppunt in de aanpak van cyberdreigingen. SURFcert biedt instellingen 24/7 ondersteuning wanneer er zich een beveiligingsincident voordoet. SURFcert staat in direct contact met het Nationaal Cyber Security Centrum (NCSC), als onderdeel van het Landelijk Dekkend Stelsel[5]. In aanvulling op SURFcert is er, op initiatief van de hoger onderwijsinstellingen, ook 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 sectorbreed wordt gedeeld. De toetreding van instellingen tot de SURFsoc zal gefaseerd plaatsvinden, in verband met de technische en contractuele voorbereidingen die per instelling moeten worden getroffen.

Recent is Wageningen University & Research als eerste instelling op SURFsoc aangesloten[6]. De andere hoger onderwijsinstellingen zullen binnenkort volgen, evenals NWO en de KNAW (inclusief de KNAW-instituten). De NWO-instituten zullen ook toetreden tot een SOC-oplossing, maar zij bekijken momenteel welke SOC-oplossing voor hen het meest geschikt is. Dit geldt ook voor de hogescholen. Zij zijn een verkenningstraject gestart waarin zij met SURF in kaart brengen wat de mogelijkheden zijn om binnen twee jaar een SOC-oplossing in te richten die past bij het risicoprofiel en de complexiteit van het netwerk van een hogeschool. De universitair medische centra hebben de intentie uitgesproken zich aan te sluiten bij de SURFsoc, een aantal in 2021 en een

[4] Kamerstukken 31 288 en 26 643, nr. 832.

[5] Het Landelijk Dekkend Stelsel is een stelsel waarin publieke en private partijen kennis en informatie met elkaar uitwisselen. Aangesloten zijn bijvoorbeeld de CERTs, sectorale en regionale samenwerkingsverbanden, het NCSC en het Digital Trust Center (DTC). Het NCSC fungeert in het Landelijk Dekkend Stelsel als centraal informatieknooppunt.

[6] De komende weken zullen ook Fontys, Universiteit Maastricht en LUMC aansluiten.

aantal in 2022. Zij zijn al lid van Z-Cert, dat is vergelijkbaar met SURF-Cert maar dan specifiek gericht op de zorg.

Om meer inzicht te krijgen in de eigen informatiebeveiliging en privacy-maatregelen, doen de instellingen ook mee aan de tweejaarlijkse SURFaudit. De SURFaudit is een zelf-assessment dat inzicht geeft in de mate waarin instellingen de informatiebeveiliging onder controle hebben en waar de prioriteiten liggen voor verbetering. Alle hoger onderwijs-instellingen hebben vorig jaar afgesproken in deze, een vergelijkbare of een zwaardere audit te participeren. Dit gebeurt op basis van het normenkader informatiebeveiliging hoger onderwijs (ISO-norm 27002), waarin ook een ambitieniveau is afgesproken.[7] Eind dit jaar vindt de volgende SURFaudit plaats, gevolgd door een benchmarkrapportage in 2022.

Naast de SURFaudits lieten alle universiteiten in 2020 ook een eenmalige externe audit uitvoeren op de informatiebeveiliging van de universiteit. Deze audits zijn inmiddels afgerond en geëvalueerd. De audits hebben een goed beeld opgeleverd van de onderdelen waarin universiteiten de komende periode extra moeten investeren. Er is afgesproken om deze externe audit nu jaarlijks uit te voeren, zodat er snel kan worden ingespeeld op de nieuwste ontwikkelingen.

Vergroten bewustzijn en aandacht voor keten-samenwerking

Voor instellingen is het belangrijk om continue technische maatregelen te nemen om incidenten tijdig te signaleren en te voorkomen. De mens blijft echter de zwakke schakel in digitale veiligheid. Daarom is het cruciaal om alle medewerkers en studenten bewuster te maken van cyberdreigingen. Instellingen investeren daartoe al geruime tijd[8] in het verbeteren van het bewustzijn door het aanbieden van trainingen, bewustwordingscampagnes en grootschalige oefeningen. Een van deze grootschalige oefeningen is de tweejaarlijkse cybercrisis-oefening OZON van SURF, waaraan veel publieke organisaties uit de sector meedoen. De deelnemers simuleren in de oefening de rol van de eigen organisatie in een crisis. De oefening kent een integrale aanpak, waarin moet worden geschakeld van operationeel en bestuurlijk tot op landelijk niveau. Alle lagen van een individuele organisatie worden daarom betrokken, zoals ICT-beheerders, de afdeling communicatie, beleidsmedewerkers en bestuurders. De laatste OZON-oefening, met meer dan 1.000 deelnemers, vond op 18 maart jl. plaats en ook mijn ministerie nam deel.

Incidenten in de afgelopen periode

Ransomware-aanval op NWO

Door de ransomware-aanval op de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) was het netwerk van NWO een aantal weken niet toegankelijk en moest het subsidieproces voor onderzoek worden stilgelegd. Hoewel het subsidieverwerkingssysteem zelf niet was geraakt, konden lopende subsidieaanvragen uit veiligheidsoverwegingen en door de ontoegankelijkheid van de ICT-infrastructuur op dat moment niet worden behandeld. De situatie is door NWO, het bedrijf Northwave, SURFcert en mijn ministerie constant gemonitord. Ook het NCSC heeft in

---

[7] Normenkader informatiebeveiliging hoger onderwijs kent zes clusters met elk een eigen volwassenheidsniveau. In de laatste SURFaudit van 2019 was de gemiddelde score van alle instellingen op de zes onderdelen 2,3. Het afgesproken ambitieniveau is 3.0.

[8] Zie het SURF cyberdreigingsbeeld 2019–2020: https://www.surf.nl/cyberdreigingsbeeld-onderwijs-en-onderzoek-20192020.

de eerste fase van het incident technische ondersteuning geboden. Daarnaast is er aangifte gedaan bij de politie en is er melding gemaakt bij de Autoriteit Persoonsgegevens.

Sinds 22 maart jl. is NWO weer volledig in bedrijf. Ik waardeer de manier waarop NWO in deze situatie heeft gehandeld. Het bestuur van NWO heeft sinds het begin van de aanval transparant gecommuniceerd naar haar eigen medewerkers, de betrokken diensten, de getroffen onderzoekers en mijn ministerie. Daarbij was het vanaf het begin helder dat NWO, als Zelfstandig Bestuursorgaan (ZBO) van de Nederlandse overheid, geen losgeld zou betalen. Dit is conform het algemene standpunt van de Nederlandse overheid dat er geen losgeld wordt betaald aan cybercriminelen. In de nasleep van de aanval blijft NWO intensief met de eigen medewerkers communiceren en biedt zij adequate, specialistische zorg waar nodig.

NWO had al voor de hack een actueel veiligheidsbeleid. Zo is NWO aangesloten bij het bovengenoemde SURFcert, voert het sinds 2017 interne audits en zogenoemde penetratietesten uit, heeft de organisatie al in 2020 een awareness-programma ingericht en voert NWO sinds 2017 NOZON-oefeningen uit.[9] Na de hack zijn er uiteraard extra maatregelen geïmplementeerd en NWO wordt 24/7 bewaakt door de SOC van het bedrijf Northwave, tot het moment dat NWO toetreedt tot de SOC van SURF. NWO heeft Northwave bovendien gevraagd om de gang van zaken rondom de hack te evalueren, waarna NWO de adviezen die daaruit voortkomen zal implementeren in de bedrijfsvoering. NWO heeft toegezegd de resultaten van de evaluatie ook met de sector te delen, zodat andere instellingen kunnen leren van deze aanval.

Cyberaanvallen op de UvA, HvA en Inholland

In februari zijn ook de UvA en de HvA doelwit geworden van een cyberaanval. Hier is snel en adequaat op gereageerd door vroege detectie door hun eigen SOC en ingrijpen van het Computer Emergency Response Team (CERT) van de UvA en HvA. De instellingen ondervonden slechts beperkt hinder van de aanval en deze heeft niet geleid tot uitval van systemen, gijzeling van gegevens of een verzoek om losgeld. Er is in beide gevallen aangifte gedaan bij de politie en melding gemaakt bij de Autoriteit Persoonsgegevens. Het onderzoek van de politie loopt nog. Net als NWO zullen ook de UvA en HvA de gang van zaken evalueren en de geleerde lessen met de sector delen.

Ook Hogeschool Inholland is in februari door cybercriminaliteit getroffen. Hackers hebben persoonlijke gegevens van een groot aantal studenten en medewerkers buitgemaakt en deze op een internetforum te koop aangeboden. Het ging om persoonsgegevens van mensen met een Moodle-account, de elektronische leeromgeving van Inholland. De hogeschool heeft direct maatregelen getroffen en een forensisch onderzoek gestart om te achterhalen hoe de hack kon plaatsvinden, wie er verantwoordelijk is en hoe dit soort situaties in de toekomst kunnen worden voorkomen. Voor de zekerheid zijn medewerkers en studenten gevraagd om hun wachtwoorden te wijzigen.

Integrale veiligheidsaanpak in het onderwijs- en onderzoeksveld

Een open maar veilige leer- en werkomgeving is een voorwaarde voor goed onderwijs, excellent onderzoek en kennisdeling. De voordelen van digitale uitwisseling, (internationale) samenwerking en open science zijn

[9] Een NOZON-oefening is een kleinschaligere variant van de eerdergenoemde OZON-oefening.

evident. Juist omdat dit in ons Nederlandse kennislandschap zulke belangrijke uitganspunten zijn, verdienen de risico's die met deze werkwijze samenhangen extra aandacht. Daarbij is een integrale veiligheidsaanpak van belang, waarin de verschillende belangen en de mogelijke maatregelen secuur worden afgewogen. Daartoe ben ik, naast de hierboven geschetste acties op het gebied van cyberveiligheid, ook met instellingen in gesprek over kennisveiligheid.[10] Er is op bestuurlijk niveau overleg tussen instellingen en mijn ministerie waarin, aan de hand van concrete casuïstiek, mogelijke handelingsperspectieven van de instellingen worden besproken. Ik roep de instellingen dan ook op 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. Bovendien wordt de cyberveiligheid van instellingen expliciet 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 de cyberveiligheidsmaatregelen in de bedrijfsvoering van de gehele sector.

De Minister van Onderwijs, Cultuur en Wetenschap,
I.K. van Engelshoven

[10] Kamerstuk 31 288, nr. 894.