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
24906882

Datum 3 juli 2020
Betreft Onderzoek naar cyberaanval Universiteit Maastricht en maatregelen cyberveiligheid

Op 12 juni heb ik uw Kamer het eerste deel van het rapport van de Inspectie van het Onderwijs (hierna: Inspectie) gezonden inzake de ransomware-aanval op de Universiteit Maastricht (hierna: UM) op 23 december 2019.[1] Zoals eerder bij uw Kamer aangegeven voert de Inspectie ook een onderzoek uit naar cyberveiligheid op stelselniveau. Ik verwacht begin volgend jaar uw Kamer hierover te informeren.

In deze brief geef ik mijn reactie op het nu uitgebrachte eerste deel van het rapport van de Inspectie. Ook ga ik in op mijn eerdere toezegging in de Kamerbrief *Cyberveiligheid in het onderwijs*[2] dat de universiteiten en hogescholen voor de zomer met aanvullende maatregelen komen betreffende cyberveiligheid en aan mijn toezegging over dit onderwerp aan het lid Smals in het algemeen overleg Wetenschapsbeleid van 24 juni 2020. Tevens ga ik in op het verzoek om informatie uit de motie Wiersma met betrekking tot afspraken rondom veiligheidsstandaarden bij onderwijsinstellingen en studentenorganisaties.[3]

Inspectierapport
De Inspectie heeft een instellingsonderzoek ingesteld met de hoofdvraag: *"Heeft de Universiteit Maastricht vooraf, tijdens en na de aanval passende maatregelen genomen om de goede voortgang van het onderwijs te waarborgen?"*. Deze hoofdvraag wordt aan de hand van drie deelvragen beantwoord, te weten wat er voorafging- *preventie*, hoe de cyberaanval werd afgehandeld- *respons*, en welk voorzieningen de UM heeft getroffen om soortgelijke incidenten in de toekomst te voorkomen- *lerend vermogen*. Omdat de WHW geen specifiek normenkader bevat voor het beoordelen van de inrichting van ICT-systemen, heeft de Inspectie gebruik gemaakt van de binnen de overheid breed gebruikte BIO-standaarden.[4]

[1] Kamerstuk | 12-06-2020 Cyberaanval Universiteit Maastricht
[2] Kamerbrief over Cyberveiligheid in het onderwijs | 14-02-2020
[3] Kamerstukken II 2019/20, 29240, nr. 113
[4] De BIO (De Baseline informatiebeveiliging Overheid) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Het is gebaseerd op internationale standaarden, de ISO-normen 27001 en 27002. Deze zijn als verplicht te gebruiken standaarden opgenomen op de pas-toe-of-leg-uit-lijst op het forum standaardisatie.

Belangrijkste bevindingen en conclusies
De Inspectie heeft onderzocht of de UM vooraf, tijdens en na de ramsomware-aanval passende maatregelen heeft genomen om de goede voortgang van het onderwijs te waarborgen. De hoofdconclusie van de Inspectie is dat er slechts voor een korte periode sprake is geweest van een continuïteitsprobleem van het onderwijs en onderzoek. Hoewel er onvoldoende detectie was en de UM heeft nagelaten in de preventieve zin alle passende maatregelen te nemen, was de respons op het incident daadkrachtig en implementeert de UM de eerste geleerde lessen op een adequate wijze. Er is geen sprake van ernstige nalatigheid en wanbeheer. De Inspectie heeft vertrouwen in het reeds geïnitieerde vervolgonderzoek van de UM, vraagt de UM haar over de uitkomsten te informeren en zal daarom geen aanvullende verbeterpunten voorschrijven.

De Inspectie geeft aan dat in recente jaren, wat betreft de preventieve kant, databeveiliging bij de UM al in toenemende mate de aandacht gekregen heeft, bijvoorbeeld via bewustwordingscampagnes. Dit zag met name op AVG-vraagstukken maar niet zo zeer op gevaren van malware. De UM was bezig met een herinrichting van de IT-organisatie die ten goede is gekomen aan de cyberweerbaarheid van de instelling. Echter, de Inspectie concludeert dat het CvB en de organisatie als geheel cyberrisico's onvoldoende prioriteerde als één van de belangrijkste risico's voor het borgen van de goede voortgang van het onderwijs en onderzoek. Daarom zijn voorafgaand aan de cyberaanval niet altijd alle passende maatregelen genomen.

Desondanks stelt de Inspectie vast dat het CvB in nauwe afstemming met het Crisis Management Team (CMT) van de UM, de Raad van Toezicht (RvT), de medezeggenschap en andere geledingen binnen de universiteit de crisis adequaat heeft afgehandeld. Ook hebben het CvB en RvT tijdens de afhandeling van het incident besloten waar mogelijk open te zijn om zo andere hoger onderwijsinstellingen en anderen de mogelijkheid te bieden lessen te trekken uit de cyberaanval bij de UM.

Uit het onderzoek wordt verder duidelijk dat de UM, direct na het afhandelen van de acute crisis, passende maatregelen heeft genomen door het invoeren van 'verhoogde dijkbewaking', dat wil onder andere zeggen continue (24/7) monitoring van de IT-systemen door externe inhuur. De Inspectie kan nog niet vaststellen of op langere termijn bij de UM sprake is van passende maatregelen om soortgelijke incidenten te voorkomen.

Reactie op Inspectierapport en door sector genomen maatregelen
Ik onderschrijf de bevindingen en conclusies van de Inspectie. De UM heeft – zo blijkt- een aantal belangrijke stappen en maatregelen genomen om de cyberweerbaarheid van de instelling te vergroten. In een breder context heeft de UM door volledige openheid te betrachten en gezamenlijk met opsporingsinstanties en overheid aan cyberveiligheid te werken ook invulling gegeven aan haar publieke taak. Wat betreft de concrete stappen die gezet zijn om de cyberweerbaarheid van de instelling te vergroten, licht ik een aantal voor mij belangrijke elementen uit en neem hier ook de concrete cyberveiligheidsmaatregelen die door hoger onderwijsinstellingen zijn genomen in mee.

Vergroten bewustzijn cyberdreigingen
Ik onderstreep het belang van het vergroten van bewustzijn, dit in samenwerking met de sector. Zoals ik in mijn brief *Cyberveiligheid in het onderwijs* heb aangegeven blijft de mens de zwakke schakel in digitale veiligheid. Medewerkers en studenten moeten bewust worden gemaakt van cyberdreigingen. Dit vergt continu aandacht. Ik zal daarom deelname blijven stimuleren aan sector brede initiatieven, zoals cyberoefeningen- en samenwerkingsverbanden. Dat de sector volop bezig is met het vergroten van bewustwording blijkt ook uit de aangekondigde maatregelen zoals hieronder wordt aangegeven.

De aanval op de UM heeft ook andere onderwijsinstellingen opnieuw doen beseffen hoe belangrijk informatiebeveiliging is. Van de SURF, VH en VSNU heb ik vernomen dat instellingen, zowel individueel als collectief, het onderzoek van de Inspectie tot zich hebben genomen en waar nodig aanvullende maatregelen hebben getroffen. Daarbij benadrukken zij dat cyberaanvallen aan de orde van de dag zijn. Nagenoeg alle aanvallen worden afgeslagen, echter, zoals eerder aangegeven in mijn brief *Cyberveiligheid in het onderwijs*, is 100% veiligheid in geen enkele sector realistisch. Ook binnen het MBO zijn de uitkomsten van het onderzoek gedeeld en tijdens netwerkbijeenkomsten van saMBO-ICT is hier aandacht aan geschonken.

Awareness
Door de Coronacrisis is in de afgelopen maanden bij de instellingen veel extra ICT-inzet gepleegd op het faciliteren van onderwijs en werken op afstand, maar ook op de daarmee gepaarde veiligheidsrisico's. Instellingen hebben tegelijkertijd lastige beslissingen moeten nemen zoals het verplaatsen van de cyberoefening OZON van oktober 2020 naar maart 2021, omdat door de Coronacrisis en een daaruit volgend gebrek aan capaciteit een goede voorbereiding in het gedrang kwam. Wel is er aandacht besteed aan het vergroten van bewustwording rondom security- en privacy. Fysieke campagneactiviteiten zijn in verband met Covid-19 uitgesteld, maar er is extra aandacht besteed aan veilig werken op afstand in relatie tot nieuwe digitale tools: zo was er aandacht voor privacy en security rond videobellen, juiste tools voor online samenwerken, gebruik van een vpn om veilig thuis te kunnen werken, hoe gebruik te maken van wifi bij online samenwerken, online proctoring en phishing[5]. Er werden diverse communicatiekanalen ingezet om medewerkers en studenten bewust te maken van privacy en security, zoals nieuwsbrieven, speciale intranetpagina/ website, infographics en vlogs van experts en bestuurders.

Digitaal brevet
Onderwerpen zoals digitalisering, privacy en cyberveiligheid staan ook bij de studentenorganisaties hoog op de agenda en ook zij hebben zorgen over privacy ten gevolge van online proctoring. Ook met het oog hierop heeft SURF samen met de instellingen een basismodule voor het Digitaal Brevet ontwikkeld, één voor studenten en één voor medewerkers: een e-learning tool voor de sector om bewustwording en vaardigheden op het gebied van security en privacy te leren en te toetsen. Daarnaast overleggen hogescholen en universiteiten met elkaar over verschillende technologische ontwikkelingen en de veiligheidsaspecten.

Borgen risicomanagement:
Het rapport maakt inzichtelijk dat de instellingen beter voorbereid moeten zijn op een cyberaanval. Het zorgvuldig inrichten van risicomanagement is nodig om

[5] Online proctoring is een vorm van online surveilleren die de mogelijkheid biedt om studenten veilig en betrouwbaar op afstand (plaats onafhankelijk) te kunnen toetsen. Bron: Whitepaper Online Proctoring SURFnet.

inzicht te krijgen in de risico's en passende maatregelen te kunnen nemen om deze risico's op kosteneffectieve wijze te mitigeren om zo de continuïteit van de primaire processen te waarborgen. Maatregelen die de hoger onderwijsinstellingen in dit kader hebben genomen, geef ik hieronder weer.

SURFaudit
Alle hoger onderwijsinstellingen hebben de afgelopen periode met elkaar afgesproken dat zij zullen gaan participeren in de tweejaarlijkse SURFaudit of een vergelijkbare dan wel zwaardere audit. De universiteiten laten dit jaar eenmalig een externe audit uitvoeren. Zij hebben hiertoe samen met SURF een gemeenschappelijke 'Auditmethodiek Informatieveiligheid' opgesteld en afspraken gemaakt over een gemeenschappelijke scope en diepgang middels een standaard opdrachtformulering.

SOC (Security Operations Center)
Detectie en monitoring, belangrijke hulpmiddelen bij risicomanagement, hebben bij hoger onderwijsinstellingen de hoogste prioriteit gekregen. Aanvullend op SURFcert, werkt SURF aan de oprichting van een SOC gericht op 24/7 monitoring van netwerken en signalering van dreigingen richting deelnemende instellingen[6]. Hierbij worden diverse diensten ontwikkeld. De overweging welke diensten de hoger onderwijsinstellingen willen afnemen doen zij op basis van risico's en kosten. Het opzetten van een uitgebreide 24/7 dienstverlening vergt veel werk en onderlinge afstemming. Sommige diensten kunnen snel starten, andere moeten aanbesteed worden. Dat vereist een (wettelijk) bepaalde doorlooptijd. Daardoor kunnen die diensten vanaf begin 2021 geïmplementeerd worden. Mbo-instellingen willen hierbij aansluiten en zijn momenteel als sector in overleg om hier handen en voeten aan te geven.

<u>Aandacht voor (keten-) samenwerking:</u>
Vooral met betrekking tot de analyse van de malware had de UM specialistische kennis nodig. Het rapport van de Inspectie onderstreept dat het voor instellingen niet mogelijk is om dit soort specialistische kennis zelf in huis te halen. Bij eventuele grote incidenten blijft ook in de toekomst specialistische kennis van buiten nodig, maar er is duidelijke behoefte aan meer samenwerking, kennis-en informatiedeling over risico's, monitoring en detectie. Daarom wordt er ook gewerkt aan de ontwikkeling van het Security Operations Centre. Naast de crisisafhandeling is ketensamenwerking cruciaal voor het herstellen van de reguliere werkzaamheden op het gebied van onderwijs en onderzoek. Zo heeft voor onderwijs afstemming plaats gevonden met de Dienst uitvoering Onderwijs (DUO) en voor onderzoek heeft de UM contact gezocht met de Nederlandse Organisatie voor Wetenschap (NWO) en de EU omwille afstemming rondom onderzoek deadlines met betrekking tot subsidieaanvragen.

Ik onderstreep het belang van ketensamenwerking en transparantie tussen de instellingen onderling en andere ketenpartners met daar waar nodig de hulp van de overheid als stelselverantwoordelijke. Organisaties moeten ook tijdig kunnen beschikken over de juiste informatie om hun eigen verantwoordelijkheid op digitale beveiliging te kunnen nemen. Binnen het Landelijk Dekkend Stelsel (LDS) van cybersecuritysamenwerkingsverbanden zijn stappen gezet om ook de informatie-uitwisseling met niet-vitale organisaties te verbeteren. Dit gebeurt

[6] SURFcert: 24/7 ondersteuning van SURF-deskundigen bij beveiligingsincidenten. Ook zijn er tools van SURFcert waarin ICT-experts zelf de beveiliging bij je instelling kunnen optimaliseren om bijvoorbeeld samen de overlast van onder andere DDoS-aanvallen te minimaliseren.

door middel van SURFcert waarmee het Nationaal Cyber Security Centrum (NCSC) ook bepaalde vertrouwelijke informatie en informatie over digitale dreigingen kan delen. De samenwerking die hoger onderwijsinstellingen al jaren in SURF verband ontwikkelen is in dit kader ook iets om trots op de zijn. Binnen netwerken van cybersecurity experts van instellingen en externe partners, wordt intensief informatie gedeeld. Dit incident bij de UM, maar ook het WRR advies over 'digitale ontwrichting' laat zien dat het noodzakelijk is om voor het thema cyberveiligheid rollen, verantwoordelijkheden en aanpak van alle betrokken partijen in kaart te brengen zodat effectief, efficiënt en veilig gehandeld kan worden. Het volgende rapport van de inspectie over het stelsel gaat naar verwachting hier meer aangrijpingspunten voor leveren.

Integrale aanpak veiligheid in het hoger onderwijs
De aanval op de UM heeft ook andere onderwijsinstellingen opnieuw doen beseffen hoe belangrijk informatiebeveiliging is. Een set van maatregelen zoals hierboven beschreven is dan ook al genomen. Een veilige leer- en werkomgeving is een voorwaarde voor goed onderwijs, onderzoek en kennisdeling. Naast cyberveiligheid zijn er meer risico's die een bedreiging vormen voor de continuïteit, integriteit en vertrouwelijkheid van onderwijs, onderzoek en kennisdeling, zoals bijvoorbeeld gebouwveiligheid, integriteit en kennisveiligheid. Zo onderzoekt het kabinet in hoeverre aanvullende maatregelen gewenst zijn met betrekking tot de risico's van ongewenste kennis- en technologieoverdracht in brede zin via de weg van (academisch) onderwijs en onderzoek. In het najaar wordt uw Kamer over de voortgang van dit traject geïnformeerd.

Het (hoger) onderwijs is door haar open karakter kwetsbaar. Tegelijkertijd is openheid een kernwaarde van het hoger onderwijs. Het is onwenselijk om in een streven naar 100% veiligheid deze kernwaarde uit het oog te verliezen en de toegankelijkheid van onderwijs, onderzoek en informatie te beperken. Het hoger onderwijs moet daarom streven naar een integrale veiligheidsaanpak waarin een afweging wordt gemaakt tussen kernwaarden, bedreigingen en de te beschermen belangen om op een bewuste manier de digitale weerbaarheid te verhogen en maatregelen te nemen die nodig zijn voor het optimaal presteren van de organisatie en de continuïteit van onderwijs, onderzoek en kennisdeling en voor het waarborgen van de integriteit en vertrouwelijkheid van de data waarover de sector beschikt. Daarbij moeten ook kosten en baten van veiligheidsmaatregelen tegen over elkaar worden afgewogen. Dat vraagt om een gedegen governance en strategische positionering van het veiligheidsrisicomanagement zodat bij instellingen geschikte technische en organisatorische maatregelen worden getroffen om relevante risico's af te dekken zonder dat dit onnodige bureaucratie of een negatieve kosten-batenverhouding oplevert.

Ik heb er vertrouwen in dat instellingen op bestuurlijk en strategisch niveau aandacht geven aan veiligheid. De betrokkenheid van interne en externe stakeholders (studenten, personeel, raden van toezicht, medezeggenschap, overheid etc.) is noodzakelijk voor het creëren en behouden van een veilige leer- en werkomgeving. De open en transparante wijze waarop de UM afhandeling van de ransomware-aanval heeft gecommuniceerd draagt bij niet alleen aan het veiliger stellen van háár leer-en werkomgeving maar ook de hele sector. Dit geldt ook voor het reeds geïnitieerde vervolgonderzoek van de UM, waarvan de uitkomsten relevant zijn voor het onderzoek van de Inspectie op stelselniveau. Hierbij zal de Inspectie onderzoeken in hoeverre er *lessons learned* zijn zodat ook

andere onderwijsinstellingen zich een beeld kunnen vormen van mogelijke kwetsbaarheden op het terrein van cyberveiligheid en passende maatregelen kunnen nemen. Mogelijk kunnen we de geleerde lessen ook vertalen naar de andere onderwijssectoren. Dit is in lijn met onze ambitie om als overheid een meer gecoördineerde aanpak te volgen om beter voorbereid te zijn op de gevolgen van een cyberaanval.

De minister van Onderwijs, Cultuur en Wetenschap,

Ingrid van Engelshoven