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
19327037

Datum 14 februari 2020
Betreft Cyberveiligheid in het onderwijs

Op 23 december 2019 heeft een ransomware-aanval op de Universiteit Maastricht plaatsgevonden. Uw Kamer heeft mij tijdens de Regeling van Werkzaamheden van 14 januari jl. verzocht u over deze aanval te informeren. Vervolgens heeft de vaste commissie voor Onderwijs, Cultuur en Wetenschap op 16 januari jl. een aanvullend, schriftelijk verzoek gedaan om informatie over de cyberveiligheid van onderwijsinstellingen.[1] Tijdens het algemeen overleg Sociale veiligheid in het onderwijs van 22 januari jl. heb ik toegezegd u na het uitkomen van het onderzoeksrapport van de Universiteit Maastricht over de ransomware-aanval gelijktijdig op beide verzoeken in te gaan. Met deze brief, die ik mede namens de minister voor Basis- en Voortgezet Onderwijs en Media stuur, voldoe ik aan die toezegging. Ook ga ik in op de verzoeken om informatie uit de motie Wiersma over een risico-inventarisatie rond cyberveiligheid.[2]

Leeswijzer
De afgelopen periode heb ik me uitgebreid laten informeren over de ontwikkelingen in de sector op het gebied van cyberveiligheid en over de precieze toedracht van de ransomware-aanval in Maastricht. In deze brief ga ik eerst in op de context waarin cyberveiligheid in het onderwijs moet worden bezien. Daarna ga ik in op het normen- en toetsingskader binnen de sector. Vervolgens schets ik een beeld van de stand van de cyberveiligheid per sector en welke acties de sector onderneemt om dit verder te verbeteren. Tot slot zal ik specifieker ingaan op de situatie rondom de ransomware-aanval op de Universiteit Maastricht.

De informatie in deze Kamerbrief is zorgvuldig afgewogen op risico's, in overleg met onderwijsinstellingen en SURF. Daar waar nodig is er contact geweest tussen mijn ministerie en de NCTV. Zo is het belang van openheid zorgvuldig afgewogen tegen de eventuele schade die het bekendmaken van beveiligingsdetails met zich meebrengt. In die afweging is ook besloten niet tegemoet te komen aan het verzoek van de vaste commissie voor Onderwijs, Cultuur en Wetenschap informatie te verstrekken over back-upbeleid per instelling. Ook informatie over een eventuele verzekering die losgeld dekt is niet aan mij om kenbaar te maken. Wel heeft SURF op mijn verzoek aangeboden uw Kamer in een vertrouwelijke bijeenkomst verder over de digitale veiligheid van onderwijsinstellingen in te lichten.

[1] Verzoek met kenmerk 2020D01148.
[2] *Kamerstukken II* 2019/20, 29240, nr. 113.

Volledigheidshalve wijs ik u erop dat de toepassing van de Wet Digitale Overheid (WDO) die onlangs in uw Kamer is behandeld, voor de onderwijssectoren bij lagere regelgeving geschiedt. Hierover ben ik nog in gesprek met de onderwijssectoren. Gezien de fase van het parlementaire proces waarin de wet zich bevindt verwijs ik u voor meer informatie naar de minister van Binnenlandse Zaken en Koninkrijksrelaties.[3]

Perspectief op digitale veiligheid
Onderwijsinstellingen zijn open leeromgevingen waarin studenten, docenten en onderzoekers als gemeenschap optimaal in staat worden gesteld te leren, onderwijzen en onderzoeken. Dit kan alleen als deze leer- en werkomgeving veilig is. Studenten, docenten en onderzoekers moeten hierop kunnen vertrouwen. In het hoger- en middelbaar beroepsonderwijs wordt veiligheid integraal benaderd, zodat incidenten en veiligheidsrisico's niet los van elkaar worden bezien, maar juist in samenhang. Cyberveiligheid maakt hier een belangrijk onderdeel van uit. Dit blijkt niet alleen uit de ransomware-aanval op Universiteit Maastricht, maar ook uit de Citrix-kwetsbaarheid die ook een aantal kennisinstellingen heeft geraakt. Hierover heeft de minister van Justitie en Veiligheid u recent separaat geïnformeerd.[4]

De digitalisering van het onderwijs en de bedrijfsvoering biedt vooral veel kansen, maar maakt ook dat instellingen steeds afhankelijker zijn van computersystemen om te kunnen functioneren. De instellingen zien een dilemma tussen open toegankelijke onderwijs- en kennisinstellingen die over grenzen samenwerken aan de ene kant en (cyber)veiligheid aan de andere kant. Juist de openheid van onderwijsinstellingen maakt dat de veiligheid goed op orde moet zijn. Daarbij zie ik dat een grote mate van decentrale aansturing van de bedrijfsprocessen van met name universiteiten, een effectieve aanpak van digitale veiligheid in de weg kan staan. Wel erken ik dat er een balans moet worden gevonden tussen het te behalen niveau van cyberveiligheid en de te maken kosten. 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".[5] De WRR stelt daarin dat het volledig voorkomen van digitale incidenten een illusie is. Als er sprake is van een digitaal incident, zoals in Maastricht, dan is het vooral zaak snel mitigerende maatregelen te (kunnen) nemen, ervan te leren en de veiligheid van de gehele sector een stap verder te brengen.

Vitale en niet-vitale sectoren
Bepaalde processen zijn zo essentieel voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting kan leiden en daarmee een bedreiging vormt voor de nationale veiligheid. Deze processen vormen de Nederlandse vitale infrastructuur, zoals elektriciteit, toegang tot internet, drinkwater en betalingsverkeer. De processen binnen het onderwijs maken geen onderdeel uit van de vitale infrastructuur op grond van de hiervoor geldende criteria.[6] Ook digitale incidenten bij niet-vitale organisaties kunnen serieuze gevolgen hebben en overlast veroorzaken. Daarom staan informatieknooppunten van niet-vitale sectoren in nauw contact met het Nationaal Cyber Security Centrum (hierna: NCSC). SURFcert (SURF Computer Emergency Response Team), dat ondersteuning biedt aan onderwijsinstellingen bij beveiligingsincidenten, is

[3] Meer informatie is ook te vinden op https://www.digitaleoverheid.nl/dossiers/wet-digitale-overheid/
[4] Brief van ministerie van Justitie en Veiligheid: Overzicht op hoofdlijnen Citrix-kwetsbaarheden, (26643, nr. 660).
[5] Wetenschappelijke Raad voor het Regeringsbeleid (2019) Voorbereiden op digitale ontwrichting, wrr-Rapport 101, Den Haag: wrr.
[6] *Kamerstukken II* 2014/15, 30821, nr. 23.

sinds 24 januari 2020 door de minister van Justitie en Veiligheid aangewezen als één van die informatieknooppunten, meer specifiek als computercrisisteam (CERT), waarmee intensievere informatie-uitwisseling met het NCSC mogelijk is gemaakt.[7]

Gezamenlijk vormen de verschillende informatieknooppunten het zogenaamde Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden dat zo veel mogelijk informatie ter verhoging van de digitale weerbaarheid deelt. Het Digital Trust Center (DTC), dat onder de verantwoordelijkheid van het ministerie van Economische Zaken en Klimaat valt, draagt met de sectorale en regionale samenwerkingsverbanden bij aan het Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden. De missie van het DTC is het bieden van informatie en advies over cybersecurity aan het niet als vitaal aangemerkte bedrijfsleven en het stimuleren van samenwerking op het gebied van cybersecurity in dit bedrijfsleven. In het geval van dreigingen of kwetsbaarheden verspreidt het NCSC, voor zover mogelijk, uitleg en handelingsperspectief onder de verschillende informatieknooppunten die vervolgens verantwoordelijk zijn voor het informeren en bijstaan van hun doelgroepen.

Kader cyberveiligheid in het mbo en hoger onderwijs

Rollen en verantwoordelijkheden in de onderwijssectoren

In het mbo en hoger onderwijs hebben instellingen een lange traditie van samenwerking ten aanzien van ICT-infrastructuur. Deze samenwerking is ondergebracht in coöperatie SURF (hbo en wo) en saMBO-ICT (mbo). In deze organisaties wordt kennis gebundeld en dit leidt tot efficiënte inzet van financiële middelen en inspanningen op het gebied van digitale veiligheid. Bij SURF en bij het netwerk van SURF, en daarmee bij SURFcert, zijn alle universiteiten en universitaire medische centra aangesloten. Alle hogescholen zijn aangesloten bij SURF, waarvan 94% ook aangesloten is bij het netwerk van SURF (en daarmee bij SURFcert). 98% van de Mbo-scholen is aangesloten bij saMBO-ICT en 83% van de Mbo-scholen is aangesloten bij het SURF-netwerk (en daarmee bij SURFcert). Verderop in deze brief ga ik nader in op de activiteiten van SURF en saMBO-ICT. In andere landen wordt deze vorm van samenwerking op ICT-gebied in het hoger onderwijs steeds vaker vormgegeven volgens dit Nederlandse model.

De verantwoordelijkheid voor een goede bedrijfsvoering, inclusief integraal veiligheidsbeleid, ligt bij de onderwijsinstelling zelf, zo vloeit voort uit de WHW en de WEB. Zoals ik in de strategische agenda hoger onderwijs en onderzoek heb uiteengezet, zie ik voor mijzelf een rol in situaties waarin (I) de kwaliteit, toegankelijkheid of doelmatigheid in het geding is, (II) instellingen (in gezamenlijkheid) hun verantwoordelijkheid niet (kunnen) nemen, of (III) versnelling gewenst is ('overheid als aanjager') om maatschappelijke doelstellingen te realiseren.[8] Een veiligheidsvraagstuk op een individuele instelling, zoals bij de Universiteit Maastricht, is primair een lokale aangelegenheid. Dit laat onverlet dat ik mij vanwege de maatschappelijke impact actief heb laten informeren. Daarnaast heb ik erop toegezien dat andere instellingen zo snel mogelijk zijn geïnformeerd om adequate maatregelen te kunnen treffen. De Inspectie van het Onderwijs (hierna: Inspectie) heeft zich eveneens actief laten informeren en zal onderzoek verrichten naar de ransomware-aanval op de Universiteit Maastricht waarbij het gebruik maakt van het onderzoek dat de universiteit zelf heeft uitgezet. De planning is dat het inspectie-onderzoek voor de zomer is afgerond.

Vanuit mijn rol als verantwoordelijke voor de borging van de continuïteit van het gehele stelsel, is het voor mij van belang dat de instellingen er zorg voor dragen

[7] Dit is bepaald in de regeling aanwijzing computercrisisteams, Staatscourant 2020, 4410.
[8] Strategische agenda hoger onderwijs en onderzoek: houdbaar voor de toekomst.

dat de kwetsbaarheden op het gebied van digitale veiligheid (pro)actief worden bestreden. Daarom heb ik de onderwijsinstellingen opgeroepen mij een beeld te verschaffen van de risico's op het gebied van digitale veiligheid. Een deel van dit beeld treft u verderop aan in deze brief. Instellingen zullen op mijn verzoek dit beeld in de komende periode verder aanvullen.

Verder is het aan de rijksoverheid en mij als minister van OCW om instellingen te ondersteunen waar nodig. Zo stimuleren we dat de sector werk maakt van veiligheidsbeleid, met name door in het primair en voortgezet onderwijs middelen beschikbaar te stellen voor de ontwikkeling van SIVON, de ICT-coöperatie in het po en vo, en door de financiële ondersteuning van het Platform Integrale Veiligheid-Hoger Onderwijs, waarin hogescholen en universiteiten samenwerken aan integraal veiligheidsbeleid. Ik wil er in het vervolg op toezien dat binnen de sector voortdurend het gesprek wordt gevoerd over (digitale) veiligheid en zorg voor de cross-sectorale verbindingen met andere organisaties om best practices uit te wisselen. En daarbij doe ik, uitgaande van hun eigen verantwoordelijkheid, een appèl op instellingen om te zorgen dat de beveiliging op orde is. Tot slot zal de Inspectie ook onderzoek doen naar de digitale veiligheid op stelselniveau in het hoger onderwijs. Dit onderzoek zal ik u na de zomer doen toekomen.

Normen en toetsing van digitale beveiliging in mbo, hbo en wo
Er is een wereldwijd erkende norm, opgesteld door de Internationale Organisatie voor Standaardisatie (ISO), waarmee wordt bepaald of een instelling de digitale beveiliging op orde heeft. Deze ISO-normen, 27001 en 27002, staan ook aan de basis van de *Baseline Informatiebeveiliging Overheid*. Ze zijn krachtens het 'pas toe of leg uit' beleid verplicht voor overheidsorganisaties.[9] In het kader van de samenwerking binnen SURF heeft de hoger onderwijssector een normenkader[10] ontwikkeld die op de ISO-norm is gebaseerd en ook voldoet aan het richtsnoer Beveiliging van Persoonsgegevens van de Autoriteit Persoonsgegevens. Voor het mbo heeft saMBO-ICT dit normenkader[11] integraal overgenomen.

In het hoger onderwijs worden verschillende onderdelen van veiligheidsbeleid getoetst aan de hand van een door Koninklijke Nederlandse Beroepsorganisatie van Accountants ontwikkeld model. In het mbo wordt bij de toetsing het normenkader zelf als basis gebruikt.[12]
In beide gevallen worden de in de ISO-norm opgenomen onderdelen van goed veiligheidsbeleid gescoord op een volwassenheidsniveau. Dit volwassenheidsniveau varieert van niveau 1, waarbij maatregelen op ad hoc basis worden genomen, tot niveau 5 waarin een proces zo is ingericht dat het continu wordt gemonitord.[13] Zoals bij alle sectoren moet per onderdeel worden vastgesteld wat het benodigde volwassenheidsniveau is. De onderwijssectoren hebben binnen SURF en saMBO-ICT vastgesteld welk streefniveau wenselijk is. Het is volgens de ICT-organisaties echter aan de instellingen zelf om te bepalen wat hun eigen ambitieniveau is.

Toetsing van de informatiebeveiliging aan de hand van het normen- en toetsingskader vindt in de sectoren in verschillende vormen plaats:

1. Op basis van een zelf-assessment. Binnen de eigen instelling wordt aan de hand van het toetsingskader zelf gescoord.

[9] https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht
[10] Normenkader informatiebeveiliging hoger onderwijs 2015.
[11] Dit normenkader mbo is identiek aan het normenkader IBHO 2015.
[12] Het normenkader is door saMBO-ICT uitgewerkt in een toetsingskader met een handreiking wat nodig is om op welk statement welk volwassenheidsniveau te scoren: www.sambo-ict.nl/ibpdoc40.
[13] https://www.nba.nl/intern-en-overheidsaccountants/volwassenheidsmodel-informatiebeveiliging/

2. Door peer-review. Professionals uit gelijksoortige organisaties reviewen elkaars assessments.
3. Door externe audit.

In de komende paragrafen zal ik per sector uiteen zetten welke initiatieven momenteel al lopen ten aanzien van cyberveiligheid, in welke mate bovenstaande normen worden gehaald en welke extra maatregelen in de komende tijd worden genomen.

Beeld cyberveiligheid in verschillende onderwijssectoren
Cyberveiligheid in het hoger onderwijs: wat gebeurt er al?
In het hoger onderwijs is SURF actief op ICT-voorzieningen en innovatie. SURF heeft nadrukkelijk ook een rol bij het onderwerp cyberveiligheid. Vanuit SURF zijn er tal van activiteiten op het gebied van cyberveiligheid voor onderwijsinstellingen. Zo is er veel contact tussen experts van verschillende instellingen om actuele dreigingen te bespreken en kennis uit te wisselen. Daarnaast is er 24 uur per dag, zeven dagen in de week ondersteuning vanuit SURFcert bij beveiligingsincidenten. SURFcert speelt een coördinerende rol bij dreigingen en incidenten, door informatie te delen, te bundelen en factsheets te publiceren. SURFcert beschikt daarnaast over instrumentarium waarmee aanvallen en de overlast ervan kunnen worden gemitigeerd en biedt cursussen aan op het gebied van security en privacy voor onderwijsinstellingen.

Daarnaast werkt de hoger onderwijssector al geruime tijd aan het versterken van cyberveiligheid op de korte en lange termijn via bewustwordingscampagnes, grootschalige oefeningen en dienstverlening, ten behoeve van studenten en medewerkers op individuele instellingen. SURF en/of het platform IV-HO leveren hier materiaal voor aan. De ervaring leert volgens de koepels VH en VSNU dat de cyberoefeningen grote impact hebben op het veiligheidsbewustzijn bij de instellingen. Resultaten van de oefening worden ook breder binnen de hoger onderwijssector gedeeld, via de koepels, conferenties en videoverslagen. Onderwijsinstellingen zetten ook zogenaamde ethische hackers in om hun netwerken te testen. In de bijlage treft u een uitgebreider beeld van de activiteiten.

Voor het signaleren van trends in dreigingen en weerbaarheid brengt SURF jaarlijks het cyberdreigingsbeeld uit. SURF treedt hierbij op als expertisecentrum en dienstverlener. Aan het meest recente onderzoek uit 2019 hebben elf hogescholen, elf universiteiten en 21 mbo-instellingen deelgenomen. Daarmee geeft het onderzoek geen volledig dekkend beeld, maar wel een indicatie van de uitdagingen waar instellingen voor staan en de manier waarop ze die het hoofd bieden. Uit het Cyberdreigingsbeeld 2019/2020[14] blijkt dat incidenten zich voornamelijk hebben voorgedaan in de categorie 'Verstoren van ICT-voorzieningen'. De verwachting in het dreigingsbeeld is dat cyberdreigingen, waaronder ransomware-aanvallen, in 2020 verder zullen toenemen. Tegelijkertijd neemt de weerbaarheid van de sector toe. Ook blijkt dat bij de deelnemende instellingen zowel beveiligings- als privacy-incidenten altijd worden gemeld aan het college van bestuur en de raad van toezicht.

Hoe staat het er voor in het hoger onderwijs?
Het *Normenkader Informatiebeveiliging Hoger Onderwijs*, opgesteld op basis van de eerder benoemde ISO-standaard, is de basis van het zelf-assessmentsysteem van de SURF-audit. Voorafgaand aan de zelfassessments worden door SURF workshops georganiseerd waarin wordt besproken aan welke eisen de documentatie moet voldoen om een bepaalde score te halen. Instellingen kunnen hun informatiebeveiliging zelf beoordelen en krijgen hierbij aanbevelingen van

[14] Cyberdreigingsbeeld 2019/2020 onderwijs en onderzoek, SURF.

SURF in feedbacksessies per sector om extra aandacht te besteden aan sterke en zwakke onderdelen van veiligheidsbeleid. Hier wordt besproken hoe de scores tot stand zijn gekomen en hoe instellingen van elkaar kunnen leren om verbetering tot stand te brengen. Daarnaast kunnen instellingen peer review laten uitvoeren door collega's van andere instellingen ter validatie van de resultaten.

De resultaten zijn vertrouwelijk. Iedere twee jaar maakt SURF een geaggregeerd beeld van en voor de sector in de SURFaudit-benchmark. In 2017 hebben tien universiteiten en tien hogescholen de resultaten van de SURFaudit beschikbaar gesteld voor de benchmark. Sinds 2011 is er op basis van de zelfassessments een groei te zien in het gemiddelde volwassenheidsniveau in het hoger onderwijs. Waar in 2011 de score nog 2,0 was, was dit in 2017 2,4. Dit niveau ligt nog wel onder het door de sector vastgestelde streefniveau van 2,93.[15]

Het niveau van samenwerken ligt volgens SURF ook in vergelijking met andere sectoren hoog. Veel instellingen kiezen vrijwillig voor deelname aan deze audit door middel van zelfassessments en peer review, waarbij een deel van de instellingen er voor kiest de audit door een externe professionele partij, anders dan SURF, uit te laten voeren. Ook worden ethische hackers ingezet om de systemen te testen. Volgens de koepels worden externe controles, in toenemende mate, bij een groot aantal hoger onderwijsinstellingen afgenomen. Er is op dit moment geen overzicht bij hoeveel instellingen dit het geval is en of dit periodiek wordt getoetst. Volgens de koepels zijn deze externe audits kostbaar en hebben ze als bijkomend nadeel dat de kennis over de kwetsbaarheden niet binnen de eigen organisatie blijft. Wel geeft het externe oordeel volgens hen een goed beeld van de kwetsbaarheden van de instelling. In de accountantscontrole van instellingen wordt het risicomanagement, waaronder cyberveiligheid, standaard beoordeeld. De raden van toezicht en colleges van bestuur bespreken deze rapportages volgens de koepels jaarlijks en nemen maatregelen als daarin zwaktes zijn aangetoond.

VH en VSNU geven aan dat in het hoger onderwijs doorlopend wordt geïnvesteerd in cybersecurity. Dit is ook nodig omdat de dreigingen in rap tempo veranderen. Uit een inventarisatie van de koepels en SURF blijkt dat de beschikbare capaciteit voor het op orde houden van digitale veiligheid verschilt tussen instellingen. Samenwerking tussen instellingen, bijvoorbeeld via SURF en de expertwerkgroepen binnen SURF, is daarom essentieel om de beschikbare capaciteit optimaal in te zetten.

Cyberveiligheid in het mbo: wat gebeurt er al?
In het mbo speelt saMBO-ICT een centrale rol in de ondersteuning van instellingen bij cyberveiligheid, naast Kennisnet en SURF. De basis voor deze ondersteuning ligt in het 'framework informatiebeveiliging en privacy met modeldocumenten en best-practices'.[16] Ook wordt steeds intensiever samengewerkt met SURF, waardoor bijvoorbeeld het cyberdreigingsbeeld onderwijs en onderzoek en de cybercrisisoefening OZON ook voor aangesloten mbo-instellingen toegankelijk zijn. Zowel Kennisnet als SURF zijn vertegenwoordigd in de Regiegroep informatiebeveiliging en privacy in het mbo, de stuurgroep van waaruit activiteiten en ondersteuning voor de mbo-instellingen wordt opgezet.

Zoals hierboven aangegeven, is 83% van de mbo-instellingen aangesloten bij het SURF-netwerk en daarmee bij SURFcert. Daarnaast geldt specifiek voor het mbo dat saMBO-ICT actief is. Deze zelfstandige organisatie van en voor alle mbo-instellingen heeft sterke banden met de MBO Raad, Kennisnet en met SURF.

[15] Resultaten SURFaudit-benchmark 2017, juli 2018.
[16] www.sambo-ict.nl/framework

saMBO-ICT is belangenbehartiger van het mbo-veld op een breed ICT-terrein. Zij pakken gezamenlijk projecten op en organiseren activiteiten op het gebied van digitale veiligheid: van netwerkbijeenkomsten rond informatiebeveiliging en privacy tot kennisdeling. saMBO-ICT stelt zich daarbij faciliterend, ondersteunend, adviserend, maar ook als ICT-kennisexpert op voor het mbo-veld.

Informatiebeveiliging staat bij het mbo hoog op de agenda. Zo wordt er gewerkt aan het inrichten van een bestuurlijk proces (via het KetenRegieOverleg), voor het uniform implementeren van beveiligingsstandaarden binnen het MBO-veld volgens de Wet Digitale Overheid en is er een practoraat Cybersecurity. Ook op ketendagen en gebruikersdagen krijgt dit onderwerp aandacht, onder meer om meer bewustwording te creëren bij het mbo-veld. Tot slot reikt saMBO-ICT een Awareness-award uit en was er tijdens de vorige saMBO-ICT conferentie een awareness-markt, met best-practices vanuit de instellingen.

Hoe staat het er voor in het mbo?
Om een goed beeld te krijgen van de cyberveiligheid in het mbo, wordt sinds 2015 jaarlijks de *Benchmark Informatiebeveiliging Privacy en Examinering in het mbo* gemaakt. Aan de vorige twee edities van deze benchmark heeft de afgelopen drie jaar volgens saMBO-ICT 95% van de mbo-instellingen deelgenomen aan de hand van een zelfassessment. Alle instellingen hebben de benchmark ten minste één keer ingevuld. Kennisnet en saMBO-ICT ondersteunen de medewerkers die het zelf-assessment uitvoeren met trainingen. De MBO Raad en saMBO-ICT laten weten sterk te sturen op een brede deelname aan deze benchmark. Om mogelijke onnauwkeurigheid te verkleinen wordt sinds 2018 *peer review* ingezet. In 2019 hebben elf instellingen (19%) deelgenomen aan *peer review*. In de benchmark van 2019 is gezamenlijk geconcludeerd dat *peer review* een vast onderdeel moet worden van de gehele benchmark vanaf 2020.

De mbo-sector maakt (nog) geen gebruik van externe audits. Volgens saMBO-ICT tonen instellingen zich eigenaar van deze problematiek en doen zij wat binnen hun macht ligt op basis van (beperkte) beschikbare middelen zoals (ICT-)kennis en capaciteit. Instellingen kunnen door de systematiek van zelfassessment en peer review open en eerlijk zijn over resultaten. Volgens saMBO-ICT speelt bij de overweging voor het nog niet inzetten van externe audits mee dat externe audits hoge kosten met zich meebrengen die in deze fase beter besteed kunnen worden aan het nemen van mitigerende maatregelen.

Het gemiddelde volwassenheidsniveau dat wordt gescoord aan de hand van de zelfassessments laat sinds 2015 elk jaar een groei zien.[17] In 2019 is de score voor zowel informatiebeveiliging, privacy als examinering een 2,5.[18] Een gemiddelde score van 2,5 is in deze, juiste, context een mooi tussenresultaat en indiceert zeker niet dat het niveau net voldoende zou zijn. Met daarbij in acht genomen dat het implementeren van dit soort processen menige jaren in beslag kan nemen om tot het gewenste niveau te komen, omdat het een groeiproces betreft.

Het minimumniveau dat SaMBO-ICT voor de sector hanteert, is een gemiddelde score van 2,0. Elf instellingen voldeden hier niet aan. Voor alle instellingen biedt saMBO-ICT op vrijwillige basis ondersteuning. Voor 2020 heeft saMBO-ICT een ambitie gesteld voor een gemiddelde volwassenheidsscore van 3,0 in de sector. SaMBO-ICT attendeert erop dat de in de benchmark gerapporteerde gemiddelde volwassenheid een goede indicator is om een beeld te schetsen van de ontwikkelingen en om eventuele groei aan te tonen.

[17] In 2015 was de gemiddelde score 1,9, in 2016 1,9, in 2017 2,1 en in 2018 2,4.
[18] De rapportage van de Benchmark IBP/E mbo 2019 is beschikbaar via het Framework IBP: www.sambo-ict.nl/ibpdoc11e

Cyberveiligheid in het primair en voortgezet onderwijs
De vaste commissie voor Onderwijs, Cultuur en Wetenschap heeft aangegeven ook graag te vernemen of een en ander ook van toepassing is op het funderend onderwijs. Ook in het primair en voortgezet onderwijs bestaat het risico van ICT-verstoringen op scholen en bij leveranciers van ICT-systemen en leermiddelen. Kennisnet en SIVON[19] werken daarom samen aan de inrichting van het Nationaal Dienstencentrum (NDC) om veilige en betrouwbare ICT-voorzieningen voor scholen te garanderen. Wij hebben hiervoor €50 mln. over vier jaar beschikbaar gesteld. Met dit dienstencentrum zorgt Kennisnet voor een basisniveau aan internettoegang en beveiliging voor scholen in het primair- en voortgezet onderwijs. Het NDC is een verzameling diensten, die communicatie via het internet en toegang tot het internet op een veilige en betrouwbare manier mogelijk maakt, waaronder anti-DDoS-maatregelen, IP- en DNS-filtering. De eerste scholen worden aan het einde van het eerste kwartaal van 2020 aangesloten. Om dit proces te versnellen is het van belang dat schoolbesturen lid worden van SIVON.

Voor het primair en voortgezet onderwijs geldt daarbij, net als in het mbo en het hoger onderwijs, dat schoolbesturen zelf primair verantwoordelijk zijn om hun digitale zaken op orde te hebben. Dat vergt kennis op scholen en bij besturen. Zij worden hierbij ondersteund door Kennisnet, in samenwerking met de sectorraden. Bovengenoemde initiatieven helpen scholen daarbij. Er is een concrete aanpak beschikbaar voor scholen om hun informatiebeveiliging te verbeteren en er zijn publicaties om de bewustwording te verhogen. Daarnaast is er een periodieke monitor informatiebeveiliging en privacy beschikbaar.[20]

ICT-dienstverleners zoals uitgeverijen en leerlingadministratiesystemen nemen zelf hun maatregelen. Er is een onderwijsstandaard beschikbaar (certificeringsschema voor informatiebeveiliging) die aanbieders en scholen hierbij technisch ondersteunt.

Ransomware-aanval Universiteit Maastricht
Zoals aan het begin van deze brief aangegeven, heeft op 23 december jl. een ransomware-aanval plaatsgevonden op de Universiteit Maastricht. Hierdoor is een deel van de systemen en data van de Universiteit Maastricht ontoegankelijk gemaakt door hackers. Er werd losgeld geëist, waarna de systemen zouden worden ontsleuteld. Vanaf 23 december is er veelvuldig contact geweest 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.

In de nacht van de aanval heeft Universiteit Maastricht informatie over de aanval gedeeld met SURFcert. Verder zijn op 24 december zogenaamde 'Indicators of Compromise' (IoC's) gedeeld via SURFcert met hogescholen, mbo-instellingen en universiteiten, zodat zij hun systemen hebben kunnen nalopen op gelijksoortige sporen.
De Universiteit Maastricht heeft, zo heeft ze aangegeven, in de dagen en weken daarna steeds, zodra dat mogelijk was, zowel via de technische als de bestuurlijke lijn, de sector voorzien van aanvullende informatie (zoals aanvullende IoC's) en waarschuwingen.

Ik heb waardering voor de open en transparante wijze waarop de Universiteit Maastricht heeft gecommuniceerd over deze ransomware-aanval. Niet alleen

[19] SIVON is de ICT-inkoopcoöperatie van en voor besturen in het funderend onderwijs. Op dit moment is ongeveer 27 procent van de scholen (gemeten naar leerlingenaantal) aangesloten bij SIVON.
[20] https://www.kennisnet.nl/artikel/monitor-ibp-scholen-goed-op-weg-met-informatiebeveiliging-en-privacy/

richting haar studenten en medewerkers, maar ook richting andere onderwijsinstellingen en de maatschappij. Het openbaar maken van het rapport van Fox-IT is een belangrijke stap om goed inzicht te krijgen in wat er op de universiteit is gebeurd en welke stappen de universiteit, andere onderwijsinstellingen en ook andere sectoren kunnen zetten.

Onderzoeken
De Universiteit Maastricht heeft op 24 december een extern gespecialiseerd adviesbureau (Fox-IT) in de arm genomen om de gevolgen te bestrijden en is in samenwerking met dit bedrijf een (forensisch) onderzoek gestart. Dit onderzoek, inclusief een schriftelijke reactie van de Universiteit Maastricht, vindt u in een openbare versie in de bijlage.

Van de ransomware-aanval is aangifte gedaan bij de Politie Eenheid Limburg, waarna een strafrechtelijk onderzoek is gestart door het Openbaar Ministerie. Ook heeft de Inspectie een tweeledig onderzoek ingesteld. Ten eerste onderzoekt de Inspectie of de universiteit in redelijkheid voldoende geprepareerd was op een ransomware-aanval en of de universiteit voldoende voorzieningen treft om herhaling van een dergelijke calamiteit te voorkomen. Ze zullen zich hierbij ook baseren op het onderzoek van Fox-IT. Ten tweede zal de Inspectie op stelselniveau onderzoeken in hoeverre er *lessons learned* zijn, zodat ook andere universiteiten (en meer in het algemeen onderwijsinstellingen) zich een beeld kunnen vormen van mogelijke kwetsbaarheden op het terrein van cyberveiligheid en passende maatregelen kunnen nemen.

Losgeld
Door de Universiteit Maastricht ben ik op de hoogte gesteld van het feit dat er losgeld is betaald aan de criminele organisatie die de ransomware-aanval uitvoerde, 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.

Het onderzoek van Fox-IT
Uit het rapport van Fox-IT blijkt dat halverwege oktober via phishing e-mails, de aanvaller 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 minimaal 267 servers alle bestanden zijn versleuteld. Onder de getroffen systemen bevonden zich zeer kritieke systemen voor de bedrijfsvoering en enkele back-upservers.

In het onderzoek is verder specifiek bekeken wat er gebeurd is met specifieke en cruciale systemen, waaronder systemen met onderzoeks- en persoonsgegevens. 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." Fox-IT geeft aan dat de werkwijze van de aanvaller overeenkomt met een bij hen bekende criminele

groepering, die –volgens hun informatie- al meer dan 150 slachtoffers heeft gemaakt in 2019.

Uit het rapport van Fox-IT blijkt dat de oorzaak van dit incident kon ontstaan door een combinatie van enkele ontbrekende belangrijke beveiligingsupdates, beperkte segmentatie binnen het netwerk, het niet opvolgen van verschillende alarmsignalen en ongelukkig menselijk handelen. Fox-IT doet diverse aanbevelingen aan de Universiteit Maastricht, waaronder het doen van vervolgonderzoek, waarmee de universiteit inmiddels is gestart. Daarnaast doet ook Fox-IT vervolgonderzoek. Deze vervolgonderzoeken zien onder andere op de zogenaamde 'kroonjuwelen'.

Bovendien is de universiteit aan de slag gegaan met een combinatie van maatregelen om het veiligheidsbewustzijn te vergroten en te zorgen dat studenten en medewerkers 'phishing-mails' beter zullen herkennen. Daarnaast treft de universiteit diverse technische maatregelen, die er toe moeten leiden dat de software accurater wordt ge-update, de servers beter worden gesegmenteerd en alarmsignalen beter worden gefilterd. Ook wordt er, zoals in het najaar van 2019 reeds door de universiteit besloten, een Security Operations Center opgericht, met als vaste en enige taak om de cyberdreigingen in de gaten te houden, de instelling te adviseren over veiligheid, feitelijke dreigingen te detecteren en in te grijpen als dat nodig is. Tot slot zijn voor elk systeem inmiddels beter afgeschermde back-ups gemaakt.

Acties en verhoogde urgentie naar aanleiding van ransomware-aanval
De MBO Raad, VH en VSNU laten weten dat de ransomware-aanval op de Universiteit Maastricht een grote impact heeft op de bij hen aangesloten instellingen. Benadrukt wordt dat de samenwerking binnen SURF en saMBO goed werkt. Door snelle uitwisseling van vitale informatie van de Universiteit Maastricht met SURF en aanvullende informatie van partners was SURF in staat elke instelling binnen 24 uur te informeren. Als er meer informatie beschikbaar kwam heeft SURF deze gedeeld om instellingen in staat te stellen zelf maatregelen te nemen.

Mbo-instellingen
De MBO Raad en saMBO-ICT laten weten dat de ransomware-aanval extra urgentie heeft gegeven aan het realiseren van het eerder vastgestelde ambitie van een volwassenheidsniveau van 3,0 in 2020. Er is daarbij ondersteuning voor mbo-instellingen in de vorm van het Framework IBP met modeldocumenten en best-practices en via de aanpak informatiebeveiliging en privacy van Kennisnet en er worden scholingsactiviteiten ondernomen voor het mbo-veld. De peer review wordt sectorbreed opgepakt en er wordt contact gezocht met de laag scorende instellingen voor inventarisatie van de eventuele ondersteuningsbehoefte. Ook zijn er werkgroepen opgestart op de gesignaleerde knelpunten en staat de eerstvolgende ALV-themabijeenkomst van de MBO Raad in het teken van cybersecurity.
De hieronder genoemde te nemen maatregelen 1 en 3 die getroffen worden binnen het hoger onderwijs zijn ook van toepassing op het mbo.

Hoger onderwijs
De VSNU benoemt dat de ransomware-aanval het thema cyberveiligheid bovenaan de bestuurlijke agenda's heeft geplaatst en het gesprek over integrale veiligheid en de inspanningen in de sector in nieuw licht plaatst. Daarbij ligt de vraag of de sector op dit moment voldoende doet, expliciet op tafel. Bij dit gesprek worden het platform IV-HO, de hoofden ICT en de functionarissen gegevensbescherming nauw betrokken. Ook de voorzitters van de hogescholen hebben inmiddels met elkaar gesproken over integrale veiligheid met een nadruk op cyberveiligheid.

De universiteiten en hogescholen verwachten in de komende weken meer duidelijkheid te krijgen en te kunnen geven over de situatie in de hoger onderwijssector en de risico's. Voor de zomer komen zij met een plan voor de te nemen maatregelen waar de hele sector mee aan de slag gaat om het gewenste ambitieniveau te bereiken. Daarbij denken de universiteiten en hogescholen aan de volgende maatregelen:

1. Informatie over de ransomware-aanval op de Universiteit Maastricht is met de andere onderwijsinstellingen gedeeld zodat andere instellingen ook kunnen leren van de casus. Daarnaast zal worden verkend of het nodig is specifieke aanvullende maatregelen te treffen in het hoger onderwijs waarbij rekening wordt gehouden met de aanbevelingen naar aanleiding van het Fox-IT onderzoek.
2. De bestaande toetsing van digitale veiligheid in het hoger onderwijs is vrijwillig, niet landelijk vergelijkbaar en/of dekkend. De VH en VSNU verkennen in welke mate (externe) toetsing plaatsvindt en of het meerwaarde heeft naar een periodieke, vergelijkbare, vorm van toetsing toe te groeien. Daarbij is aandacht voor de diversiteit van instellingen.
3. SURFcert biedt 24 uur per dag 7 dagen per week ondersteuning van SURF-deskundigen bij beveiligingsincidenten. Er wordt onderzocht – ook rekening houdend met de investeringen die dit met zich meebrengt - of in aanvulling hierop een 24/7 monitoring- en scanfunctie moet worden ingevuld in de vorm van een Security Operations Center (SOC).
4. Er wordt steviger ingezet op *awareness*. De mens blijft vaak de zwakke schakel in digitale veiligheid. Medewerkers en studenten moeten bewust worden gemaakt van cyberdreigingen.

Tot slot
Cybersecurity is een vraagstuk dat overal in de samenleving en dus ook in de onderwijssector aandacht behoeft. Uit het voorgaande blijkt dat de onderwijssectoren reeds serieus bezig waren met het vraagstuk van cybersecurity. En ook dat het incident bij de Universiteit Maastricht extra aandacht voor dit onderwerp heeft gegenereerd. Daarbij zijn op korte termijn voornemens geformuleerd om mogelijke incidenten zoals bij Universiteit Maastricht zo veel mogelijk te voorkomen.

Van een professionele sector verwacht ik dat organisaties elkaar onderling aanspreken op kwetsbaarheden. Daar hoort wat mij betreft bij dat instellingen periodiek hun eigen systeem door experts laten controleren en dit laten vergelijken met peers. Ook verwacht ik dat instellingen bij een effectieve aanpak van de digitale veiligheid rekenschap geven van de risico's bij een vergaande decentralisatie van de ICT-systemen. Alleen dan komt de sector, zonder de illusie van 100% veiligheid, samen verder en wordt samen voor een (digitaal) veilige leer- en werkomgeving gezorgd.

Onderwijsinstellingen, en met name universiteiten, moeten zich realiseren dat zij een interessant doelwit vormen voor criminele organisaties en statelijke actoren vanwege de maatschappelijke impact, economische bijdrage, innovatie en onderzoeksdata die een belangrijke waarde vertegenwoordigen. De mbo-scholen, hogescholen en universiteiten hebben acties ingezet om de ontwikkeling die ze de laatste jaren hebben doorgemaakt, versneld door te zetten. Daar heb ik waardering voor, maar ik verwacht tegelijkertijd dat de sectoren extra acties aankondigen voor de zomer van 2020.

Incidenten als bij de Universiteit Maastricht en de Citrix-kwetsbaarheid bieden de kans van elkaar te leren en de sector als geheel te versterken. Coöperaties als SURF en saMBO-ICT, organisaties met veel kennis en kunde over digitale veiligheid, waar bijna alle mbo-, hbo- en wo-instellingen bij zijn aangesloten,

zullen instellingen daarbij ondersteunen. 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.

Mede namens de minister van Basis- en Voortgezet Onderwijs en Media,

De minister van Onderwijs, Cultuur en Wetenschap,

Ingrid van Engelshoven

- SCIRT: SURFnet Community of Incident Response Teams, waarin security experts kennis uitwisselen over de nieuwste cybersecuritydreigingen en waar vanuit meerdere invalshoeken ideeën, tips en trucs worden besproken om de bedreigingen succesvol af te wenden, vooral gericht op operationele veiligheid en security incident management.
- SCIPR: SURF Community voor Informatiebeveiliging en Privacy, waarin informatiebeveiligers en privacy officers in het onderwijs samenwerken aan beleid en leidraden om de informatiebeveiliging en privacy van instellingen te verbeteren.
- SURFcert: 24 uur per dag, 7 dagen per week 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. Sinds 2006 promoot SURFcert de oprichting van lokale CSIRTs bij aangesloten instellingen. Een CSIRT is een capability/team van een organisatie dat informatiebeveiligingsincidenten managet - wat inhoudt dat mogelijke incidenten voorkomen worden, incidenten die plaatsvinden opgelost worden, en dat de daaruit geleerde lessen ter harte genomen worden.
- Cybersave yourself: een campagne waarmee op een ludieke manier het bewustzijn van medewerkers en studenten vergroot kan wordenop het gebied van security en privacy. De campagne bestaat uit een website en een online toolkit met kant-en-klaar materiaal.
- OZON: Specifiek met betrekking tot cyberveiligheid voert SURF iedere twee jaar een vrijwillige cyberoefening (OZON) uit waarmee instellingen gezamenlijk kunnen oefenen hoe gereageerd kan worden op een cybercrisis. Hiermee kan achterhaald worden hoe goed zij voorbereid zijn op een incident. In die oefeningen worden alle lagen binnen de organisatie betrokken: van ICT-beheerders tot afdeling communicatie, bestuurders en toezichthouders.
- Cyberdreigingsbeeld: dit rapport beschrijft jaarlijks de grootste dreigingen voor de sectoren onderwijs en onderzoek op het gebied van informatieveiligheid. Dit rapport wordt opgesteld op basis van een survey. Het is een inschatting van een persoon bij een instelling die die vragenlijst heeft beantwoord voor zijn eigen instelling. Het is een indicatie van hoe de sector ervoor staat, maar kan door de methodiek niet gebruikt worden voor een vergelijking met andere sectoren.
- IVHO: op bestuurlijk niveau wordt cybersecurity besproken als onderdeel van integrale veiligheid. Ook is er een normenkader IVHO opgesteld voor wat je minimaal moet regelen om de veiligheid en continuïteit van bedrijfsgegevens en de privacy van studenten en medewerkers te beschermen. Dit normenkader is de basis van ons zelfassessmentsysteem SURF-audit.
- SURFaudit: via SURFaudit kunnen instellingen op ieder gewenst moment de informatiebeveiliging beoordelen via een assessment van de instelling als geheel, of van een afdeling. Resultaten zijn vertrouwelijk.