Inspectie van het Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

CYBERAANVAL UNIVERSITEIT MAASTRICHT

UNIVERSITEIT MAASTRICHT (BRIN: 21PJ)

Utrecht, mei 2020

INHOUD

Samenvatting

De Universiteit Maastricht (UM) werd op 23 december 2019 getroffen door een cyberaanval. Naar aanleiding van de omvang van de cyberaanval – en daarmee de mogelijke risico's voor de voortgang van het onderwijs en onderzoek – heeft de Inspectie van het Onderwijs (hierna: inspectie) in de periode februari – maart 2020 een onderzoek uitgevoerd. De hoofdvraag was: *Heeft de Universiteit Maastricht vooraf, tijdens en na de aanval passende maatregelen genomen om de goede voortgang van het onderwijs te waarborgen?* Het betreft een incidenteel onderzoek conform de Wet op het onderwijstoezicht (WOT) artikel 12a derde lid.

We beantwoorden de hoofdvraag aan de hand van drie deelvragen:

1. *Preventie: Hoe was de UM voorbereid op een cyberaanval en had de UM preventieve maatregelen genomen om bij een mogelijke aanval de goede voortgang te waarborgen (cyberweerbaarheid)?*

In recente jaren was databeveiliging in toenemende mate onderwerp van gesprek en bewustwordingscampagnes. Echter, het onderwerp wat met name gericht op AVG en niet op een mogelijke cyberaanval. De UM was aangesloten bij SURFcert en nam deel aan SURF-cyberoefeningen. De laatste oefening was gericht op een cyberaanval. De UM heeft een eigen Computer Emergency Respons Team (CERT) en een Chief Information Security Officer (CISO). De interne controle op de uitvoering van het ICT-beleid en de opvolging van afspraken was beperkt ingericht. Cyberdreiging stond niet bovenaan de lijst met risico's. Activiteiten door kwaadwillenden, zoals ransomware, waren niet opgenomen in de draaiboeken voor grote incidenten. Voorafgaand aan de cyberaanval was er geen totaal (over)zicht op de IT-inrichting en daarmee slechts beperkt zicht op de cyberweerbaarheid van de universiteit als geheel. De UM staat hierin overigens niet alleen: ook andere universiteiten en hogescholen hebben een gelaagde bestuursstructuur en zijn daarmee potentieel kwetsbaar. De uitdaging is om informatiebeveiligingsbeleid, de uitvoering daarvan en de controle daarop in te richten gegeven de decentrale inrichting voor de onderwijsinstelling als geheel.

Wij stellen vast dat er bij de UM voorafgaand aan de cyberaanval aandacht was voor informatiebeveiliging, maar dat voorafgaand aan de ontdekking van de ransomware aanval op 23 december 2019 niet altijd passend maatregelen zijn genomen. Daardoor is niet opgemerkt dat derden toegang tot het netwerk hadden gekregen, en had de cyberaanval verstrekkender impact dan nodig.

2. *Respons: Welke acties heeft de UM genomen in reactie op de cyberaanval om de voortgang van het onderwijs zo snel mogelijk te herstellen?*

Fox-IT heeft vastgesteld dat na het openen van een phishingmail er onvoldoende detectie, monitoring en opvolging heeft plaatsgevonden, waardoor hackers op 23 december 2019 een ransomware aanval konden uitvoeren op een deel van het UM-netwerk. Het College van Bestuur (CvB) heeft in nauwe afstemming met het Crisis Management Team (CMT), de Raad van Toezicht (RvT), de medezeggenschap en andere geledingen binnen de universiteit de cyberaanval afgehandeld. De voortgang van het onderwijs en onderzoek stond daarbij voorop. Communicatie naar medewerkers en studenten was een essentieel parallel proces. Daarnaast hebben CvB en RvT besloten zoveel mogelijk informatie met andere instellingen voor hoger onderwijs te delen. De universiteit zag zich genoodzaakt via losgeldbetaling de

decryptiesleutel te verkrijgen Zij heeft onderzocht of een alternatief haalbaar was. Zonder de betaling zou het herstel en de herbouw maanden kunnen duren en was er geen zekerheid op volledig herstel, waarmee de goede voortgang van het onderwijs en onderzoek ernstig in het geding zou zijn. Bovendien zouden de kosten voor het zelf herstellen een veelvoud zijn van het losgeldbedrag.

Wij stellen vast dat de crisisafhandeling adequaat was: de inspectie heeft geen aanwijzingen gevonden dat de UM na het ontdekken van de ransomware aanval andere meer passende maatregelen had kunnen nemen. Bovendien heeft de UM met de organisatie van een symposium openheid gegeven om andere organisaties te waarschuwen en heeft daarmee bijgedragen aan het lerend vermogen van het stelsel van hoger onderwijs.

3. *Lerend vermogen: Welke voorzieningen heeft de UM getroffen om soortgelijke incidenten in de toekomst te voorkomen met het oog op de goede voortgang van het onderwijs?*

Tijdens het afhandelen van het cyberincident is gewerkt aan ‘verhoogde dijkbewaking’, bijvoorbeeld door continue (24/7) monitoring van de IT-systemen door externe inhuur. Daarnaast is de gehele centrale en decentrale IT-infrastructuur in kaart gebracht en is er een duidelijk besef van de preventieve maatregelen die moesten worden aangescherpt. De UM heeft behoefte aan meer samenwerking met andere onderwijsinstellingen, aan meer kennisdeling over cyberdreigingen en duidelijke steun vanuit de overheid. Medewerkers van de UM geven aan dat het gesprek over cyberveiligheid moet worden gevoerd en dat nu het moment is om maatregelen door te pakken. Er moet daarbij aandacht zijn voor het dilemma tussen investeringen in het primaire proces ‘onderwijs en onderzoek’ enerzijds en cyberweerbaarheid anderzijds. De komende periode zal moeten uitwijzen hoe het staat met het draagvlak voor informatiebeveiligingsmaatregelen binnen de UM.

De UM heeft passende maatregelen gerealiseerd door het invoeren van ‘verhoogde dijkbewaking’ in de eerste periode na afhandelen van de crisis. Of op langere termijn bij de UM sprake is van passende maatregelen om incidenten van soortgelijke omvang te voorkomen, kan op dit moment nog niet worden vastgesteld.

Conclusie
We concluderen dat door het adequaat ingrijpen tijdens de cyberaanval de goede voortgang van het onderwijs en onderzoek als gevolg van de cyberaanval slechts beperkt in gevaar is geweest. Er is slechts voor een korte periode sprake geweest van een continuïteitsprobleem voor het onderwijs en onderzoek. Het CvB van de UM heeft weloverwogen beslissingen genomen en deze gedeeld en geïmplementeerd binnen de organisatie om een goede voortgang van de geplande onderwijsactiviteiten na de vakantieperiode te realiseren. Hoewel de UM heeft nagelaten in preventieve zin voldoende passende maatregelen te nemen, waren de respons en de eerste getrokken lessen adequaat.

Vervolgtoezicht
De inspectie constateert dat de Universiteit Maastricht adequaat heeft gehandeld in het afhandelen van de cyberaanval en heeft vertrouwen in het reeds geïnitieerde vervolgonderzoek. De inspectie zal de UM daarom geen aanvullende verbeterpunten voorschrijven. Ook andere universiteiten en hogescholen kunnen kwetsbaar zijn voor cyberrisico’s. De inspectie besloot daarom begin 2020 tot het instellen van een tweeledig onderzoek: naar de instelling en naar het stelsel van hoger onderwijs. Ten behoeve van dit tweede deel vraagt de inspectie de UM haar te informeren over de uitkomsten van het door de UM ingestelde vervolgonderzoek.

1 Aanleiding en context

De Inspectie van het Onderwijs (hierna: inspectie) heeft in de periode februari – maart 2020 een onderzoek uitgevoerd bij de Universiteit Maastricht (UM). Aanleiding voor het onderzoek was de cyberaanval waar de Universiteit Maastricht op 23 december 2019 door werd getroffen. Het onderzoek richt zich op het handelen van de Universiteit Maastricht vooraf, tijdens en na afloop van de cyberaanval. Het betreft een incidenteel onderzoek conform de Wet op het onderwijstoezicht (WOT) artikel 12a derde lid.

Op 26 december 2019 stelde de vicevoorzitter van de UM de inspectie (tevens voorzitter van het crisis management team) op de hoogte van de cyberaanval op de instelling. Sinds de avond van 23 december 2019 was een deel van de systemen en data van de UM door encryptie ontoegankelijk geworden. Er werd losgeld geëist voor een sleutel waarmee de systemen konden worden 'ontsmet' en de versleuteling van de databestanden kon worden opgeheven. De vicevoorzitter heeft tevens aangegeven hoe de UM met bijstand van het bedrijf Fox-IT werkte aan herstel van de IT-omgeving van de instelling. Na dit eerste contact heeft de UM de inspectie wanneer dit relevant was van nieuwe informatie voorzien.

Naar aanleiding van de omvang van de cyberaanval – en daarmee de mogelijke risico's voor de voortgang van het onderwijs en onderzoek – heeft de inspectie besloten tot het instellen van een tweeledig onderzoek. Het eerste deel betreft een instellingonderzoek gericht op de UM. Het tweede deel is thematisch. Hierin zal de inspectie op het niveau van het stelsel van hoger onderwijs nagaan welke lessen uit de cyberaanval bij de UM breed toepasbaar zijn voor andere universiteiten en hogescholen. De inspectie heeft op 13 januari 2020 het College van Bestuur (CvB) telefonisch geïnformeerd over het besluit een onderzoek in te stellen. Het besluit is tevens schriftelijk bevestigd aan de UM met een brief van 30 januari 2020.

1.1 Leeswijzer

In het vervolg van dit hoofdstuk wordt ingegaan op de achtergrond van de problematiek. Hoofdstuk 2 bespreekt de onderzoeksopzet. Hoofstuk 3 bevat de conclusies, in hoofdstuk 4 gevolgd door de bevindingen waarop deze zijn gebaseerd. In hoofdstuk 5 wordt op het vervolgtoezicht in gegaan.

1.2 Digitale dreigingen en het hoger onderwijs

Digitale dreigingen komen nationaal en internationaal steeds vaker voor. Zo waren er in 2018 in Nederland 1,2 miljoen individuele slachtoffers van digitale criminaliteit, zoals vermogensdelicten of identiteitsfraude (CBS, 2018[1]). Digitale criminaliteit komt niet alleen bij individuen, maar ook bij bedrijven en organisaties steeds vaker voor. Hoger onderwijsinstellingen kunnen op verschillende vlakken aantrekkelijk zijn voor digitale criminelen. Onlangs bleek dat bijvoorbeeld staatshackers uit Iran bij verschillende Nederlandse instellingen onderwijsmaterialen en inloggegevens van wetenschappelijke literatuur probeerden te bemachtigen[2]. Ook worden er pogingen gedaan, zoals onlangs bij de Universiteit Maastricht, om de netwerken van instellingen te versleutelen in ruil voor een losgeld betaling. De voortgang van onderzoek en onderwijs bij instellingen voor hoger onderwijs zijn vrijwel volledig

[1] Centraal Bureau voor de Statistiek, 2019. *Digitale Veiligheid & Criminaliteit 2018.* https://www.cbs.nl/nl-nl/publicatie/2019/29/digitale-veiligheid-criminaliteit-2018

[2] https://www.nrc.nl/nieuws/2020/02/14/nederlandse-onderwijsinstellingen-doelwit-van-iraanse-hackers-a3990472 (geraadpleegd op 10 maart 2020)

afhankelijk van digitale netwerken, waardoor deze instellingen een aantrekkelijk doelwit vormen.

De beveiliging van het ICT-netwerk van een instelling voor hoger onderwijs is door de aard van deze organisaties een uitdaging. Onderwijsinstellingen zijn open leeromgevingen met veel verschillende gebruikers, zoals studenten, onderzoekers, docenten, medewerkers en gastgebruikers en daardoor veel verschillende behoeftes en wensen ten aanzien van de ICT-voorzieningen. Dat vereist een op maat gesneden beveiliging van het ICT-netwerk. Universiteiten hebben bovendien een gelaagde bestuursstructuur met verschillende bestuursorganen: op centraal niveau wordt een universiteit aangestuurd door het CvB en op decentraal niveau bestaat de organisatie uit decanen op faculteitsniveau, onderwijs- en onderzoekdirecteuren op opleidingsniveau en professoren, universitair (hoofd) docenten op onderzoeksniveau. Het ICT-beleid en de ICT-beveiliging speelt zich af op de verschillende niveaus en verlangt ook daarom extra aandacht voor een goede beveiliging.

1.2.1 Verantwoordelijkheid digitale veiligheid hoger onderwijs

De overheid heeft een vitale infrastructuur gedefinieerd. Deze infrastructuur bestaat uit processen die zo essentieel zijn voor de Nederlandse samenleving, dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid (NCTV, 2020[3]). Voorbeelden van de vitale processen zijn elektriciteit, toegang tot internet, drinkwater en betalingsverkeer.
Sinds het inwerkingtreden van de ‘Wet beveiliging netwerk- en informatiesystemen’ geldt voor sommige aanbieders van een vitale infrastructuur een zogenaamde zorgplicht: deze aanbieders behoren adequate maatregelen te nemen voor de beveiliging van hun netwerk- en informatiesystemen.

Organisaties en bedrijven in Nederland die geen onderdeel uitmaken van de vitale infrastructuur hebben geen vastgelegde richtlijnen voor hun digitale informatieveiligheid. Dit geldt ook voor instellingen voor hoger onderwijs. De verantwoordelijkheid voor een goede bedrijfsvoering ligt bij de instelling zelf. Dat geldt dus ook voor het integraal veiligheidsbeleid waar digitale informatiebeveiliging deel van uitmaakt. In het hoger onderwijs werken instellingen al een lange tijd samen op het gebied van ICT-infrastructuur. Deze samenwerking is terug te vinden in ‘SURF’. Dit is een coöperatieve vereniging van Nederlandse onderwijs- en onderzoeksinstellingen waarin de leden gezamenlijk digitale diensten inkopen of ontwikkelen. De onderwijsinstellingen zijn als leden ook eigenaar van SURF. SURF brengt jaarlijks een cyberdreigingsbeeld uit met trends in dreigingen voor het onderwijs en onderzoek[4]. SURF verzorgt voorlichting en coördineert de uitvoering van informatiebeveiliging, bijvoorbeeld digitale veiligheidsaudits en ondersteuning bij beveiligingsincidenten. Dit krijgt vorm door deelname van instellingen voor hoger onderwijs aan het zogenaamde SURFcert. SURFcert is een team dat onderwijsinstellingen ondersteuning biedt bij beveiligingsincidenten. Alle bekostigde universiteiten en universitaire medische centra zijn bij SURF en het SURFcert aangesloten. Alle bekostigde hogescholen zijn aangesloten bij SURF, waarvan 94% ook aangesloten is bij SURFcert.

SURFcert is sinds 24 januari 2020 door de minister van Justitie en Veiligheid aangewezen als één van de informatieknooppunten van niet-vitale sectoren die in nauw contact staat met Nationaal Cyber Security Centrum (NCSC)[5]. NCSC verspreidt informatie onder de verschillende informatieknooppunten wanneer er

[3] https://www.nctv.nl/onderwerpen/vitale-infrastructuur (geraadpleegd op 6 maart 2020)
[4] zie: SURF, 2018. *Cyberdreigingsbeeld*. https://www.surf.nl/files/2019-03/surf_cyberdreiging_2018_web.pdf
[5] Dit is bepaald in de regeling aanwijzing computercrisisteams, Staatscourant 2020, 4410.

dreigingen of kwetsbaarheden zijn. De verschillende informatieknooppunten zijn vervolgens verantwoordelijk voor het informeren en bijstaan van hun doelgroepen.

1.2.2 Standaarden voor digitale informatiebeveiliging

Er zijn wereldwijd verschillende standaarden en methoden ontwikkeld voor het beveiligen van digitale informatie. De Internationale Organisatie voor Standaardisatie (ISO) heeft de internationale informatiebeveiligingsstandaarden beschreven in ISO 27001. Deze standaarden beschrijven het volledige proces van informatiebeveiliging en zijn hiervoor de wereldwijd erkende norm. ISO 27002 geeft aanvullende standaarden, waarin adviezen worden gegeven hoe je de beveiliging kunt implementeren die vermeld zijn in ISO 27001. Deze internationale standaarden zijn wereldwijd de basis voor andere uitwerkingen van digitale veiligheidsstandaarden. De Nederlandse Rijksoverheid heeft de ISO 27001 en 27002 uitgewerkt in de Baseline Informatiebeveiliging Overheid (BIO). Dit normenkader voor informatiebeveiliging geeft het basisniveau voor informatiebeveiliging aan waar alle overheidspartijen aan moeten voldoen[6]. Voor overheidsinstellingen wordt geadviseerd om de BIO standaard te hanteren. Het gebruik hiervan is echter nog niet wettelijk vastgelegd.

SURF heeft ook een normen- en toetsingskader ontwikkeld die op de ISO-norm is gebaseerd en tevens voldoet aan het richtsnoer Beveiliging van Persoonsgegevens van de Autoriteit Persoonsgegevens. SURF heeft maatregelen uit de ISO-norm geselecteerd die in ieder geval ingeregeld moeten worden in een onderwijsinstelling. Deze maatregelen zijn in de volgende clusters ingedeeld: 1) beleid en organisatie, 2) personeel, studenten en gasten, 3) ruimten en apparatuur, 4) continuïteit, 5) vertrouwelijkheid en integriteit en 6) controle en logging. Dit normen- en toetsingskader vormt de basis van de SURFaudit. Onderwijsinstellingen kunnen daarmee de informatiebeveiliging van de universiteit of hogeschool beoordelen. Dat kan voor de instelling als geheel of voor afzonderlijke afdelingen. SURF voert tweejaarlijks de SURFaudit-benchmarks uit. Dit laat zien hoe het wetenschappelijk onderwijs en het hoger beroepsonderwijs ervoor staan. De benchmark geeft individuele onderwijsinstellingen inzicht in de eigen scores ten opzichten van andere hoger onderwijsinstellingen. Instellingen aangesloten bij SURF kunnen vrijwillig de eigen informatiebeveiliging toetsen door het uitvoeren van interne audits op basis van self-assessment. Aanvullend kunnen peer reviews van de self-assessment worden gedaan door professionals uit gelijksoortige organisaties of kunnen externe audits worden georganiseerd.

1.2.3 Preventie, incident response en risicomanagement

Het inrichten van informatiebeveiliging is onder andere gericht op preventie van mogelijke incidenten. Onderdelen van preventie zijn bijvoorbeeld het beheer van incidenten, veranderingen in het netwerk, toegangsrechten, configuraties en patches. De ICT-afdelingen van organisaties zijn verantwoordelijk voor de uitvoering van maatregelen rondom deze onderdelen. Naast het inrichten van preventieve maatregelen is het volgens de informatiebeveiligingsstandaarden noodzakelijk om binnen de organisatie een Computer Security Incident Response Team (CSIRT), ook wel Computer Emergency Respons Team (CERT) genoemd, op te zetten. Zo'n team is verantwoordelijk voor het afhandelen van beveiligingsincidenten in netwerken. Het team wordt over het algemeen geleid door de Chief Information Security Officer (CISO). Binnen het hoger onderwijs ondersteunt SURFnet het opzetten van deze

[6] De BIO is (nog) niet op wetgeving gebaseerd. Wel 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, zie: https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uit (geraadpleegd op 10 maart 2020). Vanuit het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties wordt gewerkt aan wettelijke verankering van BIO.

CSIRT teams. Ten slotte is het belangrijk dat er ten behoeve van de informatiebeveiliging risicomanagement plaatsvindt binnen alle lagen van de organisatie. (Het bestuur van) de organisatie in een niet-vitale infrastructuur kan na reflectie op basis van verschillende standaarden zorgen voor het effectief managen van risico's rondom informatiebeveiliging. In het normenkader van de Nederlandse Rijksoverheid, de BIO, worden zeven handzame standaarden beschreven die bestuurders kunnen benutten voor het informatiebeveiligingsbeleid van de organisatie. Deze zeven standaarden zijn: 1. vergroten bewustzijn, 2. veilige en open cultuur, 3. inrichten risicoteam, 4. borgen risicomanagement, 5. aandacht voor ketensamenwerking, 6. controleren en evalueren en 7. geld investeren in informatiebeveiliging. Deze standaarden hebben wij in ons onderzoek gebruikt. Hier wordt in het volgende hoofdstuk verder op ingegaan.

2 Onderzoeksopzet

2.1 Onderzoeksvraag en afbakening

Dit inspectieonderzoek had tot doel om na te gaan of met het handelen van de Universiteit Maastricht vooraf, tijdens en na afloop van de cyberaanval sprake was van wanbeheer. Onder wanbeheer verstaan we ernstige nalatigheid van bestuurders of toezichthouders om maatregelen te treffen die noodzakelijk zijn voor het waarborgen van de goede voortgang van het onderwijs aan de instelling (WHW artikel 9.9a). Het onderzoek beperkt zich tot de goede voortgang van het bachelor- en masteronderwijs en de promoties. De inspectie verricht in het hoger onderwijs zelf geen onderzoek naar de kwaliteit van het onderwijs, die taak is (middels accreditatie) belegd bij de Nederlands Vlaamse Accreditatie Organisatie (NVAO). Indien de inspectie signalen heeft dat de kwaliteit niet op orde is, informeert zij daarover de NVAO. Er zijn vooraf noch tijdens dit onderzoek signalen geweest dat de kwaliteit van het onderwijs in het geding is geweest.

De hoofdvraag van dit onderzoek luidt:

> *Heeft de Universiteit Maastricht vooraf, tijdens en na de aanval passende maatregelen genomen om de goede voortgang van het onderwijs te waarborgen?*

De hoofdvraag is onderverdeeld in de volgende drie deelvragen:

- Preventie: Hoe was de UM voorbereid op een cyberaanval en had de UM preventieve maatregelen genomen om bij een mogelijke aanval de goede voortgang te waarborgen (cyberweerbaarheid)?
- Respons: Welke acties heeft de UM genomen in reactie op de cyberaanval om de voortgang van het onderwijs zo snel mogelijk te herstellen?
- Lerend vermogen: Welke voorzieningen heeft de UM getroffen om soortgelijke incidenten in de toekomst te voorkomen met het oog op de goede voortgang van het onderwijs?

Het onderzoek richt zich tot de situatie ultimo 18 februari 2020 (datum locatieonderzoek).

2.2 Beoordelingskader

De inspectie verricht onderzoek naar naleving van de wettelijke voorschriften en de financiële rechtmatigheid bij instellingen voor hoger onderwijs op grond van artikel 12a, eerste lid, van de WOT.

Dit onderzoek richt zich op de vraag of/in hoeverre er sprake is geweest van wanbeheer. De WHW omschrijft wanbeheer als volgt: *ernstige nalatigheid van bestuurders of toezichthouders om maatregelen te treffen die noodzakelijk zijn voor het waarborgen van de kwaliteit en goede voortgang van het onderwijs aan de instelling* (artikel 9.9a, tweede lid, onder b, van de WHW).
Van ernstige nalatigheid is sprake als:

- Er zich een falen of incident voordoet doordat nagelaten is (effectief) actie te ondernemen terwijl dat objectief gezien wel mogelijk en geboden was; en/of
- Er nagelaten is om (effectief) op te treden op het moment en nadat het falen zich voordeed terwijl dat objectief gezien mogelijk en geboden is; en/of
- Er nagelaten is om vergelijkbare incidenten in het vervolg te voorkomen en passende organisatorische maatregelen te nemen.

Door ernstige nalatigheid duurt een probleemsituatie nodeloos voort en/of ontstaan extra en ernstige problemen. Ernstige nalatigheid betreft dus een verzuim dat is toe te rekenen aan het bestuur of de raad van toezicht (RvT). [7]

De WHW bevat geen normenkader voor het beoordelen van de inrichting van ICT-systemen van instellingen voor hoger onderwijs. Wel bevat de WHW voorschriften voor het bestuur en de inrichting van de universiteiten (hoofdstuk 9 WHW) respectievelijk hogescholen (hoofdstuk 10 WHW). De voor dit onderzoek relevante bepalingen staan opgenomen in bijlage 1.

In het huidige onderzoek gebruiken we de BIO-standaarden voor de bestuurstafel (zie paragraaf 1.2.3) als kapstok voor het beantwoorden van onze onderzoeksvragen. We zullen voor iedere onderzoeksvraag nagaan welke maatregelen getroffen zijn voor, tijdens en na het incident op ieder van de zeven standaarden. De betreffende standaarden vloeien voort uit de ISO standaarden 27001 en 27002 en zijn daarom toepasbaar op iedere organisatie die de ISO-normen nastreeft, zo ook de Universiteit Maastricht. Zoals eerder genoemd zijn instellingen niet wettelijk verplicht om aan deze standaarden te voldoen, ze dienen enkel als richtlijnen voor het vormgeven en implementeren van informatiebeveiliging. De zeven standaarden die bestuurders kunnen benutten, worden als volgt beschreven in de BIO:

1. *Vergroten bewustzijn:* Bestuurders agenderen tijdens overleggen met regelmaat het belang van informatiebeveiliging. Er bestaan bewustwordingsmaatregelen onder studenten, onderzoekers, docenten en medewerkers die met regelmaat worden ingezet.
2. *Veilige en open cultuur:* Informatiebeveiliging is in essentie risicomanagement wat begint bij identificatie. Het bestuur bevordert een open en veilige cultuur waarin medewerkers zich vrij voelen om (potentiele) risico's proactief te melden bij de juiste persoon.
3. *Inrichten risicoteam:* Maak gebruik van de kennis en verantwoordelijkheden van proces- en systeemeigenaren. Er is samenwerking tussen een risicoteam door de Chief Information Security Officer (CISO), Functionaris Gegevens-bescherming (FG) en Controller. Deze systeemeigenaren functioneren tevens als onafhankelijk adviseur voor het bestuur.
4. *Borgen risicomanagement:* Risicomanagement is een cyclisch, iteratief en terugkerend proces: dreigingen, omgeving en wetgeving veranderen. Er wordt rekening gehouden met deze veranderingen zodat maatregelen doeltreffend en doelmatig zijn.
5. *Aandacht voor ketensamenwerking:* Partners en leveranciers kunnen op afhankelijke wijze aantonen dat deze partijen aan de geldende eisen voldoen.
6. *Controleren en evalueren:* Regelmatige controle en evaluatie zijn belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie (e.g., regelmaat, rapportages).
7. *Geld investeren in informatiebeveiliging:* Er worden voldoende middelen beschikbaar gesteld om de onderkende risico's op een adequate manier te behandelen.

2.3 Instellingsbezoek en documentanalyse

Voor dit onderzoek maakte de inspectie gebruik van het rapport dat door Fox-IT is opgesteld over de cyberaanval[8]. Het rapport beschrijft de resultaten van hun

[7] 33475, nr, 15, wet versterking kwaliteitswaarborgen hoger onderwijs

[8] M. Dijkstra & M. van Dantzig (2020) *Spoed Ondersteuning Project Fontana*. Ondersteuning bij ransomware aanval. (projectnr 190346) versie 3.0. public versie inclusief reactie Universiteit Maastricht beschikbaar gesteld via de site van de universiteit op 05-02-2020.

forensisch onderzoek en gaat onder andere in op de uitkomsten van de root-cause analysis[9] naar de ransomware[10] aanval van 23 december 2019 en de vraag of gegevens zijn ingezien of ontvreemd. In aanvulling op de rapportage van Fox-IT heeft de inspectie documentatie van de Universiteit Maastricht ingezien (zie bijlage 2) en gesprekken gevoerd met verschillende geledingen uit de organisatie (zie bijlage 3). De gesprekken vonden plaatst op 17 en 18 februari en op 9 maart 2020.

2.4 Rapportage

Na het bezoek is een conceptrapport opgesteld dat op 14 april 2020 aan de instelling is voorgelegd.

Op 23 april 2020 vond over het conceptrapport telefonisch overleg plaats met een vertegenwoordiging van het bestuur. De instelling gaf op 24 april 2020 haar schriftelijke reactie op het rapport. Waar nodig is het rapport aangepast. Het rapport is op 12 mei 2020 vastgesteld en aan de instelling verzonden.

[9] Root Cause Analysis is een systematische aanpak om de onderliggende oorzaken ("root causes") van een probleem te identificeren. De analyse is tevens gericht op het vinden van maatregelen om deze oorzaken weg te nemen.

[10] Ransomware is een type malafide software waarmee toegang tot bestanden en/of systemen kan worden geblokkeerd totdat een losgeldsom wordt betaald (Fox-IT, verklarende woordenlijst). Ransomware wordt ook wel gijzelsoftware genoemd.

3 Conclusies

3.1 Hoofdvraag

Aanleiding voor het onderzoek was de cyberaanval waar de Universiteit Maastricht (UM) eind 2019 door werd getroffen. De inspectie onderzocht de volgende hoofdvraag: *heeft de Universiteit Maastricht vooraf, tijdens en na de aanval passende maatregelen genomen om de goede voortgang van het onderwijs te waarborgen?*

Samenvattend stellen wij vast dat de UM voorafgaande aan de cyberaanval niet altijd passende maatregelen heeft genomen waardoor de cyberaanval verstrekkender impact had dan nodig. Ook tijdens de eerste fase van het incident bleken de maatregelen niet passend, waardoor niet is opgemerkt dat derden toegang tot het netwerk hadden gekregen. De crisisafhandeling zelf was daarentegen adequaat: in deze tweede fase van het incident die startte na het ontdekken van de ransomware aanval, heeft de inspectie geen aanwijzingen gevonden dat de UM andere, meer passende maatregelen had kunnen nemen. Ook zijn er voor de eerste periode nadat de crisis is afgehandeld met de ‘verhoogde dijkbewaking’ passende maatregelen gerealiseerd. Bovendien heeft de UM met de organisatie van een symposium openheid gegeven om andere organisaties te waarschuwen en heeft daarmee bijgedragen aan het lerend vermogen van het stelsel van hoger onderwijs. Of op langere termijn bij de UM sprake is van passende maatregelen om incidenten van soortgelijke omvang te voorkomen, kan op dit moment nog niet worden vastgesteld.

We concluderen bovendien dat door het uiteindelijk adequaat ingrijpen de goede voortgang van het onderwijs en onderzoek als gevolg van de cyberaanval slechts beperkt in gevaar is geweest. In de periode vanaf 24 december 2019 tot 2 januari 2020 was er geen toegang tot de UM systemen voor medewerkers en studenten. Daarmee was er alleen voor die korte periode sprake van een continuïteitsprobleem voor het onderwijs en onderzoek. De UM heeft zich met alle middelen gericht op de voortgang van de geplande onderwijsactiviteiten na de vakantieperiode. Daarin heeft het College van Bestuur (CvB) van de UM weloverwogen beslissingen genomen en deze gedeeld en geïmplementeerd binnen de organisatie. Daardoor konden alle geplande onderwijsactiviteiten vanaf 6 januari 2020 doorgang vinden. Hierdoor heeft de UM de voortgang van het onderwijs en onderzoek tijdig weer hersteld waardoor het op lange termijn niet in gevaar is geweest. Hoewel de UM heeft nagelaten in preventieve zin alle passende maatregelen te nemen is er van ernstige nalatigheid en van wanbeheer geen sprake: ook voor de aanval was er al aandacht voor cyberweerbaarheid, de respons op het incident was daadkrachtig en de UM implementeert de eerste getrokken lessen adequaat.

3.2 Antwoord op deelvragen

De conclusie uit paragraaf 3.1 wordt in deze paragraaf nader onderbouwd door de drie onderliggende deelvragen te beantwoorden. Hierbij gebruiken we de BIO-standaarden die bestuurders kunnen benutten (zie paragraaf 2.2) als kapstok. Wanneer een standaard toepasbaar is op een conclusie staat deze schuingedrukt vermeld.

Deelvraag 1 - Preventie: Hoe was de UM voorbereid op een cyberaanval en had de UM preventieve maatregelen genomen om bij een mogelijke aanval de goede voortgang te waarborgen (cyberweerbaarheid)?

De UM is een internationaal georiënteerde instelling en kent vanuit de historie een sterk decentrale organisatievorm. Die decentrale inrichting en aansturing geldt ook voor de IT-inrichting. Dat is een bewuste keuze die met name ten dienste staat aan het onderzoek: door de decentrale inrichting hebben wetenschappers veel vrijheden om te bepalen welke systemen voor het onderzoek gewenst zijn *(standaard 2: veilige en open cultuur)*. Als gevolg van de organisatorische inrichting was er voorafgaande aan de cyberaanval geen totaal (over)zicht op de IT-inrichting van de UM organisatie en daarmee slechts beperkt zicht op de cyberweerbaarheid van de universiteit als geheel *(standaard 2: veilige en open cultuur)*. De faculteiten zijn zelf verantwoordelijk voor de beveiliging van hun eigen ICT voorzieningen binnen de kaders van het centrale ICT-beleid. Er worden weinig tot geen restricties opgelegd vanuit de centrale ICTS afdeling aan de faculteiten en diensten van de UM, deze is primair dienstverlenend naar de faculteiten toe. Door de klant-georiënteerde relatie tussen de centrale ICTS afdeling en de faculteiten, is er naast dienstverlening voornamelijk sprake van advisering. In recente jaren was databeveiliging in toenemende mate wel onderwerp van gesprek en waren er bewustwordingscampagnes binnen de UM. Dit was echter gericht op het eigen handelen – zoals de veilige omgang met data en het gebruik van sterke wachtwoorden – en minder op de kans dat derden zich via ongewenste activiteiten toegang zouden verschaffen tot het UM-netwerk *(standaard 1: vergroten bewustzijn)*. De UM beschikt sinds 1994 over een Computer Emergency Respons Team (CERT) en sinds 2003 over een Chief Information Security Officer (CISO) en over een draaiboek voor grote incidenten (waaronder ook ICT), maar daarin waren ransomware aanvallen niet opgenomen *(standaard 3: inrichting crisisteam)*. De interne controle op de uitvoering van het ICT-beleid en de opvolging van afspraken is nauwelijks ingericht: de externe controle is procesmatig en enkel gericht op het financiële en HR pakket van de centrale IT van de UM *(standaard 6: controleren en evalueren)*. Het UM-CERT is aangesloten bij het SURFcert en wisselde zo informatie uit met andere ketenpartners over informatiebeveiliging en de UM nam deel aan de SURF-cyberoefeningen *(standaard 5: ketensamenwerking)*. De UM was bezig met het herinrichten van de IT-organisatie *(standaard 7: investeren/maatregelen)*, echter, het CvB en de organisatie als geheel prioriteerde cyberrisico's onvoldoende als één van de belangrijkste risico's voor het borgen van de goede voortgang van het onderwijs en onderzoek *(standaard 4: borgen risicomanagement)*. De UM maakt gebruik van de jaarlijkse cyberdreigingsbeelden van SURF. Ook daarin stond een cyberaanval niet bij de hoogst geprioriteerde risico's. Daarnaast wordt het incorporeren van cyberveiligheid in risicomanagement bemoeilijkt doordat deze risico's bovenop de al aanwezige afwegingen ten aanzien van de uitgaven komen en er inhoudelijke verdieping nodig is om het gesprek te voeren (*standaard 4: borgen risicomanagement*). De keuze voor een decentrale organisatievorm, zoals van de UM, kan een organisatie kwetsbaar maken. Andere universiteiten en hogescholen kennen ook een gelaagde bestuursstructuur en zijn daarmee potentieel dus kwetsbaar. De uitdaging zit in de combinatie van het ICT-beleid, de uitvoering van de digitale informatiebeveiliging in de gehele organisatie en de controle daarop gegeven de organisatievorm.

Deelvraag 2 - Respons: Welke acties heeft de UM genomen in reactie op de cyberaanval om de voortgang van het onderwijs zo snel mogelijk te herstellen?

Op 15 oktober 2019 werd een phishingmail geopend. Fox-IT heeft vastgesteld dat door onvoldoende detectie, monitoring en opvolging hackers op 23 december 2019 een ransomware aanval konden uitvoeren op een deel van het UM-netwerk *(standaard 1: vergroten bewustzijn)*. In de periode nadat de ransomware aanval was ingezet, heeft het CvB in nauwe afstemming met het Crisis Management Team (CMT) van de universiteit, de Raad van Toezicht (RvT), de medezeggenschap en

andere geledingen binnen de universiteit de cyberaanval afgehandeld *(standaard 3: inrichten crisisteam; standaard 2: open en veilige cultuur)*. Communicatie naar medewerkers en studenten stond eveneens voorop en is uitgevoerd via dagelijkse updates via de UM-website *(standaard 3: inrichten crisisteam; standaard 2: open en veilige cultuur)*. Naast brede afstemming is weloverwogen besloten hoe het onderwijs en onderzoek na de Kerstperiode weer kon aanvangen *(standaard 4: borgen risicomanagement)*. De universiteit zag zich genoodzaakt via losgeldbetaling de decryptiesleutel te verkrijgen ten behoeve van de continuïteit van de organisatie. De verwachting was dat zonder de betaling het herstel en de herbouw enkele maanden zou duren, waarmee de goede voortgang van het onderwijs en onderzoek ernstig in het geding zou zijn. Bovendien was er geen zekerheid dat zonder de decryptiesleutel de IT-infrastructuur en data volledig kon worden hersteld. Er is een brede afweging gemaakt van verschillende scenario's. Op verzoek van RvT is er tevens een kosteninschatting gemaakt van het alternatief om zelf de IT te herstellen. Deze kosten waren naar schatting een veelvoud van het scenario om losgeld te betalen. *(standaard 4: borgen risicomanagement; standaard 7: investeren/maatregelen)*. Het CvB en de RvT hebben tijdens de afhandeling van het incident besloten waar mogelijk open te zijn, zodat andere hoger onderwijsinstellingen lessen kunnen trekken uit de cyberaanval bij de Universiteit Maastricht *(standaard 5: ketensamenwerking; standaard 2: open en veilige cultuur)*.

Deelvraag 3 - Lerend vermogen: Welke voorzieningen heeft de UM getroffen om soortgelijke incidenten in de toekomst te voorkomen met het oog op de goede voortgang van het onderwijs?

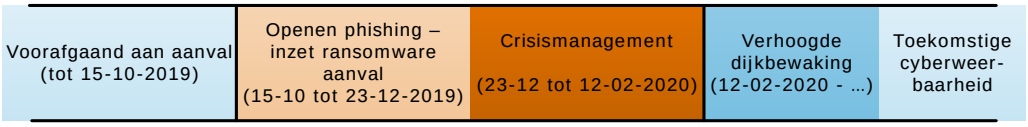
Aangezien dit onderzoek plaatsvond in de twee maanden na de ransomware aanval, beperkt de inspectie zich tot de eerste lessen die de UM heeft getrokken. Naast de met name technisch georiënteerde kwetsbaarheden die Fox-IT heeft blootgelegd, is de inspectie van mening dat de universiteit daarnaast voor meerdere organisatorische uitdagingen staat om de cyberweerbaarheid te vergroten. De universiteit geeft aan behoefte te hebben aan kennisdeling over cyberdreigingen en duidelijke steun vanuit de overheid *(standaard 5: ketensamenwerking*). Tijdens het afhandelen van het cyberincident, is er gewerkt aan 'verhoogde dijkbewaking'. Externe inhuur realiseert in deze fase de continue monitoring van de IT-systemen. Daarnaast is de gehele centrale en decentrale IT-infrastructuur in kaart gebracht *(standaard 4: borgen risicomanagement; standaard 6: controleren en evalueren)*. Er is een duidelijk besef van de preventieve maatregelen die moesten worden aangescherpt. De UM wenst op lange termijn samen met andere onderwijsinstellingen continue (24/7) monitoring van het netwerk *(standaard 5: ketensamenwerking; standaard 6: controleren en evalueren)*. Vanuit de gehele UM-organisatie wordt aangegeven dat het gesprek over cyberveiligheid moet worden gevoerd *(standaard 1: vergroten bewustzijn)*. Doordat de dagelijks gebruikte systemen weer hersteld zijn, lijkt de cyberaanval voor sommigen volledig afgehandeld en gaan delen van de organisatie weer over tot de orde van de dag *(standaard 1: vergroten bewustzijn)*. ICT-medewerkers geven aan dat het juist nu het moment is om met maatregelen door te pakken, bijvoorbeeld door aandacht voor details te verhogen, blijvend zicht te houden op alle aanwezige en nieuwe IT-systemen, de audit beter in te richten en een periodieke test uit te voeren op zwakke plekken in de infrastructuur *(standaard 4: borgen risicomanagement; standaard 6: controleren en evalueren)*. De komende periode moet uitwijzen hoe het staat met het draagvlak voor dergelijke maatregelen binnen de UM wanneer in gesprekken over budgetten het dilemma tussen investeringen in het primaire proces 'onderwijs en onderzoek' enerzijds en cyberweerbaarheid anderzijds worden gevoerd *(standaard 2: veilige en open cultuur)*.

4 Bevindingen

De conclusies in hoofdstuk 3 baseren we op ons instellingsbezoek en documentanalyse. In dit hoofdstuk beschrijven we per deelvraag onze feitelijke bevindingen die hebben geleid tot deze conclusies. De bevindingen zijn geordend aan de hand van de aspecten uit de BIO-richtlijn die bestuurders kunnen benutten. In paragraaf 4.1 beschrijven we eerst de chronologie van de cyberaanval op de Universiteit Maastricht (UM). In de daaropvolgende paragrafen bespreken we de bevindingen op het gebied van preventie, respons en lerend vermogen.

4.1 Tijdlijn cyberaanval

Figuur 1: Verloop van de cyberaanval bij de Universiteit Maastricht



In de tijdlijn (zie Figuur 1) onderscheiden we vijf fases. De eerste fase (linker blokje in de figuur) betreft de periode voorafgaande aan het openen van de phishingmail die uiteindelijk tot de cyberaanval heeft geleid. Op 15 oktober 2019 werd een document via een link in een phishingmail geopend. Dit verschafte de hackers een eerste toegang tot het netwerk van de UM. Deze fase komt in paragraaf 4.2 aan bod.

De tweede fase betreft de periode vanaf het moment dat de hackers het netwerk verder hebben verkend na het openen van de phishingmail tot aan het inzetten van de aanval met ransomware (gijzelsoftware) op de avond van 23 december 2019 (tweede blokje in de figuur). Nadat de aanval was opgemerkt doordat de UM geen toegang meer had tot delen van de IT-systemen, startte de UM het crisismanagement. In deze derde fase vond de besluitvorming plaats die uiteindelijk leidde tot betaling van losgeld aan de hackers om vervolgens met de verkregen sleutel de IT-infrastructuur te kunnen herstellen (derde blokje in de figuur). De tweede en derde fase samen staan in paragraaf 4.3 centraal.

Op 12 februari 2020 heeft de UM het crisismanagement afgeschaald naar ‘verhoogde dijkbewaking’ (vierde bokje in de figuur). Bij de start van deze fase was het merendeel van de IT-infrastructuur hersteld. De UM realiseerde verhoogde waakzaamheid door externe monitoring voort te zetten. Tevens continueerde de afhandeling van de crisis waaronder een coulanceregeling voor studenten en aanvullend onderzoek naar de cyberaanval zelf. Bij het schrijven van dit rapport is nog niet bekend wanneer de UM overgaat van verhoogde dijkbewaking naar het nieuwe regiem van reguliere cybersecurity. Paragraaf 4.4 richt zich op de lessen die de UM reeds heeft getrokken naar de toekomst toe (de twee laatste fasen in blauw in de figuur).

4.2 Bevindingen deelvraag 1: Preventie - Voorafgaand aan de cyberaanval

Onderstaande bevindingen hebben betrekking op de eerste deelvraag: *hoe was de UM voorbereid op een cyberaanval en had de UM preventieve maatregelen genomen om bij een mogelijke aanval de goede voortgang te waarborgen (cyberweerbaarheid)?*
De bevindingen in deze paragraaf hebben betrekking op de periode vooraf aan de cyberaanval - de periode tot 15 oktober 2019.

Vergroten bewustzijn

- Op het vlak van bewustwording heeft de UM in de afgelopen jaren verschillende campagnes georganiseerd. Een belangrijke katalysator daarbij was de veranderende privacywetgeving (de 'AVG'). Op de privacybescherming lag dan ook de nadruk bij campagnes, zoals: 'treat your password as if its your underwear'. Dit was gericht op bewustwording: wachtwoorden niet delen met anderen, met regelmaat wijzigen en niet laten rondslingeren. Ook zijn er in allerlei geledingen van de universiteit presentaties over de Algemene Verordening Gegevensbescherming (AVG) gehouden. Omdat de CISO op dat moment tevens de FG functie vervulde kwamen ook cybersecurity onderwerpen in deze presentaties aanbod. Echter, medewerkers en studenten noemen tijdens de gesprekken met de inspectie geen campagnes gericht op gevaren van malware. De medezeggenschap merkt tijdens die gesprekken op dat ze niet weten wat het niveau van bewustzijn binnen de UM is. De gesprekspartners nemen aan dat ze zelf niet op phishingmails klikken, maar of dat zo is weten ze niet. Anderzijds heeft de centrale ICTS organisatie wel aandacht gehad voor onderzoek door UM-medewerkers naar malware, zij hebben voor dat onderzoek een afgeschermd netwerk ingericht.
- De privacywetgeving AVG was voor sommige eenheden tevens aanleiding om het gebruik van externe dataopslag via Dropbox kritisch tegen het licht te houden. Binnen een faculteit werden medewerkers bijvoorbeeld niet alleen gewezen op een alternatief, maar werd de overstap 'begeleid' doordat de informatiemanager op eigen initiatief zorgde dat er SURFdrive[11] voor individuele onderzoekers binnen de faculteit beschikbaar werd gesteld.
- Een aanscherping van het wachtwoordbeleid, om sterkere wachtwoorden te gebruiken, is in eerste instantie alleen voor personeel ingevoerd. Voor studenten is er volgens verschillende geledingen in de fase voorafgaande aan de aanval lang over gesproken. Na de cyberaanval is de maatregel waarbij studenten overschakelen naar sterkere wachtwoorden wel snel doorgevoerd. Hierbij zijn geen problemen opgetreden die de invoering, voorafgaande aan de aanval, wel steeds tegen hielden.
- Binnen de universiteit is over cyberdreigingen gesproken maar dit werd niet als een van de hoogste risico's geprioriteerd, zo geven verschillende gesprekspartners waaronder het College van Bestuur (CvB) aan.
- Begin oktober 2019 was op verzoek van de Raad van Toezicht (RvT) een scholingsdagdeel georganiseerd voor de RvT rond IT-security en privacy in het kader van de permanente educatie. Deze training werd verzorgd door verschillende UM-geledingen: de Chief Information Security Officer (CISO) en twee UM-hoogleraren van het UM-instituut ECPC. Het belang van vergroten van awareness is een van de lessen uit die scholing.

Veilige en open cultuur

- De UM-organisatie kenmerkt zich, zoals meer universiteiten, door veel vrijheidsgraden in de organisatie. Dit zien we terug in het Bestuurs- en beheersreglement UM. Dit geldt ook op het IT-vlak. De IT-inrichting verschilt daardoor per faculteit. Dit is historisch gegroeid. Wensen vanuit onderwijs en onderzoek binnen de organisatieonderdelen zijn leidend. Faculteiten en diensten bepalen zelf wat ze willen afnemen van ICTS en wat bij een eigen netwerkbeheer wordt ondergebracht.
- De centrale ICTS organisatie wordt door iedereen binnen de UM gekarakteriseerd als serviceverlener. De klant, waaronder decentrale organisatieonderdelen, bepaalt de gewenste IT-inrichting. De inrichting is

[11] SURFdrive is een opslag, vergelijkbaar aan Dropbox, maar gehost door SURF en beschikbaar gesteld via ICTS.

daarmee decentraal verschillend. Dit betekent ook dat er veel en verschillende uitzonderingen op meer centrale uitgangspunten zijn.
- De centrale organisatie waaronder ICTS en de CISO hebben binnen de UM beperkt zicht op alle IT binnen de gehele universiteit. Als gevolg van de verschillen in inrichting tussen organisatieonderdelen van de universiteit, komen signalen van IT-systemen deels op verschillende plaatsen in de organisatie binnen en werden deze voorafgaande aan de cyberaanval niet allemaal naar één centraal punt doorgeleid. Hoewel er dus reeds veel logfiles op een centrale plek verzameld worden en aanvallen gedetecteerd worden, bleven er ook nog zaken buiten het zicht. Leden van het UM-CERT gaven tijdens de gesprekken met de inspectie aan dat monitoring in die zin te kort schoot: juist omdat bijvoorbeeld malicious[12] activiteiten (waaronder malware) er ‘steeds normaler uit gaat zien’ is het lastig dit direct te herkennen. Op het moment dat meerdere meldingen kunnen worden gekoppeld, ga je zaken herkennen gaf men aan.
- Signalen over de ICT kunnen ook afkomstig zijn van medewerkers en studenten. Zij kunnen meldingen doen bij de servicedesk. Echter, uit gesprekken met medewerkers en studenten blijkt dat zij als ze dingen niet vertrouwen er soms ook voor kiezen om zelf een virus check uit te voeren en het niet te melden bij de servicedesk. Uit het Informatiebeveiligingsbeleid van de UM blijkt dat elk organisatieonderdeel zelf verantwoordelijk is voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging.
- Faculteiten hebben elk een informatiemanager (IM-er). De IM-ers zijn aanspreekpunten voor de CISO en de Functionaris Gegevensbescherming (FG) vanuit respectievelijk security en AVG perspectief. De IM-ers hebben ook een gezamenlijk overleg gericht op kennisdeling en sparren.
- Verschillende geledingen ervaren openheid voor gesprekken binnen de UM. Wel is het lastig om tot operationele afspraken te komen. Over veel onderwerpen die inrichtingsvraagstukken aangaan wordt vaak lang gesproken.

Inrichting crisisteam
- De UM beschikt al sinds november 1994 over een Computer Emergency Respons Team (CERT). De voorzitter hiervan is de CISO. In het UM-CERT zitten elf personen, nagenoeg helemaal ingevuld met medewerkers uit de centrale ICTS afdeling. De CERT-leden zijn op vrijwillige basis op afroep beschikbaar, ook buiten kantooruren.
- De UM heeft een algemeen draaiboek voor grote incidenten, waarin onder andere is bepaald hoe het crisisteam wordt ingericht en wat de betrokkenheid is van het bestuur en van de communicatieafdeling. Het draaiboek biedt geen specifieke kaders voor een ransomware aanval van de omvang waarmee ze in december 2019 werd geconfronteerd.
- Indien zich een beperkt cyberincident voordoet wordt dit normaal gesproken door 2-4 personen afgehandeld. Een probleem wordt nooit door één persoon alleen opgelost maar minimaal met ‘vier ogen’.
- De UM participeert in oefeningen rond digitale veiligheid van SURF. Ook zijn er UM-lokale oefeningen. De oefeningen beperken zich niet tot de technici, het CERT. Het was een bewuste keuze ook bestuur en communicatie daarin te betrekken.

Borgen risicomanagement
- Voorafgaand aan de aanval had het risico op externe cyberdreigingen niet de hoogste prioriteit voor de UM. Risico’s voor het UM-onderwijs en onderzoek rond de politieke en maatschappelijke discussie over taal en internationalisering stonden hoger op de agenda. In gesprekken tussen CvB en medezeggenschap

[12] Malicious activiteiten betreffen activiteiten met een kwaadwillend doel.

had ook de discussie rond werkdruk een belangrijke plaats, wat niet uniek is voor de UM. De UM maakt gebruik van de jaarlijkse cyberdreigingsbeelden voor het hoger onderwijs die SURF opstelt. Ook daarin stond een cyberaanval niet bij de hoogst geprioriteerde risico's.
- Het inrichten van randvoorwaarden voor de instelling, zoals cybersecurity en huisvesting, vergt volgens het CvB altijd een lastige afweging in de te besteden budgetten die dan niet beschikbaar zijn voor het primaire proces: (de goede voortgang van) onderwijs of onderzoek. Het zijn onderwerpen waarin het CvB en de gesprekspartners (medezeggenschap en RvT) zich moeten verdiepen om het gesprek te voeren.
- De centrale organisatie neemt tweejaarlijks deel aan de SURFaudit. In 2019 was de UM score 2,5. In 2019 was 2,3 de gemiddelde score van deelnemende hogescholen en van deelnemende universiteiten[13]. De meest recente audit is door één persoon uitgevoerd, mede op basis van de auditinformatie met betrekking tot de jaarrekening. De audit is tot nu toe gefocust op de centrale IT, niet op de diversiteit aan IT-inrichtingen bij de verschillende UM-organisatieonderdelen. De SURFaudit en de uitkomsten hiervan is bij weinig van de UM-medewerkers waar de inspectie mee heeft gesproken bekend. Vragen die als onderdeel van de financiële audit door de externe accountant zijn gesteld over bedrijfsgevoelige IT-systemen waaronder het HR systeem hebben meer bekendheid.
- De RvT heeft in de scholingsbijeenkomst in het najaar van 2019 kennis genomen van het samenwerkingsverband binnen SURF en van de auditstandaarden die in de SURFaudit worden toegepast.
- In verschillende gesprekken kwam aan de orde dat op het vlak van informatiebeveiliging UM in de Deming cirkel (PDCA) de check en act vaak achterwege laat. Onder het onderwerp 'controle en evaluatie' dat later in deze paragraaf aan de orde komt, wordt hierop teruggekomen.

Ketensamenwerking
- Op het vlak van cybersecurity wisselen CERT's van universiteiten, hogescholen en enkele mbo instellingen informatie uit. Ze doen dit in de SURFnet Community van Incident Response Teams (SCIRT) en met SURFcert. Het UM-CERT is aangesloten op het SURFcert. Binnen het SURFcert is in het verleden gesproken over de afhankelijkheid van externe bedrijven bij cybercrises en over een gezamenlijke inspanning om externe dreigingen te monitoren. Tot de aanval bij de UM heeft dit niet tot concrete afspraken geleid. Wel wordt vanuit het SURFcert tweejaarlijks een grootschalige cyberoefening uitgevoerd. Dergelijke oefeningen hebben in 2016 en 2018 plaatsgevonden. De UM heeft aan beide landelijke oefeningen deelgenomen.
- Aangezien binnen de UM-organisatieonderdelen binnen de kaders van het centrale beleid kunnen bepalen hoe de IT wordt ingericht, is ook binnen de UM-organisatie sprake van ketensamenwerking. Netwerkbeheerders geven aan dat per (type) systeem verschillende configuraties binnen de UM worden gebruikt. De centrale netwerkbeheerder weet welke varianten beschikbaar zijn binnen de centrale inrichting. Echter bij sommige organisatieonderdelen kunnen afwijkende configuraties voorkomen. Het ontbreekt de centrale ICTS-afdeling aan zicht op de verschillende keuzes die binnen de UM worden gehanteerd. Daarmee wordt het 'pas-toe-of-leg uit'-principe binnen de UM-organisatie niet volledig gehanteerd.

[13] Zie: B. Bosma (2020) *SURFaudit benchmark 2019 – rapport*. Versie 1.0. https://www.surf.nl/files/2020-04/surfaudit-benchmark-2019-rapport-v1-def.pdf

Controleren en evalueren

- Zoals aangegeven bij het onderwerp risicomanagement is de 'controle' functie bij de UM voor wat betreft informatiebeveiliging beperkt ingevuld. De UM heeft een interne centrale auditdienst die geen rol heeft gespeeld in onderzoeken naar risico's van ICT-systemen. Risico's naar IT-systemen zijn wel onderdeel van de jaarlijkse onderzoeken/controles van de externe accountants. In het kader van hun opdracht, de controle op de jaarrekening, beperken de externe accountants hun jaarlijkse onderzoeken en daarmee ook de cyberrisico's op de financiële en HRM-systemen van hun cliënt. Die systemen zijn volgens de UM overigens niet het doelwit geweest van de hackaanval.
- In de afgelopen vijf jaar hebben externe accountants op een zeer globaal niveau gerapporteerd over de risico's die samenhangen met cybercrime en cybersecurity. Eventuele vormen van cyberrisico's specifiek voor de UM zijn hierbij niet genoemd. De accountants hebben van de UM geen aanvullende opdracht gekregen tot een gericht onderzoek naar cyberrisico's. De accountants hebben wel in het algemeen de ICT-risico's besproken en vastgesteld dat het bestuur van de UM regelmatig bestedingsafwegingen hiervoor heeft gemaakt. Die afwegingen moesten telkens worden gemaakt binnen de financiële kaders (beschikbare bekostiging en middelen) en de snel en dynamisch ontwikkelende technische complexiteit van de ICT.
- Medewerkers die verantwoordelijk zijn voor het beheer van bedrijfsgevoelige informatiesystemen binnen de UM geven aan dat ze vragen hebben beantwoord ten behoeve van de externe accountant. Zij merken op dat die vragen gericht zijn op een procesmatige check terwijl bij een controle op het securityniveau juist de details van groot belang zijn. Met een proces georiënteerde audit wordt de informatiebeveiliging wat hen betreft niet voldoende op de proef gesteld.
- De RvT geeft op het vlak van controleren van de informatiebeveiliging aan dat ontwikkelingen op dit terrein zo snel gaan dat ze in toenemende mate behoefte heeft aan regelmatige informatie van experts.
- Op het vlak van gegevensbescherming heeft ook de FG een controlerende (toezichthoudende) taak binnen de UM. Op het vlak van informatiebeveiliging geldt dat de CISO binnen de UM tot op heden vooral een adviserende rol heeft. De CISO adviseert over de voorwaarden door aan te geven op welke vlakken wel risico's of juist geen risico's genomen kunnen worden. Er vinden geen controles op de daadwerkelijke uitvoering van de IT-inrichting plaats. Ter illustratie een voorbeeld uit de gesprekken: in één van de faculteiten moeten subsidieaanvragen altijd langs een beleidsmedewerker en budgetcontroller. Afhankelijk van welke beleidsmedewerkers de aanvraag bekijkt wordt een IM-er ingeschakeld op het moment dat er op basis van subsidiegelden aanpassingen in systemen worden aangevraagd.
- Een andere faculteit heeft gekozen om zo veel mogelijk door ICTS (centraal) te laten hosten. Deze faculteit heeft steeds minder in eigen beheer en medewerkers gebruiken bijna allemaal een Virtual Desktop Infrastructure (VDI) werkplek. Indien gewenst kunnen medewerkers hiervan afwijken. Advisering door de IM-er over werkplek en programmawensen van individuele medewerkers komt daardoor bij deze faculteit minder voor.

Investeren/maatregelen

- Investeren in IT-infrastructuur voor de UM is altijd een afweging tussen uitgaven aan ICT of uitgaven aan de primaire processen: het wetenschappelijk onderwijs en onderzoek. Een vraagstuk dat niet uniek is voor de UM, maar voor het hele hoger onderwijs geldt.
- De UM heeft in 2017 de UM-I-Strategy 2018-2021 geformuleerd waarmee de huidige IT-koers is ingezet. In deze strategie is zowel het creëren van meerwaarde van de inzet van IT voor onderwijs en onderzoek opgenomen als

het beschermen van data en voldoen aan beveiligings- en privacyregelgeving. De eerste periode die aan het inzetten van de IT-koers vooraf ging, was gericht op het inrichten van de organisatie waaronder aantrekken van een nieuwe Chief Information Officer (CIO).

- Nadat alle posities waren ingevuld zijn de wensen voor het inrichten van een Security Operations Center (SOC)/Security Information and Event Managent (SIEM) aangegeven. Leden van dit team richten zich volledig op beveiligingsproblemen. Dit is anders dan CERT-leden die in geval van een crisis hun normale bezigheden stilleggen en zich dan toeleggen op de crisis. Met een SOC komt er capaciteit voor monitoring van de IT-infrastructuur. Enkele jaren geleden heeft de UM in SURF-verband geparticipeerd in een onderzoek naar de vraag of het inrichten van een specialistisch team voor monitoring door universiteiten gezamenlijk door SURF kan worden opgepakt. Dit omdat de UM niet verwacht met eigen middelen een 24/7 faciliteit te kunnen inrichten. Daar is destijds een negatief advies uit voortgekomen. De UM had gepland per januari 2020 zelf een SOC te starten.
- Medewerkers kunnen programmatuurwensen aangeven bij de IM-er van de eigen faculteit of dienst. Er zijn zeer uiteenlopende wensen mede ingegeven door samenwerking met instituten uit andere landen. Bij nieuwe wensen stemmen IM-ers van verschillende faculteiten en diensten met elkaar af om na te gaan of er de mogelijkheid voor een universiteitsbrede licentie is.
- De keuze voor werkplekinrichting verschilt per organisatieonderdeel van de UM. Dit loopt uiteen van eenheden waar standaard wordt uitgegaan van een VDI werkplek tot eenheden waarbij de keuze vrij is aan de medewerker. Deze vrijheden worden mede ingegeven door voorkeuren van decanen en kan dus van periode tot periode verschillen.
- Het komt ook voor dat een groep binnen een faculteit vanuit een onderzoeksproject subsidiegelden heeft en daarmee zelf apparatuur aanschaft en deze in het netwerk geplaatst wenst te hebben. Over het algemeen is de aanschaf van de apparatuur in de subsidie opgenomen, echter de extra kosten om ook de informatiebeveiliging hiervan te organiseren zijn dat vaak niet. Door de diversiteit aan apparatuur is het aantal (Windows) operatingssystemen dat wordt gebruikt groot. In enkele gevallen gaat het ook om oude operatingssystemen die niet langer door de fabrikant ondersteund worden.
- Binnen de UM wordt voor de werkplek met diverse rechtenstructuren gewerkt. Het verkrijgen van meer dan standaardgebruikersrechten gebeurt regelmatig. Een ICT-medewerker gaf tijdens de interviews met de inspectie aan over beheerdersrechten op de laptop te beschikken, maar deze voor 99% van de werkzaamheden niet nodig te hebben. Dit zal ook gelden voor onderzoekers. Zij hebben diverse werkzaamheden, zoals beantwoorden van e-mails, zoeken van informatie op internet, schrijven, waar geen uitgebreide rechten voor nodig zijn. Het is niet gebruikelijk om in gesprek te gaan over wanneer je uitgebreide rechten gebruikt.
- Medewerkers geven aan dat het uitgeven van een nieuwe werkplek weinig omvattend is. Je haalt het device op en kan aan de slag. Er is geen specifieke instructie die je wijst op wat wel en niet kan en de risico's waarvan de gebruiker zich bewust moet zijn. Ook voor studenten geldt dat zij na de eerste keer inloggen direct aan de slag kunnen.

4.3 Bevindingen deelvraag 2: Respons – cyberaanval en crisisbestrijding

Onderstaande bevindingen betreffen de tweede deelvraag: *Welke acties heeft de UM genomen in reactie op de cyberaanval om de voortgang van het onderwijs zo snel mogelijk te herstellen?*

We beschouwen de periode vanaf 15 oktober 2019 tot het moment dat het crisismanagement van de UM over ging tot 'verhoogde dijkbewaking' op 12 februari

2020. De inspectie richt zich op het handelen van de organisatie, niet op de technische details van de aanval. Het Fox-IT rapport geeft hier aanvullend inzicht in.

Toegang tot het netwerk via malware (vergroten bewustzijn)

- Op 15 oktober 2019 opende een medewerker van de UM een Excel-document via een link uit een ontvangen email. Uit het forensisch onderzoek dat Fox-IT uitvoerde bleek dit Excel-document malware te bevatten die de hackers een eerste toegang tot het netwerk van de UM hebben gegeven. Op 16 oktober heeft een tweede medewerker een soortgelijk Excel-document via een link uit een phishingmail geopend. De hackers konden vervolgens het netwerk van de UM in kaart gaan brengen.
- In oktober 2019 werden binnen het UM-domein meerdere phishingmails ontvangen, waarover door enkele andere medewerkers ook melding is gedaan bij de ICT-helpservicedesk. Deze meldingen, zo blijkt uit het Fox-IT rapport, hebben niet allemaal voldoende opvolging gehad.
- Verschillende tests bij universiteiten en hogescholen laten zien dat er altijd mensen zijn die op dergelijke phishingmails ingaan. Zo vulde 31% van de medewerkers van de HAN Hogeschool in april 2017 hun gegevens in op een mail die ging over het afschaffen van kerstpakketten[14] en bij de Erasmus Universiteit ging ruim een jaar geleden 9% van de medewerkers in op een tevredenheidsonderzoek[15] dat niet van de eigen organisatie kwam. Ook kort na de cyberaanval bij de UM vulde medewerkers van Avans Hogeschool in februari 2020 persoonlijke gegevens in om een valentijnsboodschap te versturen[16].

Propagatie binnen UM-netwerk niet tegengegaan (veilige en open cultuur)

- Een aantal zwakheden in de IT-infrastructuur en organisatie van de UM hebben bijgedragen aan de omvang van de uiteindelijke ransomeware aanval, zoals blijkt uit de root-cause analysis door Fox-IT. Bij een aantal servers in het netwerk waren de laatste beveiligingsupdates niet uitgevoerd en er was beperkte segmentatie binnen het UM-netwerk. Daarnaast was de monitoring gebrekkig waardoor geen opvolging werd gegeven aan meldingen van een virusscanner die uiteindelijk door de hackers handmatig is uitgeschakeld. Hierdoor heeft men onder andere gefaald in het detecteren van de malware. De complexiteit van de IT-infrastructuur van de UM, het ontbreken van een totaaloverzicht van de inrichting van de IT-infrastructuur en het ontbreken van een centrale plaats voor alle meldingen van de diverse systemen in het UM-netwerk werden reeds in de paragraaf 4.2 besproken.
- De beperkte segmentatie heeft volgens het Fox-IT rapport zowel betrekking op de netwerkarchitectuur als de gebruikersrechten. In het Fox-IT rapport is te lezen dat de hackers eerst administrator-rechten verkregen op een aantal onvoldoende ge-update servers om op 21 november 2019 volledige beheerrechten tot het UM-netwerk te krijgen. Dit was mogelijk omdat er te weinig segmentatie was aangebracht tussen de beheerdersdomeinen. In paragraaf 4.2 is al aangegeven dat UM-medewerkers bij verschillende organisatieonderdelen binnen de UM-organisatie eenvoudig meer gebruikersrechten kunnen krijgen. Uit voorbeelden in de gespreken bleek dat men niet vaak spreekt over bewuster omgaan met uitgebreide rechten.

[14] Zie: https://www.businessinsider.nl/hogeschool-han-doet-een-test-met-phishingmails-en-31-van-het-personeel-trapt-erin/ (geraadpleegd op 7-03-2020)
[15] Zie: https://www.ad.nl/rotterdam/erasmus-universiteit-test-medewerkers-een-op-de-elf-trapt-in-val-phishingmail~a6883d30/ (geraadpleegd op 7-03-2020)
[16] Zie: https://punt.avans.nl/2020/02/geen-valentijnsactie-bij-avans-maar-phishingtest/ (geraadpleegd op 7-03-2020)

Opstarten van de crisisorganisatie (inrichting crisisteam)

- Op de avond van 23 december 2019 werd duidelijk dat er sprake was van een omvangrijk cybersecurity incident. De directeur van de centrale ICTS-afdeling werd daarom gebeld door een UM-CERT lid. UM-CERT leden konden van thuis niet als administrator inloggen. Enkele van hen zijn naar Maastricht gekomen. Ook de vicevoorzitter van het CvB werd op de hoogte gebracht. Er is besloten het volledige UM-netwerk te isoleren door de systemen offline te zetten en de gebouwen van de universiteit te sluiten. De opschaling naar bestuursniveau was overeenkomstig met het handelingsperspectief dat was geoefend in de laatste landelijke SURF-oefening OZON.
- UM-CERT leden beschikken over de contactgegevens van het SURFcert en van Fox-IT. In de nacht van 23 op 24 december 2019 is contact met beide organisaties opgenomen en om bijstand gevraagd. Het werd in de loop van de nacht duidelijk dat dit incident een regulier cybersecurity probleem oversteeg. Daarop is volgens de reguliere UM-protocollen het crisismanagement in werking getreden.
- Op de ochtend van 24 december 2019 kwam het crisismanagement team (CMT) voor het eerst bijeen. Het team bestond uit: de vicevoorzitter van het CvB, de directeur ICTS, de Chief Information Officer (CIO), de CISO, de directeur Bestuurlijk-Juridische Zaken (tevens secretaris CvB), de adjunct-Bestuurlijk-Juridische Zaken, drie personen van marketing en communicatie in afwisselende samenstelling en medewerkers van Fox-IT.
- De focus voor het CMT is in de loop van de cybercrisis gewijzigd. Na het inventariseren en veiligstellen van systemen werd voorrang gegeven aan de goede voortgang van het onderwijs en onderzoek. Met als uiterste consequentie dat hierdoor forensische data verloren zou kunnen gaan. Later, na verkrijgen van de sleutel van de hackers is dit verschoven naar het herstellen van de volledige IT door de UM en het veiligstellen van forensische data door Fox-IT om zo onderzoek te kunnen doen naar zowel de root-causes (toedracht, oorzaak en omvang) als het benaderen van data door de hackers (denk aan inzien, ontvreemden of op andere manier verwerken). Fox-IT is vanaf de middag van 24 december 2019 op locatie in Maastricht aanwezig geweest en heeft naast het onderzoek geadviseerd over mitigatie en herstelmaatregelen.

Communicatie na de ransomware aanval (inrichting crisisteam)

- Als gevolg van het offline halen van alle systemen was er geen communicatie via de emailadressen van de UM mogelijk. Via SURF kreeg de UM de beschikking over een aantal tijdelijke emailadressen (zoals info@m-u.nl) zodat studenten en medewerkers daar vragen aan konden stellen. Een medewerker gaf aan dat een email[17] werd ontvangen over de cyberaanval. Omdat de medewerker geen toegang kreeg tot het eigen UM-emailaccount, ging de medewerker bij een collega na of dit bericht waar was.
- Naast de formele communicatie was er behoeften aan contact onderling. Daardoor ontstonden binnen de UM diverse WhatsApp groepen.
- Omdat de website van de UM niet was geïnfecteerd is deze wel online gebleven en heeft het CMT dit als communicatiekanaal ingezet. Dagelijks verschenen er updates waarbij de informatie aan de interne organisatie, medewerkers en studenten, voorop stond. Deze informatie was zo ook voor externe partijen beschikbaar.
- Faculteiten en studentenverenigingen hielpen mee om deze informatie via hun social media kanalen onder de aandacht te brengen. Nadat de gebouwen weer zijn geopend zijn er informatiebalies ingericht. Medewerkers en studenten gaven

[17] Het betrof een email gestuurd aan het privé emailadres, immers de UM-emailadressen konden niet worden benaderd.

in de gesprekken met de inspectie aan dat de updates die enkele dagen na de cyberaanval op de website verschenen begrip creëerden en zorgen konden wegnemen. Met de informatie wist je wat werkte en wat nog niet.
- In de week na Kerst heeft het CvB in afstemming met de RvT besloten openheid van zaken te geven en daarbij de lessen te delen via een symposium. De UM ziet dat als haar maatschappelijke taak.

Afwegingen om de cyberaanval het hoofd te bieden (borgen risicomanagement)
- De ransomware die op 23 december 2019 in de avond werd ingezet, vond plaats in een voor de universiteit relatief rustige periode. Medewerkers en studenten zijn niet in grote getalen aanwezig wegens de feestdagen. De onderwijsperiode zou vanaf 6 januari 2020 worden hervat. Dit gaf het CvB en de crisisorganisatie meer tijd dan in een reguliere onderwijsperiode om de impact van de aanval te inventariseren en scenario's om de IT-infrastructuur te herstellen uit te zoeken. De omvang van de cyberaanval bleek aanzienlijk groter dan in de SURF-OZON en UM-NOZON oefeningen werden gesimuleerd. Afwegingen waar het bestuur voor kwam te staan zijn nooit onderdeel van de cyberoefeningen geweest.
- Het CvB en het CMT stonden voor de taak te kiezen welke primaire processen het eerst hersteld moesten worden. Dit is in afstemming met alle decanen en directeuren gedaan. Het onderwijs kreeg prioriteit boven het onderzoek. De voortgang van het geplande onderwijs en de tentamens vanaf 6 januari 2020 kregen de hoogste prioriteit. Gecoördineerd door het CMT is toen vanaf 6 januari teruggerekend wat er moest gebeuren om op die datum gereed te kunnen zijn om het onderwijsproces weer te kunnen starten.
- De keuze voor het CvB om de crisis het hoofd te bieden bestond uit drie scenario's:
  1. Het bouwen van een eigen decryptor om de versleuteling op te heffen;
  2. De IT-infrastructuur geheel opnieuw opbouwen en vervolgens back-ups terugzetten om de situatie van voor de aanval terug te krijgen; of
  3. Ingaan op de losgeldeisen van de hackers.
- Onderzoek van Fox-IT naar de versleuteling leerde dat de eerste optie niet reëel was. Als het al zou slagen zou de voortgang van het onderwijs en onderzoek meer dan een kwartaal worden verstoord. De tweede optie, opnieuw opbouwen van de IT-infrastructuur, werd geschat op twee tot drie maanden. Dit zou betekenen dat een hele onderwijsperiode verloren zou gaan zowel voor de opleidingen als het wetenschappelijk onderzoek. Bij deze optie was bovendien niet duidelijk of alle data hersteld kon worden. Het feit dat de back-ups door de UM vooral online in plaats van offline waren gemaakt, bemoeilijkte deze optie. De UM werkte voornamelijk met online back-ups die als voordeel hebben om in geval van verstoringen medewerkers en studenten relatief snel weer over de onderwijs- en onderzoeksdata te kunnen laten beschikken. Online back-ups kunnen in principe ook geïnfecteerd worden door malware en zijn daardoor onbruikbaar als back-up.
- Gezien de onderwijsperiode die binnen twee weken zou aanvangen, is het CvB zich gaan oriënteren op het ingaan op de eisen van de hackers. In de besluitvorming over de scenario's heeft het CvB in nauw contact gestaan met de RvT, de decanen, het directeurenoverleg en de voorzitter van de centrale medezeggenschap. Tevens is er extern juridisch advies ingewonnen met betrekking tot het scenario waarin de UM in contact zou treden met de hackers. Het CvB heeft naast de interne geledingen, het ministerie van OCW, de inspectie en de Politie (Team High Tech Crime) op de hoogte gebracht van de uitkomst van de besluitvorming. Ook is contact geweest met de Autoriteit Persoonsgegevens in verband met het data lek doordat derden zich ongeoorloofd toegang tot het netwerk van de UM hadden verschaft.

Contact met hackers en losgeldbetaling (borging risicomanagement)

- De algemene lijn van de Rijksoverheid is dat transacties met criminele organisaties wordt afgeraden. De UM onderschrijft de onwenselijkheid hiervan volmondig. In de praktijk is zo'n algemene lijn toch complex gebleken. Deze overwegingen in het algemeen belang konden voor het bestuur van de universiteit niet prevaleren boven het instellingsbelang, en dat belang bestond uit zo spoedig mogelijk 'back in business' te komen zodat UM haar verplichtingen jegens haar studenten en medewerkers kon nakomen.
- Alvorens in te gaan op de eisen van de hackers heeft de UM een aantal waarborgen getracht te realiseren. Deze bestonden uit:
  - Verzenden van een klein aantal versleutelde bestanden aan de hackers – zonder persoonsgevoelige informatie – om deze te laten ontsleutelen
  - Doen van een proefbetaling met bitcoins aan de hackers, waarna de hackers is gevraagd aan te geven welk bedrag zij hebben ontvangen
- Deze waarborgen waren erop gericht enige zekerheid te verkrijgen dat de UM met de juiste personen in contact stond en een beeld te krijgen van de betrouwbaarheid van hun organisatie. Om dezelfde redenen zijn enkele technische vragen aan de hackers gesteld. Daarnaast was het vaststellen van het emailadres van de hackers informatief voor mogelijke opsporing van de criminelen.
- De inspectie is als onderdeel van dit onderzoek nagegaan of de betaling van circa € 0,2 mln (in bitcoints) aan de hackers past binnen de grenzen van de doelmatige aanwending van de rijksbijdrage. De UM heeft in de dagen van de cyberaanval een kostenoverweging gemaakt om zelf het herstel van de hack ter hand te nemen. De UM kwam tot de conclusie dat vanwege de omvang en complexiteit van hun ICT-systeem het tenminste een aantal weken tot drie maanden zou kosten om alle systemen weer veilig in de lucht te krijgen en oude bestanden bereikbaar te maken. Voorts is daarbij de inzet van gespecialiseerde externe inhuur noodzakelijk. De langdurige periode en de hoge kosten voor zowel interne inzet als externe inhuur en de dan oplopende aansprakelijkheid richting studenten zou een veelvoud zijn van de betaling aan de hackers van de cyberaanval.
- De UM heeft voor de betaling van bitcoins gebruik gemaakt van een zelf gekozen extern bedrijf die in die valuta kon betalen. Voor de betaling put de UM in 2020 uit dividendbetalingen van de dochterbedrijf Universiteit Maastricht Holding BV. Deze Holding heeft recent een start up dochter verkocht en daartoe ruim voldoende liquiditeiten voor het betalen van een dividend dat ruim hoger is dan het bedrag dan aan de hackers is betaald. Omdat de UM nooit onderscheid heeft gemaakt tussen publiek en privaat eigen vermogen, wordt deze betaling uit het publiek eigen vermogen betaald.

Delen Indicators of Compromise en assistentie (ketensamenwerking)

- Fox-IT heeft in het forensisch onderzoek Indicators of Compromise (IoC's) geïdentificeerd. IoC's kunnen duiden op malafide activiteiten in een digitale omgeving. De UM heeft op 24 december 2019 de IoC's via het SURF-CERT met andere aangesloten universiteiten en hogescholen gedeeld. Met de IoC's kunnen andere hoger onderwijsinstellingen nagaan of er verdachte activiteiten op hun netwerken plaatsvindt. Het delen van de IoC's zien het CvB en de RvT als hun verplichting als universiteit die publieke middelen ontvangt.
- Anderzijds geeft de UM aan dat het ontvangen van IoC's van andere instanties voor een universiteit niet vanzelfsprekend is. Dit gaat zowel om informatie binnen Nederland maar ook vanuit het buitenland. Cybercriminaliteit is immers niet uitsluitend een Nederlandse aangelegenheid. Zo was de UM niet op de hoogte van het feit dat de Universiteit Antwerpen recent in oktober 2019 slachtoffer was geworden van een ransomeware aanval. Dit incident was niet

vermeld op de waarschuwingslijst over cyberaanvallen die SURF regelmatig aan universiteiten beschikbaar stelt. SURF wist zelf evenmin van deze aanval. De aanval in Antwerpen vond plaats in de fase dat er al toegang tot het netwerk van de UM was verkregen.
- Zoals eerder aangegeven heeft de UM geen specifiek protocol voor de afhandeling van een cyberaanval en is de crisisorganisatie ingericht op grond van het UM-protocol voor grote incidenten. Op het IT-vlak richt zich dit op grote verstoringen zonder kwaadwillende opzet. Op 24 december 2019 heeft de UM met het Nationaal Cyber Security Centrum (NCSC) contact opgenomen om te vragen of er een protocol beschikbaar is. Dit was niet het geval. Op dezelfde dag is nog een aantal keer contact geweest. De UM verschaft informatie waarmee het NCSC het Zorg-Cert op de hoogte kon brengen zodat zij voorzorgsmaatregelen konden nemen. Het NCSC geeft de UM contactgegevens van het Team High Tech Crime van de Politie en geeft tevens aan dat om juridische redenen informatie alleen via SURFcert gedeeld kan worden, niet rechtstreeks aan de UM. Het NCSC is de instantie voor vitale sectoren en de Rijksoverheid.

Herstel bedrijfsvoering (ketensamenwerking)
- In de loop van de crisisafhandeling veranderde de focus van het CMT naar het herstellen van de (reguliere) bedrijfsvoering. Voor het onderwijs heeft er afstemming met de Dienst Uitvoering Onderwijs (DUO) plaatsgevonden omtrent de sluitingstermijn voor inschrijving bij fixusopleidingen. Met DUO is afgesproken dat de inschrijving bij Studielink gewoon kon geschieden maar dat aspirant-studenten de benodigde documentatie voor de selectieprocedure later konden aanleveren.
- Het onderzoek kent deadlines met betrekking tot subsidieaanvragen voor onderzoek. De UM heeft hierover contact gezocht met Nederlandse Organisatie voor Wetenschap (NWO) en de EU. Omdat de meeste onderzoekers hun belangrijke data, waaronder aanvragen, op meerdere plekken bewaren, kon met NWO worden afgesproken dat aanvragen volgens de deadlines werden ingediend maar dat de UM-onderzoekers uitstel kreeg voor de verplichte bijlagen bij een aanvraag (e.g., informatie uit de bedrijfssystemen van de UM). De EU gaf geen uitstel. Het CvB heeft geen signalen dat onderzoekers hun voorstellen niet hebben kunnen indienen.
- Hierbij moet de kanttekening geplaatst worden dat het elders bewaren van data (bijvoorbeeld Dropbox) door medewerkers in sommige gevallen ingaat tegen het informatiebeveiligingsbeleid van de UM. Dit is een kwetsbaarheid ten aanzien van informatiebeveiliging door de gebruikers in de reguliere situatie toen er nog geen cyberaanval was, zie ook paragraaf 4.2. Ten tijden van de cyberaanval heeft dit echter positief uitgepakt en daarmee medewerkers onterecht bevestigd dat het elders opslaan van data goed is.

Controleren en evalueren
- Zoals eerder in deze paragraaf aangegeven was bij de start van het incident de netwerkmonitoring niet afdoende om de propagatie tussen 15 oktober en 23 december 2019 tegen te gaan. Nadat de ransomeware aanval een feit was, heeft Fox-IT in overleg met de UM een aantal netwerksensoren geïnstalleerd en is op Windows Servers en werkstations de monitoringtool ‘Carbon Black’ geïnstalleerd. Met deze tools kan centraal gedetecteerd worden of er sprake is van onregelmatigheden op systemen en in het netwerk.
- Zoals in paragraaf 4.2 is aangegeven zou de UM per januari 2020 een SOC inrichten. De keuze voor een monitoringtool moest met de inrichting van het SOC nog worden gemaakt. Door de cyberaanval is deze keuze, namelijk Carbon Black, intussen genomen. De tool is in eerste instantie ingezet op de gehackte

servers ten behoeve van het forensisch onderzoek dat Fox-IT uitvoerde. Daarna is dit uitgerold binnen de rest van de Windows Servers en tot slot op de Windows werkplekken, zowel fysieke werkplekken als VDI systemen. Windows Servers kregen de monitoringtool voordat deze weer beschikbaar werden binnen het netwerk. Vanaf de live-gang (2 januari 2020) heeft de UM 24/7 monitoring ingericht in samenwerking met Fox-IT.

- Met betrekking tot haar controlerende taak geeft de RvT aan dat het CvB veel informatie verschafte, waardoor ze naar haar inzicht over de belangrijkste feiten beschikte. De RvT heeft ingestemd met de gekozen lijn van het CvB en heeft gevraagd om een specificatie van de financiële gevolgen op te stellen van het alternatief om de IT-infrastructuur zelf te herstellen. Daarnaast heeft de RvT verzocht zo transparant mogelijk te communiceren (in- en extern) over de cyberaanval en de lessen die daaruit te trekken zijn.
- Fox-IT heeft de aanvallersactiviteiten op een aantal kritische datasystemen ‘de kroonjuwelen’ onderzocht. Het onderzoek heeft zich beperkt tot een tweetal UM-systemen op basis van de bekende IoC’s. Naar aanleiding van deze inventarisatie heeft Fox-IT aangegeven dat er geen andere sporen zijn gevonden dan de ransomeware. Wel maakt Fox-IT hierbij de kanttekening dat met deze bevindingen nog niet kan worden uitgesloten dat data is ingezien, ontvreemd of verwerkt door de hackers. Fox-IT adviseert de UM-vervolgonderzoek uit te voeren om een uitspraak met grotere waarschijnlijkheid te kunnen doen.
- In de gesprekken met de medezeggenschap en medewerkers en studenten zijn de aanvallersactiviteiten aan bod gekomen. Studenten gaven aan dat zeker onder afstudeerders angst bestond dat (ruwe) data verloren was gegaan. Men wil graag weten wie er ‘in huis’ was geweest. Daarbij gaf men aan behoefte te hebben aan kennis over de systemen die *niet* zijn geraakt, waarover mensen zich dus geen zorgen hoeven te maken. De huidige uitkomsten zijn in die zin (nog) niet bevredigend.

Investeren/maatregelen

- Tijdens het herstellen van de IT-infrastructuur zijn verschillende maatregelen genomen om de digitale veiligheid van de UM te vergroten. Naast de netwerkmonitoring door de sensoren en het programma Carbon Black zijn de volgende maatregelen getroffen om controle en evaluatie te verbeteren:
  - Reset van wachtwoorden en sterk(er) wachtwoordbeleid voor iedereen: alle medewerkers en studenten moesten een nieuw wachtwoord aanmaken op het moment dat ze na 2 januari 2020 voor het eerst inlogden op het UM-netwerk. Voor studenten ging daarbij bovendien het nieuwe sterke wachtwoordenregime gelden. Dit beleid gold al voor de medewerkers van de UM maar niet voor studenten. Het wachtwoordbeleid werd als één van de voorbeelden genoemd van zaken die eerder traag werden opgepakt maar nu snel gerealiseerd werden en op begrip konden rekenen.
  - Minimale vereisten ten aanzien van operating systemen op werkplekken en servers: waardoor oudere operating systemen die door de fabrikant niet langer worden ondersteund uit het UM-netwerk worden geweerd.
  - Verdere restricties aanbrengen op de netwerksegmentatie binnen het UM-netwerk. Hierdoor neemt het overzicht op het gehele netwerk toe, wat tevens de monitoring ten goede komt.
  - Inrichten van offline back-ups voordat een systeem live kan gaan.
- Op de combinatie van de reeds ingezette maatregelen werd door ICT-medewerkers aangegeven dat het van belang is dat de monitoring op hoog niveau blijft, er zullen immers altijd besmettingen plaatsvinden omdat deze niet tegen te houden zijn. Om de aanvaller niet verder te laten binnendringen is het belangrijk om ‘eindpunten’ optimaal te beveiligen (goed serverbeheer).

- Een andere herstelmaatregel was het instellen van de coulanceregeling voor studenten die nadeel of schade hebben ondervonden als gevolg van de cyberaanval. De regeling is ingesteld in afstemming met onder andere de examencommissies. Tot half februari 2020 is een beperkt aantal meldingen ontvangen (zeven). De meldingen worden individueel afgehandeld en opgelost, bijvoorbeeld door een financiële compensatie (e.g., een maand collegegeld omdat het afstuderen met een maand verlengd moet worden).

4.4 Bevindingen deelvraag 3: Lerend vermogen – voorkomen toekomstige incidenten

De bevindingen in deze alinea betreffen de derde deelvraag over het lerend vermogen van de organisatie: *Welke voorzieningen heeft de UM getroffen om soortgelijke incidenten in de toekomst te voorkomen met het oog op de goede voortgang van het onderwijs?*
In deze paragraaf beschouwen we de periode vanaf 12 februari 2020. Vanaf dat moment is de UM niet langer in crisisorganisatie bijeen. De afhandeling van de cyberaanval gebeurt nu op basis van ‘verhoogde dijkbewaking’ onder anderen door het inhuren van Fox-IT voor het kunnen realiseren van 24/7 monitoring. De inspectie gaat in deze paragraaf in op de lessen die de UM reeds heeft getrokken om tot een nieuw niveau van cyberweerbaarheid voor de universiteit te komen.

Vergroten bewustzijn

- Fox-IT beveelt aan om ter preventie het veiligheidsbewustzijn door middel van periodieke aandacht op niveau te houden. Het gaat Fox-IT niet alleen om campagnes maar ook om bijvoorbeeld het uitvoeren van phishing-tests binnen de organisatie. In het verlengde hiervan is door de medezeggenschap aangegeven dat de UM *digitale hygiëne regels* heeft opgesteld, om deze kenbaar te maken zijn medewerkers en studenten niet klassikaal bij elkaar geroepen. Of klassikale bijeenkomsten gepland staan is hen onbekend.
- Zowel vanuit het CMT als de ICT-medewerkers wordt aangegeven dat het gevaar bestaat dat de UM-gemeenschap terugvalt en te weinig lessen trekt. Ze merken immers niet langer dat er nog altijd hard wordt gewerkt aan het laatste herstel en het op hoog niveau houden van de informatiebeveiliging. In een aantal gesprekken bleek inderdaad dat bij een deel van de UM-gemeenschap de indruk bestaat dat de organisatie weer functioneert als voorheen, omdat de UM erg snel is ‘live’ gegaan. Dat ervaarde men bijvoorbeeld toen er weer geprint kon worden binnen UM-gebouwen.
- Daarnaast zijn medewerkers gesterkt in hun oude gedrag om data in bijvoorbeeld een Dropbox te zetten, immers daarmee kon ondanks dat de universiteit ‘op slot zat’ worden doorgewerkt. Men moet bewust worden gemaakt dat dit niet verstandig is, aldus de ICT-medewerkers.
- Het CvB merkt op dat door de cyberaanval bij de UM en door de Citrix problematiek die kort daarop optrad er in het gehele land nu een debat wordt gevoerd. De medezeggenschap geeft aan het wat hen betreft belangrijk is dat het hele CvB de kar trekt.

Veilige en open cultuur

- Fox-IT beveelt ook aan om er zorg voor te dragen dat gebruikers (onbedoelde) incidenten vaker melden en dat de meldingen vervolgens opvolging en adequate adressering krijgen. Fox-IT geeft aan dat de reeds aanwezige open communicatie-cultuur gebruikt kan worden om de meldingsbereidheid te vergroten.
- Het verbeteren van incidentmeldingen en opvolging is in verschillende gesprekken aan de orde gekomen. Zo gaf men aan dat er mogelijkheden zijn om

een melding digitaal door te geven, maar dat er niet altijd een terugkoppeling naar de melder wordt gegeven.
- De uitdagingen waar de ICT-medewerkers voor staan – gezien de veelzijdigheid en diversiteit binnen de IT-infrastructuur van de UM – werd reeds in paragraaf 4.2 besproken. Op veel systemen vindt er logging plaats, maar dit wordt niet allemaal samengebracht op één plek. Het CvB ziet op dit vlak een belangrijk verbeterpunt. Dit is tevens door Fox-IT aangegeven als maatregel (monitor logbestanden voor anomalieën) om de detectiekans te vergroten. Tijdens de verhoogde dijkbewaking is de monitoring gedeeltelijk uitbesteed zodat dit dag en nacht mogelijk is.
- De aanval heeft het belang van cyberveiligheid voor de medezeggenschap geïllustreerd. Wat hen betreft is het gesprek hierover met het CvB nog niet afgerond ook niet op het moment dat de nieuwe medezeggenschapsraad start. Het CvB stelt zich open voor het gesprek over afwegingen en obstakels volgens de medezeggenschap, maar affiniteit met het onderwerp cybersecurity verschilt uiteraard.
- De Raad van Toezicht geeft aan dat er veel mensen met kennis bij de universiteit zelf zitten. Dit kan de organisatie benutten ten behoeve van de toekomstige cyberweerbaarheid.
- De verschillende gesprekspartners zijn trots op de organisatie en op hoe de cyberaanval is opgelost. Er was loyaliteit en commitment, ook in de Kerstvakantie. Het CvB is zich er van bewust dat er ook kritische geluiden zijn, zoals bleek uit reacties van studenten over het betalen van losgeld. Overwegend waren de reacties van studenten en medewerkers echter waarderend.
- Ook ICT-medewerkers zijn blij met de manier waarop de crisis is aangepakt. Echter, zoals eerder genoemd spreken zij ook hun zorgen uit over het gevaar te weinig lessen te trekken.

Inrichting crisisteam
- Zoals eerder in paragrafen 4.2 en 4.3 aangegeven beschikt de UM niet over een specifiek kader of protocol hoe met een ransomware aanval van deze omvang moet worden omgegaan. Fox-IT beveelt aan om een incident response plan voor dit soort calamiteiten op te stellen. De UM heeft aangegeven dat de algemene UM-procedures voor crisisafhandeling zijn gevolgd. Het CMT geeft daarbij aan dat deze aanpak werkbaar was. Vanuit het CMT is in overleg met het CvB specifieke expertise toegevoegd, bijvoorbeeld expertise over Bitcoin betalingen.
- Als onderdeel van de verslaglegging heeft de ICTS in kaart gebracht hoe de crisisorganisatie heeft gefunctioneerd. Het gaat dan zowel om de organisatie als de belangrijkste werkzaamheden die zijn uitgevoerd.
- Het UM-CERT werkte voor het incident buiten kantoortijden met een bellijst op basis van vrijwilligheid. De vrijwilligheid wordt op dit moment heroverwogen. Dat hangt ook af van de inrichting van het SOC en mogelijkheden voor samenwerking met andere hoger onderwijsinstellingen.

Borgen risicomanagement
- Het is moeilijk in te schatten of de UM kwetsbaar is voor de terugkeer van deze of andere hackers. Het CvB geeft aan dat het onderzoek van Fox-IT wijst op een groep die sinds februari 2019 zo'n 150 keer succesvol een cyberaanval heeft gedaan. Tot dusver is er geen aanwijzing dat dezelfde groep terugkeert. Het lijkt eenmalig om het losgeld te gaan. Anderzijds merkt het CvB op dat uit criminologisch onderzoek blijkt dat als je één keer slachtoffer bent geworden, de kans op herhaling groter is. Het CvB is van mening dat ze sowieso beter voorbereid moeten zijn.
- De RvT geeft aan dat een herhaling van een dergelijke situatie, waarbij er een kans bestaat dat tienduizenden studenten enkele maanden niet weten of het

onderwijs doorgaat, ze examens kunnen doen of dat ze geslaagd zijn, niet mag voorkomen. Zij geeft aan dat de betaling, hoewel moreel verwerpelijk, een oplossing bood voor het doorgaan van de geplande tentamens.
- ICT-medewerkers geven aan dat er meer aandacht moet komen voor cyberveiligheid, ook landelijk. Zij hopen dat dit voor een beweging zal zorgen. Anderzijds geven ze ook aan dat nu doorgepakt moet worden, anders is de crisis voor niets geweest. Ze wijzen op voorbeelden als het afbranden van een serverruimte bij de Universiteit Twente enkel jaren geleden. Dat leidde tijdelijk tot verhoogde aandacht, die vervolgens wegzakte.
- Ook geven de ICT-medewerkers aan dat de UM nooit Fox-IT kan worden, waarmee wordt bedoeld dat het opsporen van afwijkende activiteiten binnen de IT-omgeving de corebusiness is van Fox-IT, maar niet van een universiteit. De ICT-medewerkers en het CMT geven aan dat er op het vlak van cyberveiligheid binnen de UM meer oog moet komen voor de details.
- Het incident heeft aan de medezeggenschap duidelijk gemaakt dat afwegingen rond cyberveiligheid kritisch besproken moeten worden, de kosten van maatregelen maar ook de nadelen van het ontbreken van maatregelen. Dat gesprek wordt sinds de aanval gevoerd en zal gevoerd moeten blijven worden.
- Andere medewerkers en studenten nuanceerden dit beeld en gaven aan dat de huidige inspanning rond de verhoogde waakzaamheid niet ten koste zou moeten gaan van de andere ambities die rond ICT al waren ingezet. Daarbij gaat het bijvoorbeeld om de op korte termijn geplande vervanging van Blackboard door Canvas (digitale leeromgeving).

Ketensamenwerking
- Het CvB geeft aan in de afhandeling van het incident zoekende te zijn geweest naar externe partijen die kunnen helpen. Het SURFcert heeft geholpen bij de analyse van de malware. Verder was de UM aangewezen op Fox-IT. Ook naar de toekomst toe geeft het CvB aan dat universiteiten van bedrijven als Fox-IT afhankelijk zijn. De specialistische kennis van het bedrijf kan de UM niet zelf in huis halen. Het CvB geeft aan dat naast Fox-IT ook SURF beschikbaar is om informatie te delen, maar databeveiliging is niet de enige activiteit van SURF.
- De UM wil ten behoeve van de monitoring en detectie van ongewenste activiteiten zoals malware het gesprek over samenwerking aangaan met andere universiteiten. Continue monitoring voor een instelling alleen is namelijk financieel niet haalbaar.
- Het CvB geeft aan dat er wat hen betreft meer informatiedeling moet komen over risico's. Wat de RvT betreft gaat de uitwisseling om databeveiligingsrisico's in brede zin. Dus naast een aanval gericht op losgeld ook activiteiten gericht op het verkrijgen gevoelige (onderzoeks)data. De RvT geeft aan dat ook de overheid transparant moet zijn over waar de risico's zijn.
- De behoefte aan kennisdeling wordt door verschillende gesprekspartners ervaren door vragen die zij hebben gekregen vanuit andere onderwijsinstellingen in binnen- en buitenland, onderzoeksinstituten en ook uit het bedrijfsleven. Ook het door de UM georganiseerde symposium op 5 februari 2020 is door diverse onderwijsinstellingen en anderen online bekeken.

Controleren en evalueren
- Fox-IT heeft een beperkt onderzoek naar aanvallersactiviteiten uitgevoerd, zoals in paragraaf 4.3 is vermeld. Fox-IT heeft geadviseerd een breder onderzoek te doen om met grotere waarschijnlijkheid uitspraken te kunnen doen over data extractie. Het CvB heeft tot aanvullend onderzoek besloten. Voor wetenschappers is het van belang ook in discussie met partners aan te kunnen geven dat de data betrouwbaar is. Met aanvullend onderzoek neemt de zekerheid toe, maar 100% uitsluiten is niet mogelijk.

- Binnen de UM geven gesprekspartners aan dat de (externe) controle op de IT-infrastructuur moet worden verbreed. In verschillende gesprekken werd aangegeven dat de self-assessment alleen niet (langer) voldoende is. Sinds half februari 2020 staat er een vacature voor een IT-auditor online. De privacy en security audits moeten samen gaan optrekken. Volgens de CISO kan de audit dan uitgroeien tot een reguliere (jaarlijkse) self-assessment, regelmatig een audit met peer review en periodiek een externe audit. De contouren van deze systematiek zijn opgenomen in het nieuwe concept informatiebeveiligingsbeleid van de UM.
- ICT-medewerkers en ook de RvT geven dat een proces audit niet voldoende is, en dat de infrastructuur periodiek beproefd zou moeten worden op zwakke plekken.

Investeren/maatregelen

- Fox-IT heeft in het rapport verschillende aanbevelingen gedaan die bij kunnen dragen aan het verhogen van het beveiligingsniveau van de UM. In de reactie op het Fox-IT rapport geeft het CvB aan de adviezen mee te nemen in het eigen interne volgonderzoek waarmee de UM haar beveiligingsbeleid wil toetsen en bepalen welke bestaande plannen aangepast en/of uitgebreid dienen te worden. Naast de eerder in deze paragraaf genoemde maatregelen, doet Fox-IT aanbevelingen om:
  - Vermijden van beheerswerkzaamheden met domein administrator accounts: het rapport beveelt aan dat beheerswerkzaamheden zoveel mogelijk vanuit het principe van “least privilege” worden uitgevoerd. Dit sluit aan bij voorbeelden van ICT-medewerkers die aangeven dat medewerkers gedurende een groot deel van de werkzaamheden niet over de meest uitgebreide rechten te hoeven beschikken.
  - Fox-IT adviseert om het gebruik van (ongetekende) macro’s niet toe te staan, te werken met een beschermde gebruikersgroep, in het bijzonder voor accounts die hogere privileges hebben, en besturingssystemen up-to-date te houden.
  - Met betrekking tot response na een incident wordt voorts geadviseerd een data recovery plan op te stellen en dit ook te oefenen.
  - Met het herstellen van de IT-infrastructuur na de cyberaanval is tevens het zicht op de systemen binnen het netwerk vergroot. Fox-IT adviseert de response te verbeteren door een centraal beheerde Configuration Management Database te realiseren.
- De medezeggenschap merkt op dat er voldoende middelen beschikbaar moeten worden gesteld om de noodzakelijke beveiligingsmaatregelen te treffen en in control te komen.
- Tijdens het incident heeft de UM besloten om “Carbon Black” ten behoeve van monitoring in te zetten. In het gesprek met ICT-ers werd aangekaart dat men zich afvraagt of binnen de gehele UM is geregeld en wordt gecontroleerd dat ook nieuwe systemen van Carbon Black worden voorzien. De installatie van Carbon Black had betrekking op het weer in het netwerk plaatsen van de bestaande systemen. Het is de gesprekspartners niet bekend of op het moment van het gesprek nog altijd dezelfde hoge dekking van Carbon Black van toepassing is.
- Wat betreft het toekomstige niveau van cyberweerbaarheid geeft het CvB aan dat het SOC nu wordt ingericht. Hiervoor worden nieuwe mensen geworven of er worden werknemers vrijgesteld van de taken die ze nu hebben.

5 Vervolgtoezicht

De inspectie constateert dat de Universiteit Maastricht adequaat heeft gehandeld in het afhandelen van de cyberaanval en heeft vertrouwen in het reeds geïnitieerde vervolgonderzoek van de UM. De inspectie zal de UM daarom geen aanvullende verbeterpunten voorschrijven. Wel vraagt de inspectie de UM haar te informeren over de uitkomsten van het ingestelde vervolgonderzoek. Dit mede in het kader van het stelselonderzoek dat de inspectie zal uitvoeren. Voor de UM is het de uitdaging het momentum vast te houden om meer draagvlak te creëren voor het doorvoeren van effectieve maatregelen in de gehele organisatie door gebruik te maken van de verhoogde aandacht voor informatiebeveiliging, ook nu er zich een andere externe dreiging (Corona) voordoet. De cyberaanval op de UM was een *wake up call* voor het gehele hoger onderwijs. Ook andere universiteiten en hogescholen zijn gezien de aard van de organisaties potentieel kwetsbaar. Ook andere universiteiten en hogescholen moeten dagelijks afwegen waar het geld en de tijd aan wordt besteed. Bestuurders, medezeggenschap en interne toezichthouders staan voor de uitdaging in gesprek te blijven over het beleid, de uitvoering daarvan en controle op de uitvoering die rechtdoet aan de organisatievorm en de (digitale) dreigingen.

Begin 2020 heeft de inspectie besloten tot het instellen van een tweeledig onderzoek: naar de Universiteit Maastricht als instelling en naar het stelsel van hoger onderwijs. Het onderhavige rapport doet verslag van het instellingsdeel. Sinds het besluit van de inspectie tot het instellen van een onderzoek, heeft de Minister van Onderwijs op 14 februari 2020 op verzoek aan de Tweede Kamer een brief gestuurd over de cyberveiligheid van onderwijsinstellingen[18]. Op 20 maart 2020 heeft de Minister van Justitie en Veiligheid de Tweede Kamer een kabinetsreactie[19] gestuurd op het verschenen WRR rapport over “Digitale Ontwrichting”[20]. In de kabinetsreactie is aangegeven dat de Inspectieraad wordt gevraagd om te komen met een voorstel hoe brede samenwerking en afstemming tussen de rijksinspectie en toezichthouders op cybersecurity het beste tot stand kan worden gebracht. Het onderhavige rapport, het lopende vervolgonderzoek door de UM, bovengenoemde kamerbrieven en de opdracht aan de Inspectieraad zijn allen relevant voor het stelselonderzoek door de inspectie.

Nederlandse universiteiten en hogescholen hebben naast de digitale dreiging die door de aanval bij de UM dichterbij is gekomen, deze dagen een tweede grote uitdaging gezien de pandemie als gevolg van het Coronavirus. Als gevolg van de overheidsmaatregelen verzorgen universiteiten en hogescholen het onderwijs sinds 12 maart 2020 alleen online, zijn promotiezittingen uitgesteld en is de vraag hoe de examinering kan plaatsvinden. Opnieuw een externe dreiging die de voortgang van het onderwijs en onderzoek mogelijk in gevaar brengt. De digitale infrastructuur en online onderwijsvoorzieningen, die universiteiten en hogescholen in het afgelopen decennium ontwikkelden, zijn in de Corona aanpak niet het knelpunt maar juist een onderdeel van de oplossing om de goede voortgang van onderwijs en onderzoek te kunnen behouden. Dit illustreert tevens het belang van de digitale infrastructuur voor de continuïteit van primaire processen als onderwijs en onderzoek.

[18] Tweede Kamer, vergaderjaar 2019–2020, 31 288, nr. 832.
[19] Tweede Kamer, vergaderjaar 2019-2020, 26 643, nr. 673.
[20] Wetenschappelijke Raad voor het Regeringsbeleid (2019) *Voorbereiden op digitale ontwrichting*, WRR-Rapport 101, Den Haag: WRR.

Bijlage 1: Wettelijk kader

Per onderzoek bepaalt de Inspectie van het Onderwijs welke wettelijke bepalingen van toepassing zijn en waaraan de aangetroffen situatie getoetst kan worden. Op basis daarvan zijn voor dit onderzoek de onderstaande aandachtspunten geselecteerd.

In paragraaf 2.2 staat uiteengezet dat het onderzoek zich richt op ernstige nalatigheid zoals aangegeven in de WHW artikel 9.9a, tweede lid, onder b. Dit artikel luidt:

ernstige nalatigheid om, in ieder geval in strijd met artikel 1.18, maatregelen te treffen die noodzakelijk zijn voor het waarborgen van de kwaliteit en goede voortgang van het onderwijs aan de instelling en om te voorkomen dat de kwaliteit van het stelsel van wetenschappelijk onderwijs in gevaar komt;

Gerelateerde bepalingen van de WHW voor dit onderzoek zijn:

Artikel	
2.9, lid 1:	Het instellingsbestuur dient jaarlijks voor 1 juli bij Onze minister een verslag in. Het verslag bestaat uit de jaarrekening met bijbehorende begroting, het bestuursverslag en overige financiële gegevens, alsmede een verantwoording over de wijze waarop van een branchecode voor goed bestuur is afgeweken, voor zover een zodanige code overeenkomstig artikel 2.14 is aangewezen. Uit het verslag dient te blijken in hoeverre sprake is van een behoorlijke uitvoering van de werkzaamheden ten behoeve waarvan de rijksbijdrage is verleend en van een doelmatige aanwending van de rijksbijdrage, mede in het licht van het instellingsplan. Van niet doelmatige aanwending van de rijksbijdrage is in ieder geval sprake, voorzover bedragen daaruit worden aangewend voor het uitvoeren van de procedure voor erkenning van verworven competenties of het op enigerlei wijze compenseren van studenten of extraneï voor collegegeld, examengeld, cursusgeld of voor de bijdrage bedoeld in artikel 7.50, tweede lid, tenzij er sprake is van een financiële ondersteuning als bedoeld in de artikelen 7.50, derde lid, of 7.51 tot en met 7.51k.
2.10	De accountant die door Onze minister is belast met het onderzoek van de ministeriële jaarrekening, heeft met het oog op het verrichten van dat onderzoek toegang tot elke instelling. De accountant kan door Onze minister tevens worden belast met een onderzoek naar de doelmatigheid van het beheer van de instelling. Aan de accountant worden alle inlichtingen verstrekt die hij voor de uitvoering van zijn taak nodig oordeelt.
9.2, lid 1:	Het college van bestuur is belast met het bestuur van de universiteit in haar geheel en met het beheer daarvan, onverminderd de bevoegdheden van de raad van toezicht volgens dit hoofdstuk
9.4:	Het college van bestuur stelt een bestuurs- en beheersreglement ter regeling van het bestuur, het beheer en de inrichting van de universiteit vast.
9.5:	Het college van bestuur kan richtlijnen vaststellen met het oog op de organisatie en coördinatie van de uitoefening van de in de artikelen 9.14, derde lid, en 9.15, eerste lid, bedoelde bevoegdheden.

9.6:	Het college van bestuur is verantwoording verschuldigd aan de raad van toezicht. Het college van bestuur verstrekt de raad van toezicht de gevraagde inlichtingen betreffende zijn besluiten en andere handelingen. Het college van bestuur verstrekt Onze minister de gevraagde inlichtingen omtrent de universiteit.
9.8, lid 1:	De raad van toezicht houdt, met het oog op de taken van de universiteit, bedoeld in artikel 1.3, eerste lid, toezicht op de uitvoering van werkzaamheden en de uitoefening van bevoegdheden door het college van bestuur en staat dit college met raad ter zijde. De raad van toezicht is in elk geval belast met: a. […] b. het goedkeuren van het bestuurs- en beheersreglement; c. het goedkeuren van de begroting, de jaarrekening, het bestuursverslag en het instellingsplan; d. […] e. het toezien op de naleving door het college van bestuur van wettelijke verplichtingen en de omgang met de branchecode, bedoeld in artikel 2.9; f. […] g. […] h. […] i. het jaarlijks afleggen van verantwoording over de uitvoering van de taken en de uitoefening van de bevoegdheden, bedoeld onder a tot en met h, in het bestuursverslag van de universiteit.
9.12:	1. verzorging van het onderwijs en de beoefening van de wetenschap geschieden in de faculteit. Aan het hoofd van de faculteit staat de decaan van de faculteit. 2. In afwijking van het eerste lid kan in het bestuurs- en beheersreglement worden bepaald dat aan het hoofd van de faculteit een bestuur staat, bestaande uit de decaan van de faculteit, tevens voorzitter, en een of meer andere leden. Indien de eerste volzin toepassing heeft gevonden, wordt in deze titel en in titel 2 met uitzondering van artikel 9.13, vierde en zesde lid, onder decaan tevens verstaan het bestuur van de faculteit. Indien aan het hoofd van de faculteit een meerhoofdig bestuur staat, wordt een student van de desbetreffende faculteit in de gelegenheid gesteld de vergaderingen van dit bestuur bij te wonen in welke vergaderingen deze student een adviserende stem heeft. In het bestuurs- en beheersreglement wordt bepaald, op welke wijze de in de vorige volzin bedoelde student wordt aangewezen.
9.14:	1. De decaan is belast met de algemene leiding van de faculteit. De decaan is voorts belast met het bestuur en de inrichting van de faculteit voor het onderwijs en de wetenschapsbeoefening. 2. De decaan werkt mede aan het bestuur van de universiteit door onder meer het plegen van overleg met het college van bestuur terzake van de voorbereiding van het instellingsplan en de begroting. 3. Onverminderd artikel 9.5 stelt de decaan ter nadere regeling van het bestuur en de inrichting van de faculteit het faculteitsreglement vast. 4. Het faculteitsreglement behoeft de goedkeuring van het college van bestuur. De goedkeuring kan slechts worden onthouden wegens strijd met het recht of het algemeen belang. 5. Indien binnen een door het college van bestuur te bepalen termijn het faculteitsreglement niet of niet volledig is vastgesteld, stelt het college van bestuur het reglement of het ontbrekende gedeelte daarvan vast

Naast de WHW onderschrijven de universiteiten de Code Goed Bestuur van de VSNU. Op het moment van de aanvang het openen van de eerste phishingmail (15 oktober 2019) en later de ransomware aanval (23 december 2019) was de versie 2017 van kracht. Sinds 1 januari 2020 is er een nieuwe versie van de Code Goed Bestuur. Deze branchecode gaat uit van zelfregulering. Relevante artikelen uit de codes staan hieronder:

Code Goed Bestuur VSNU (VERSIE 2017) (pas toe of leg uit)

ART 2.1.4 het cvb draagt ervoor zorg dat de activiteiten van de universiteit bestuurlijk, juridisch, organisatorisch en financieel deugdelijk geregeld zijn, transparant zijn en verantwoord kunnen worden.

CODE Goed Bestuur VSNU (versie 2020)

9. De universiteit beschikt over professionele interne risicobeheersings- en controlesystemen.

WHW-artikelen 2.10 en 9.8 raken aan deze uitwerkingen.

9.1. Het college van bestuur is verantwoordelijk voor het identificeren en beheersen van de risico's verbonden aan de strategie en de uitvoering van de activiteiten van de universiteit.

9.2. Het college van bestuur is verantwoordelijk voor de aanwezigheid en werking van interne risicobeheersings- en controlesystemen. Onderdeel van dit systeem zijn in ieder geval:

i. een beschrijving van de belangrijkste risico's die zijn verbonden aan de realisatie van de strategie of die van invloed kunnen zijn op de continuïteit van de universiteit;

ii. het bepalen van in welke mate er bereidheid is risico's te nemen op de belangrijkste strategische thema's en activiteiten ('risicobereidheid') en rapportering hierover in het jaarverslag;

iii. systematische beheersing van risico's in alle investerings- en innovatieprojecten. Besluitvorming, inclusief de daarbij gebruikte adviesnotities, worden vastgelegd;

iv. adequaat ingerichte processen en bedrijfsvoeringsystemen, gericht op de beheersing van risico's bij de uitvoering van de activiteiten van de universiteit.

9.3. Het college van bestuur monitort de werking van de interne risicobeheersings- en controlesystemen en voert ten minste jaarlijks een systematische beoordeling uit van de opzet en de werking van de systemen. Het college van bestuur legt in het jaarverslag verantwoording af over de inrichting, het functioneren, de belangrijkste resultaten en eventuele aanpassingen van de interne risicobeheersings- en controlesystemen.

9.4. Het college van bestuur is verantwoordelijk voor de interne auditfunctie. De interne auditfunctie beoordeelt de opzet en werking van het interne risicobeheersings- en controlesystemen. De raad van toezicht houdt toezicht op de interne auditfunctie en heeft regelmatig contact met de interne auditor. Indien er geen interne auditfunctie is ingericht, beoordeelt de raad van toezicht jaarlijks of adequate alternatieve maatregelen zijn getroffen.

9.5. Het college van bestuur bespreekt de effectiviteit van de opzet en de werking van de interne risicobeheersings- en controlesystemen in ieder geval één keer per jaar met de raad van toezicht. Daarnaast bespreekt de raad van toezicht in ieder geval één keer per jaar de meerjarenprognoses en beoordeelt hij of de financiële continuïteit van de organisatie daarin geborgd wordt.

Bijlage 2: overzicht UM documentatie

Op verzoek van de inspectie is de volgende documentatie ter beschikking gesteld:

- Het bestuurs- en beheersreglement UM geldend op 1-10-2019 en daarna
- Faculteitsreglement, van een van de UM faculteiten (als voorbeeld)
- Informatiebeveiligingsbeleid van de UM geldend op 1-10-2019 en daarna
- Beleid gegevensbescherming AVG, AVG protocol geldend op 1-10-2019 en daarna
- UM beleid tav Bring-Your-Own-Device op 1-10-2019 en daarna
- Managementletters van de boekjaren 2015 tot en met 2019
- Accountantsrapportages van de jaren 2015 tot en met 2018
- Opdracht, taakomschrijving en inrichting CERT team
- Uitkomsten van de laatste twee UM-Audits uitgevoerd in het kader van de SURF-IT-Audit
- Protocol/werkproces met betrekking tot onderhoud en updates van het UM-netwerk geldend op 1-10-2019 en daarna
- Protocol/werkproces met betrekking tot back-up faciliteiten geldend op 1-10-2019 en daarna
- Medewerkers en studentinstructie met betrekking tot UM-werkplek en virtuele werkplek (bij in gebruik name)
- Protocol/werkwijze mbt digitale werkomgeving voor studenten, medewerkers en in bijzonder IT-functionarissen
- Voorbeeld recente incidentrapportage mbt digitale veiligheid aan het management
- Protocol/werkwijze incidentmelding door medewerker (in bijzonder gerelateerd aan digitale veiligheid)
- Protocol/werkwijze incidentafhandeling door servicedesk, ICT en netwerkbeheer
- De meest recente bewustwordingscampagne over digitale veiligheid naar medewerkers en studenten van voor 23 december 2019
- Feitenrelaas rond de cyberaanval contact met ransomware aanvaller, IT-maatregelen, bestuurlijk-juridisch, communicatie interne UM organisatie en extern.
- Documentatie ten aanzien van verbeteracties die op dit moment door de UM zijn geformuleerd naar aanleiding van de cyberaanval.

De Universiteit Maastricht heeft hiernaast aanvullend documentatie geleverd die inzicht geeft in de cyberweerbaarheid van de instelling. Dit betreft documentatie mbt:

- Documentatie uitvoeringsbeleid van een tweetal faculteiten mbt informatiebeveiliging en privacy
- Awareness-communicatie
- Verbeteracties en vernieuwingen, waaronder SOC, IAM, verbeteringen netwerkvoorzieningen, 2-factor authentication
- Risicomanagementdocumentatie met daarin aandacht voor cybersecurity en privacy als onderdeel van het risicomanagement
- Documentatie rond I-strategie en I-board
- AVG awareness
- Aanvullende documentatie mbt de cyberaanval zelf

Bijlage 3: Overzicht gesprekken

Op 17 en 18 februari 2020 vonden gesprekken plaatst met:

- het voltallige College van Bestuur
- een vertegenwoordiging van het Crisis Management Team (CMT) dat betrokken was bij de afhandeling van de cyberaanval
- een vertegenwoordiging van het Cyber Emergency Response Team van de Universiteit Maastricht (UM-CERT)
- een gesprek met de Chief Information Security Officer (CISO) van de UM
- een vertegenwoordiging van medewerkers ICT/netwerkbeheerders van de centrale UM organisatie en uit een tweetal faculteiten
- een vertegenwoordiging van medewerkers en studenten uit de medezeggenschap van de centrale U-raad en enkele faculteiten of diensten
- een groepsgesprek met studenten en medewerkers uit verschillende opleidingen, faculteiten en diensten van de UM
- drie leden van de Raad van Toezicht

op 9 maart 2020 vonden gesprekken plaats met:

- financieel directeur en directeur ICT van de UM
- de externe accountants van de afgelopen vijf boekjaren

Lijst van afkortingen

AVG	Algemene Verordening Gegevensbescherming
BIO	Baseline Informatiebeveiliging Overheid
CvB	College van Bestuur
CERT	Computer Emergency Respons Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMT	Crisis Management Team
DUO	Dienst Uitvoering Onderwijs
FG	Functionaris Gegevensbescherming
IoC's	Indicators of Compromise
ISO	Internationale Organisatie voor Standaardisatie
NVAO	Nederlands Vlaamse Accreditatie Organisatie
NCSC	Nationaal Cyber Security Centrum
NWO	Nederlandse Organisatie voor Wetenschap
RvT	Raad van Toezicht
SCIRT	SURFnet Community van Incident Response Teams
SOC	Security Operations Center
UM	Universiteit Maastricht
VDI	Virtual Desktop Infrastructure
VSNU	Vereniging van Universiteiten
WHW	Wet op het hoger onderwijs en wetenschappelijk onderzoek
WOT	Wet op het onderwijstoezicht
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

Colofon

Inspectie van het Onderwijs
Postbus 2730 | 3500 GS Utrecht
www.onderwijsinspectie.nl

Een exemplaar van deze publicatie is te downloaden vanaf de website van de Inspectie van het Onderwijs: www.onderwijsinspectie.nl.