



Inspectie van het Onderwijs
*Ministerie van Onderwijs, Cultuur en
Wetenschap*

BINNEN ZONDER KLOPPEN

DIGITALE WEERBAARHEID IN HET HOGER ONDERWIJS

Utrecht, juli 2021

Samenvatting

In december 2019 werd de Universiteit Maastricht (UM) geconfronteerd met een cyberaanval die de voortgang van het onderwijs en onderzoek tijdelijk in gevaar bracht. De omvang van de cyberaanval was aanleiding voor de Inspectie van het Onderwijs (hierna inspectie) om een stelselonderzoek uit te voeren naar cyberveiligheid in het hoger onderwijs. Kort gezegd: wat kan het hoger onderwijs doen om de weerstand tegen cyberdreigingen te vergroten en zo de goede voortgang en kwaliteit van het onderwijs en onderzoek te waarborgen? Daartoe heeft de inspectie in de periode juli 2020 – juni 2021 deskresearch uitgevoerd, gesprekken gevoerd met veertien instellingen voor hoger onderwijs (ho-instellingen), en gesprekken gevoerd met betrokken partijen op het gebied van hoger onderwijs en op het gebied van cyberveiligheid. Dit onderzoek beantwoordt drie deelvragen:

1. In hoeverre is er bij hoger onderwijsinstellingen aandacht voor cyberdreigingen en welke maatregelen worden er genomen om de weerstand te vergroten?
2. In hoeverre vragen kenmerken van hoger onderwijsinstellingen om andere accenten binnen het cyberrisicomanagement?
3. Wie heeft zicht op en is verantwoordelijk voor de informatiebeveiliging van het Nederlandse hoger onderwijs?

Welke aandacht en maatregelen voor cyberveiligheid bij instellingen

Mede door de aanval op de UM is cyberveiligheid onderwerp van gesprek (geworden) bij besturen van hoger onderwijsinstellingen. De mate waarin is echter nog niet altijd voldoende. Er is niet altijd aandacht in alle lagen van de organisatie en niet bij alle instellingen. Ook ligt de focus vaak op beschermen van privacygegevens en minder op brede informatiebeveiliging. Instellingen hebben extra maatregelen genomen, bijvoorbeeld op het gebied van monitoring en detectie, een strenger wachtwoordbeleid, investeringen in meer en betere back-ups, segmentatie van het netwerk, bewustwording, en een meer actieve rol van bestuur en intern toezicht. Echter, de continue evaluatie van de informatiebeveiligingsaanpak in de praktijk kan worden versterkt; (decentrale) onderzoeks- en onderwijseenheden zien cyberveiligheid vaak niet als hoogste prioriteit, instellingen controleren en evalueren niet altijd structureel, en leveranciers wordt niet altijd gevraagd of de beveiliging op orde is. Verder zijn niet alle onderwijsinstellingen even sterk betrokken bij gezamenlijke initiatieven om monitoring te versterken en de informatiepositie ten aanzien van actuele dreigingsinformatie te verbeteren, waardoor niet alle instellingen toegang hebben tot de gedeelde kennis.

Welke kenmerken van instellingen in relatie tot cyberrisicomanagement

Voor grote onderwijsinstellingen blijkt het een uitdaging zicht te hebben op de verschillende organisatieonderdelen, bijvoorbeeld doordat faculteiten of afdelingen zelf hun ICT inrichten. Daarom controleren en evalueren grote instellingen structureler en grootschaliger dan kleine instellingen. De diversiteit in aanpak en aandacht voor cyberveiligheid onder kleinere instellingen is groot. Cyberveiligheid is bij de ene instelling een regulier aandachtspunt en bij anderen nog nauwelijks. Deelname aan specialistische cyberveiligheid platforms en netwerken is vrijblijvend, waardoor niet elke hoger onderwijsinstelling toegang heeft tot gedeelde kennis, informatie over cyberdreigingen, of betrokken is bij gezamenlijke audits en evaluaties. Voor belangrijke platforms zoals SURF en het platform Integrale Veiligheid Hoger Onderwijs (Platform IV-HO) geldt dat met name grote bekostigde hoger onderwijsinstellingen structureel betrokken zijn. Rechtspersonen voor hoger

onderwijs (hierna rpho's) kunnen zich in de regel niet bij deze partijen aansluiten en kleine instellingen zijn vaak afhankelijk van een beperkte ICT-capaciteit.

Wie is verantwoordelijkheid voor informatiebeveiliging

Onderwijsinstellingen zijn zelf verantwoordelijk voor de (cyber)veiligheid van hun instelling, waardoor er maatwerk mogelijk is. Maar de huidige aanpak isoleert wel een deel van de hoger onderwijsinstellingen. Ook beperkt deze aanpak de mogelijkheden om op stelselniveau de cyberweerbaarheid te verbeteren. In het stelsel van hoger onderwijs ontbreekt een sluitende informatievoorziening, een escalatieladder en een gedeeld normenkader met een minimaal volwassenheidsniveau. Hierdoor is het op dit moment niet mogelijk om vast te stellen hoe het gesteld is met de cyberveiligheid van hoger onderwijsinstellingen. Zonder een volledig beeld ontstaan blinde vlekken. In de totale keten van cyber en onderwijs is veel kennis en kunde aanwezig, maar door gebrek aan eigenaarschap ontbreekt het aan sturing. De overheid speelt tot op heden slechts een beperkte rol in beleid en toezicht op het gebied van cyberveiligheid. Meer regie is nodig om gaten op stelselniveau te voorkomen.

Concluderend kunnen instellingen en het stelsel hoger onderwijs het volgende doen om de cyberweerbaarheid te verhogen:

- Cyberveiligheid een integraal onderdeel maken van het risicomanagement door centrale regie vanuit het bestuur, kennis en kunde te vergroten, bewustzijn in alle niveaus van de organisatie te vergroten, vrijheden in decentrale delen van de organisatie ter discussie te stellen.
- Monitoren en verbeteren door het ambitieniveau op basis van een gedeeld normenkader van de cyberveiligheid met de hele organisatie – en het stelsel – te expliciteren en periodiek vast te stellen welke verbeteringen en maatregelen nodig zijn.
- Informatie meer en breder delen door alle instellingen de toegang te geven tot informatie over kwetsbaarheden en specifieke cyberdreigingen. Anders zullen de verschillen in het niveau van cyberweerbaarheid tussen ho-instellingen (bijvoorbeeld groot versus klein, bekostigd versus niet-bekostigd) toenemen.
- Samenwerken in de hele keten hoger onderwijs zodat instellingen gezamenlijk maatregelen kunnen nemen die onderwijsinstellingen niet individueel kunnen realiseren.
- Eigenaarschap vergroten en expliciteren door naast de bestaande krachtige informele uitwisselingen in het stelsel het eigenaarschap voor cyberveiligheid duidelijk te beleggen binnen het stelsel.
- Meer regie vanuit de overheid door bij universiteiten, hogescholen en rpho's de reflectie op het gekozen ambitieniveau te vergroten, en de stappen naar dat ambitieniveau af te stemmen tussen besturen, beleid en toezicht.

DEEL C: CONCLUSIES EN AANBEVELINGEN

Conclusies

Met dit onderzoek wil de inspectie een bijdrage leveren aan het beeld van cyberveiligheid in het hoger onderwijs. Vanuit de Wet op het hoger onderwijs zijn instellingen zelf verantwoordelijk voor de inrichting van de organisatie en voor een goede bedrijfsvoering. Het bestuur wordt geacht de kwaliteit en goede voortgang van het onderwijs en onderzoek te waarborgen. We hebben dit onderzoek uitgevoerd nadat een grote cyberaanval op een Nederlandse universiteit wereldkundig werd. Daarna werd de samenleving geconfronteerd met de COVID-19 pandemie waardoor de afhankelijkheid van de digitale infrastructuur enorm toenam. Mede door deze gebeurtenissen werd het onderwerp cyberveiligheid tijdens de uitvoering van dit onderzoek in het maatschappelijke debat in toenemende mate onderwerp van gesprek.

Hoofdvraag: hoe weerstand tegen cyberdreigingen vergroten?

Met dit onderzoek wil de inspectie antwoord geven op de vraag: *Hoe kan het stelsel hoger onderwijs, met in het bijzonder besturen van hoger onderwijsinstellingen, handelen om de weerstand tegen cyberdreigingen te vergroten en zo de goede voortgang en kwaliteit van het onderwijs en onderzoek te waarborgen?* In dit onderzoek hebben we gekeken naar de positie van instellingen en naar de weerbaarheid van het stelsel als geheel.

Door een integrale aanpak door instellingen vanuit bestuurlijke betrokkenheid

Allereerst de instellingen. We concluderen dat het gesprek en daardoor de maatregelen binnen instellingen mede door de aanval op de UM in een stroomversnelling terecht zijn gekomen en dat daarmee de cyberweerbaarheid van instellingen is verbeterd. Bij veel hoger onderwijsinstellingen is cyberveiligheid onderwerp van gesprek (geworden) van het bestuur. Het startpunt van ho-instellingen is echter zeer divers, waardoor de mate waarin cyberveiligheid onderwerp van gesprek is sterk verschilt.

Het meest kansrijk vinden we de integrale benadering van cyberveiligheid. Deze integrale benadering zien we bij een groep instellingen van met name de grotere universiteiten en (bekostigde) hogescholen. Die integrale aanpak is nodig om cyberweerbaarheid echt effectief te verbeteren. De voorlopers hebben nagedacht over hun risicoprofiel en hebben daarop een informatiebeveiligingsplan of cybersecurityplan gebaseerd. Ook maakt cyberveiligheid onderdeel uit van hun risicomanagement. Bij deze instellingen zoekt het bestuur naar antwoord op de vraag: hoe cyberweerbaar is onze organisatie werkelijk? Juist de bestuurders en de kwaliteit van de vragen die zij stellen en de prioriteit die zij geven, zien we als een doorslaggevende factor. 'Cyber' is voor bestuur en intern toezicht vaak complex en minder tastbaar dan andere te beheersen risico's. Bestuurders en toezichthouders zullen zich dus moeten verdiepen in dit onderwerp om de juiste vragen te kunnen stellen. De in onze optiek succesvolle instellingen zijn bovendien op zoek naar een goede balans tussen enerzijds de vrijheden voor decentrale onderdelen van de instelling om onderwijs te kunnen verzorgen en onderzoek uit te kunnen oefenen, en anderzijds de beheersbaarheid van cyberincidenten die de gehele instelling kunnen raken. Die balans is aan het verschuiven en wij denken dat dat een goede zaak is. De aanpak van cyberdreigingen is complex en niet vrijblijvend en heeft stevige centrale regie nodig. Die centrale regie hoeft ook niet strijdig te zijn met een decentrale sturing op onderwijs en onderzoek.

Door het steeds monitoren en verbeteren van wat er is

Alle ho-instellingen zullen verdere stappen moeten zetten om de weerbaarheid van de eigen organisatie te verhogen en ook toekomstige cyberincidenten het hoofd te kunnen bieden. Cyberveiligheid is van de gehele universiteit, hogeschool of rpho; dat vraagt om het met elkaar expliciteren van het ambitieniveau, om het periodiek vaststellen welke verbeteringen nodig zijn en om het vervolgens kiezen van een afgewogen maatregelenpakket. Omdat de dreigingen steeds veranderen vraagt dat om een lerend systeem waarin sprake is van continue herijking van de plannen en aanpassing van de checks van het veiligheidsniveau van de instelling. We zien in ons onderzoek nog te veel instellingen waar de aanpak minder systematisch is en waar er minder aandacht is vanuit het bestuur. Cyberveiligheid wordt binnen deze instellingen – meestal zeer kleine bekostigde instellingen en kleinere rpho's die zich richten op hele specifieke onderwijsgebieden – gezien als opdracht van de ICT-afdeling. Cyberbeleid is binnen deze instellingen reactief, er is geen planmatige verbeteraanpak en vooral: instellingen staan er verregaand alleen voor als het gaat om het nadenken over en inrichten van een cyberweerbare organisatie en het nemen van passende maatregelen. Voor alle instellingen – maar zeker voor de achterblijvers – geldt dat er veel geleerd kan worden uit de evaluaties van recente incidenten elders. Daarom ook is de openheid van zaken die de Universiteit Maastricht heeft gegeven zo lovenswaardig. Uit alle evaluaties die sindsdien het licht hebben gezien, blijkt dat er een set met basismaatregelen is die een enorme bijdrage levert aan de cyberweerbaarheid. We concluderen dan ook dat ongeacht de verschillen tussen instellingen, het voor hen allen van belang is de basismaatregelen zoals geformuleerd door het NCSC op orde te hebben.

Door het vergroten en expliciteren van eigenaarschap binnen het stelsel

Als we uitzoomen naar het hoger onderwijs als geheel dan zien we eenzelfde beweging. Gesprekken, investeringen en maatregelen zijn in een versnelling geraakt door de recente incidenten. Die versnellingen zijn ook nodig om de toenemende dreiging een goed weerwoord te kunnen bieden. Dat betekent niet dat er niets was, integendeel. We vinden dat de uitgangspositie van het hoger onderwijs een goede basis biedt. Het lerend vermogen in combinatie met de openheid van de sector betaalt zich terug. Zwakheden die bij een eerdere aanval nog misbruikt werden, werden bij andere instellingen gerepareerd waardoor die weg werd afgesloten. Het bekostigd hoger onderwijs kent een jarenlange traditie van gezamenlijk innoveren op het gebied van digitalisering in het onderwijs. De activiteiten onder de vlag van SURF zijn zowel binnen als buiten het onderwijs bekend en we horen daar brede waardering voor. Er vindt veel kennisuitwisseling plaats, ook over cyberveiligheid en vanuit de primaire functie – onderwijs en onderzoek – van ho-instellingen wordt er nieuwe kennis gegenereerd. De informele uitwisselingen in het stelsel zijn een kracht van het stelsel. Desondanks concluderen we dat er geen duidelijk eigenaarschap voor cyberveiligheid van het stelsel als geheel.

Geen enkele partij in de keten van cyberveiligheid in het onderwijs kan zelfstandig het probleem oplossen en de risico's tot een acceptabel niveau terugdringen. Samenwerking is broodnodig. Deuren moeten worden geopend voor meer samenwerking en de zoektocht naar (nieuw) eigenaarschap zal verder moeten worden ontwikkeld. Samenwerking binnen de regio bijvoorbeeld, zoals dat bij de aanpak van COVID-19 snel van de grond is gekomen. Dat betekent samenwerking tussen ho-, mbo- en vo-instellingen; kennis en kunde, maar ook faciliteiten delen. Daarnaast samenwerking ook tussen kleine en grote instellingen en ook samenwerking tussen bekostigde en niet-bekostigde instellingen.

Door meer regie vanuit de overheid

SURF vervult op veel gebieden zeker de rol van 'eigenaar', meer dan enig andere partij in het stelsel. Maar we denken niet dat een ledenorganisatie zoals SURF de voornaamste partij kan zijn om 'achterblijvers' aan te sporen de cyberweerbaarheid te vergroten en de aanspreekcultuur in dat platform te vergroten. Binnen de informele circuits bestaat zeker ook een zelfcorrigerend vermogen, maar uiteindelijk ligt de bal bij de instelling. SURF is geen toezichthouder en geen van onze gesprekspartners lijkt dat als een wenselijke uitbreiding van de rol van SURF te zien. Wij denken dat dat terecht is. Dit zou immers ten koste kunnen gaan van de kracht van het informele uitwisselen die de instellingen heeft gebracht waar ze op dit moment zijn. Bovendien zijn lang niet alle instellingen aangesloten bij SURF en ook niet in dezelfde mate. Dat betekent wel dat er een gat bestaat. Reflectie van alle universiteiten, hogescholen en rpho's op het gekozen ambitieniveau en de stappen daar naar toe van het stelsel en instellingen binnen het stelsel, hoort te liggen bij de besturen in afstemming met beleid en toezicht. Die reflectie moet niet alleen gaan over het streefniveau maar ook over het huidige gerealiseerde niveau (Weten we welk niveau dat is? Of dit de hele ICT-inrichting betreft? Wat vinden we ervan?). Dat gezamenlijke gesprek voor het hele hoger onderwijs ontbreekt nu. Een gezamenlijk ambitieniveau, en het kunnen en willen ingrijpen als een instelling niet voldoet.

Door het erkennen en benoemen van verschillen

We vinden dat er binnen het stelsel onvoldoende expliciet rekening wordt gehouden met de grote diversiteit die er tussen instellingen bestaat en onvoldoende zicht is op wie er wel en niet goed is aangesloten op de bestaande infrastructuren en netwerken om informatie te delen. Zo kunnen rpho's zich niet als lid aansluiten bij SURF, maar alleen als klant van een aantal diensten gebruik maken. Daarnaast zijn niet alle bekostigde instellingen nauw betrokken bij de cybersecurity werkgroepen van SURF. Het gevaar is dat hierdoor de diversiteit in niveau van cyberweerbaarheid die er al is tussen ho-instellingen verder zal toenemen.

Door informatie meer en breder te delen

Onderdeel van dat gezamenlijke gesprek moet ook zijn de belemmeringen om het ambitieniveau te behalen. We vinden dat er nu nog te weinig oog is voor de verantwoordelijkheidsverdeling van verschillende partijen in ketens en het stelsel en voor mogelijke maatregelen die door individuele ho-instellingen niet gerealiseerd kunnen worden maar gezamenlijk wel. De belangrijkste belemmering die we nu zien is de informatiepositie van instellingen aangaande kwetsbaarheden en specifieke dreigingen. Die informatievoorziening is zeker nog niet tot volle wasdom gekomen, maar in elk geval bestaat er een ongewenst verschil in informatiepositie tussen instellingen, dat mede gebaseerd is op volwassenheidsniveau en bekostigingskenmerken van ho-instellingen.

Beantwoording deelvragen

De conclusie wordt nader onderbouwd aan de hand van de drie onderliggende deelvragen.

Deelvraag 1: In hoeverre is er bij hoger onderwijsinstellingen aandacht voor cyberdreigingen en welke maatregelen worden er genomen om de weerstand te vergroten?

Aandacht voor cyberveiligheid bij hoger onderwijsinstellingen is groter geworden

Cyberdreigingen staan in het hoger onderwijs volop in de aandacht. Als gevolg van de cyberaanval bij de Universiteit Maastricht is deze aandacht – en het bewustzijn

van de risico's – vergroot. In het algemeen is het voor bestuurders evident dat cyberweerbaarheid wordt gerealiseerd door de ICT-beveiliging en de mensen in de organisatie samen. Daarom onderstrepen zij het belang van terugkerende bewustwordingscampagnes. De focus ligt daarbij vaak op beschermen van privacygegevens en minder op andere dreigingen rond de bredere informatiebeveiliging. Informatiebeveiliging is een uitdaging voor hoger onderwijsinstellingen. Traditioneel staat onderwijs en onderzoek voorop en daarbij worden veel vrijheden voor de invulling en de inrichting gelaten aan decentrale eenheden (zoals faculteiten, opleidingen en onderzoeksgroepen). Steeds meer instellingen vinden het belangrijk om zicht te hebben op hun volledige ICT-landschap: welke uitzonderingen er bij welke onderdelen van de organisatie zijn op de standaard gebruikersafspraken voor medewerkers, studenten en derden. Dat betekent niet dat het zicht er nu al altijd is, maar wel dat er stevige stappen zijn genomen om het zicht te verbeteren. Veel instellingen hebben concrete maatregelen genomen om hun cyberweerbaarheid te verhogen. Zeker de ICT'ers en security specialisten binnen instellingen zijn zich terdege bewust van dreigingen en gaan serieus om met elke melding. Het realiseren van een veilig en laagdrempelig meldsysteem is weerbarstig en vraagt constante aandacht en duidelijkheid van bestuurders en leidinggevendenden. Wel zien we binnen instellingen een spanningsveld rond de ervaren veiligheid van het melden. Dit spanningsveld wordt vaak veroorzaakt door aan de ene kant de juridische verplichtingen van de AVG en aan de andere kant de wens om laagdrempelig melden van bredere ICT incidenten te stimuleren zodat kwetsbaarheden en mogelijke aanvallen snel worden gesignaleerd.

Cyberveiligheid is onderdeel van het risicomanagement van instellingen, maar de check op het functioneren moet verder worden versterkt

Bij veel hoger onderwijsinstellingen is het identificeren van cyberrisico's integraal onderdeel van de werkprocessen en het risicomanagement. Welke plek cyber exact inneemt in het geheel aan risico's en hoe je risico's moet duiden op de bestuurstafel is nog wel een zoektocht. Niet elk bestuur voelt zich voldoende geëquipeerd en veel bestuurders en toezichthouders zien cyberveiligheid als een specialistisch en moeilijk tastbaar onderwerp. Daarnaast worden cyberrisico's door decentrale eenheden – met uitzondering van de ICT afdeling – wel als heel belangrijk maar niet als allerhoogste prioriteit gezien, terwijl op centraal bestuursniveau dit onderwerp meestal wel op de agenda staat. Bestuurders en toezichthouders zoeken nog naar de juiste controlevragen om zicht te krijgen op hoe de universiteit of hogeschool er werkelijk voor staat en zij zoeken naar een goede balans binnen de organisatie van onderwijs en onderzoek enerzijds en bedrijfsvoeringsaspecten anderzijds. Als cyberrisico's niet structureel op de agenda staan en worden uitgewisseld binnen de onderdelen van de organisatie, levert dit een verhoogde kwetsbaarheid op voor de hele organisatie. Ho-instellingen erkennen dat er controle en evaluatie plaats moet vinden om een sluitend risicomanagementsysteem te hebben. Soms is er een specifiek streefniveau voor volwassenheid gedefinieerd, maar we zijn geen breed gedragen definitie tegengekomen van het na te streven weerbaarheidsniveau voor alle instellingen. Mede daardoor zien we verschillen; niet bij alle instellingen wordt structureel gecontroleerd of het werkelijke informatiebeveiligingssysteem functioneert zoals beoogd. Daarnaast zijn evaluaties en de eventuele gevolgtrekking naar aanleiding van de uitkomsten nog regelmatig een aangelegenheid van alleen de (ICT/cyber)specialisten. Dezelfde kanttekening op een check op de praktijk zien we terug op het vlak van ketensamenwerking. Ho-instellingen hebben verwerkingsovereenkomsten met leveranciers afgesloten en zijn zich bewust van het uitbesteden van de verantwoordelijkheid van bijvoorbeeld omgang met persoonsgegevens. Echter, instellingen vertrouwen doorgaans op de overeenkomsten en vragen aan leveranciers nauwelijks om te tonen dat gegevens volgens de afspraken worden beveiligd. Daarmee wordt de kans op kwetsbaarheden

vergroot, kwetsbaarheden die bovendien buiten het zicht van de instelling blijven. Waar het gesprek met externe leveranciers wel plaats vindt, levert dit meerwaarde op.

Instellingen hebben de afgelopen periode maatregelen genomen

Niet alleen de cyberaanval op de UM maar in het bijzonder ook de COVID-19 pandemie heeft de aandacht voor ICT binnen het crisismanagement vergroot. Verschillende instellingen hebben intussen de crisismanagementplannen aangescherpt door ook de aanpak van cybercrises daarin op te nemen. De verantwoordelijkheden in decentrale onderdelen van sommige instellingen en de lijnsturing van de crisisaanpak blijken niet altijd duidelijk. Om de crisisaanpak in de praktijk te laten werken, zullen instellingen deze moeten blijven oefenen. Daarnaast zullen ook de lessen van de crisisaanpak rond de pandemie vastgelegd moeten worden in de crisismanagementplannen.

Instellingen hebben hun lessen geleerd uit de aanval op de UM. De gevolgen van incidenten of zelfs cyberaanvallen die in 2020 of 2021 plaatsvonden konden worden beperkt door specifieke maatregelen die de UM had gecommuniceerd. Alle instellingen die we hebben gesproken, hebben naar aanleiding van de hack bij de Universiteit Maastricht maatregelen genomen. Dit gaat onder andere om maatregelen op het gebied van monitoring en detectie, de invoering van strenger wachtwoordbeleid, om investeringen in betere en meer back-ups, in segmentatie van het netwerk, in bewustwording en in een meer actieve rol van bestuur en intern toezicht. De maatregelen zijn echter zeer lokaal en ongelijksoortig. Op het moment dat er incidenten optreden is de instelling waar dit plaats vindt aan zet – tijdens de afhandeling van een incident kunnen bestuurders nauwelijks tot niet terugvallen op een gezamenlijk crisisteam of op andere instellingen in het stelsel. Snelle informatiedeling naar aanleiding van een crisis vindt nu voornamelijk plaats tussen bekostigde instellingen. Dat delen van informatie zorgt er voor dat de monitoring en detectie bij de andere instellingen wordt verhoogd en zo vervolgincidenten mogelijk kunnen worden voorkomen of beperkt. Dergelijke informatie bereikt echter niet alle ho-instellingen. Daarnaast werd bij incidenten in 2021 niet ervaren dat de informatiepositie door aanwijzing van het SURF CERT om dreigingsinformatie van het NCSC te ontvangen, was verbeterd ten opzichten van de aanval eerder bij de UM.

Ook op stelselniveau worden maatregelen genomen, maar niet iedereen is goed aangesloten op alle netwerken

De recente cyberaanvallen hebben ook tot een verscherpt bewustzijn op stelselniveau geleid. Na de cyberaanval op de Universiteit Maastricht was er in het bijzonder bij de universiteiten de wens om samen een beeld te krijgen van waar deze instellingen staan en was er behoefte om het gesprek aan te gaan over het risicoprofiel van universiteiten. Ook binnen de Vereniging van Hogescholen was er behoefte aan meer zicht op het niveau van cyberweerbaarheid van het gehele stelsel. Experts van universiteiten en hogescholen weten elkaar van oudsher te vinden bij SURF. Naast SURF is er het Platform Integraal Veilig Hoger Onderwijs (IV-HO), ook hier vinden bekostigde instellingen elkaar om ervaringen te delen. Voor zowel SURF als het Platform IV-HO geldt dat hoger onderwijsinstellingen niet in gelijke mate betrokken zijn, waardoor niet elke hoger onderwijsinstelling toegang heeft tot deze gedeelde kennis. Zowel SURF als het Platform IV-HO brengen uitdagingen van het stelsel in kaart, met respectievelijk het Cyberdreigingsbeeld Onderwijs en Onderzoek en het Risico- en dreigingsbeeld HO. De informatie in deze beelden is niet herleidbaar tot instellingen. De follow-up van mogelijke kwetsbaarheden is daardoor ook niet op stelselniveau mogelijk. De landelijke netwerken kenmerken zich bovendien door kennisdeling met elkaar en gezamenlijk verbeteren. Hoewel er dus veel kennis en ervaring gedeeld wordt, bemoeien noch

SURF noch instellingen onderling zich met elkaars bedrijfsvoering of de opvolging van adviezen. Dat is ook niet de opdracht van SURF. Instellingen voelen gezamenlijk de urgentie om de informatiepositie van hoger onderwijsinstellingen over dreigingen te verbeteren en waar mogelijk krachten te bundelen om tot continue bewaking te komen, bijvoorbeeld door het in 2021 opgezette Security Operations Center. Deelname aan het SOC is vervolgens weer een eigen keuze van elke instelling. Al met al is er op meerdere vlakken sprake van een zekere mate van vrijblijvendheid in het stelsel, waardoor de op veel plaatsen aanwezige kennis en kunde niet een optimaal bereik heeft en niet voldoende effectief wordt ingezet.

Deelvraag 2: In hoeverre vragen kenmerken van hoger onderwijsinstellingen om andere accenten binnen het cyberrisicomanagement?

Het hoger onderwijs is divers en dat zien we terug in het risicomanagement

Nederland bestaat uit zo'n 120 hoger onderwijsinstellingen. Dit zijn zeer diverse instituten, waaronder grote algemene universiteiten en hogescholen, technische universiteiten, sectorale hogescholen (denk aan Pabo en kunstinstellingen), en zeer kleine universiteiten en hogescholen. Sommige van deze instellingen hebben locaties verspreid over het hele land, anderen in verschillende gemeenten, verspreid over één gemeente of met het hele instituut in één pand. Er zijn bekostigde en niet-bekostigde instellingen. Kortom, er is sprake van grote diversiteit. Deze diversiteit zorgt ervoor dat individuele instellingen hun eigen keuzes maken om tot een effectief risicomanagementsysteem te komen. Grotere universiteiten en hogescholen hebben een systeem waarbij het centrale risicomanagement gevoed wordt door de verschillende decentrale organisatieonderdelen. Bij de grote onderwijsinstellingen is het een uitdaging zicht te hebben op de verschillende organisatieonderdelen, door bijvoorbeeld eigen ICT-inrichtingen binnen faculteiten of afdelingen. Bij hele kleine instellingen is dit niet aan de orde. De diversiteit onder kleinere instellingen is groot. Cyberveiligheid is bij de ene instelling een regulier aandachtspunt in de bedrijfsvoering en bij andere nog nauwelijks. Hoewel bij verschillende instellingen bestuurders en intern toezichthouders moeite hebben om voldoende kennis en affiniteit te creëren rond cyberveiligheid, speelt dit vaker bij de kleinste ho- instellingen. De omvang is ook van invloed op inrichtingskeuzes bijvoorbeeld bij cloud-oplossingen. We zien dat vooral kleine instellingen kiezen voor cloud-oplossingen om zo 'ontzorgd' te worden.

Grote verschillen in bewustzijn en afhandeling van risico's

Niet alle instellingen zijn zich even goed bewust van de risico's die ze lopen en besteden hier voldoende aandacht aan binnen hun instelling. Met name bij kleinere en bij niet-bekostigde instellingen wordt geen profiel vastgesteld of vindt periodiek geen gesprek plaats om vast te stellen of het huidige profiel nog volstaat. Om medewerkers en studenten bewust te maken van cyberrisico's, ondernemen instellingen verschillende acties. Bestuurders kiezen regelmatig een aanpak die past bij de instelling. Een deel van de instellingen kiest bijvoorbeeld een bewustwordingscampagne passend bij de specifieke kennis en ervaring van medewerkers of studenten. Hoe incidenten gemeld worden, hangt in sterke mate af van schaal. In kleinere eenheden en hogescholen is dit vaak informeel. Voordeel daarvan is dat het laagdrempelig is en vaak tot snelle oplossingen leidt. In grote organisatie-eenheden en grotere instellingen is er vaak een incidentmeldingssysteem. Het voordeel van die aanpak is dat de meldingen vaak anoniem gedaan kunnen worden en dat ze gedocumenteerd zijn. Ook op het vlak van crisisaanpak zijn er verschillen die voor een deel samenhangen met cultuurverschillen tussen instellingen, en voor een deel voortkomen uit verschillen in hoe instellingen omgaan met cyberveiligheid in hun organisatie. Een voorbeeld van cultuurverschillen is te zien in de afhandeling van cyberincidenten. Dit gaat via een

aparte eenheid bij grotere hoger onderwijsinstellingen, maar binnen de reguliere lijnen bij kleinere hoger onderwijsinstellingen. De verschillen in structurele omgang met cyberveiligheid zien we terug in het feit dat door bekostigde instellingen regulier gezamenlijk wordt geoefend met cybercrisis. Hierin lopen bekostigde instellingen voor op niet-bekostigde instellingen. Niet bij elke instelling wordt naast de operationele crisisafhandeling ook door het bestuur geoefend.

Evalueren is belangrijk, maar niet iedereen evalueert even grondig en regelmatig

Grote instellingen controleren en evalueren vaker dan kleine instellingen. Dat is deels verklaarbaar vanuit hun complexiteit en omvang. Alleen door goed en regelmatig evalueren komen zij risico's op het spoor. Bij kleinere instellingen is er meer sprake van informele feedbackloops. Universiteiten hebben in gezamenlijkheid besloten een externe controle uit te voeren naast de voorheen gebruikte self-assessment aan de hand van de SURF-audit. Kleinere universiteiten zijn bij deze afspraak niet aangesloten. Bekostigde hogescholen voerden voor de genoemde cyberaanval nog niet allemaal een SURF-audit uit, maar zijn dit in de toekomst wel van plan. Hogescholen denken eerst aan onderlinge peerreview en hebben op dit moment geen afspraken gemaakt over een externe controle. Bij rpho's is het beeld rond controle en evaluatie heel divers. Er zijn grote instellingen die een ISO-certificering hebben, bewuste keuzes maken voor evaluatiemethoden, terwijl andere instellingen voornamelijk op basis van incidenten handelen. Dat de inrichting van audits en evaluaties verschilt tussen instellingen vinden we begrijpelijk. Dat zou echter niet moeten betekenen dat de diepgang en inhoud van de evaluaties onderling verschilt. We constateren dat dat nu wel het geval is, waardoor er onnodige risico's en verschillen blijven bestaan.

Op stelselniveau is de aansluiting van hogere onderwijsinstellingen ongelijk verdeeld

Universiteiten lopen voorop in de aandacht voor cyberveiligheid. Het risicoprofiel van universiteiten is op een breder palet aan cyberdreigingen gericht. Op stelselniveau is een langere geformaliseerde traditie van uitwisseling tussen CIO's en CISO's van universiteiten. Dit zien we ook terug op bestuurlijk niveau, waarbij in VSNU verband afspraken zijn gemaakt over het controleren van informatiebeveiliging en daarbij inzetten van een externe audit. Bij de ontwikkeling van het SURF-SOC lopen grote universiteiten mede vanuit het belang op basis van het risicoprofiel voorop.

Bekostigde hogescholen benutten SURF als belangrijke speler op het vlak van cyberveiligheid. Er is sinds kort sprake van een formeel CISO overleg tussen hogescholen. Voorheen was dit sterk gedreven door informele contacten via verschillende SURF werkgroepen. De aansluiting is dan afhankelijk van de vraag of een hogeschool medewerkers beschikbaar heeft om daarin te participeren. Daarin zien we dat in het bijzonder hele kleine instellingen (hogescholen maar ook kleine universiteiten) niet altijd worden bediend door de kennis en de informatie die binnen het stelsel van hoger onderwijs wel beschikbaar is. Voor rpho's geldt daarbij dat zij wel producten kunnen afnemen van SURF en daarmee gebruik kunnen maken van diensten, maar geen lid van de coöperatie kunnen worden. Niet alle rpho's zijn daardoor aangesloten op specifieke dreigingsinformatie over actuele incidenten. Specialisten werkzaam voor rpho's zijn vaker aangewezen op informele contacten buiten het onderwijs om gewaarschuwd te worden. De verschillen in aandacht en informatievoorziening tussen de verschillende groepen van instellingen zijn vooral historisch gegroeid en vanuit het perspectief van cyberweerbaarheid niet altijd logisch verklaarbaar noch gewenst.

Deelvraag 3: Wie heeft zicht op en is verantwoordelijk voor de informatiebeveiliging van het Nederlandse hoger onderwijs?

Onderwijs en cyber ontmoeten elkaar

Aan de traditionele samenwerking- en verantwoordelijkheidsketen van het onderwijs is een loot toegevoegd: de cyberketen. De onderwijsketen vereist op zichzelf zowel lokaal als landelijk al een flink complex samenspel, cyber voegt daar een complicerende factor aan toe. De onderwijswerkelijkheid en de cyberwerkelijkheid moeten op elkaar gaan aansluiten. We zien lacunes op de volgende terreinen als het gaat om deze samenwerkingsketen:

- De informatievoorziening is weliswaar verbeterd, maar is nog niet sluitend
- Een escalatieladder ontbreekt, zodat onduidelijk is wie op welk moment in the lead is, wie geïnformeerd moet worden en wie ingrijpt als dat echt nodig is
- Een duidelijk en gedeeld normenkader ontbreekt: waaraan moet je voldoen en wat is eigenlijk ons ambitieniveau?

Instellingen zijn zelf verantwoordelijk voor cyberveiligheid

Universiteiten, hogescholen en rpho's zijn zelf verantwoordelijk voor de cyberveiligheid van de eigen instelling. Daarbij hebben zij een grote mate van vrijheid om hier invulling aan te geven. De eigen verantwoordelijkheid is niet uniek voor de onderwijssector. Ook in andere sectoren – zowel vitale als niet-vitale infrastructuur – zet het bestuur naar aanleiding van het eigen risicoprofiel het beleid uit, stemt investeringsplannen daarop af en moet via risicomanagement zelf zicht houden op de weerbaarheid van de eigen organisatie. Hierop kan het bestuur kritisch worden bevraagd in eerste instantie door de intern toezichthouder, bij bekostigde instellingen de Raad van Toezicht. Dat instellingen zelf verantwoordelijk zijn is zowel een kracht als zwakte. De kracht is dat er heel specifiek maatwerk mogelijk is, de zwakte zit hem in de geïsoleerde positie die het op kan leveren. Uit ons onderzoek blijkt dat niemand die kracht kwijt wil, maar dat de zwakte wel in toenemende mate een risico vormt. Dat vraagt om een herbezinning op de sturing op cyberweerbaarheid binnen het hoger onderwijs: hoe zorgen we dat er lokaal maatwerk mogelijk blijft binnen heldere en afgestemde kaders en ambities die voor iedereen gelden?

Landelijk ambitieniveau voor cyberweerbaarheid vaststellen is nodig

In de onderwijssector bestaan geen (wettelijke) afspraken over de wijze van informatiebeveiliging en het beheersen van cyberrisico's. Diverse bekostigde instellingen hanteren de NIHO-standaard van SURF. Universiteiten en bekostigde hogescholen hebben sinds kort afspraken gemaakt over hun minimale volwassenheidsniveau. Echter, er is (nog) geen afgestemde eenduidige auditaanpak om te bepalen wat het volwassenheidsniveau van een instelling is. Universiteiten hebben hierover onderling uitgangspunten opgesteld ten behoeve van de externe audit die zij met elkaar hadden afgesproken. Bij bekostigde hogescholen en rpho's is geen sprake van een gezamenlijk uitgangspunt. Het staat instellingen vrij zelf de aanpak van een controle te bepalen en daarmee dus ook de reikwijdte en de diepte van die audit. De bekendheid met de SURF-audit bleek in ons onderzoek beperkt. Ook bleek de kennis over de inhoud en de validiteit van de audit vaak beperkt tot een enkele inhoudelijke expert. De audit werd en wordt vaak uitgevoerd door diezelfde expert, of de audit is alleen uitgevoerd op instellingsniveau en niet op alle onderliggende niveaus. Op instellingsniveau is er sprake van een gemiddelde, externe reflectie ontbreekt en de audit sluit niet aan op andere processen. De focus komt soms te liggen op technische issues door wat kritische ICT'ers allemaal (bijna) mis zien gaan bij de onderwijsinstelling. Dit alles kan een vertekend beeld opleveren mede omdat de verslaglegging van de uitkomsten van audits beperkt blijft tot de instelling. Landelijke afspraken over het (laten) uitvoeren van een externe audit zijn

dus pas voor een beperkt deel van het hoger onderwijs gemaakt. Daarmee is het op dit moment onmogelijk vast te stellen hoe dichtbij of hoe ver instellingen en het stelsel als geheel af staan van het eigen ambitieniveau. Voor niet-bekostigde instellingen is op dit vlak nog minder informatie beschikbaar.

De informatiepositie voldoet nog niet in het bijzonder voor rpho's

Het SURF-CERT bedient het hoger onderwijs door informatie over een specifieke aanval (IoC's) die bij een universiteit of hogeschool zijn aangetroffen door te geven aan andere instellingen. Maar feitelijk worden instellingen niet in gelijke mate bediend. SURF is van en voor de instellingen; grotere betrokkenheid betekent betere aansluiting, maar dat hangt in de praktijk vaak af van de omvang en soms van de interesse van enkele medewerkers. Dat zet kleinere bekostigde instellingen potentieel op een achterstand, maar ook rpho's die geen lid kunnen worden en op basis van informele contacten binnen en buiten het onderwijs aan informatie moeten komen. Ook het NCSC verzamelt en verspreidt specifieke dreigingsinformatie. Dit gaat zowel om het voorkomen als de afhandeling van specifieke incidenten. Het NCSC heeft deze taak ten behoeve van de Nederlandse vitale infrastructuur. Het onderwijs is thans geen vitale infrastructuur. Wel is het SURF-CERT aangesloten en kan van het NCSC dreigingsinformatie ontvangen ten behoeve van het hoger onderwijs. Echter, gezien de structuur van SURF is het de vraag of alle onderwijsinstellingen daar in dezelfde mate van kunnen profiteren. Bij het afhandelen van een omvangrijk incident dat van buiten de onderwijsinstelling komt, kan de aanvaller door commerciële specialistische partijen worden geduid. Voor deze commerciële partijen is dit dagelijks werk. Hoewel we op zich geen bezwaar zien tegen de inzet van specialistische kennis van dergelijke bureaus, is hun rol niet volstrekt duidelijk: welk mandaat hebben zij, is er een kosten-baten of een inhoudelijke afweging mogelijk wanneer het inzetten van deze bureaus onontbeerlijk is en in welke mate wil het hoger onderwijs afhankelijk zijn van hun inbreng?

Sturing op cyberweerbaarheid van de sector als geheel is nodig

In de totale keten van cyber en onderwijs is veel kennis en kunde aanwezig. Het ontbreekt echter aan een 'eigenaar'. Door de overheid is binnen het onderwijs relatief veel eigenaarschap 'gemandateerd' bij instellingen, bij koepels en bij ledenorganisaties. Dat bemoeilijkt de sturing op de cyberweerbaarheid van het stelsel als geheel. Ook is het lastig uitspraken te doen over de cyberweerbaarheid van het (hoger) onderwijs en het gewenste ambitieniveau. Het schetsen van een beeld van het stelsel is complex maar ook essentieel. Zonder een volledig beeld, inclusief de verantwoordelijkheidsverdeling, is het systeem niet effectief en ontstaan er blinde vlekken. Dat beeld moet niet gemaakt worden vanuit controle of dwang, maar vanuit het gezamenlijke belang. Instellingen geven aan behoefte te hebben aan sturing, heldere kaders en een gezamenlijke ambitie. Daarbij tekenen ze ook direct aan dat het geen knellende dwangbuis moet worden. Dat lijken tegenstrijdige geluiden. We denken dat binnen de cyber-onderwijsketen deze wensen als volgt kunnen worden samengevat.

De instelling moet verantwoordelijk zijn voor:

- Continuïteit en verzorging van onderwijs en onderzoek
- De onderwijslogistiek: inschrijving, roostering, beschikbaarheid van leermiddelen, uitreiken van getuigschriften
- Het vertalen van landelijke en regionale ontwikkelingen naar de eigen bedrijfsvoering
- Het formuleren en evalueren van eigen ambities en het afleggen van verantwoording

De overheid is verantwoordelijk voor:

- Zorgdragen voor voldoende financiële middelen

- Wet- en regelgeving: duidelijke kaders en normering
- Toezicht op naleving, gericht op de continuïteit van onderwijs en onderzoek
- Het monitoren van en informeren over bedreigingen op stelselniveau, in andere domeinen en internationaal
- Het voorkomen van gaten en overlap in rollen en verantwoordelijkheden op systeemniveau

Er is een gedeelde verantwoordelijkheid voor:

- Delen van kennis en kunde
- Gedeelde infrastructuur en delen van data
- Samenwerking tussen onderwijssectoren en maatschappelijke domeinen
- Het uitwerken van het streefniveau naar haalbare doelen per domein

Aanbevelingen

De inspectie beveelt aan **hoger onderwijsinstellingen** aan:

- Draag zorg voor een actueel cyberveiligheidsbeleid gebaseerd op het risicoprofiel van de instelling dat is afgestemd op het onderwijs en onderzoek dat de instelling verzorgt en uitvoert. Cyberincidenten kunnen elk onderdeel van de organisatie treffen. Daarom moet het bestuur het voortouw nemen in het behouden van de balans tussen onderwijs en onderzoek enerzijds en (cyber)veiligheid anderzijds.
- Zorg voor bewustzijn binnen alle niveaus van de organisatie. Bespreek binnen de instelling het gestelde ambitieniveau alsmede wat op basis van de ambities over en weer wordt verwacht van medewerkers, studenten, ICT en het bestuur. Ga expliciet in op uitzonderingen en de verantwoordelijkheden die dit legt bij decentrale eenheden of individuen. Zorg tevens voor veilige en laagdrempelige mogelijkheden om incidenten te melden.
- Stel periodiek de cyberweerbaarheid vast en controleer daarbij of de praktijk overeenkomt met het instellingsbeleid en op welke punten maatregelen nodig zijn. Heb daarbij oog voor de basismaatregelen die door het NCSC worden aanbevolen als uitgangspunt voor het cyberweerbaar maken van een organisatie.
- Ambieer op langere termijn te streven naar een volwassenheid op het gebied van cyberweerbaarheid hoger dan 3. Straal uit dat de onderwijsinstelling wil leren op het gebied van cyberveiligheid, om te voorkomen dat toekomstige cyberdreigingen uitgroeien tot incidenten en om incidenten die wel optreden eerder en effectiever te kunnen oplossen.
- Implementeer de basismaatregelen zoals geformuleerd door de NCSC.

De inspectie beveelt aan **koepels** en **overige netwerkpartijen** aan:

- Bespreek in sectorverband met elkaar de uitgangspunten rond cyberveiligheid en herijk deze periodiek. Het gaat daarbij in elk geval om:
 - Wat is een cyberweerbare ho-instelling?
 - Welke (minimale) basis in termen van beleid, organisatie-inrichting, maatregelen en controle wordt van een ho-instelling zelf verwacht?
 - Welke ondersteunende aanpak en maatregelen is alleen of efficiënter door het stelsel gezamenlijk te organiseren?
- Onderken bij het vaststellen van de uitgangspunten van een cyberweerbare ho-instelling de verschillen tussen cyberveiligheid en aanpalende terreinen zoals privacy/AVG en kennisveiligheid. Onderken tevens dat, gezien de diversiteit aan ho-instellingen, de relevantie van deze terreinen per universiteit, bekostigde hogeschool of rpho kunnen verschillen.
- Breek waar mogelijk met de traditionele scheiding tussen universiteiten en hogescholen en tussen bekostigde en niet-bekostigde partijen op het vlak van cyberveiligheid.
- Formaliseer betrokkenheid van ho-instellingen bij bijvoorbeeld CISO-netwerken en het onderwijs-CERT zodat instellingen minder afhankelijk zijn van (toevallige) deelname van medewerkers in werkgroepen.
- Behoud de kracht van de informele contacten via bijvoorbeeld SURF en het Platform Integraal Veilig Hoger Onderwijs en vergroot de verantwoording om door externe ogen te leren en de cyberweerbaarheid van individuele instellingen en het stelsel als geheel te vergoten.

De inspectie beveelt ten aanzien van het **overheidsbeleid** en het **toezicht** aan:

- Versterk de aandacht voor cyberveiligheid. Dit is gezien de ontwikkelingen op dit terrein voortdurend nodig bij de afzonderlijke spelers ho-instellingen, actoren in het stelsel van hoger onderwijs, het beleidsdepartement en het toezicht, en in afstemming met elkaar.
- Kom samen met de sector tot eenduidige uitgangspunten ten aanzien van cyberveiligheid en in lijn daarmee de externe verantwoording door ho-instellingen over hun (cyber)veiligheidsbeleid, en
 - Overweeg hierbij koepels en instellingen te stimuleren te komen tot een veldnorm.
 - Stem de uitgangspunten af met andere beleidsdepartementen en toezichthouders om te komen tot een generieke aanpak, waarbij oog is voor onderwijsspecifieke elementen die zorgen voor verschillen in risicoprofielen.
- Maak keuzes en expliciteer deze, ten aanzien van de verantwoordelijkheden van stelselpartijen en verschillende soorten ho-instellingen (universiteit, bekostigde hogeschool en rpho), zodat alle onderwijsinstellingen ongeacht omvang worden bediend door informatie en expertise op basis van de risico's die instellingen lopen. Wees daarbij bewust van de huidige positie van SURF in het stelsel die vanuit haar structuur logischerwijs niet alle instellingen in dezelfde mate kan bedienen. Overweeg of dit afdoende is.
- Realiseer de ingezette koers om de informatiepositie van het hoger onderwijs te versterken door beschikbare specifieke dreigingsinformatie van het NCSC met ho-instellingen te delen.
- Indien de overheid een groot belang hecht aan het nooit betalen van losgeld uit publieke middelen, vraagt dit om een actieve rol om instellingen te ondersteunen die door een grootschalig cyberincident worden getroffen. Dit ontslaat individuele instellingen echter nooit van de eigen verantwoordelijkheid.
- Vergroot de kennis op het vlak van cyberveiligheid bij beleidsdepartement, toezicht en in het stelsel, door:
 - Het risicoprofiel, de huidige cyberweerbaarheid en het gekozen ambitieniveau en van instellingen en het stelsel op het vlak van cyberveiligheid te bespreken. Bespreek tevens de consequenties van gekozen ambitieniveaus.
 - Aansluiting te zoeken bij andere beleidsdepartementen en toezichthouders om gezamenlijk te professionaliseren.
- Heb oog voor nationale en Europese ontwikkelingen op het vlak van cyberveiligheid. Trek hierbij op met andere beleidsdepartementen en toezichthouders ten aanzien van verschillende (wetgevings)initiatieven en sluit aan op reeds bestaande praktijken, onder andere uit de vitale sectoren. Ontwikkel en bespreek processen en werkwijzen, met in achtname van sectorspecifieke kenmerken zodat kennis en mensen uitgewisseld kunnen worden.

Literatuurlijst

AP (2020) *Meldplicht datalekken: facts & figures, Overzicht feiten en cijfers 2019*. Den Haag: Autoriteit Persoonsgegevens. Zie: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarcijfers_meldplicht_datalekken_2019.pdf (geraadpleegd op 19-7-2021)

AP (2021) *Meldplicht datalekken: facts & figures. Overzicht feiten en cijfers 2020*. Den Haag: Autoriteit Persoonsgegevens. Zie: <https://autoriteitpersoonsgegevens.nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken/cijfers-datalekken-2020> (geraadpleegd op 19-7-2021)

Bart Bosma en René Ritzen (2021) *Cyberdreigingsbeeld 2020 – 2021; Onderwijs en Onderzoek*. Utrecht en Amsterdam: SURF. Zie: <https://www.surf.nl/cyberdreigingsbeeld-onderwijs-en-onderzoek-2020-2021> (geraadpleegd op 19-7-2021)

Bart Bosma (2020) *SURFaudit benchmark 2019 – rapport*. Utrecht en Amsterdam: SURF. Zie: <https://www.surf.nl/files/2020-04/surfaudit-benchmark-2019-rapport-v1-def.pdf> (geraadpleegd op 19-7-2021)

CBS (2021) *Cybersecuritymonitor 2020*, Den Haag: Centraal Bureau voor de Statistiek. Zie: <https://www.cbs.nl/nl-nl/publicatie/2021/18/cybersecuritymonitor-2020> (geraadpleegd op 19-7-2021)

CIP (september 2019) *Informatiebeveiliging: onderwerp voor de bestuurstafel*. Amsterdam: Centrum informatiebeveiliging en privacybescherming. Zie: <https://www.bio-overheid.nl/media/1355/bio-leaflet-voor-bestuurders.pdf> (geraadpleegd op 19-7-2021)

COT (2021) *'Aanval afgeslagen' Leerevaluatie cyberaanval Hogeschool van Amsterdam en Universiteit van Amsterdam 2021*. Rotterdam: Instituut voor Veiligheids- en Crisismanagement in opdracht van Universiteit van Amsterdam en Hogeschool van Amsterdam. Zie: <https://www.hva.nl/binaries/content/assets/hva/nieuws/2021/leerevaluatie-cyberaanval-hva-uva-definitief-7-juli-2021.pdf> (geraadpleegd op 19-7-2021)

COT (2021) *Risico en Dreigingsbeeld Hoger Onderwijs 2021*. Rotterdam: Instituut voor Veiligheids- en Crisismanagement in opdracht van Utrecht: Platform Integraal Veilig Hoger Onderwijs (IV-HO). Zie: <https://integraalveilig-ho.nl/wp-content/uploads/Platform-Integrale-Veiligheid-hoger-onderwijs-Risico-en-Dreigingsbeeld-Hoger-Onderwijs-2021.pdf>

CSR (2021) *Adviesrapport Integrale aanpak cyberweerbaarheid*, Den Haag: Cyber Security Raad. Zie: <https://www.cybersecurityraad.nl/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid> (geraadpleegd op 19-7-2021)

Inspectie JenV (2021) *Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021*. Den Haag: Inspectie Justitie en Veiligheid. Zie: <https://www.inspectie-jenv.nl/Publicaties/rapporten/2021/06/29/rapport-samenhangend-inspectiebeeld-cybersecurity-vitale-processen-2020-2021> (geraadpleegd op 19-7-2021)

IvHO (mei 2020) *Cyberaanval Universiteit Maastricht*. Utrecht: Inspectie van het Onderwijs. Zie: <https://www.onderwijsinspectie.nl/documenten/rapporten/2020/06/12/rapport-cyberaanval-universiteit-maastricht>

IvHO (2020) *Covid-19 monitor: hoger onderwijs (derde meting)*. Utrecht: Inspectie van het Onderwijs. Zie: <https://www.onderwijsinspectie.nl/onderwerpen/corona-onderzoeken/documenten/publicaties/2020/11/24/covid-19-monitor-ho-derde-meting>

NCTV (juni 2021) *Cybersecuritybeeld Nederland 2021 (CSBN 2021)*. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid. Zie: <https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021> (geraadpleegd op 19-7-2021)

NCTV (juni 2020) *Cybersecuritybeeld Nederland 2020 (CSBN 2020)*. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid. Zie: <https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten/publicaties/2020/06/29/cybersecuritybeeld-nederland-2020>

NCTV (februari 2020) *Nationaal Crisisplan Digitaal*. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid. Zie: <https://www.nctv.nl/documenten/publicaties/2020/02/21/nctv-nationaal-crisisplan-digitaal--webversie> (geraadpleegd op 19-7-2021)

NCSC (2021) *Handreiking cybersecuritymaatregelen. Stap voor stap naar een digitaal veilige organisatie*. Den Haag: Nationaal Cyber Security Centrum. Ministerie van Justitie en Veiligheid. Zie: <https://www.ncsc.nl/onderwerpen/basismaatregelen/documenten/publicaties/2021/juni/28/handreiking-cybersecuritymaatregelen> (geraadpleegd op 21-7-2021)

Petra Oldengarm en Liesbeth Holterman (redactie) *Cybersecurity Woordenboek. Van cybersecurity naar Nederlands*. 2e druk. Den Haag Cyberveilig Nederland. Zie: www.cyberveilignederland.nl/woordenboek (geraadpleegd 26 juli 2021)

SURF (2021) *Wageningen University & Research (WUR) sluit als eerste instelling aan op SURFsoc*, online nieuwsbericht 15-4-2021. Zie: <https://www.surf.nl/nieuws/wageningen-university-research-sluit-als-eerste-instelling-aan-op-surfsoc> (geraadpleegd op 19-7-2021)

Tweede Kamer, vergaderjaar 2019–2020, 31 288 en 26 643, nr. 832.

Tweede Kamer, vergaderjaar 2019–2020, 31 288 en 26 643, nr. 872.

Tweede Kamer, vergaderjaar 2019–2020, 26 643, nr. 673.

Tweede Kamer, vergaderjaar 2020–2021, 31 288 en 26 643, nr 910.

Tweede Kamer, vergaderjaar 2020–2021, 26 643 nr. 767.

Staatscourant 2020, *Regeling aanwijzing computercrisisteam*s, 4410.

WRR (2019) WRR-Rapport 101: *Voorbereiden op digitale ontworping*, Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid. Zie: <https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontworping> (geraadpleegd op 19-7-2021)