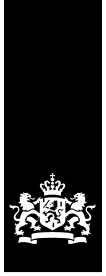


Inspectie van het Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

BINNEN ZONDER KLOPPEN

DIGITALE WEERBAARHEID IN HET HOGER ONDERWIJS

Utrecht, juli 2021

Voorwoord

Op afstand werken, op afstand zaken doen, op afstand leren: dankzij de informatie- en communicatietechnologie hoeven we veelal de deur niet meer uit. Zeker in deze corona-crisistijd merken we dat de hedendaagse samenleving vooral dankzij digitale middelen kan functioneren. Die afhankelijkheid heeft een keerzijde. Particulieren en allerlei organisaties in Nederland zijn steeds vaker en op steeds grotere schaal slachtoffer van digitale aanvallen. En het onderwijs is zeker geen uitzondering. De aanval met gijzelsoftware in december 2019 bij de Universiteit Maastricht toonde nog eens extra aan dat ook het hoger onderwijs een potentieel doelwit is.

Wat doen universiteiten en hogescholen momenteel aan hun digitale veiligheid en hoe kunnen de sector en de overheid ervoor zorgen dat het hoger onderwijs minder kwetsbaar is? Dat hebben we nu onderzocht, in vervolg op het instellingsonderzoek dat we in 2020 uitvoerden bij de Universiteit Maastricht na de digitale aanval.

We zien dat besturen in het hoger onderwijs digitale veiligheid serieus nemen – zeker sinds die aanval. Maar we zien ook dat een deel van de instellingen nog niet genoeg kennis en beschermingsmogelijkheden heeft. Daarnaast krijgt niet iedere onderwijsinstelling evenveel informatie om actuele dreigingen het hoofd te kunnen bieden. Dat vormt een risico voor de voortgang van onderwijs en onderzoek.

Daarom is het nodig dat besturen de krachten bundelen. Beter samenwerken, informatie delen en gezamenlijk actief blijven leren en vernieuwen: de ict-ontwikkelingen gaan immers razendsnel. Ieder individueel bestuur zou digitale veiligheid bovendien voortaan ook een vast onderdeel moeten maken van het risicomanagement. Hoe onwennig het onderwerp soms ook is. Digitale veiligheid kan niet meer worden overgelaten aan enkele toegewijde specialisten.

Digitale veiligheid kan ook niet worden overgelaten aan de individuele instellingen. Daarom moet ook de overheid meer verantwoordelijkheid en regie nemen op dit onderwerp. Want de kennis en kunde blijkt in het veld zeker aanwezig, maar de sturing ontbreekt.

Digitale veiligheid stevig op de bestuursagenda, structureel samenwerken en kennis actualiseren, en goed sturen op stelselniveau. In het hoger onderwijs, maar ook in de andere onderwijssectoren. Zo zorgen we er samen voor dat alleen de deur opengaat voor wie echt naar binnen mag, en dat de deur alleen openstaat voor wat veilig naar buiten kan.

Alida Oppers
inspecteur-generaal van het Onderwijs

INHOUD

Voorwoord 2
Samenvatting 5

DEEL A: INLEIDING EN ACHTERGROND

1 Inleiding 8
1.1 Aanleiding 8
1.2 Doelstelling en onderzoeksvragen 9
1.3 Wettelijk kader 9
1.4 Gebruikt normenkader in dit onderzoek 10
1.5 Onderzoeksopzet 11
1.6 Leeswijzer 13

2 Achtergrond: cyberveiligheid en ontwikkelingen 14
2.1 Soorten cyberdreigingen 14
2.2 Cyberveiligheid in het (hoger) onderwijs 16
2.3 Betrokken actoren bij cyberveiligheid in het hoger onderwijs 18
2.4 Ontwikkelingen in andere sectoren 21

DEEL B: BEVINDINGEN - CYBERVEILIGHEID IN HET HOGER ONDERWIJS

1 Standaard 1: vergroten bewustzijn 24
1.1 Instellingen hoger onderwijs 24
1.2 Bevindingen 25
1.3 Stelsel hoger onderwijs 31
1.4 Bevindingen 32

2 Standaard 2: veilige en open cultuur 35
2.1 Instellingen hoger onderwijs 35
2.2 Bevindingen 36
2.3 Stelsel hoger onderwijs 40
2.4 Bevindingen 40

3 Standaard 3: inrichten risicoteam 44
3.1 Instellingen hoger onderwijs 44
3.2 Bevindingen 45
3.3 Stelsel hoger onderwijs 48
3.4 Bevindingen 49

4 Standaard 4: borgen risicomanagement 55
4.1 Instellingen hoger onderwijs 55
4.2 Bevindingen 57
4.3 Stelsel hoger onderwijs 60
4.4 Bevindingen 62

5 Standaard 5: aandacht ketensamenwerking 65
5.1 Instellingen hoger onderwijs 65
5.2 Bevindingen 66
5.3 Stelsel hoger onderwijs 69

5.4 Bevindingen 69

6 Standaard 6: controleren en evalueren 73
6.1 Instellingen hoger onderwijs 73
6.2 Bevindingen 74
6.3 Stelsel hoger onderwijs 78
6.4 Bevindingen 79

7 Standaard 7: geld investeren in informatiebeveiliging 85
7.1 Instellingen hoger onderwijs 85
7.2 Bevindingen 86
7.3 Stelsel hoger onderwijs 90
7.4 Bevindingen 91

DEEL C: CONCLUSIES EN AANBEVELINGEN

Conclusies 94
Hoofdvraag 94
Beantwoording deelvragen 96

Aanbevelingen 104

Literatuurlijst 106

Bijlage I: Lijst van gesproken organisaties en gesprekspartners 108

Bijlage II: Lijst van afkortingen 109

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 informatiebeveiligings-aanpak 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 A: INLEIDING EN ACHTERGROND

1 Inleiding

1.1 Aanleiding

Op de avond van 23 december 2019 werd de Universiteit Maastricht (UM) geconfronteerd met een cyberaanval waardoor de goede voortgang van het onderwijs en onderzoek tijdelijk in gevaar was. Tien dagen, tot 2 januari 2020, was de universiteit digitaal op slot waardoor medewerkers en studenten geen gebruik konden maken van het netwerk en de ICT-diensten van de universiteit. De omvang van de cyberaanval was aanleiding voor de Inspectie van het Onderwijs (hierna inspectie) om een tweeledig onderzoek in te stellen: i – een instellingsonderzoek en ii – een stelselonderzoek.

In de periode februari – maart 2020 heeft de inspectie het instellingsonderzoek naar de cyberaanval bij de Universiteit Maastricht uitgevoerd[1]. De inspectie stelde vast dat de UM voorafgaande aan de cyberaanval niet altijd passende maatregelen heeft genomen, waardoor de cyberaanval verstrekkender impact had dan nodig. Ook in de aanloop tot de ransomware aanval bleken de maatregelen niet passend, waardoor lang niet is opgemerkt dat derden toegang tot het netwerk hadden gekregen. De crisisafhandeling zelf was daarentegen adequaat: de inspectie heeft geen aanwijzingen gevonden dat UM na het ontdekken van de ransomware aanval 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.

Het voorliggende rapport presenteert de resultaten van het vervolg op het instellingsonderzoek bij de Universiteit Maastricht: een stelselonderzoek dat zich richt op de aandacht voor cyberdreigingen in het gehele stelsel van hoger onderwijs. Dit onderzoek is uitgevoerd in de periode juli 2020 – juni 2021. Met het stelselonderzoek wil de inspectie een bijdrage leveren aan en een beeld schetsen van de cyberveiligheid in het hoger onderwijs. Met de aanval op de UM kwam het idee van een digitale dreiging voor Nederlandse universiteiten en hogescholen heel dichtbij. Daar bleef het ook niet bij; tijdens de onderzoeksperiode zijn ook andere onderwijsinstellingen geconfronteerd met de gevolgen van cyberproblematiek, waaronder de Universiteit Utrecht, de Technische Universiteit Delft, Universiteit van Amsterdam, Hogeschool van Amsterdam en Hogeschool InHolland.

Cyberdreiging is één van de externe dreigingen waar het hoger onderwijs mee te maken heeft. De afgelopen periode hadden onderwijsinstellingen ook te maken met een andere externe dreiging die de voortgang van het onderwijs en onderzoek in gevaar bracht: de pandemische uitbraak van COVID-19 (Coronavirus). Sinds half maart 2020 verzorgen hogescholen en universiteiten het onderwijs veelal online en wordt slechts beperkt onderwijs op de eigen locatie verzorgd. De digitale infrastructuur en online onderwijsvoorzieningen die hbo- en wo-instellingen in het afgelopen decennium ontwikkelden waren nu onderdeel van de oplossing. Daarmee onderstreepte de coronacrisis het belang van een goed werkende en veilige digitale infrastructuur voor de continuïteit van onderwijs en onderzoek.

[1] 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

1.2 Doelstelling en onderzoeksvragen

Met dit stelselonderzoek wil de inspectie een bijdrage leveren aan het beeld van cyberveiligheid in het hoger onderwijs zodat alle betrokken partijen, in het bijzonder hogescholen en universiteiten, zich een beeld kunnen vormen van mogelijke kwetsbaarheden en daarop passende maatregelen kunnen nemen.

De hoofdvraag van dit onderzoek luidt:
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?

De hoofdvraag is onderverdeeld in de volgende 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[2] 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?

1.3 Wettelijk kader

Dit onderzoek betreft een stelselonderzoek. Op basis van artikel 12a van de Wet op het Onderwijs Toezicht (WOT) onderzoekt de inspectie de ontwikkelingen in het stelsel van hoger onderwijs. Met het stelselonderzoek onderzoekt en agendeert de inspectie knelpunten die zich bij diverse hoger onderwijsinstellingen (hierna ho-instellingen) voordoen en die de verantwoordelijkheid van een enkele instelling overstijgen. Daarom onderzoeken we binnen een stelselonderzoek niet alleen de rol van instellingen, maar kijken we breed naar alle belanghebbenden in het stelsel. Het stelseltoezicht richt zich op zowel bekostigde als niet-bekostigde instellingen.

Het inhoudelijk kader wordt gevormd door de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW). 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 bekostigde universiteiten (hoofdstukken 9 en 11 WHW) respectievelijk bekostigde hogescholen (hoofdstuk 10 WHW). Op grond van de artikelen 9.9a (bekostigde universiteiten), 10.3e (bekostigde hogescholen) en 11.7a (Open Universiteit) kan de minister de Raad van Toezicht een *aanwijzing* geven indien er sprake is van wanbeheer. In geval van cyberveiligheid en andere externe dreigingen betekent wanbeheer het nalaten van noodzakelijk maatregelen waardoor *het waarborgen van de kwaliteit en goede voortgang van het onderwijs in gedrang komt*.

Naast bekostigde instellingen bestaat het stelsel van hoger onderwijs uit instellingen die geen rijksbijdrage ontvangen. Dit zijn de rechtspersonen voor hoger onderwijs (hierna rpho). Ook deze instellingen zijn onderdeel van dit stelselonderzoek. De WHW kent geen apart hoofdstuk met voorschriften ten aanzien van het bestuur en de inrichting van rpho's. In de beleidsregel *bevoegdheid graadverlening hoger onderwijs* is evenwel vastgelegd dat om toe te treden tot het stelsel van hoger onderwijs en om graden te mogen verlenen, er sprake moet zijn van voldoende continuïteit. De inspectie onderzoekt daarom de continuïteit van de rechtspersoon

[2] Het gaat om: a) wettelijk onderscheidende verschillen (universiteit, bekostigde hogeschool en rpho), b) onderwijs en onderzoekinhoudelijke verschillen (breed aanbod, monosectoraal aanbod, nichemarkt), en c) verschillen in verschijningsvorm waaronder omvang en locatie (meerdere vestigingsplaatsen, meerdere gebouwen, één gebouw).

voorafgaande aan het verkrijgen van het recht om graden te verlenen (cf WHW art. 6.9). Ook kan de minister de bevoegdheid tot graad verlenen intrekken als de financiële of bestuurlijke continuïteit van de rechtspersoon naar oordeel van de minister en op basis van inspectieonderzoek niet langer is gewaarborgd, waardoor onvoldoende waarborgen bestaan dat kan worden voldaan aan hetgeen bij of krachtens de wet is bepaald ten aanzien van kwaliteitszorg, de registratie, het onderwijs, de examens of de vooropleidingseisen.

Samengevat geldt voor zowel bekostigde als niet-bekostigde instellingen dat de WHW geen expliciete verwijzing maakt naar de invulling van cyberweerbaarheid, maar dat van het bestuur verwacht wordt dat zij passende maatregelen neemt om te waarborgen dat er sprake is van continuïteit van onderwijs en onderzoek.

1.4 Gebruikt normenkader in dit onderzoek

In dit onderzoek richten we ons op het bestuurlijk handelen rondom cyberveiligheid, gericht op de continuïteit van onderwijs en onderzoek. Omdat de WHW geen nadere invulling geeft van dit handelen, sluiten we voor ons onderzoek aan de Baseline Informatiebeveiliging Overheid (BIO)[3]. De overheid gebruikt de BIO vanaf 1 januari 2020. Net als vrijwel alle informatiebeveiligingstandaarden is de BIO afgeleid van de ISO 27001 en 27002[4]. Als onderdeel van de BIO zijn speciaal voor (overheids- en gemeente)bestuurders de normen vertaald naar zes normen voor aan de bestuurstafel[5]. Deze betreffen de onderwerpen waar het bestuur, bijgestaan door de eigen ICT'ers en cyberexperts, zicht op moet hebben om afwegingen over de cyberweerbaarheid van de eigen ho-instelling te kunnen maken. Deze standaarden sluiten aan bij de verantwoordelijkheid van de besturen van ho-instellingen en hebben we daarom zowel in ons onderzoek naar de hack bij de Universiteit Maastricht als in het voorliggende stelselonderzoek gebruikt. Aan de hand van deze standaarden zijn we nagegaan hoe het stelsel hoger onderwijs, met in het bijzonder besturen van ho-instellingen, kunnen handelen om de weerstand tegen cyberdreigingen te vergroten en zo de goede voortgang en kwaliteit van het onderwijs en onderzoek te waarborgen. De standaarden die besturen kunnen benutten, worden als volgt beschreven.

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 (potentiële) 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.

[3] De BIO is een concretisering van een aantal normen naar concrete maatregelen die verplicht door alle bestuurslagen moeten worden nageleefd. Dit is vastgelegd in de circulaire van 9 januari 2020 (2019-0000684575). Vanuit het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties wordt gewerkt aan wettelijke verankering.
[4] De Internationale Organisatie voor Standaardisatie (ISO) heeft in ISO 27001 het volledige proces van informatiebeveiliging beschreven. ISO 27002 geeft aanvullende standaarden, waarin adviezen worden gegeven hoe je de beveiliging kunt implementeren.
[5] 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)

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).

Aan deze zes normen hebben we ten behoeve van ons onderzoek een zevende norm toegevoegd die ziet op de investeringen die gedaan worden in passende maatregelen.

7. ***Geld investeren in informatiebeveiliging***: Er worden voldoende middelen beschikbaar gesteld om de onderkende risico's op een adequate manier te behandelen.

De zeven standaarden zijn oorspronkelijk geformuleerd op het niveau van de individuele instelling en bestuur. Met ons onderzoek willen we echter een stap verder gaan en ook het stelsel als geheel beschouwen. Om dat te kunnen doen hebben we elke standaard ook beschreven als stelselstandaard. Samen geven deze 2x7 standaarden ons een breed inzicht in de verschillende facetten van het bestuurlijk handelen inzake cyberveiligheid en helpen ze ons om de hoofd- en deelvragen te beantwoorden.

1.5 Onderzoeksopzet

Voor dit onderzoek hebben we gebruik gemaakt van de volgende bronnen:

1. Gesprekken met deskundigen en belanghebbenden
2. Analyse van instellingswebsites en jaarverslagen
3. Gesprekken met veertien instellingen
4. Analyse van diverse websites, nieuwsberichten en tijdens het onderzoek verkregen documenten (zoals plannen en evaluaties)

1. Gesprekken met deskundigen en belanghebbenden.
Gedurende het hele project zijn gesprekken gevoerd met de koepels en verschillende (specialistische) actoren op het vlak van onderwijs, cyberveiligheid, toezicht en beleid. Die gesprekken hebben ons geholpen om een beeld te krijgen van het stelsel als geheel en om vanuit verschillende standpunten te horen waar sterke punten en ontwikkelpunten zitten. Ook hebben de eerste gesprekken ons geholpen om standaarden te formuleren op stelselniveau. In bijlage I is een volledige lijst te vinden van alle gesprekspartners.

2. Analyse van instellingswebsites en jaarverslagen.
Om zicht te krijgen op de externe verantwoording en om op het spoor te komen van goede voorbeelden, hebben we deskresearch uitgevoerd. In de deskresearch hebben we de jaarverslagen[6] over 2018 en 2019 en websites[7] van ho-instellingen geanalyseerd. Dit betreft de jaarverslagen en websites van alle bekostigde instellingen (N=54), waarvan 18 universiteiten en 36 hogescholen. Daarnaast rapporteren we over de rechtspersonen voor hoger onderwijs (rpho's) die een

[6] Voor bekostigde instellingen betreft dit de jaarverslagen zoals bedoeld in art 2.9 lid 1 WHW. Rechtspersonen voor hoger onderwijs sturen jaarlijks een verslag van werkzaamheden aan de inspectie als bedoeld in art 1.12 lid 3 WHW.
[7] Dit betreft de externe websites, toegankelijk voor iedereen.

jaarverslag hebben opgestuurd over het jaar 2018 én het jaar 2019 (N=56[8]). De analyse van websites kon voor N=58 rechtspersonen voor hoger onderwijs worden geanalyseerd[9]. De jaarverslagen geven in het bijzonder een indruk van de mate waarin besturen extern verantwoording afleggen over risicomanagement rond cyberveiligheid. De websites geven een indruk van de informatie, initiatieven en de mate van aandacht die informatiebeveiliging krijgt op de extern beschikbare website. De aantallen die we rapporteren geven een indicatie maar geen exact beeld over de daadwerkelijke aandacht voor cyberdreigingen. Als we geen informatie in jaarverslagen of op websites vinden, betekent dat niet dat de instelling geen aandacht heeft voor informatiebeveiliging. Zo kan informatie bedoeld voor studenten of medewerkers ook op andere manieren beschikbaar gemaakt zijn – bijvoorbeeld op het intranet – en daarom niet op de openbare website te vinden zijn. Toch kunnen onze bevindingen een beeld schetsen van de diversiteit van de manieren waarop instellingen omgaan met cyberveiligheid voor de eigen organisatie. Aantallen worden daarom alleen gepresenteerd als het gaat over het aantal instellingen dat zich nu extern verantwoordt (jaarverslagen) en indien het betrekking heeft op incidentafhandeling (externe website). Er zijn immers cyberincidenten denkbaar waarbij het niet mogelijk is via het intranet na te gaan hoe een incident gemeld of opgelost kan worden.

3. Gesprekken met veertien instellingen.
In de gesprekken met de veertien instellingen konden we dieper ingaan op de invulling van de aandacht voor cyberveiligheid. Bij vrijwel alle gesprekken waren zowel bestuurders als verantwoordelijken voor de informatiebeveiliging en ICT aanwezig. Het huidige onderzoek is inventariserend van aard. Door het beperkt aantal gesprekken zijn de resultaten die we presenteren op basis van de gesprekken dan ook niet representatief voor het hele hoger onderwijsveld. Bij de selectie van universiteiten en hogescholen hebben we vooral gezocht naar diversiteit (mede op basis van de uitkomsten van de deskresearch en de gesprekken met externen) om zo de breedte van vraagstukken binnen het hoger onderwijs aan bod te laten komen. Bij de resultaten wordt aangegeven of het een voorbeeld is op basis van één gesprek, of dat het voorbeeld voorkwam in meerdere, of in alle gesprekken. Een lijst van de universiteiten, hogescholen en rechtspersonen voor hoger onderwijs die we hebben gesproken, is opgenomen in bijlage I.

4. Analyse van diverse websites, nieuwsberichten en tijdens het onderzoek verkregen documenten (zoals plannen en evaluaties).
Gedurende het hele onderzoek stuitten we op nieuwe publicaties over ontwikkelingen rond cyberveiligheid van Nederlandse bedrijven en overheidsorganisaties en nieuwsberichten over aanvallen binnen en buiten het onderwijs. Ook hebben we diverse websites geanalyseerd van partijen die zich bezighouden met cyberveiligheid en ontvingen we geregeld aanvullende documenten en achtergrondinformatie van onze gesprekspartners. Deze informatie is benut om de bevindingen in een breder perspectief te plaatsen, in het bijzonder als het gaat om kenmerken van onderwijsinstellingen. Wanneer we bij de bevindingen spreken over grote versus zeer kleine ho-instellingen, hebben we het over grote universiteiten of hogescholen met bijvoorbeeld meer dan twintig- of dertigduizend studenten, versus de allerkleinste instellingen die onderwijs verzorgen in nicemarkten aan in totaal slechts enkele tientallen studenten. De omvang van het personeelsbestand van de allerkleinste onderwijsinstellingen kan vergeleken worden

[8] Er zijn 9 rpho's niet meegenomen in de analyse van jaarverslagen, omdat we van deze instellingen niet over de jaarverslagen van 2018 én 2019 beschikken.
[9] Er zijn 7 rpho's niet meegenomen in de analyse van de websites. Dit betreft vier rpho's die in afbouw zijn. Daarnaast zijn 3 rpho's verbonden aan een bekostigde hogeschool. Op het vlak van cyberveiligheid hebben deze instituten geen zelfstandige website.

met de omvang van het midden- en kleinbedrijf (MKB). De informatie uit aanvullende documenten hebben we gebruikt om onze bevindingen uit de gesprekken met ho-instellingen en de analyses van websites en jaarverslagen nader te duiden en in een bredere context te plaatsen.

Waar functioneel hebben we binnen dit onderzoek ook naar andere externe dreigingen gekeken, zoals gezondheidsrisico's (waaronder het omgaan met de COVID-19 pandemie), fysieke veiligheid, sociale veiligheid en kennisveiligheid. Deze voorbeelden zijn bekeken om de afwegingen die betrokkenen rond cyberveiligheid maken te vergelijken met de afwegingen die zij maken rond andere externe dreigingen, en cyberveiligheid zo in een breder kader te kunnen plaatsen.

1.6 Leeswijzer

Dit rapport is opgebouwd uit drie delen. Deel A bestaat naast deze inleiding uit een achtergrondhoofdstuk. Dat hoofdstuk bevat een schets van het concept cyberveiligheid en van de ontwikkelingen binnen cyberveiligheid. In Deel B worden onze bevindingen beschreven aan de hand van de zeven standaarden. In elk van de zeven hoofdstukken staat één standaard centraal. We beschrijven de bevindingen eerst op het niveau van de instelling hoger onderwijs (eerste en tweede paragraaf). Daarna beschrijven we de bevindingen op het niveau van het stelsel hoger onderwijs (derde en vierde paragraaf). We starten zowel het instellings- als het stelseldeel met de definitie van de standaard. Op het instellingsniveau hanteren wij de standaarden zoals deze door de overheid voor bestuurders zijn vertaald, zie ook paragraaf 1.4. De standaarden op stelselniveau hebben we geformuleerd aan de hand van de gesprekken met deskundigen en belanghebbenden. We vatten na de definitie van iedere instellings- en stelselstandaard de bevindingen van ons onderzoek samen in de sterktes, zwaktes, kansen en bedreigingen. Daarna volgt een uitgebreide uiteenzetting van alle bevindingen. Elk van de hoofdstukken is afzonderlijk te lezen. In Deel C beantwoorden we op basis van de bevindingen onze onderzoeksvragen, we presenteren onze conclusies en doen aanbevelingen.

2 Achtergrond: cyberveiligheid en ontwikkelingen

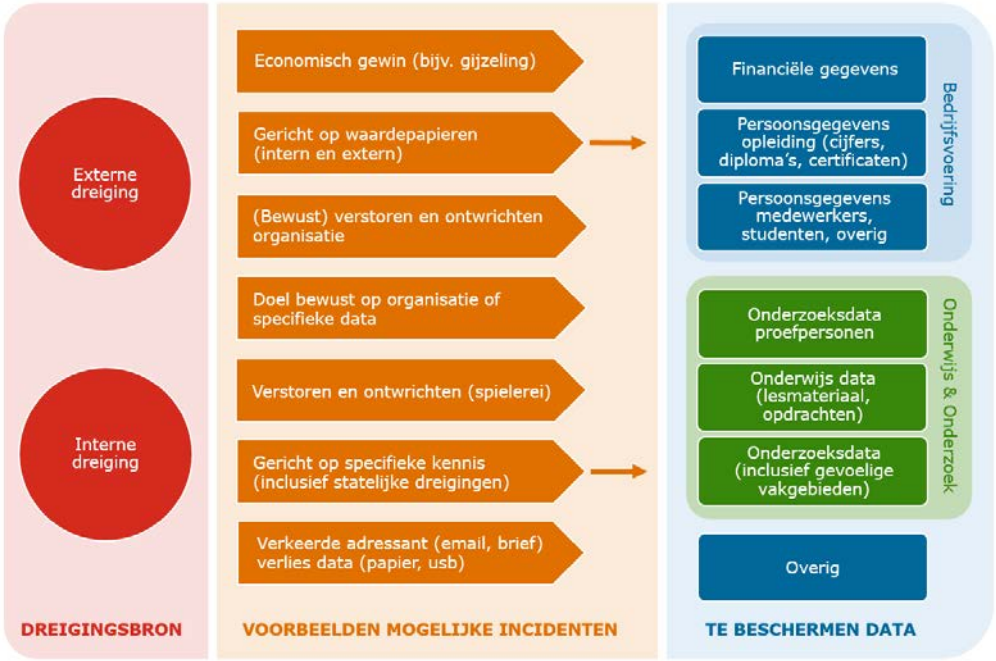
In dit hoofdstuk geven we een introductie op het onderwerp cyberveiligheid. We bespreken verschillende soorten cyberdreigingen (paragraaf 2.1), cyberveiligheid in het hoger onderwijs (paragraaf 2.2), belangrijke actoren voor het hoger onderwijs (paragraaf 2.3) en ontwikkelingen in andere sectoren (paragraaf 2.4).

2.1 Soorten cyberdreigingen

Volgens het meest recente cyberdreigingsbeeld uitgebracht door de NCTV[10] wordt cybersecurity gedefinieerd als:

> Het geheel aan maatregelen om (relevante) risico's tot een aanvaardbaar niveau te reduceren. De maatregelen kunnen zijn gericht op het voorkomen van cyberincidenten en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau is, is de uitkomst van een risicoafweging.

Figuur 2.1a Een schematisch overzicht van de oorsprong (links), de mogelijke vormen (midden) en de mogelijke doelen (rechts) van cyberdreigingen.



In figuur 2.1a hebben we een schematische overzicht gemaakt van de mogelijke oorsprong, de mogelijke vormen, en mogelijke doelen van cyberdreigingen. Cyberincidenten kunnen een oorsprong buiten of binnen de organisatie hebben (externe of interne dreigingsbron). Externe dreigingsbronnen zijn bijvoorbeeld hackers die proberen het netwerk binnen te dringen. Interne dreigingsbronnen zijn bijvoorbeeld medewerkers die fouten maken in hun handelen of falende techniek. De meeste interne incidenten vinden onbedoeld plaats. Door menselijk falen kunnen er bijvoorbeeld datalekken ontstaan doordat een usb-stick is verloren of een email

[10] 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)

verkeerd is geadresseerd. Het aantal medewerkers en studenten dat hiervan hinder ondervindt is beperkt. Indien er sprake is van opzet – zoals bij een gijzeling voor economisch gewin, het ontwrichten van een organisatie, of verkrijgen van specifieke data – kan er eerder hinder voor een gehele organisatie optreden. De aantrekkelijkheid van een onderwijsinstelling hangt af van het doel van het incident. Aanvallen gericht op specifieke kennis (waaronder statelijke dreiging) kan bijvoorbeeld interessant zijn wanneer een onderwijsinstelling belangwekkend toegepast onderwijs verzorgt of innovatieve wetenschappelijke ontdekkingen heeft gedaan. Als het doel gericht is op specifieke onderwijs- of onderzoekskennis, kunnen zowel grote als kleine instellingen interessant zijn. De omvang alleen kan echter ook een rol spelen; grote instellingen zijn mogelijk aantrekkelijker voor losgeldeisen en incidenten gericht op waardepapieren.

In tabel 2.1a staat een niet uitputtend overzicht van mogelijke cyberincidenten en risico's die door het Nationaal Crisisplan Digitaal zijn geïdentificeerd met daarbij door ons ingevulde voorbeelden die specifiek zijn voor het onderwijs. De voorbeelden laten zien dat cyberincidenten plaats kunnen vinden in ieder type organisatie en in iedere sector. Het risico ontstaat vanuit de dreiging en laat zich niet inperken tot universiteiten dan wel hogescholen of tot een vorm van bekostiging. Ook de traditionele onderverdelingen tussen sectoren in het onderwijs (van primair tot hoger onderwijs) is op het vlak van cyberrisico's minder relevant. Het specifieke doel van de cyberdreiging bepaalt of een instelling aantrekkelijk is en daarmee kwetsbaar. Wanneer de aanvaller bijvoorbeeld geïnteresseerd is in het verkrijgen van kennis, richt hij of zij zich op aanbieders van bepaalde soorten fundamenteel of toegepast onderzoek. Als het doel is het verkrijgen van geld, zal de aanvaller zich richten op partijen waar potentieel gemakkelijk betaald wordt. Daarnaast kunnen instellingen verschillen in aantrekkelijkheid door de bekendheid van een instituut.

Tabel 2.1a Mogelijke cyber-incidenten en risico's die door het Nationaal Crisisplan Digitaal zijn geïdentificeerd met voorbeelden voor het onderwijs.

Mogelijke cyber-incidenten en risico's geïdentificeerd door het Nationaal Crisisplan Digitaal[11]	**Voorbeelden voor het onderwijs**
Lek: aantasting van de vertrouwelijkheid als gevolg van natuurlijk, technisch of menselijk falen	Datalek (AVG-gerelateerd) door onbedoeld open staan van delen van het netwerk voor onbevoegden of door medewerker of student als gevolg van email aan verkeerd geadresseerde(n) of verlies van opslagbron (laptop, usb-stick, externe harde schijf).
Storing/uitval: aantasting van de integriteit of beschikbaarheid als gevolg van natuurlijk, technisch of menselijk falen	Stroomuitval eventueel in combinatie met niet functionerende back-up waardoor systemen geheel of gedeeltelijk onbereikbaar zijn.
Systeemmanipulatie: aantasting van informatiesystemen of –diensten; gericht op de vertrouwelijkheid of integriteit van systemen of –diensten. Deze worden daarna ingezet om andere aanvallen uit te voeren.	Cyberaanval die een organisatie verstoort, gericht op economisch gewin door een losgeldeis (ransomware na bijv. malware) eventueel in combinatie met dreigen AVG/privacy gevoelige informatie openbaar te maken of te verkopen.

[11] 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)

Spionage: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie door statelijke of staatsgelieerde actoren.	Oneigenlijk verkrijgen van toegang of data tbv statelijke actoren (digitale spionage) gericht op specifieke vakgebieden, kroonjuwelen van een instelling of die onder kennisembargo vallen.
Informatiediefstal: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie.	Verkrijgen van toegang tot systemen voor bedrijfsvoering, onderwijs en onderzoek gericht op kopiëren of wegnemen van data door een externe of interne partij.
Informatiemanipulatie: aantasting van de integriteit van informatie door het opzettelijk wijzigen van informatie.	Verkrijgen van toegang tot systemen voor studievoortgang, diplomaregistratie of onderzoeksgegevens waarna data kan worden gemanipuleerd (fraude plegen) door studenten, medewerkers of een externe partij.
Verstoring/sabotage: het opzettelijk aantasten van de beschikbaarheid van informatie, informatiesystemen of –diensten.	Cyberaanval gericht op ontwrichting van de organisatie (bijv. Ddos-aanval) doelbewust of als spielerei door een externe of interne partij.

2.2 Cyberveiligheid in het (hoger) onderwijs

Het hoger onderwijs is om verschillende redenen aantrekkelijk voor digitale criminelen en het aantal cyberincidenten neemt dan ook toe. Het Cyberdreigingsbeeld Onderwijs en Onderzoek 2020-2021[12] laat zien dat het aantal dreigingen in het ho en het mbo toeneemt ten opzichte van het voorgaande jaar. Nadere analyse leerde de onderzoekers dat financieel gewin het meest voorkomende doel is, en dat er een stijging lijkt te zijn van dreiging afkomstig van statelijke actoren. Dreigingen zijn daarnaast vaker afkomstig van partijen die samenwerken bij een aanval. Ook worden aanvallen complexer doordat geavanceerdere software wordt ingezet.

Indien instellingen een vermoeden hebben dat persoonsgegevens in handen van derden zijn gekomen, zijn zij verplicht een melding maken bij de Autoriteit Persoonsgegevens (AP). Uit het jaarbericht 2019[13] van de AP blijkt dat 3 procent van de meldingen van datalekken bij de AP het gevolg is van *hacking*, *malware* (waaronder *ransomware*) en/of *phishing*. In 2020[14] is het totaal aantal meldingen bij de AP afgenomen, maar is het aantal meldingen van een datalek naar aanleiding van *hacking*, *malware* en *phishing* verder gestegen tot 5 procent van de meldingen. De onderwijssector wordt relatief vaak getroffen. In 2019 kwamen de meeste meldingen uit de sector zakelijke dienstverlening, gevolgd door de sectoren zorg en onderwijs. In het jaar 2020 kwam dit type datalek het meeste voor in de sectoren zorg en onderwijs. Hoewel dit type datalekken een klein aandeel in het totaal aantal meldingen is, is het aantal personen dat getroffen is per melding vaak groot. Dat zagen we ook bij de aanval op de Universiteit Maastricht waardoor alle bijna 19.000 studenten en 4.000 medewerkers geen toegang meer hadden tot het netwerk van de onderwijsinstelling. We zien dat de voortgang van onderwijs en onderzoek bij

[12] 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)

[13] 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)

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

instellingen voor hoger onderwijs vrijwel volledig afhankelijk is van digitale netwerken.

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 zijn er veel verschillende behoeftes en wensen ten aanzien van de ICT-voorzieningen. Het hoger onderwijs heeft een open karakter waarin samenwerking en kennisdelen wordt gestimuleerd om innovatie te bevorderen/ondersteunen. Dat vereist een op maat gesneden beveiliging van het ICT-netwerk. Het bekostigde hoger onderwijs kent bovendien een gelaagde bestuursstructuur met verschillende bestuursorganen: op centraal niveau wordt een ho-instelling aangestuurd door het CvB en op decentraal niveau bestaat de organisatie uit decanen/directeuren op faculteits-/domeinniveau, onderwijs- en onderzoekdirecteuren op opleidingsniveau, en professoren/lectoren/(hoofd)docenten op afdelings-/vakgroep-/onderzoeksniveau. Het ICT en cyberveiligheidsbeleid speelt zich af op al die verschillende niveaus en verlangt daarom ook aandacht voor een goede ICT-beveiliging op alle niveaus. De gelaagde bestuursstructuur van universiteiten en bekostigde hogescholen is vastgelegd in de WHW. Voor rpho's zijn in de wet geen voorschriften ten aanzien van de aansturing binnen de instelling vastgelegd.

Sinds de cyberaanval op de Universiteit Maastricht eind 2019, is cyberveiligheid extra onder de aandacht gekomen. De minister van OCW heeft de Kamer op 14 februari 2020[15], 3 juli 2020[16] en 19 mei 2021[17] geïnformeerd over de aanpak van cyberveiligheid in het onderwijs en de voortgang van maatregelen die de sector neemt naar aanleiding van de cyberaanval. Deze maatregelen hebben betrekking op verschillende facetten van cyberveiligheid waaronder vergroten bewustzijn van cyberdreigingen, borging cyberveiligheid in risicomanagement van onderwijsinstellingen en ketensamenwerking. De minister geeft in deze kamerbrieven aan dat goede samenwerking op het gebied van kennis- en informatiedeling tussen ho-instellingen over cyberrisico's, monitoring en detectie van cyberaanvallen de cyberveiligheid ten goede komt. Ook roept de minister in haar brief van 19 mei 2021 instellingen op hun cyberveiligheidsbeleid op te nemen in de jaarverslaglegging wanneer dit nog niet het geval is, structureel te bespreken met hun Raden van toezicht, en een meerjarenvisie ten aanzien van het cyberveiligheidsbeleid te presenteren. Daarnaast zal het onderwerp cyberveiligheid expliciet worden meegenomen in de reguliere gesprekken die het ministerie met instellingen en koepels voert.

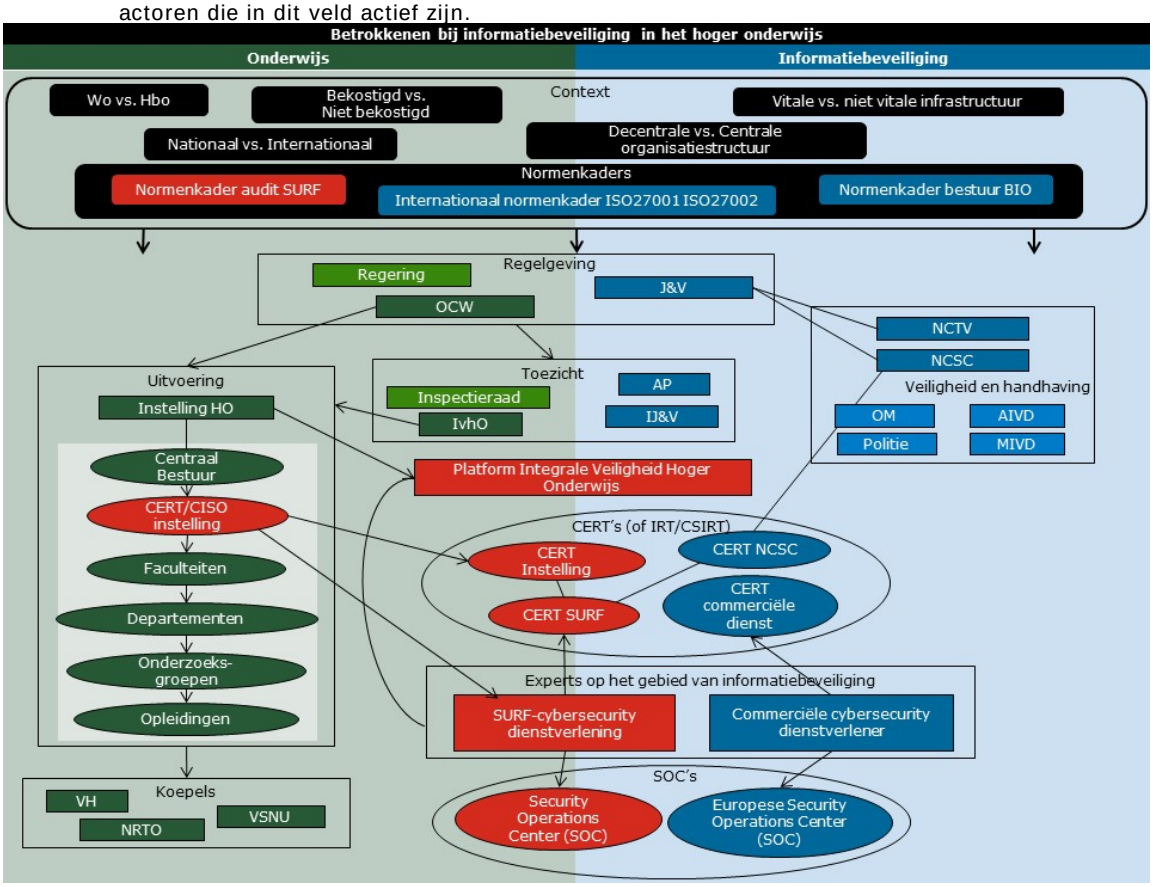
In 2020 werd met de uitbraak van COVID-19 de afhankelijkheid van de digitale infrastructuur voor ho-instellingen nog groter. Instellingen zetten het studiejaar 2019/2020 vanaf 12 maart online voort. Het nieuwe studiejaar 2020/2021 startte gedeeltelijk via digitaal onderwijs, maar werd volledig online vanaf 16 december 2020 tot 26 april 2021, toen er sprake was van de tweede lockdown. Het abrupt overgaan naar digitaal onderwijs in de eerste lockdown bracht ook andere digitale risico's in beeld, zoals digitale storingen waardoor tentamens niet konden worden afgenomen. Ook waren en vragen over privacybescherming naar aanleiding van controle op fraude bij tentaminering via online proctoring. Met COVID-19 is de gehele hoger onderwijssector geconfronteerd met de afhankelijkheid van de eigen ICT-infrastructuur en organisatie.

[15] Tweede Kamer, vergaderjaar 2019–2020, 31 288 en 26 643, nr. 832.
[16] Tweede Kamer, vergaderjaar 2019–2020, 31 288 en 26 643, nr. 872.
[17] Tweede Kamer, vergaderjaar 2020-2021, 31 288 en 26 643, nr 910.

2.3 Betrokken actoren bij cyberveiligheid in het hoger onderwijs

Figuur 2.3a geeft een overzicht van de wereld van cyberweerbaarheid in het hoger onderwijs en de verschillende actoren die in dit veld actief zijn. De figuur laat zien dat er twee systeemwerelden zijn die voor een groot deel naast elkaar bestaan: onderwijs en cyber. Het voert te ver om binnen dit rapport voor elk van de actoren te beschrijven wat hun taken zijn. Daarnaast zijn er partijen actief die niet opgenomen zijn in deze figuur. Het overzicht heeft niet tot doel compleet te zijn, maar om inzicht te geven in het complexe netwerk met betrekking tot cyberweerbaarheid. We concentreren ons in dit onderzoek met name op de plekken waar de netwerken van onderwijs en cyber elkaar raken.

Figuur 2.3a Een overzicht van de wereld van cyberweerbaarheid in het hoger onderwijs en de actoren die in dit veld actief zijn.



Actoren informatiebeveiliging binnen instelling hoger onderwijs

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 uitvoeren. 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). Risicomanagement ten behoeve van de informatiebeveiliging beperkt zich niet tot de ICT-afdeling, maar behoort plaats te vinden binnen alle lagen van de organisatie. De kennis en verantwoordelijkheid van

proces- en systeemeigenaren, zoals de CISO en de CERT, zal met vaste regelmaat moeten worden gedeeld met het bestuur. Een bestuur kan alleen de juiste beslissingen nemen als de relevante informatie hem bereikt.

Het onderwijsstelsel: SURF als centrale spil

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. SURF is een coöperatieve vereniging van Nederlandse onderwijs- en onderzoeksinstellingen waarin de leden gezamenlijk digitale diensten inkopen of ontwikkelen. De bekostigde onderwijsinstellingen zijn als leden ook eigenaar van SURF. Via verschillende acties, evenementen, *special interest groups* en mailinglijsten werkt ze aan de kennisuitwisseling- en bevordering. Daarnaast verkoopt SURF diensten en producten aan particulieren, studenten en organisaties, waaronder particuliere onderwijsinstellingen (ook rpho's). SURF brengt jaarlijks het in de vorige paragraaf vermelde cyberdreigingsbeeld uit met trends in dreigingen voor het onderwijs en onderzoek. SURF verzorgt voorlichting en coördineert de uitvoering van informatiebeveiliging, bijvoorbeeld door digitale veiligheidsaudits en ondersteuning bij beveiligingsincidenten. Dit krijgt vorm door deelname van instellingen voor hoger onderwijs aan het zogenaamde SURF-CERT. SURF-CERT is een team dat onderwijsinstellingen ondersteuning biedt bij beveiligingsincidenten. Alle grote bekostigde universiteiten en universitaire medische centra zijn bij SURF en het SURF-CERT aangesloten. De meeste bekostigde hogescholen zijn aangesloten bij SURF, waarvan 94 procent ook aangesloten is bij SURF-CERT. SURF-CERT is sinds 24 januari 2020[18] door de minister van Justitie en Veiligheid aangewezen als één van de informatieknooppunten van niet-vitale infrastructuren die in nauw contact staat met Nationaal Cyber Security Centrum (NCSC). Het SURF-CERT is daardoor in staat om actuele informatie over cyberdreigingen van en met het NCSC te kunnen delen. Niet-bekostigde instellingen zijn niet als leden aangesloten bij SURF, maar kunnen als klant wel gebruik maken van de diensten van SURF.

Platform Integraal Veilig Hoger Onderwijs verbindt veiligheidsthema's

Een tweede partij naast SURF, die handreikingen verzorgt op het vlak van diverse mogelijke crises is het Platform Integraal Veilig Hoger Onderwijs (Platform IV-HO). Handreikingen gaan over een integraal veilige aanpak, crisismanagement en door het platform gedefinieerde thema's. Het platform IV-HO richt zich op het bekostigde onderwijs en wil onderwijsinstellingen de mogelijkheid bieden informatie met elkaar uit te wisselen en van elkaar te leren. Universiteiten en hogescholen trekken in het platform gezamenlijk op. Het platform IV-HO stelt daarbij 9 thema's centraal: 1. Integriteit, 2. Arbo en milieu, 3. Sociale veiligheid, 4. Zorgwekkend gedrag en radicalisering, 5. Gebouwveiligheid, BHV en fysieke veiligheid, 6. Internationalisering, 7. Informatieveiligheid, 8. Privacy, en 9. Kennisveiligheid en ongewenste beïnvloeding. In 2021 bracht het Platform IV-HO voor de tweede keer het risico- en dreigingsbeeld hoger onderwijs[19] uit. Dit beeld geeft een risicoschatting net als het cyberdreigingsbeeld van SURF, waarbij ook andere IV thema's die een ho-instellingen kunnen bedreigen zijn opgenomen. In het recente dreigingsbeeld worden informatieveiligheid en privacy als belangrijkste thema's voor dreigingen aangemerkt. Daarnaast worden ook risico's op het thema sociale veiligheid hoog geacht onder andere door polarisatie, psychische problematiek, grensoverschrijdend gedrag, radicalisering en discriminatie.

[18] Dit is bepaald in de regeling aanwijzing computercrisisteams, Staatscourant 2020, 4410.
[19] 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 (geraadpleegd op 20-7-2021)

Actoren in vitale en niet-vitale infrastructuren

De 'Wet beveiliging netwerk- en informatiesystemen' (Wbni) is erop gericht de digitale weerbaarheid van Nederland te vergroten, de gevolgen van cyberincidenten te beperken en zo maatschappelijke ontwrichting te voorkomen. Sinds het inwerkingtreden van de Wbni geldt voor aanbieders van een vitale infrastructuur een zogenaamde zorgplicht. Deze aanbieders behoren adequate maatregelen te nemen voor de beveiliging van hun netwerk- en informatiesystemen. Ook zien de verschillende sectorale toezichthouders erop toe dat de vitale diensten zo veel mogelijk aan deze zorgplicht proberen te voldoen. De overheid heeft deze vitale infrastructuur gedefinieerd als organisaties die zich bezig houden met 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[20]). Voorbeelden van de vitale processen zijn elektriciteit, toegang tot internet, drinkwater en betalingsverkeer. Voor organisaties en bedrijven in Nederland die geen onderdeel uitmaken van de vitale infrastructuur kent de sectorwetgeving over het algemeen 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.

NCTV namens de overheid verantwoordelijk voor cybersecurity

De NCTV is verantwoordelijk voor terrorismebestrijding, cybersecurity, nationale veiligheid, crisisbeheersing en statelijke dreigingen. De NCTV valt onder de verantwoordelijkheid van de minister van Justitie en Veiligheid[21]. De NCTV heeft het 'Nationaal Crisisplan Digitaal (NCP-Digitaal)' opgesteld[22]. Dit plan beschrijft op hoofdlijnen de crisisaanpak op rijksniveau en de samenwerking en aansluiting met betrokken publieke en private partners en netwerken op internationaal en regionaal niveau. Instellingen in het hoger onderwijs hebben zelf geen rechtsreeks contact met het NCTV.

Het NCSC verzamelt en verspreidt informatie over dreigingen

Het NCSC (Nationaal Cyber Security Centrum) is net als het NCTV onderdeel van het ministerie van Justitie en Veiligheid. De taken van het NCSC op het gebied van cybersecurity zijn wettelijk vastgelegd in de Wet beveiliging netwerk- en informatiesystemen (Wbni) sinds november 2018[23]. Organisaties in vitale sectoren zijn verplicht om ernstige digitale veiligheidsincidenten te melden bij het NCSC. Wanneer er dreigingen of kwetsbaarheden zijn, verspreidt het NCSC informatie onder de verschillende informatieknooppunten. De verschillende informatieknooppunten zijn vervolgens verantwoordelijk voor het informeren en bijstaan van hun doelgroepen. Het (hoger) onderwijs valt niet onder de meldplicht omdat zij niet behoort tot de vitale infrastructuren. Begin 2020 is een viertal CERTs waaronder het Z-CERT (zorg) en het SURF-CERT (onderwijs) aangewezen op grond van de Wet beveiliging netwerk- en informatiesystemen om vertrouwelijke informatie van en met het NCSC te kunnen delen. Dat is belangrijk, omdat zorg en onderwijs geen vitale sectoren zijn en zij zonder deze afspraak dus verstoken zouden blijven van informatie.

---

[20] Voor meer informatie zie: https://www.nctv.nl/onderwerpen/vitale-infrastructuur (geraadpleegd op 19-7-2021)
[21] Voor een nadere toelichting op het NCTV zie https://www.nctv.nl/organisatie (geraadpleegd op 19-7-2021)
[22] NCTV (februari 2020) *Nationaal Crisisplan Digitaal*. Den Haag: Nationaal Coördinator Terrorisme bestrijding en Veiligheid. Zie: https://www.nctv.nl/documenten/publicaties/2020/02/21/nctv-nationaal-crisisplan-digitaal-_-webversie (geraadpleegd op 19-7-2021)
[23] Voor meer informatie over de wettelijke taak van het NCSC zie: https://www.ncsc.nl/over-ncsc/wettelijke-taak (geraadpleegd op 19-7-2021)

2.4 Ontwikkelingen in andere sectoren

Cyberveiligheid is een onderwerp dat breder in de Nederlandse samenleving in de belangstelling staat. De NCTV publiceert jaarlijks het Cybersecuritybeeld Nederland (CSBN). In deze rapportage gaat ze in op de ontwikkelingen op het vlak van digitale dreigingen, belangen en weerbaarheid van met name de vitale infrastructuur (voor uitleg vitale versus niet-vitale infrastructuur, zie paragraaf 2.4). Vanuit nationale veiligheid kijkt men naar risico's van sabotage en spionage, en naar risico's van uitval van digitale diensten, processen of systemen. Het CSBN 2020[24] laat zien dat digitale risico's onverminderd groot zijn. De werkwijze en de middelen die door criminele actoren wordt ingezet is grotendeels gelijk gebleven. Actoren maken gebruik van bekende kwetsbaarheden en *phishing* is de meest gebruikte eerste stap bij een aanval. Het CSBN 2020 geeft aan dat er nog geen totaalbeeld is van de cyberweerbaarheid van de vitale infrastructuur in Nederland. Wel is duidelijk dat de weerbaarheid niet op orde is doordat basismaatregelen ontbreken. Zo vraagt *phishing* om voortdurende alertheid, voeren organisaties niet altijd tijdig beveiligingsupdates uit en is vroegtijdige detectie van aanvallen een aandachtspunt. Het CSBN 2020 geeft aan dat het verhogen van de digitale weerbaarheid een gezamenlijke opgave is van technische experts en vooral een vraagstuk van governance en/of risicomanagement voor bestuurders. Het Cybersecuritybeeld Nederland 2021[25] gaat voort op het CSBN 2020. In het afgelopen jaar vonden in Nederland talloze cyberincidenten plaats, waarbij COVID-19 werd aangegrepen voor het doen van aanvallen. De weerbaarheid is nog niet voldoende aangezien er nog niet of niet voldoende sprake is van het nemen van basismaatregelen zoals sterke wachtwoorden en tijdig *patchen*[26] van kwetsbaarheden. Verschillen tussen bedrijven zijn op dit vlak groot. Ook omdat grote bedrijven kunnen investeren in kennis en kunde op het vlak van cyberveiligheid, terwijl kleinere bedrijven veelal niet over de expertise en middelen beschikken. Het CSBN 2021 onderstreept het belang dat cyberveiligheid niet alleen vanuit een technische invalshoek moet worden benaderd.

Naast het CSBN van de NCTV maakt het CBS een cybersecuritymonitor[27] die de cyberweerbaarheid van bedrijven in Nederland in kaart brengt. De monitor wordt al enkele jaren gemaakt en is gebaseerd op een ICT enquête onder 20.000 bedrijven waarin onder andere is gevraagd naar het inzetten van twaalf verschillende ICT-veiligheidsmaatregelen. Voor elk van de maatregelen geldt dat deze vaker wordt ingezet door grotere bedrijven dan door kleinere. Een veiligheidsmaatregel die steeds meer wordt toegepast is het gebruik van een token voor inloggen (twee-factor authenticatie). In vergelijking tot voorgaande jaren stagneert bij grotere bedrijven de toename van het aantal maatregelen, terwijl bij de kleinste bedrijven het aantal maatregelen nog toeneemt. De CBS-monitor laat tevens zien dat grotere bedrijven de ICT-beveiliging vaker uitbesteden, terwijl bij de kleinste bedrijven vaker uitsluitend het eigen personeel de ICT-beveiliging verzorgt. Een mix met eigen personeel en een extern bedrijf komt bij de grootste bedrijven het meeste voor.

---

[24] 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 (geraadpleegd op 19-7-2021)

[25] 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)

[26] Een patch is een nieuwe versie van software. In deze nieuwe versie heeft de leverancier kwetsbaarheden in het systeem hersteld. Hij heeft geen nieuwe functies toegevoegd. (uit: P. Oldengarm & L. Holterman (redactie) *Cybersecurity Woordenboek. Van cybersecurity naar Nederlands.* 2e druk. Den Haag Cyberveilig Nederland. Zie: www.cyberveilignederland.nl/woordenboek (geraadpleegd 26 juli 2021))

[27] 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)

De afgelopen jaren heeft ook de Cyber Security Raad (CSR) het kabinet van diverse adviezen over cyberveiligheid voorzien. In maart 2021[28] verscheen een advies waarin de belangrijkste speerpunten voor de volgende kabinetsperiode worden benoemd. Een van die speerpunten is dat bedrijven soms een (te beperkt) inzicht kunnen verkrijgen in mogelijke cyberaanvallen doordat in Nederland gekozen is om belangrijke acute dreigingsinformatie slechts met een deel van de bedrijven en organisaties te delen. Het gaat in het bijzonder om specifieke dreigingsinformatie, die het Nationaal Cyber Security Center (NCSC) alleen deelt met bedrijven die vitaal zijn voor de Nederlandse infrastructuur, maar niet met andere bedrijfstakken. Bedrijven kunnen alleen meer algemene informatie over cyberdreigingen delen via het Digital Trust Center (DTC). In juli 2021[29] informeerde de minister van Justitie en Veiligheid de Kamer dat hij aan een voorstel tot wijziging van de Wbni werkt zodat het NCSC meer dreigings- en incidentinformatie met betrekking tot netwerk- en informatiesystemen kan delen met partijen in niet-vitale sectoren via het DTC. Net als in eerdere adviezen roept de CSR in zijn advies op om zorg te dragen voor het opleiden van voldoende gekwalificeerde cyberveiligheidsexperts en het investeren in programma's om kennis van deze experts *up to date* te houden. Ook roept het CSR op om te denken over zorgplicht voor leveranciers van digitale producten en diensten, zodat er een minimum veiligheidsniveau voor leveranciers komt.

Het kabinet heeft cyberveiligheid op de agenda staan. Op 20 maart 2020 heeft de minister van Justitie en Veiligheid de Tweede Kamer een kabinetsreactie[30] gestuurd op het verschenen WRR rapport over "Digitale Ontwrichting"[31]. In de kabinetsreactie is aangegeven dat de Inspectieraad wordt gevraagd om te komen met een voorstel voor hoe brede samenwerking en afstemming tussen de rijksinspectie en toezichthouders op cybersecurity het beste tot stand kan worden gebracht. In de reactie gaat de minister van JenV tevens in op de ontwikkelingen van het landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden (LDS). Binnen het LDS wordt informatie over dreigingen, incidenten en kwetsbaarheden gedeeld tussen publieke en private partijen. Onder coördinatie van de Inspectie Justitie en Veiligheid verscheen in juni 2021 het eerste samenhangende inspectiebeeld[32]. Dit beeld richt zich op de ontwikkelingen in het toezicht in de vitale sectoren op het onderwerp cyberveiligheid. Deze eerste gezamenlijke rapportage laat zien dat ook het toezicht in ontwikkeling en beweging is. Toezichthouders maken jaarlijks op basis van sectorspecifieke afwegingen keuzes voor het toezicht. De scope en onderwerpen die in verschillende sectoren aandacht krijgen verschilt daarom per toezichthouder. Daarnaast is de kennis en expertise over cyberveiligheid bij toezichthouders op vitale processen verschillend.

[28] 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)
[29] Tweede Kamer, vergaderjaar 2020-2021, 26 643 nr. 767.
[30] Tweede Kamer, vergaderjaar 2019-2020, 26 643, nr. 673.
[31] WRR (2019) WRR-Rapport 101: *Voorbereiden op digitale ontwrichting*, Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid. Zie: https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting (geraadpleegd op 19-7-2021)
[32] 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)

DEEL B: BEVINDINGEN – CYBERVEILIGHEID IN HET HOGER ONDERWIJS

1 Standaard 1: vergroten bewustzijn

1.1 Instellingen hoger onderwijs

Definitie van de standaard voor instellingen:

Bestuurders agenderen tijdens overleggen met regelmaat het belang van informatiebeveiliging. Er bestaan bewustwordingsmaatregelen onder studenten, onderzoekers, docenten en medewerkers die met regelmaat worden ingezet.

Sterktes

- Ho-instellingen doen veel rond het vergroten van bewustzijn bij het verwerken van persoonsgegevens. Hierbij is duidelijk sprake van een groot bewustzijn en een breed gevoelde verantwoordelijkheid in de instelling.
- Er is overeenstemming over vier aspecten die samenhangen bij het vergroten van het bewustzijn: basisinformatie of algemene voorlichting over ICT en ICT-beveiliging, *awareness* campagnes, *security by design* en laagdrempelig en veilig melden. Met *awareness* campagnes alleen ben je er niet.

Zwaktes

- Als het gaat om het vergroten van het bewustzijn ligt de focus op privacygegevens en minder op brede informatiebeveiliging.
- Bij het risicomanagement zien we dat het bewustzijn van technische kwetsbaarheden niet altijd doordringt tot op beslisniveau; dit geldt daarmee ook voor het vergroten van het bewustzijn.

Kansen

- Er is toenemend bewustzijn van het gevaar en besturen zijn zich bewust van het belang van *awareness* campagnes. Daarnaast is er meer bewustzijn van de integraliteit van ICT en het primair proces. Besturen kiezen voor een aanpak die past bij de instelling.
- Door de coronacrisis is het onderwijs meer afhankelijk geworden van digitale middelen. Daarmee is de aandacht voor veilig werken gegroeid. Dit kan als vliegwiel voor de bewustwording werken, zoals de invoering van de AVG dat deed voor de omgang met privacygevoelige gegevens.

Bedreigingen

- Het bewustzijn verdwijnt weer met het verdwijnen van risico's en met nieuwe dreigingen.
- De inzet op het vergroten van bewustzijn is soms afhankelijk van de inzet van individuele betrokkenen.
- De cultuur binnen ho-instellingen komt voor een groot deel voort uit het principe van academische vrijheid. Dit gaat niet altijd samen met een veilige inrichting van de ICT.

Toelichting op de standaard

Cyberveiligheid heeft een technische en menselijke kant. Systemen en processen zijn bij voorkeur zo ontworpen dat de kans op kwetsbaarheden zo klein mogelijk is. Toch kan een gebruiker een kwetsbaarheid creëren door bijvoorbeeld een zwak wachtwoord te gebruiken of een cyberincident veroorzaken door op een link in een, mogelijk zeer geloofwaardige, *phishing* mail te klikken. Om de risico's op beide aspecten te borgen is het nodig dat besturen binnen hun instellingen het belang van informatiebeveiliging regelmatig agenderen. Daarbij moet er aandacht zijn voor zowel de techniek, processen en actuele dreigingen als voor de bewustwording onder de studenten, onderzoekers, docenten, overige medewerkers en gasten.

Standaard 1 – vergroten bewustzijn – richt zich op de menselijke kant van cyberveiligheid. Het gaat om blijvend aandacht vragen voor het belang en de noodzaak van veilig omgaan met informatie, waardoor de organisaties en hun

gebruikers zich steeds duurzamer bewust worden van dreigingen en dat ze leren veilig digitaal te handelen. Binnen instellingen maken veel verschillende groepen gebruik van ICT-middelen. Dat zijn bijvoorbeeld de studenten, onderzoekers, docenten, staf medewerkers, administratief en facilitair personeel, gasten en natuurlijk ICT'ers zelf. Deze groepen hebben een verschillend kennisniveau ten opzichte van cyberveiligheid en maken mogelijk gebruik van andere programma's. Bij het vergroten van het bewustzijn is het van belang hier rekening mee te houden. Daarnaast richt standaard 1 zich op het bewustzijn bij bestuurders en andere spelers in het stelsel van hun verantwoordelijkheid voor cyberveiligheid, zodat zij tijdig maatregelen kunnen nemen en de benodigde investeringen kunnen doen. Ook in tijden met weinig actuele incidenten of dreigingen.

1.2 Bevindingen

Elementen voor het vergroten van bewustzijn

Uit de gesprekken met instellingsbesturen en interne betrokkenen bij de informatiebeveiliging blijkt dat instellingen zoeken naar de balans tussen beveiliging geregeld via de techniek (*security by design*) en het vergroten van het bewustzijn bij gebruikers. Ze zoeken naar de beste vormen van bewustwordingscampagnes (awareness campagnes) en wanneer die in te zetten. Als we de onderwerpen uit de gesprekken op een rij zetten komen we op vier elementen die het bewustzijn van cyberveiligheid kunnen vergroten: A) basisinformatie/voorlichting, B) *awareness*, C) *security by design*, D) laagdrempelig en veilig melden, zie tabel 1.2a.

Al deze onderwerpen kwamen in de gesprekken met instellingen in meer of mindere mate terug. Ze werden genoemd als elementen die allemaal nodig zijn bij het vergroten van het bewustzijn. Instellingen geven aan dat ze zoeken naar manieren die het beste past bij hun specifieke instelling, groot of klein, met veel zelfstandig werkende wetenschappers, vast personeel of ZZP'ers. Instellingen realiseren zich dat er meer nodig is dan ze nu doen en dat alleen gebruik maken van awareness campagnes niet genoeg is. Verschillende instellingen benadrukken hierbij het belang van het risicoprofiel van de specifieke instelling. Er zijn instellingen die op hun eigen terrein werken met gevaarlijke stoffen of juist met veel persoonsgevoelige informatie. Andere instellingen werken veel internationaal of met tijdelijke medewerkers. Deze verschillen hebben consequenties voor de benodigde ICT-beveiliging en daarmee ook voor de inhoud van bewustwordingscampagnes.

Tabel 1.2a Vier elementen die het bewustzijn van cyberveiligheid kunnen vergroten, met een beschrijving van de toepassing van het element.

Elementen die bewustzijn kunnen vergroten	Omschrijving van de toepassing van het element
A. Basisinformatie / voorlichting	Algemene bewustwording via een makkelijk vindbare website over veilig online werken. Waar makkelijk contactgegevens van de helpdesk te vinden zijn, het belang van melden van verdachte zaken wordt benadrukt, maar ook voorlichting wordt gegeven over het herkennen van *phishing* mails en de omgang met privacygevoelige informatie.

Elementen die bewustzijn kunnen vergroten	Omschrijving van de toepassing van het element
B. Awareness campagnes	Voor het vasthouden van het bewustzijn is herhaling nodig. De instellingen geven aan dat wanneer de acute dreiging weg is, dat ook zorgt voor het verslappen van de aandacht. Voor mensen is het risico pas zichtbaar als het er is. Bij diefstal uit je boekenkast is gelijk duidelijk dat je iets mist, bij diefstal uit je systemen kun je van alles kwijt zijn zonder het in de gaten te hebben. Daarnaast verandert het type dreiging met de tijd. Daarom zijn regelmatig terugkerende en wisselende awareness campagnes noodzakelijk. Uit de gesprekken halen we de volgende voorbeelden van awareness campagnes: - Simulatie *phishing* mails; - Waarschuwingsmails, waarin gewaarschuwd wordt voor *phishing* of andere acute dreiging; - Gaming omgeving voor medewerkers over cyberveiligheid gestoeld op de eigen leeromgeving van de instelling met steeds nieuwe afleveringen; - Colleges van cyberveiligheidsexperts zoals (ethisch) hackers; - Voorlichting over de omgang met privacygevoelige informatie, ook bij het doen van onderzoek; - Dashboards op de in- of externe website met daarop actuele storingen en bedreigingen; - Voorlichting geven bij de '*onboarding*' van nieuwe medewerkers; - Bij de introductie van nieuwe applicaties, veilig gebruik direct meenemen.
C. Security by design	Hierbij gaat ICT uit van de onbetrouwbaarheid van de eindgebruiker. Onwetendheid en onoplettendheid is een inherente kwetsbaarheid. Er wordt vanuit de techniek zoveel mogelijk zichtbare en onzichtbare preventie ingebouwd, zodat fouten onmogelijk zijn. Een voorbeeld hiervan is een helder toegangsbeleid. Waarbij niet iedereen overal bij kan en er periodiek, maar in ieder geval bij veranderingen in functie gecontroleerd wordt of iemand bepaalde toegang nog nodig heeft.
D. Laagdrempelig en veilig melden	Voor cyberveiligheid is het belangrijk om zoveel mogelijk meldingen te krijgen van mogelijke risico's. Om te zorgen dat gebruikers meldingen doen is het nodig dat zij zich veilig voelen en op een laagdrempelige en open manier een melding kunnen doen. (Hier gaan we verder op in bij standaard 2)

Hieronder geven we voor ieder van de in tabel 1.2a uitgewerkte elementen aan in hoeverre deze terugkomen in onze bevindingen.

A. Basisinformatie / voorlichting

Welke basisinformatie of voorlichting over ICT en cyberveiligheid geven hogescholen en universiteiten aan gebruikers?

Basisinformatie en voorlichting komt via verschillende kanalen. Bij incidenten kan het zijn dat gebruikers geen toegang hebben tot de interne omgeving (intranet), waardoor ze niet weten hoe ze moeten handelen, met wie ze contact moeten zoeken of hoe ze een incident kunnen melden. We hebben daarom onderzocht welke

informatie er op de externe websites te vinden is. Weinig instellingen hebben een algemene extern toegankelijke pagina gericht op ICT. Daar waar wel informatie te vinden is, gaat het vaak, soms zelfs alleen over privacyaspecten. Nog minder instellingen hebben een externe pagina gericht op cyberveiligheid. Daar waar wel een algemene pagina met betrekking tot cyberveiligheid is gevonden is sprake van heel diverse resultaten. Opvallend is het verschil tussen universiteiten en hogescholen. Universiteiten hebben verhoudingsgewijs veel informatie op hun website staan over ICT en ICT-beveiliging.

Op de externe websites van ho-instellingen zien we een grote diversiteit aan onderwerpen waarover voorlichting wordt gegeven. Op sommige websites kan zo goed als alle denkbare informatie over cyberveiligheid gevonden worden, maar op veel websites ook weinig of helemaal niets. De vindbaarheid is soms goed, maar meestal slecht en soms is de informatie versnipperd. Opvallend is dat de toonzetting van de informatie een gevoel van veiligheid oproept, maar soms ook juist onveiligheid en daarmee wellicht drempels oproept om te (durven) melden. In tabel 1.2b staat een overzicht met voorbeelden die we gevonden hebben op websites van ho-instellingen over algemene ICT en over cyberveiligheid. In enkele gevallen gaat het om vrij complete informatie over een beperkt aantal onderwerpen, zoals *phishing*, wachtwoord aanpassen of contactgegevens van de helpdesk. We hebben vrijwel geen openbare voorbeelden gevonden van awareness campagnes[33]. Daarnaast zien we dat bijna alle instellingen wel openbare informatie verstrekken over het privacybeleid. Bij standaard 2 gaan we hier uitgebreider op in, dat geldt ook voor de diversiteit die we zien in de gebruikte toonzetting.

Tabel 1.2b Voorbeelden van informatie op websites van ho-instellingen over algemene ICT (links) en over cyberveiligheid (rechts).

Algemeen ICT	**Cyberveiligheid**
- Software	- Basisbeveiliging
- Hardware	- Veilig gegevens opslaan en verzenden
- ICT-gedragsregels	- Incidenten (melden en/of afhandelen)
- Wachtwoord aanpassen	- Gegevensbeveiliging
- Helpdesk	- Wat te doen bij een verdachte e-mail, verlies usb, diefstal, malware
- Privacybeleid of -regelingen	- Waarschuwing voor *ransomeware*, *phishing* en spam
	- Hoe herken je *phishing*?
	- Tips, trics en tools
	- Wat is een veilig wachtwoord
	- Bewaken van je privacy
	- Advies en voorlichting over hoe je weinig digitale ‘sporen’ nalaat
	- Veilig digitaal werken
	- Responsible disclosure
	- CERT
	- Verwijzing naar websites van SURF, de Autoriteit Persoonsgegevens, het NCSC en IT Circle-Nederland, waaronder cybersaveyourself.nl en veiliginternetten.nl

[33] Bij standaard 1 beschrijven we de aanwezigheid van informatie over cyberveiligheid, zoals een algemene pagina over ICT, een pagina over cyberveiligheid en handleidingen voor medewerkers en studenten. Bij standaard 2 (veilige en open cultuur) gaan we wat dieper in op de transparantie, duidelijkheid en de toon van de informatie.

Voertaal op websites
Bij diverse ho-instellingen spreekt een (groot) deel van de medewerkers en studenten geen Nederlands, dus zal de informatie ook in andere talen aanwezig moeten zijn om het bewustzijn te bevorderen. De meeste informatie over ICT, cyberveiligheid en melden van incidenten en risico's op de websites van ho-instellingen is in het Nederlands of Engels beschikbaar. Er zijn uitschieters waarbij de website beschikbaar is in zeven talen. Niet alle pagina's zijn (even uitgebreid) vertaald. Hogescholen geven in het algemeen minder taalopties dan universiteiten. Er zijn hogescholen die naast de Nederlandse website een losse Engelstalige website hebben met een andere url. Er zijn ook hogescholen die de website alleen in het Nederlands aanbieden. De taal waarin informatie beschikbaar is, lijkt afhankelijk van de studentenpopulatie en medewerkers van een instelling.

Radboud Universiteit Nijmegen
De website van de Radboud Universiteit heeft een makkelijk vindbare en heel complete set informatie over ICT en cyberveiligheid gericht op verschillende doelgroepen. Het is een zeer functionele pagina, waar ieder op snelle wijze de informatie kan vinden die nodig is voor veilig digitaal werken. Op de website staan bijvoorbeeld een paar in het oog springende 'knoppen' waarmee men direct een melding kan doen of hulp kan zoeken bij de helpdesk. (zie www.ru.nl/beveiliging)

AVG in relatie tot informatiebeveiliging
Wat opvalt in de *websearch* en de jaarverslagen is dat wanneer er ingegaan wordt op informatiebeveiliging het meestal gaat om de algemene verordening gegevensbescherming (AVG). Deze wet is op 25 mei 2018 in werking getreden. In de gesprekken was de dominantie van de AVG minder groot. We zien dat instellingen in hun jaarverslagen veelal rapporteren over de acties die zij ondernomen hebben om hieraan te voldoen. In de *websearch* zien we dat vrijwel alle instellingen informatie verstrekken over het privacybeleid. Dit komt mede doordat voorlichting aan gebruikers over wat er gebeurt met hun persoonsgegevens een verplichting is die voortvloeit uit de wet. Dit is ook te zien aan de data van documenten op de website. Daar waar we data vonden, ging het grotendeels om stukken van 2018. Maar de aandacht voor de AVG gaat verder dan alleen het publiceren van het privacyreglement. Het is ook zichtbaar rondom het melden van risico's, kwetsbaarheden en incidenten. Het is zichtbaar dat deze wet een vliegwiel effect heeft gehad op de aandacht voor informatiebeveiliging. Het is echter ook duidelijk dat in deze jaren de focus lag op privacyaspecten en niet op het bredere onderwerp van informatiebeveiliging.

Bij zeven instellingen zien we in hun jaarverslag op welke manier ze juist vanuit een breder perspectief op cyberveiligheid bewustwording stimuleren. Overigens is er in de jaarverslagen geen toename te zien van bewustwordingscampagnes van 2018 naar 2019. Instellingen noemen verschillende vormen van bewustwordingsacties. Om het verschil in de aandacht voor AVG en brede informatiebeveiliging te illustreren hebben we een aantal voorbeelden van de acties die in de jaarverslagen worden vermeld onder elkaar gezet.
Op het gebied van privacy geven instellingen aan dat:

- er in multidisciplinaire projectgroepen aandacht wordt gegeven aan AVG, zodat het niet alleen een ICT onderwerp blijft;
- bewustwordingscampagnes rondom de AVG veelal worden uitgevoerd onder leiding van de functionaris gegevensbescherming;
- er voorlichting en scholing wordt gegeven over AVG;
- decentrale privacymanagers in een vaste structuur collega's ondersteunen bij privacyvragen;

- webpagina's over privacy zijn ingericht, met beleidsdocumenten, procedures, praktische tips, formats en FAQ's;

Op het gebied van bredere informatiebeveiliging geven instellingen aan dat:

- er onderzoek gedaan wordt naar de mate van bewustzijn van medewerkers en/of studenten;
- *awareness* campagnes zich richten op voorlichting over *phishing* of dreigmails. Ook worden er door de instelling simulatie *phishing* mails verzonden naar medewerkers. Soms in combinatie met een toets op de snelle en adequate afhandeling van een melding.

Aan deze opsomming is te zien dat er voor privacy een integraal en complete aanpak rondom bewustwording wordt beschreven en dat men zich hier publiek over verantwoordt. Daar tegenover staan de meer summiere verantwoording en de losse acties die we identificeerden vanuit de bredere informatiebeveiliging.

B. Awareness

Bereiken we wel iedereen?

Als we kijken naar de *awareness* campagnes die tijdens de gesprekken met instellingen genoemd werden, geven de gesprekspartners aan dat het niet altijd duidelijk is of alle gebruikers (medewerkers en studenten) wel worden bereikt. De deelname aan centrale bijeenkomsten valt tegen, en het is niet duidelijk hoe vaak waarschuwingsmails of een centraal dashboard echt worden gelezen. Eén instelling gaf aan bewust te hebben gekozen voor één methode, een centrale plek op de interne website. De instelling gaf echter ook aan dat dit niet genoeg is, omdat dat de pagina niet altijd goed wordt gelezen. Een andere instelling gaf aan dat ze niet steeds van centrale massacommunicatie wil uitgaan, omdat blijkt dat dit niet alle doelgroepen bereikt. Door decentraal veiligheidsverantwoordelijken aan te wijzen hopen ze op termijn dichter op de werkvloer medewerkers te bereiken. Sommige instellingen proberen de inhoud van de boodschap eenvoudig te brengen, bijvoorbeeld door gebruik van een praatplaat, of door op zoek te gaan naar relevante onderwerpen.

We zien daarnaast dat de aandacht voor cyberveiligheid soms afhangt van bevlogen individuen in plaats van de inzet van het bestuur, bijvoorbeeld de inzet van de Functionaris Gegevensbescherming. Uiteindelijk willen instellingen die we gesproken hebben dat informatiebeveiliging niet alleen iets is van de centrale ICT-afdeling, maar van de hele organisatie en dat het bewustzijn doordringt tot de haarvaten van de organisatie.

Betrokkenheid van het personeel en studenten

Er zijn instellingen die in de gesprekken aangeven dat er specifieke groepen medewerkers zijn die zich minder betrokken voelen bij de bedrijfsvoering van de gehele organisatie. Dan gaat het bijvoorbeeld om docenten voor wie administratieve of beheerstaken minder interessant zijn, of om freelancers. Met name in grote organisaties is het niet altijd duidelijk of zij de weg naar de centrale ICT weten te vinden. De ervaringen hierbij verschillen tussen instellingen; er zijn ook instellingen die geen verschil in betrokkenheid ervaren.

Daarnaast geven verschillende ho-instellingen aan het een uitdaging te vinden om bewustzijn bij alle gebruikers te creëren, vanwege grote verschillen in de achterban. Sommige medewerkers en studenten zijn zeer vaardig en technisch onderlegd, die zijn al bewust en weten de weg. Andere gebruikers zijn niet ICT vaardig en hebben weinig gevoel voor het risico. Desondanks vinden incidenten ook plaats met technisch zeer onderlegde medewerkers of studenten. Tot slot worden ook

wetenschappers als groep genoemd die geen aandacht hebben voor cyberveilig werken of voor de voorlichting hierover. Dit komt volgens de instellingen doordat zij veel werkdruk ervaren en een grote focus hebben op hun eigen onderzoek. Specifiek voor kleine instellingen speelt dat zij (voor Corona) veel steunden op informeel contact op de werkvloer om elkaar scherp te houden. Het was makkelijk om elkaar even te spreken en je thuis te voelen. Dat maakte het ook makkelijk om elkaar dingen te vragen of iemand even mee te laten kijken. Dat lukt nu met het werken op afstand minder goed en er wordt gezocht naar nieuwe methoden.

C. Security by design

Academische vrijheid en wensen vanuit het onderwijs

Security by design lijkt enigszins los te staan van het vergroten van het bewustzijn. Toch werden ze door ons gesprekspartners duidelijk aan elkaar gekoppeld. Dit komt doordat er bij de inrichting van het ICT-landschap sprake is van een wisselwerking met de organisatie(cultuur) van een ho-instelling. Wanneer die uitgaat van veel vrijheid, is de behoefte dat de ICT hetzelfde biedt. Uiteindelijk wordt ook de voorlichting over cyberveiligheid mede bepaald door de organisatiecultuur en de mate van *security by design*. Ook over de noodzaak van bepaalde beveiligingsmaatregelen moet begrip en bewustzijn zijn bij de eindgebruiker, zodat deze geen workarounds gaat bedenken.

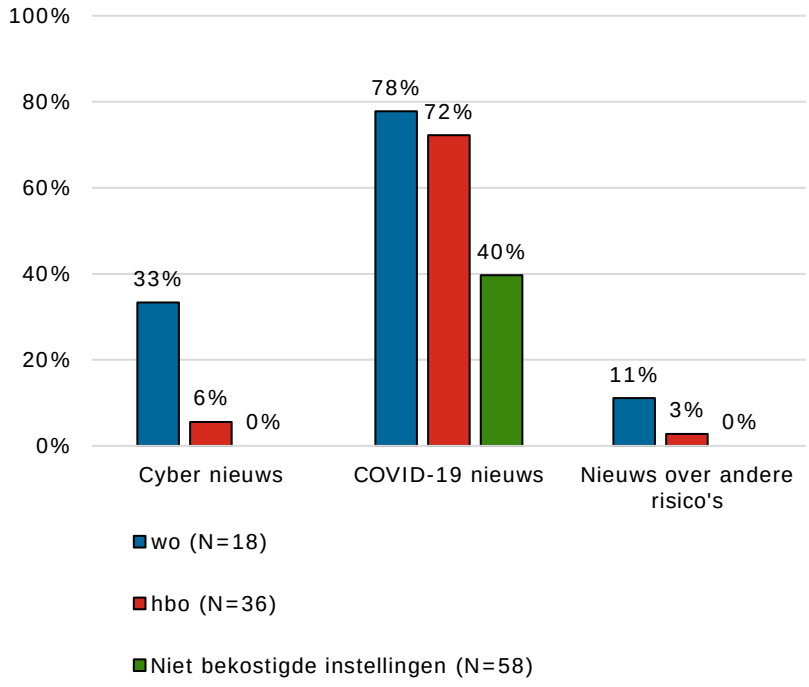
Uit de gesprekken blijkt dat in het bijzonder bij universiteiten een geschiedenis speelt waarin wetenschappers, onder andere vanuit het principe van academische vrijheid, zelfstandig hard- en/of software aan kunnen schaffen. Specifieke domeinen binnen onderwijs en onderzoek hebben bovendien behoefte aan nieuwe en andere ICT-toepassingen die voor kwetsbaarheden kunnen zorgen. ICT-opleidingen hebben bijvoorbeeld andere behoeften dan economisch opleidingen of opleidingen uit het domein maatschappij. Vrijwel alle gesprekspartners geven aan dat het netwerk van de organisatie minder vrijblijvend en open moet worden, om te kunnen voldoen aan de huidige cyberveiligheidsstandaarden. In plaats van medewerkers de vrije keuze te geven voor verschillende soorten ICT-techniek, wordt daarom door steeds meer instellingen in de bestaande techniek zoveel mogelijk zichtbare en onzichtbare preventie ingebouwd. Een instelling beschrijft dit bijvoorbeeld door aan te geven dat de systemen misschien wel van 20 (*high security*) - 80 (*high trust*) moet veranderen naar 80 (*high security*) - 20 (*high trust*). Dit is een aanpassing die ook een cultuurverandering met zich meebrengt en in eerste instantie weerstand oproept binnen instellingen.

Security by design kan een nadelig effect hebben voor gebruikers, zij kunnen door de gebruikte techniek soms ongemak ervaren. Een kleine instelling noemde als voorbeeld dat freelancers die niet op tijd hun contract verlengen, per direct uit het systeem gegooid worden. Dat is erg effectief, maar een werkwijze die de instelling niet te veel wil inzetten. Instellingen geven aan dat personeel zich wel bewust is van de veiligheidsaspecten, maar dat het toch voor discussie kan zorgen. Zeker omdat in het verleden op opleidings- of afdelingsniveau software kon worden aangeschaft. Een hogeschool inventariseerde dat zij een zevental verschillende pakketten had om stages van verschillende opleidingen in te registreren. Voor de meeste instellingen geldt dat er soft- of hardware wordt gebruikt waar op centraal niveau geen zicht op is. Instellingen zoeken naar een gezond evenwicht tussen wat centraal en wat decentraal geregeld wordt. Anders gezegd: waar ontmoeten de wens om het onderwijs en onderzoek maximaal te ondersteunen en cyberveiligheid elkaar? Een instelling gaf hierbij aan dat uiteindelijk het belang van de instelling groter is en de individuele onderzoeker of onderzoeksgroep mogelijk langer moet wachten tot iets beschikbaar is.

Corona als vliegwiel voor digitalisering

Alle instellingen beschrijven in de gesprekken dat de coronacrisis als een vliegwiel heeft gewerkt voor digitalisering en de bewustwording voor informatiebeveiliging. De afhankelijkheid van ICT gedurende de coronacrisis heeft mensen meer bewust gemaakt van wat er wel en niet veilig online kan. Door deze afhankelijkheid is niet alleen bij het bestuur, maar ook bij directeuren en management het bewustzijn gegroeid. Instellingen willen het momentum dat dit gecreëerd heeft vasthouden. Ze zien het wel als een uitdaging om het bewustzijn vast te houden, te institutionaliseren, zodra er fysiek weer meer kan. Dit effect van de coronacrisis zien we ook op de websites van instellingen. We hebben gekeken naar de nieuwsberichten die op de websites van instellingen staan (zie figuur 1.2a). Op de websites van instellingen is weinig tot geen aandacht voor cyber(veiligheid) voor de eigen organisatie. Er wordt net iets meer aandacht aan cyber gegeven dan aan andere dreigingen. Dit staat echter in contrast met de aandacht die er in nieuwsberichten is voor de coronacrisis en de effecten van de maatregelen voor studenten en medewerkers.

Figuur 1.2a Het percentage instellingen in het wo (N=18) en hbo (N=36) en rpho's (N=58) dat op de eventueel aanwezige nieuwssite en/of het archief van de nieuwssite berichten geeft over cyberveiligheid/informatiebeveiliging, Corona/COVID-19 en/of andere risico's.



1.3 Stelsel hoger onderwijs

Definitie van de standaard voor het stelsel:

Instellingen en alle belanghebbenden houden elkaar onderling scherp; men bespreekt interne en externe dreigingen. Er zijn landelijke bewustwordingscampagnes rondom veilig werken en cyberdreigingen.

Sterktes

- De (inter)nationale cyberveiligheid maand ondersteunt de initiatieven van instellingen en het stelsel.

- SURF heeft de cybersave yourself materialen en die worden benut.
- Bij alle partijen in het stelsel is een stevig bewustzijn van de het belang van cyberweerbaarheid en bereidheid om hierover mee te denken.

Zwaktes

- Veel hangt af van eigen initiatief van instellingen. Er is nationaal weinig aandacht besteed aan cybersecurity specifiek gericht op onderwijs. De koepelorganisaties hebben beperkt aandacht voor het onderwerp.
- Instellingen ondersteunen elkaar maar in heel beperkte mate bij het vergroten van het bewustzijn

Kansen

- Er is toenemend bewustzijn van het gevaar, er is meer bewustzijn van de integraliteit van ICT en het primair proces bij alle partijen.
- Er is al een goede infrastructuur met SURF en het Platform Intergraal Veilig Hoger Onderwijs, waarin interne en externe dreigingen besproken zouden kunnen worden.
- Door de coronacrisis is er veel aandacht voor online onderwijs en daarmee het belang van veilig digitaal werken.
- Aan de invoering van de AVG, maar ook de coronapandemie, is te zien dat nationale steun helpt bij het aangaan van collectieve ontwikkeling.

Bedreigingen

- Bestaande netwerken van instellingen weten elkaar steeds beter te vinden, wat andere nu niet aangesloten instellingen uitsluit.
- Verschillen in het bewustzijn betekent dat instellingen in verschillende mate weerbaar zijn tegen cyberdreigingen. Dit maakt het stelsel als geheel kwetsbaar.
- Op stelselniveau ontbreekt het aan structurele samenwerking tussen ho-instellingen om als collectief na te denken over '*security by design*'.

Toelichting op de standaard

Op stelselniveau kijken we of er vergelijkbare initiatieven zijn om het bewustzijn rond cyberveiligheid te vergroten. We willen weten hoe instellingen en partijen in het hoger onderwijsstelsel samenwerken en kennis delen met als doel elkaar bewust en scherp te houden op het gebied van cyberveiligheid. Zijn er bijvoorbeeld belemmerende factoren om elkaar bewust en scherp te houden, zoals concurrentie tussen bekostigde en niet-bekostigde instellingen, of het delen van vertrouwelijke informatie? Daarnaast willen we graag weten op welk organisatieniveau er behoefte is aan meer aandacht voor cyberveiligheid en waar instellingen zien dat de meeste winst te behalen is op het gebied van het vergroten van bewustzijn.

1.4 Bevindingen

Vergroten bewustzijn op nationaal niveau

Naast de verantwoordelijkheid die instellingen hebben voor het vergroten van het bewustzijn van studenten en medewerkers zijn er ook overkoepelende initiatieven. Op nationaal- en stelselniveau wordt er bijvoorbeeld meegedaan met de wereldwijde cybersecuritymaand in oktober. In deze maand zetten meerdere organisaties zich in om de cyberweerbaarheid van mensen en organisaties te vergroten, bijvoorbeeld SURF en het NCSC. Beide organisaties hebben een website die zich doorlopend richt op veilig gebruik van ICT, respectievelijk cybersaveyourself.nl en veiliginternetten.nl. Daarnaast hebben ze in de maand oktober actieve *awareness* campagnes met specifieke aandachtspunten. Organisaties kunnen bij hen ook kant en klare producten afnemen die gebruikt kunnen worden voor een *awareness* campagne of structurele voorlichting. Naast deze *awareness* campagne helpen (inter)nationale oefeningen ook mee bij het vergroten van het bewustzijn. Bijvoorbeeld de OZON-oefening, waarin een cybercrisis wordt geoefend of de Overheidsbrede Cyberoefening (ook in oktober).

Wat duidelijk zichtbaar is in ons onderzoek is de enorme impact die de invoering van de AVG in 2018 heeft gehad op het hele stelsel hoger onderwijs, en daarbuiten. De overheid zou in het kader van informatiebeveiliging en het overlappende terrein van kennisveiligheid een vergelijkbare stimulerende werking kunnen hebben.

Incidenten en bewustzijn
Daarnaast zien we dat incidenten zoals bij de Universiteit Maastricht maar ook de gemeente Hof van Twente helpen om het bewustzijn voor cyberveiligheid in het stelsel hoger onderwijs te vergroten. Deze getroffen organisaties hebben zelf actief bijgedragen aan het vergroten van het bewustzijn door het publiekelijk delen van hun ervaring. In de jaarverslagen over 2019 hebben vijf instellingen expliciet stilgestaan bij de cyberaanval op de UM. Dit betrof het jaarverslag van de UM zelf en in het verslag van drie universiteiten en één bekostigde hogeschool. Vooral uit de gesprekken met instellingen bleek dat de cyberaanval bij UM aanleiding is geweest tot direct handelen. Instellingen spreken daarnaast hun waardering uit voor de snelheid waarmee informatie is gedeeld en de grote openheid van de UM over wat er mis is gegaan en wat zij anders hadden moeten doen. Dit heeft bijgedragen aan het cyberweerbaar maken van meerdere instellingen.

Ondersteuning op stelselniveau
Uit de gesprekken met instellingen blijkt een sterke behoefte aan regie en ondersteuning op stelselniveau. Het verschilt wel tussen instellingen en functies wat voor soort regie en ondersteuning zij nodig hebben. Dit hangt mede af van de fase van ontwikkeling waar de instellingen zitten. De ambities van (grotere) bekostigde instellingen gaan een stuk verder dan de niet-bekostigde instellingen. Die laatste hebben maar beperkt toegang tot partijen zoals SURF. Onder de vlag van SURF is begin 2021 een SOC opgericht (zie ook standaard 3). Hierbij zijn niet alle bekostigde instellingen aangesloten. De VSNU en VH spelen een steeds grotere rol bij het samenbrengen van instellingen en het omschrijven van doelstellingen op het gebied van cyberveiligheid. De NRTO lijkt vooralsnog weinig actief op het gebied van bewustwording van cyberveiligheid. Dat is jammer omdat uit de gesprekken blijkt dat juist de rpho's behoefte hebben aan kennisdeling en systematische ondersteuning. De behoefte aan kennisdeling en samenwerking laat zien dat instellingen in het stelsel zich bewust zijn van de cyberrisico's.

De koepelorganisaties samen met het Ministerie van Onderwijs, Cultuur en Wetenschap (OCW) en SURF kunnen een grote rol spelen in het ondersteunen van *awareness* campagnes voor het hoger onderwijs. Onder andere door landelijke campagnes te voeren, door kennis uit te wisselen over effectieve vormen van *awareness* campagnes en manieren om een veilige meldcultuur in te richten. Net zoals cyberveiligheid binnen een instelling niet alleen de taak van de ICT-afdeling is, is het in het stelsel ook niet alleen de taak van de instellingen. Het Platform IV-HO van de VH en VSNU zou een grotere rol kunnen spelen in het verbinden van al deze partijen.

Kenniscentra en regionale samenwerking
Verschillende initiatieven zoals het oprichten van kenniscentra en regionale samenwerking, zorgen ervoor dat men elkaar scherp houdt op mogelijke risico's. Meerdere instellingen geven in gesprek of op hun website aan dat zij voor cyberveiligheid samenwerken met andere organisaties binnen de regio of beschikken over een kenniscentrum. Binnen de regionale samenwerkingsverbanden hebben bijvoorbeeld verschillende onderwijsinstellingen samen met andere organisaties of gemeenten contact over cyberveiligheid. Ze leren van elkaar en delen soms expertise. Daarnaast zijn er instellingen die vanuit het onderwijs of onderzoek kennis delen door andere organisaties te adviseren over cyberveiligheid of ICT.

In- en extern toezicht bij kennisdeling en agendering

Het in- en extern toezicht kan een stimulerende werking hebben op het vergroten van het bewustzijn. Door de stand van zaken te monitoren, hierover te rapporteren en het onderwerp te agenderen wordt er blijvend aandacht gevraagd voor het onderwerp. Dit kan op het niveau van de individuele instelling, maar ook op die van het stelsel door middel van bijvoorbeeld thematische onderzoeken.

2 Standaard 2: veilige en open cultuur

2.1 Instellingen hoger onderwijs

Definitie van de standaard voor instellingen:

Informatiebeveiliging is in essentie risicomanagement wat begint bij identificatie. Het bestuur bevordert een open en veilige cultuur waarin medewerkers zich vrij voelen om (potentiële) risico's proactief te melden bij de juiste persoon.

Sterktes

- Ho-instellingen en hun besturen hechten veel waarde aan een veilige en open cultuur. De cultuur en opdracht van academische vrijheid draagt hier aan bij.
- Besturen zijn zich terdege bewust van de kwetsbaarheid van het gevoel van veiligheid en de noodzaak hier continu aandacht voor te blijven hebben.

Zwaktes

- Het is onduidelijk of instellingen voorbereid zijn op het moment waarop gebruikers door technische problemen geen toegang hebben tot interne informatie over cyberveiligheid en het doen van een melding. De openbare websites geven beperkt informatie over het doen van een melding. Mogelijk kunnen gebruikers als ze geen gebruik kunnen maken van de interne omgeving niet bij de benodigde informatie.
- Er lijkt veel aandacht te gaan naar acute dreigingen. Mogelijk is de balans tussen verschillende dreigingen onvoldoende in evenwicht, bijvoorbeeld tussen melden in het kader van de AVG en de brede cyberveiligheid.

Kansen

- De bereidheid tot leren is groot.
- Veel instellingen kunnen op hun publieke website vooruitgang boeken door meer en eenduidiger te communiceren, in ieder geval over ICT beveiliging en meldingsmogelijkheden. Hierbij kunnen ze een voorbeeld nemen aan andere instellingen.
- In de WHW zijn inspraak en medezeggenschap helder geregeld. Dit geeft ruimte voor tegenspraak in de organisatie ook als het gaat om de omgang met signalen en meldingen.

Bedreigingen

- Wanneer de reactie van (functionarissen binnen) de instelling of de wijze van communiceren over het doen van een melding er één is van hard ingrijpen en beschuldigen ('domme eindgebruiker') is dat schadelijk voor het gevoel van veiligheid.
- Door een focus op actuele onderwerpen en dreigingen krijgen structurele dreigingen minder aandacht. Daarmee ontstaat een disbalans en het risico dat veiligheid bij het ene onderwerp meer en het andere minder aandacht krijgt. Terwijl deze pas echt goed werkt als het integraal wordt aangepakt.

Toelichting op de standaard

Om de urgentie van cyberrisico's te kunnen analyseren, is het nodig te weten hoe, waar en wanneer: 1) kwetsbaarheden in systemen en processen zitten, 2) of kwetsbaarheden ontstaan door verkeerd gebruik, en 3) of er incidenten plaatsvinden waarbij derden proberen toegang te krijgen tot systemen. De meest actuele informatie is afhankelijk van de aansluiting van de instelling op informatiebronnen over risico's van buiten de instelling, maar is ook afhankelijk van het gemak waarmee ICT-gebruikers snel en vaak potentiële risico's kunnen melden binnen de instelling.

Onderdeel van een veilige en open cultuur (standaard 2) is de vrijheid die medewerkers voelen om (potentiële) cyberrisico's proactief te melden bij de juiste persoon. Dat begint bij makkelijk vindbare contactgegevens, heldere informatie over

hoe een kwetsbaarheid gemeld kan worden en hoe deze wordt afgehandeld. Deze informatie zorgt voor meer transparantie over de manier waarop er omgegaan wordt met de melder en de melding; (potentiële) melders weten wat de kaders zijn en wat ze kunnen verwachten na het doen van een melding. Door aan te geven dat de instelling vertrouwelijk omgaat met gegevens en meldingen, zorgt de instelling ervoor dat personen sneller geneigd zijn een melding te doen. Daarnaast is een veilige en open cultuur mede afhankelijk van de manier waarop het bestuur van een instelling dit stimuleert, bijvoorbeeld door melders niet af te rekenen op hun openheid.

Bij standaard 1 hebben we gekeken naar de mate en inhoud van informatie die beschikbaar is om het bewustzijn van cyberveiligheid te vergroten. Bij standaard 2 gaan we dieper in op drie elementen die nodig zijn om een veilige en open cultuur te creëren. We beginnen met de rol van het bestuur, spreken dan over de toon en beschikbaarheid van de informatie op de websites, en kijken vervolgens naar in hoeverre ICT-gebruikers meldingen (kunnen) doen.

2.2 Bevindingen

Voorbeeldfunctie bestuur

Uit de gesprekken blijkt dat instellingen veel waarde hechten aan een veilige en open cultuur en ze geven ook diverse voorbeelden waaruit blijkt dat eindgebruikers zich ook werkelijk veilig voelen om te melden. Bestuurders zijn zich erg bewust van het belang hiervan voor (cyber)veiligheid en het onderwijs. Daarom werken zij actief mee aan het creëren van een veilige en open cultuur.

De meeste instellingen geven aan dat er op hun instelling een veilige en open cultuur heerst en dat er veel gemeld wordt. Daarnaast geven ze aan bezig te zijn en blijven met de ontwikkeling en groei hiervan. De gesprekspartners noemen drie dingen die belangrijk zijn voor het stimuleren en borgen van een veilige en open cultuur:

1. het bestuur is in gedrag een voorbeeld voor anderen. Door te tonen dat fouten maken mag, maar ook door het gesprek aan te gaan over oplossingen.
2. er is een zorgvuldige handelswijze richting melders vastgelegd en geborgd.
3. het bestuur laat zien dat zij achter de procedure en mensen die de regels uitvoeren en naleven staan.

Als voorbeeld wordt de AVG regelgeving genoemd. Sommige medewerkers vinden de informatiebeveiligingsmaatregelen rond de AVG irritant. Het helpt als het bestuur laat zien dat zij achter de principes staan, ook als het consequenties heeft voor de organisatie. Het helpt daarbij als het bestuur de functionarissen ondersteunt bij de uitvoering van hun taken en waar nodig de organisatie er op aanspreekt. Het zorgt ervoor dat deze functionarissen geen roepende in de woestijn zijn. Het geeft een bestuurlijke legitimiteit die er voor zorgt dat medewerkers zich voegen.

Uit de gesprekken bleek dat zelfs wanneer het bestuur deze dingen doet en procedures zijn vastgelegd, de praktijk anders kan lopen. Medewerkers die een melding doen, handelen vanuit een groot verantwoordelijkheidsgevoel en worden hard geraakt door negatieve reacties. Een instelling gaf een voorbeeld van een medewerker die een melding deed over een (mogelijk) datalek. Vanwege de grote gevolgen die dit had op de organisatie werd de melder vervolgens door een direct leidinggevende op het matje geroepen. Dit gebeurde ondanks duidelijke afspraken voor de gehele organisatie over hoe om te gaan met een datalekmelding. Het had een groot effect op de betreffende medewerker. Het bestuur gaf aan dat het in zo'n situatie nodig is aandacht te hebben voor de melder, erover met elkaar in gesprek

te gaan, eventueel procedures aan te passen en de organisatie te informeren over het ongewenste voorval en de procedures om het in de toekomst te voorkomen.

Informatie over ICT, cyberveiligheid en melden op openbare website
Zoals we bij standaard 1 beschreven zijn op de websites van bekostigde hogescholen en rpho's weinig algemene pagina's te vinden over ICT of cyberveiligheid. Daar tegenover staat dat een meerderheid van de universiteiten dat wel heeft. We beschreven ook dat de mate waarin en de manier waarop informatie wordt gegeven op de websites heel divers is. Datzelfde geldt voor hoe vindbaar deze is en welke informatie wordt gegeven, onder andere over het melden van incidenten en het afhandelen ervan. Op dit laatste punt gaan we verderop uitgebreider in. Op de meeste websites was het even zoeken naar contactgegevens van de helpdesk, informatie over ICT en cyberveiligheidsonderwerpen. Soms was de informatie goed vindbaar (via het menu) en stond de informatie bij elkaar. Vaker was het zoeken en vonden we dingen versnipperd geplaatst op de website door gebruik te maken van de zoekfunctie. Wanneer deze informatie ook intern moeilijk vindbaar is, heeft dit consequenties voor de toegankelijkheid van informatie voor medewerkers en studenten en daarmee mogelijk gevolgen voor de mate waarin zij cyberveilig handelen.

De toon in de gevonden informatie
Bij standaard 1 (vergroten bewustzijn) hebben we stilgestaan bij het soort informatie dat instellingen gebruiken bij de voorlichting en het vergroten van het bewustzijn. Hier gaan we in op wat de toonzetting in de gevonden informatie kan doen voor het veiligheidsgevoel. De toon van de informatie en documenten over ICT en cyberveiligheid op websites verschilt, zowel tussen instellingen als binnen de website van één instelling. Over het algemeen kunnen we zeggen dat de toon van de gevonden documenten overwegend neutraal of zakelijk is. Een enkele keer staat expliciet vermeld dat er vertrouwelijk met de informatie rondom meldingen wordt omgegaan waardoor medewerkers en studenten zich mogelijk eerder geneigd voelen om (potentiële) risico's proactief te melden. Daarentegen zien we ook instellingen die in juridische teksten de verantwoordelijkheid hoofdzakelijk bij de gebruiker neerleggen. Een voorbeeld van een onderwerp waarbij we verschillen zien in de benadering van gebruikers is bij het onderwerp *responsible disclosure*. Het gaat hierbij om een melding die je als gebruiker of ethisch hacker bij een organisatie doet op het moment dat je een beveiligingsprobleem of kwetsbaarheid in een ICT-systeem of organisatie ontdekt. Op dit gebied ligt de grens tussen fatsoenlijk en strafbaar handelen dicht bij elkaar. We zien instellingen die hiervoor beleid hebben opgesteld en *responsible disclosure* van derden verwelkomen. Dat doen ze bijvoorbeeld door hier expliciet aandacht voor te vragen, een werkwijze te omschrijven en contactgegevens te vermelden voor *ethical hackers* om zich met hun bevindingen te melden. Hierbij wordt door enkele zelfs de mogelijkheid tot een beloning genoemd, mits bij het onderzoek geen strafbare feiten zijn begaan. Daarnaast zijn er instellingen die aangeven geen behoefte te hebben aan het werk van *ethical hackers* en in juridische termen de (mogelijke) strafbaarheid meer benadrukken.

Veiligheidsgevoel stimuleren
In de gesprekken werd een aantal initiatieven besproken waarmee het bewustzijn over informatiebeveiliging (standaard 1) wordt vergroot, maar die ook belangrijk zijn voor het stimuleren van een veilige en open cultuur. Er is bijvoorbeeld een instelling die elke twee á drie maanden een privacy lunch organiseert. Daar wordt gesproken met een gastspreker of wordt er een specifiek onderwerp of een *phishing* mail besproken. Een andere instelling stelt e-learning modules van cybersafeyourself van SURF beschikbaar via het intranet. Andere dingen die worden genoemd zijn

nieuwsbrieven, quizzen, het inzetten van privacy contactpersonen of momenten. Bij al deze initiatieven is één van de doelen op een open en veilige manier met elkaar in gesprek gaan over cyberveilig handelen en de drempel om een melding te doen te verlagen.

Melden over brede informatiebeveiliging of AVG
In de gesprekken met instellingen valt het op dat wanneer het gesprek gaat over melden, het meestal direct gaat over meldingen van datalekken in het kader van privacygegevens. Daarbij wordt gesproken over de betrokkenheid van ICT bij een privacy-overleg en er contact is met de Functionaris Gegevensbescherming voor een melding bij de Autoriteit Persoonsgegevens. Bij enkele instellingen gaat het in de gesprekken juist over de veiligheid in brede zin. Over een overkoepelende open en veilige cultuur als voorwaarde voor goed onderwijs en onderzoek. Deze instellingen geven aan dat een veilige en open cultuur zich niet beperkt tot één onderwerp. Het is volgens hen van belang dat het gevoel van veiligheid op meer vlakken aanwezig is. Elke soort veiligheid vraagt een andere aanpak en deskundigheid.

Melden zonder schaamte of nadelige gevolgen
In de gesprekken wordt aangegeven dat er vaak schaamte speelt bij melders of schroom is om te melden. Er hangt een gevoel van ‘ik heb iets verkeerd gedaan’ aan. Daarnaast worden de (mogelijke) consequenties van een melding voor de organisatie genoemd als remming voor het melden van een risico of incident. Processen kunnen bijvoorbeeld tijdelijk stilgelegd moeten worden, er moeten controles plaats vinden, het kost tijd en energie om de melding af te handelen. Uit de gesprekken komt een duidelijk beeld naar voren over wat nodig is om een veilige cultuur rondom het melden van risico’s of incidenten te bevorderen. Instellingen ervoeren dat het aantal meldingen omhoog ging wanneer de veiligheid in de procedure aangepast werd. Sommige instellingen geven zelfs aan dat, mede door *awareness* programma’s, de *mindset* of *social enigineering* zo is veranderd dat melden en vragen gewoon kan en gebeurt.

Uiteindelijk willen instellingen een cultuur neerzetten waarbij:
- mensen melden zonder remming;
- mensen elkaar aanspreken;
- er begrip is voor fouten maken en dingen vergeten - dat kan gebeuren;
- melden veilig is vanuit persoonlijk perspectief;
- ‘*naming and shaming*’ of een bestraffend vingertje wordt voorkomen;

Dat doen instellingen bijvoorbeeld door:
- geen sancties te verbinden aan melden of fouten maken;
- op in- en externe websites de meldingsmogelijkheden zo toegankelijk mogelijk te maken;
- positief te reageren op elke melding, laten zien dat je blij bent met de melding;
- iemand die een kwetsbaarheid meldt op een passende manier te bedanken;
- het individu bij een incident vanuit vertrouwen te begeleiden;
- zorgvuldig en vertrouwelijk om te gaan met mensen die bijvoorbeeld op een *phishing* mail hebben geklikt;
- te helpen bij een al dan niet gemeld datalek door naast elkaar te staan en dingen samen op te lossen.

Wanneer instellingen zich richten op een aanpak met een veilige en open cultuur, zijn zij zich bewust van hun diverse doelgroep. Ze willen iedereen aanspreken, en dat vraagt voor sommige doelgroepen een andere benadering. Het gaat niet alleen om alle medewerkers en studenten die een verdacht mailtje binnen krijgen, maar ook om ICT-technici die het melden als dingen niet goed geregeld zijn, studenten

die proberen in te breken op het eigen netwerk en medewerkers die kwetsbaarheden zien.

Aantal meldingen
In de gesprekken bleek dat instellingen het aantal meldingen sinds de invoering van de AVG zien groeien. Dit zien ze ook wanneer er waarschuwingsmails zijn verstuurd. Of meldingen een goede afspiegeling zijn van cyberincidenten die optreden kunnen instellingen niet zeggen.

In de jaarverslagen en de verslagen van werkzaamheden staat weinig over het aantal meldingen of over de veilige en open cultuur (zie verder standaard 3). Er is geen informatie te vinden over het melden van datalekken in de brede zin van cyberveiligheid, enkel over meldingen in het kader van AVG. Er zijn wel een aantal instellingen die ingaan op andere aspecten van veiligheid en hoe zij hier mee om gaan. Er zijn 24 bekostigde instellingen die aandacht geven aan functionarissen en procedures rondom sociale veiligheid. Bij de meeste (20) gaat het om de aanwezigheid van een vertrouwenspersoon of een klachtencommissie waar medewerkers en/of studenten terecht kunnen met hun klachten, bijvoorbeeld rondom ongewenst gedrag. Sommige instellingen noemen ook het aantal kwesties dat behandeld is door een vertrouwenspersoon en/of door de klachtencommissie. Daarnaast zijn er enkele instellingen die de aanwezigheid noemen van reglementen, beleid, of lopende onderzoeken op het gebied van sociale veiligheid en/of benoemen het belang van een veilige sociale werkomgeving.

Betrokken functies bij meldingen
Uit de gesprekken wordt duidelijk dat verschillende functionarissen een rol spelen bij de afhandeling van meldingen. Dit zijn in ieder geval de helpdesk of de afdeling ICT, maar ook de Functionaris Gegevensbescherming, Privacy-officer of een privacy contactpersoon; in een enkel geval ook het team integraal veilig. Ongeacht waar ICT en ICT-beveiliging gepositioneerd zijn, is het van belang dat er overal binnen de organisatie aandacht is voor informatiebeveiliging en dat bij alle bestuurslagen binnen de organisatie gewerkt wordt aan een open en veilige cultuur waarbij medewerkers en studenten zich vrij voelen om (potentiële) risico's proactief te melden – en dat de melding daarna op de juiste plek belandt: bij een afdeling of persoon die verantwoordelijk is voor het afhandelen van de meldingen.

Universiteit Twente
Op de website van de Universiteit Twente staat het document 'Wegwijzer integriteit voor medewerkers'. In deze wegwijzer kun je eenvoudig vinden wie je benadert bij welk ethisch dilemma: wetenschappelijke integriteit, knelpunten PHD traject, ongewenst gedrag en cyber security. We vinden dit een mooi voorbeeld van een integrale benadering. Het is een heel beknopt document met vier heldere categorieën en beschrijvingen van de ethische dillema's. Het document stuurt de gebruiker direct door naar de relevante contactgegevens en eventuele toelichting bij de specifieke functionaris. Van vertrouwenspersoon tot het CERT en de privacy functionaris.
(zie: https://www.utwente.nl/organisatie/over-de-ut/integriteit/#contact)

2.3 Stelsel hoger onderwijs

Definitie van de standaard voor het stelsel:

Alle belanghebbenden stimuleren dat er een veilige en open cultuur is: meldingen kunnen in vertrouwen worden gedaan. Melders worden niet afgerekend op hun openheid. Het lerend vermogen van het stelsel staat voorop. Er is een ter zake kundig loket waar meldingen kunnen worden gedaan.

Sterktes

- Via SURF houden ICT'ers van bekostigde instellingen elkaar op de hoogte over risico's en leren ze van elkaar.
- De open manier waarop de UM heeft gecommuniceerd na de hack in 2019 heeft instellingen in het hele stelsel verder geholpen.
- Bekostigde instellingen hebben steun aan elkaar en vinden elkaar binnen de netwerken van SURF.

Zwakte

- Er is geen stelselbreed (voor bekostigde en niet-bekostigde instellingen) meldpunt voor onveilige situaties en geen duidelijk of eenduidig aanspreekpunt op stelselniveau.
- Niet alle partijen zien dat bekostigde en niet-bekostigde instellingen op dit onderwerp behoren tot dezelfde doelgroep. Daarmee zit er een blinde vlek in het stelsel, waardoor een aantal spelers niet (kunnen) deelnemen aan het open gesprek of het creëren van een veilige cultuur.

Kansen

- De bereidheid tot leren en samenwerking tussen belanghebbenden is groot. Er is op dit moment een heel open gesprek mogelijk over cyberveiligheid.
- Instellingen zijn zich bewust van de (intern)nationale aard van cyberveiligheid en daarmee de noodzaak tot samen optrekken.

Bedreigingen

- Instellingen zijn zich niet bewust van de verschillen tussen instellingen in aard, omvang en informatiepositie. De noodzaak om informatie breder te delen dan nu, wordt daardoor niet door alle instellingen gezien.
- De harde scheidslijn tussen bekostigde en niet-bekostigde instellingen zorgt voor kwetsbaarheden op stelselniveau.
- Hard ingrijpen op instellingsniveau kan de bereidheid om open het gesprek te voeren, te melden en informatie te delen verkleinen.
- Een gebrek aan centrale ondersteuning kan openheid tussen met name bekostigde en niet-bekostigde instellingen beperken.

Toelichting op de standaard

Op stelselniveau geldt hetzelfde als op instellingsniveau. Het kunnen melden begint bij makkelijk vindbare centrale contactgegevens. We onderzoeken of op stelselniveau instellingen en hun besturen onderling een veilige en open cultuur onderhouden. Bijvoorbeeld of er ruimte is om risico's, kwetsbaarheden en incidenten onderling te delen en in elkaars keuken te kijken. Daarnaast kijken we naar de informatiestructuur op stelsel- en nationaal niveau.

2.4 Bevindingen

Verschillende behoefte aan informatie

Er is een groot verschil tussen hoe instellingen hun informatiepositie beoordelen. Voornamelijk grote bekostigde instellingen voelen zich duidelijk onderdeel van een netwerk waar veel wordt gedeeld en zijn daar tevreden over. Daarbij gaat het hoofdzakelijk over SURF, SURF-CERT, SURF-SOC, maar ook de koepelorganisaties en het Platform Integraal Veilig Hoger Onderwijs. In de standaarden 3 en 5 gaan we hier nader op in. Bij standaard 2 ligt de focus op hoe spelers binnen het stelsel deze

samenwerking ervaren en of deze bijdraagt aan de meldingsbereidheid en het lerend vermogen van het stelsel.

Uit gesprekken met bestuurders van grotere universiteiten komt naar voren dat zij geen behoefte hebben aan meer of andere informatie dan via SURF wordt verstrekt. Dit ligt anders op operationeel niveau en bij instellingen met een ander karakter. Daar is meer behoefte aan het delen van kennis en informatie over kwetsbaarheden. Daarnaast hebben kleinere bekostigde instellingen meer moeite met de aansluiting bij SURF initiatieven. Dit heeft vaak te maken met kosten, het feit dat ze kleine ICT-afdelingen hebben en één medewerker vaak verschillende taken heeft. Niet-bekostigde instellingen voelen zich daarentegen echt weinig tot niet verbonden en missen toegang tot ondersteuning en informatie over cyberdreigingen bij een organisatie als SURF. Bij hen leeft een grote behoefte aan betere ketensamenwerking.

Uit de gesprekken blijkt dat bestuurders van bekostigde hogescholen via een bestuurders-app van de Vereniging Hogescholen snel informatie doorgeven als er sprake is van een incident. In hoeverre er ook sprake is van een onderlinge aanspreekcultuur is ons niet helemaal duidelijk geworden, maar de basis voor het open en veilig delen van informatie lijkt aanwezig. Vanuit SURF is tussen januari en juli 2021 een seminarreeks aangeboden aan bestuurders om te kijken naar hoe besturen samen kunnen optrekken om de publieke waarde van het onderwijs in ICT te beschermen. Daarbij keken ze onder andere naar de regie die zij kunnen pakken in relatie tot de grote tech-reuzen. Bestuurders zien SURF als een belangrijke ‘versneller’ op het gebied van digitalisering.

In de gesprekken wordt wel aandacht gevraagd voor het internationale perspectief van het hoger onderwijs. De ontwikkelingen in de digitale wereld, maar ook de dreigingen, gaan heel snel en zijn internationaal. Bestuurders geven aan dat instellingen daarom de overheid hierbij nodig hebben. Op dat vlak missen instellingen aansluiting tussen regelgeving in verschillende landen, bijvoorbeeld op het gebied van de AVG. Dat bemoeilijkt de samenwerking. Er mag wat hen betreft op hoog niveau internationaal en in de Europese Unie veel meer aandacht komen voor cyberveiligheid. Via het GÉANT netwerk[34] is het hoger onderwijs verbonden met het internationale hoger onderwijs. Het NCSC staat ook in verbinding met centra in andere Europese landen. Dit geeft mogelijkheden, maar mist centrale coördinatie.

Niet-bekostigde instellingen

Het beeld dat we hebben van de mate waarin niet-bekostigde instellingen deelnemen aan een veilig en open gesprek binnen het stelsel is volledig anders. Er is weinig tot geen contact tussen bekostigde instellingen en rpho’s op het vlak van ICT of cyberveiligheid, maar ook niet structureel tussen rpho’s onder elkaar. Daarnaast hebben ze in mindere mate toegang tot SURF en de informatie die vanuit het SURF-CERT wel met bekostigde instellingen wordt gedeeld. Dit gebrek aan contact tussen bekostigde en niet-bekostigde instellingen speelt ook op het gebied van het onderwijs. Er zijn enkele onderwijsinitiatieven waar beide soorten instellingen met elkaar praten, bijvoorbeeld bij hybride organisaties (met een bekostigde en niet-bekostigde tak of samenwerking). Een ander voorbeeld dat wordt genoemd waarbij wel over deze grens gewerkt wordt is binnen het experiment leeruitkomsten. Dit zijn echter initiatieven op beperkte schaal en met specifieke scope. Het beeld dat hier uit voortkomt is dat een rpho in sterke mate afhankelijk is van hun eigen ICT’ers en

[34] GÉANT is een netwerkorganisatie voor samenwerking op het gebied van digitale infrastructuur en diensten voor onderzoek en onderwijs. SURF is als lid bij dit netwerk aangesloten. Zie: https://www.geant.org/ (geraadpleegd op 19-7-2021)

leveranciers. Dat neemt niet weg dat rpho's in de basis tevreden zijn over de beheersing van de cyberveiligheid voor hun instelling. Tegelijk is er wel degelijk een grote behoefte aan het stelselbreed delen van informatie over risico's, kwetsbaarheden en incidenten. Omdat deze informatie uiteindelijk nodig is voor het maken van goede en complete risicoanalyses om de cyberveiligheid te borgen.

Veilig en open maar voor wie?

Het beeld dat uit de gesprekken naar voren komt, is dat instellingen op zeer verschillende manieren aangesloten zijn en zich aangesloten voelen op belangrijke informatie voor hun risicomanagement. Instellingen blijken zich lang niet allemaal bewust te zijn van de positie en uitdagingen van collega instellingen, zoals kleine instellingen of niet-bekostigde instellingen. Instellingen leunen sterk op informeel contact van bestuurders tot individuele ICT'ers. Daardoor is sprake van een grote mate van toevalligheid bij het ontdekken van zwakke punten in de beveiliging. Om een stelselbrede veilige en open cultuur te kunnen bewerkstellingen is het nodig dat instellingen weten wie hun partners zijn. Vervolgens is van belang na te denken over hoe je formeel en informeel op dit onderwerp met elkaar omgaat.

Openheid over aanpak incidenten

De manier waarop de Universiteit Maastricht handelde tijdens en na het oplossen van het cyberincident dat 2019/2020 bij hen plaatsvond, is een goed voorbeeld van het open delen van informatie. De andere universiteiten werden direct geïnformeerd en tussen Kerst en Oud & Nieuw werden andere instellingen direct via de UM en via SURF steeds van updates voorzien. Andersom hebben andere universiteiten aangeboden de UM te helpen. De UM heeft al snel besloten haar lessen met anderen te delen vanuit de overtuiging dat dit bij alle universiteiten had kunnen gebeuren. Een gevolg hiervan is dat instellingen intern en onderling zijn gaan nadenken, zowel over directe concrete acties die nodig waren als op de lange termijn na te denken over de inbedding van ICT-beveiliging in het risicomanagement van de instelling. Wat de casus van de UM ook duidelijk maakte is dat er op het moment dat duidelijk wordt dat er sprake is van een hack, dan wel losgeldeis, je op jezelf bent aangewezen. Er was geen spoorboekje waar in stond wat te doen; een leidraad waar in staat wie kan helpen, wat de politie doet in een dergelijk geval of wie op de hoogte moeten worden gesteld en hoe en wanneer we dit in- en extern communiceren. De burgemeester van de gemeente Hof van Twente verwoordde dit tijdens de persconferentie op 16 maart 2021[35] als de behoefte aan een noodnummer zoals dat vroeger met een sticker op je meterkast geplakt zat. Van één instelling die later getroffen werd door een incident hoorden we dat het bestuur vrij snel contact zocht met het bestuur van de UM. Om zo een snel beeld van het 'spoorboekje' te krijgen. Uiteindelijk zou het wenselijk zijn om een dergelijk contactpunt op stelselniveau te organiseren.

Rol van intern en extern toezicht

Bij het borgen van een veilige en open cultuur op stelselniveau heeft ook de in- en externe toezichthouder een rol. In- en extern toezicht monitort en spreekt instellingen en stelselpartijen aan op hun rol bij het stimuleren van een veilige en open cultuur. Daarnaast treedt zij op in geval van onveilige situaties die zorgen voor schade aan personen, instellingen en het stelsel. De rol van het interne toezicht is hierbij volgens de gesprekspartners die van een kritische vriend. Het is een belangrijke partij om in alle veiligheid over incidenten en meldingen en dilemma's te sparren. Ze moeten wel de juiste vragen kunnen stellen, bijvoorbeeld over risicomanagement of over de communicatiestrategie bij incidenten. Een enkel lid van

[35] Hof van Twente (2021, Maart 16). *Persconferentie onderzoeksresultaten cyberaanval*. 16 maart 2021 [Video]. YouTube. https://www.youtube.com/watch?v=aw56vvOb1rM (geraadpleegd op 22 juli 2021)

de Raden van Toezicht waar wij mee hebben gesproken, gaat nog een stap verder: cyberexpertise en risicomanagement horen bij het standaardprofiel van tenminste een lid van elke RvT.

Tijdens de gesprekken merkten we dat alle gesprekspartners aan ons als externe toezichthouder zeer open inzicht gaven in de manier waarop zij met cyberveiligheid bezig zijn. Onze gesprekken met de Inspectie Gezondheidzorg en Jeugd (IGJ) en met het Agentschap Telecom (AT) bevestigen de noodzaak om ook als externe toezichthouder in te zetten op het stimuleren van een veilige en open cultuur. In beide domeinen is er sprake van een grote diversiteit van aanbieders met soms tegenstrijdige belangen. Interessant is de afspraak die geldt in de het stelsel waar het AT toezicht op houdt: niet concurreren op veiligheidsvraagstukken. Het idee daarbij is dat dit zo'n belangrijke taak is dat het nodig is dat CISO's, onder andere best practices, configuraties en kwetsbaarheden/incidenten uitwisselen. We zijn niet nagegaan of dit akkoord ook werkt zoals het bedoeld is, maar het uitgangspunt laat zien dat de noodzaak gezien wordt en de wens er is. Dit zou een voorbeeld kunnen zijn voor het dichten van het gat tussen bekostigde en niet-bekostigde instellingen.

3 Standaard 3: inrichten risicoteam

3.1 Instellingen hoger onderwijs

Definitie van de standaard voor instellingen:

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 Gegevensbescherming (FG) en Controller. Deze systeemeigenaren functioneren tevens als onafhankelijk adviseur voor het bestuur.

Sterktes

- De meeste ho-instellingen kennen een security officer of hebben een soortgelijke taak belegd bij een secretaris CvB. Verschillende ho-instellingen beschikken over een specialistisch team of cyberincidenten af te handen.
- Ho-instellingen hebben de afgelopen jaren de crisismanagementplannen aangevuld met de aanpak bij een cyberincident.

Zwaktes

- Verantwoordelijkheid in relatie tot decentrale onderdelen en lijnsturing is niet altijd duidelijk.
- Kleine instellingen beschikken niet over alle expertise en zijn afhankelijk van één of enkele medewerkers voor detectie en afhandeling van incidenten.
- Er is bij andere actoren in het stelsel beperkt inzicht in en informatie over cyberincidenten bij individuele instellingen.

Kansen

- De positie van en aandacht voor centrale risicofunctie lijkt verbeterd.
- Grote universiteiten investeren in een actievere aanpak; daartoe hebben ze een eigen Security Operations Center (SOC) opgezet of overwegen dit te doen.
- Ho-instellingen hebben tijdens de COVID-19 pandemie ervaring opgedaan met het functioneren van de eigen crisismanagement organisatie en kunnen de lessen benutten om de organisatie waar nodig te verbeteren.

Bedreigingen

- Belang verdwijnt weer naarmate risico's minder op bestuurlijk agenda staan en andere onderwerpen aandacht vragen.

Toelichting op de standaard

De derde standaard richt zich op het organiseren van de respons op (mogelijke) cyberdreigingen en -incidenten. Dit is een activiteit voor zowel instellingen als het stelsel. Het risicoteam brengt dreigingsinformatie uit verschillende bronnen continu en tijdig samen, zodat zij indien nodig kan reageren op de dreigingsinformatie en in geval van een cyberincident direct kan bepalen wanneer er opgeschaald moet worden binnen en buiten de organisatie. Indien zich een incident voordoet wordt dit afgehandeld door een specialistisch team (zoals een CERT). Voor zo'n team is een signaal over een incident het moment om actief te worden. Anders gezegd: een CERT is reactief. Leden van een CERT hebben daarom ook andere functies binnen een onderwijsinstelling. Afhankelijk van de omvang van een incident zijn naast dit specialistische team ook de bestuurders betrokken, bijgestaan door juridische- en communicatieadviseurs (in een aangewezen crisismanagementteam).

3.2 Bevindingen

Lokale aanpak

Binnen het Nederlandse hoger onderwijs zijn er zowel hele kleine als zeer grote hogescholen en universiteiten die op één of op meer locaties zijn gevestigd. Het is dan ook niet verwonderlijk dat ho-instellingen verschillende structuren kennen, ook in het geval van crisisafhandeling van een cyberincident. Zo heeft een kleine universiteit of hogeschool een beperkt aantal informatiebeveiligingsprofessionals waardoor een aparte organisatie naast de reguliere lijn niet altijd mogelijk is. Anderzijds zijn in kleinere onderwijsinstellingen de lijnen kort waardoor mensen elkaar snel kunnen vinden in geval van een crisis, hoewel bij zeer grote instellingen het een uitdaging kan zijn om de juiste personen te vinden. In ons onderzoek troffen we zowel hogescholen als universiteiten aan, zowel bekostigd als niet-bekostigd, waarbij cyberdreigingen binnen reguliere lijnen worden afgehandeld als wel waarbij specifieke teams zijn ingericht.

Een cybercrisisteam als onderdeel van integrale risicomanagement

Uit gesprekken met instellingen blijkt dat bij verschillende instellingen de afgelopen jaren het crisismanagementplan en/of businesscontinuïteitplan vernieuwd zijn en bijvoorbeeld een crisismanager is aangesteld of het integraal veiligheidsmanagement is opgezet. In het crisismanagement zijn over het algemeen scenario's opgenomen met betrekking tot individuen (uiteenlopend van rouw, verward persoon tot sociale veiligheid) en gebouwen (fysieke veiligheid). Enkele instellingen die wij spraken hebben cyber-gerelateerde risico's toegevoegd aan de crisismanagementplannen. Dit wil niet zeggen dat er geen aanpak was voor cyberincidenten, maar dat deze aanpak nog niet altijd in de algemene crisisaanpak was opgenomen. Door cyberincidenten op te nemen in het crisismanagement hebben deze instellingen aangescherpt wanneer er bij de afhandeling van een cyberincident een operationeel team met aanvullende expertise wordt geactiveerd en wanneer andere geledingen worden ingelicht. Daarnaast is de aanpak van een specialistisch team (zoals een *Computer Emergency Response Team*, CERT) op strategisch niveau meer verbonden met integrale veiligheidsverantwoordelijken. De aanpak van een cyberincident, zo geven instellingen aan, verschilt van andere risico's omdat dit direct de hele instelling kan treffen – immers is er bij verschillende onderwijsinstellingen sprake van één ICT-(netwerk)voorziening – terwijl bijvoorbeeld sociale of fysieke veiligheidsvragen zich op een locatie manifesteren. In standaard 4 wordt nader ingegaan op het inschatten van risico's en in hoeverre de expertise uit het operationele crisismanagement daarin wordt benut.

Computer Emergency Response Team (CERT)

Bij de instellingen met een CERT die de inspectie sprak heeft dit CERT inderdaad een rol op operationeel niveau als er een cyberincident plaatsvindt. Grotere instellingen, met name universiteiten, hebben soms ook decentrale CERT-teams die kunnen opschalen naar een centrale CERT. De hogescholen die wij spraken hebben één centraal CERT-team, ook wanneer de hogeschool meer locaties in het land heeft. Signalen die aanleiding geven voor een CERT om in actie te komen, kunnen vanuit de organisatie zelf komen (zie ook standaard 2 mogelijkheden tot melden) of van buiten de onderwijsinstellingen. Signalen van buiten worden vaak verkregen via SURF. De Chief Information Security Officer (CISO) van de onderwijsinstelling is meestal de voorzitter van het CERT. De rollen van andere leden verschillen per instelling. Sommige instellingen hebben zich bij de inrichting van het team vooral gericht op AVG-regelgeving en richten zich daarom vaak op datalekken in plaats van algemene informatiebeveiligingsincidenten. De Functionaris Gegevensbescherming (FG) heeft dan een vaste rol of er is direct een jurist betrokken. In hoeverre er een vaste rol is of wordt opgeschaald naar communicatie, HR functionaris en het bestuur

verschilt per instelling. Bij enkele instellingen wordt de FG en/of een controller ingezet om de incidentenafhandeling te evalueren.

Instellingen met een eigen Security Operations Center (SOC)

Voor een CERT is een signaal over een (mogelijk) incident hét moment om actief te worden. Anders gezegd een CERT is in de praktijk met name responsief. Sinds de cyberaanval op de Universiteit Maastricht wordt nadrukkelijker over de inzet van Security Operations Centers (SOCs) gedacht. Met een SOC wordt ingezet op actiever detecteren van cyberdreigingen om incidenten eerder op te sporen en eventuele aanvallen af te wenden of wat impact betreft te beperken. Cyberdeskundigen werkzaam voor een SOC staan in tegenstelling tot de medewerkers in een CERT volledig ten dienste het (voorkomen) van eventuele cyberincidenten. Met name universiteiten beschikken intussen over een eigen SOC of hebben deze in voorbereiding. Zo hebben de Universiteit van Amsterdam (UvA) en de Hogeschool van Amsterdam (HvA) in de tweede helft van 2020 een eigen SOC ingericht[36]. Op het moment dat UvA en HvA getroffen werden door een incident in februari 2021 was dit SOC vijf dagen per week, 8 uur per dag bemenst. Hierdoor werd de aanval op maandag 15 februari 2021 ontdekt. De aanval was in de loop van het weekend gestart. Na de aanval bij de UM is bij de UvA en HvA het SOC ingericht en besloten tot bovengenoemde beschikbaarheid. De ervaring met het incident bij de instellingen zelf heeft de besturen doen besluiten om naar continue beschikbaarheid (24u/7d) te gaan. De hogescholen die de inspectie sprak hebben eerst andere prioriteiten of wachten de ervaringen voor andere instellingen en de kosten voor aansluiting bij het SURF-SOC af.

Grote versus kleine instellingen

Grote en kleine ho-instellingen verschillen in de afhandeling van cyberincidenten, maar ook op het vlak van inschatten van risico's. Bij kleinere instellingen die de inspectie sprak, zowel bekostigd als niet-bekostigd, wordt de ICT vaak door een kleine groep medewerkers verzorgd. Er is niet altijd een medewerker die zich exclusief bezig houdt met cybersecurity. Echter, voor een effectieve afhandeling van incidenten is er voldoende kennis in huis nodig en op het moment van een crisis kan een instelling niet afhankelijk zijn van slechts één specialist. Kleine(re) instellingen ervaren dat ze operationeel slagvaardig zijn in het crisismanagement. De kleine schaal van de onderwijsinstelling heeft als voordeel dat mensen elkaar snel weten te vinden. De kleine instellingen zijn zich echter ook bewust van de nadelen. De beperkte fte's van de ICT-medewerkers zorgt ervoor dat zij veel (of bijna alle) ICT-diensten moeten verzorgen. Dit zorgt voor dubbelrollen: ze handelen incidenten af, maar zijn na afloop ook de controleur. Daarnaast houden ze weinig tijd over om zicht te houden op eventuele kwetsbaarheden of te oefenen naar aanleiding van incidenten. ICT-medewerkers zijn genoodzaakt keuzes te maken over bij welke (landelijke) netwerken en initiatieven ze aansluiten. Hierdoor zijn kleinere instellingen niet allemaal in dezelfde mate en op hetzelfde moment op de hoogte van recente en meest actuele dreigingsinformatie. Voor bekostigde instellingen is SURF een belangrijke bron van dreigingsinformatie. De meeste rpho's die wij hebben gesproken krijgen echter geen dreigingsinformatie via SURF. Hele kleine rpho's zijn voor informatie afhankelijk van het zelf natrekken van websites, fora en informele contacten om op de hoogte te komen van nieuwe kwetsbaarheden.

[36] 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)

Oefenen draagt bij aan inrichting crisisafhandeling
Instellingen geven aan dat het oefenen van een cyber-crisissituatie hen heeft geholpen, met name om de communicatielijnen te verbeteren tijdens een crisisbestrijding. Vooral wanneer ook het bestuur deelnam (OZON deelname op niveau 'goud', zie paragraaf 3.4), ervaren instellingen de oefeningen als positief. Met de oefening zag de instelling wie rollen oppakt maar ook op welke delen van het beleid aanscherping nodig is. Daarnaast blijft door de oefening de structuur van de crisisaanpak bekend. Uit een jaarverslag van een Pabo bleek dat zij nog niet deel hebben genomen maar dat medewerkers van de Pabo als observant bij een nabijgelegen groter ROC aanwezig waren bij de OZON oefening uit 2018. Verschillende bestuurders plaatsten als kanttekening dat je niet zult weten of je echt voldoet; dat blijkt pas als de instelling door een (groot) incident zoals de Universiteit Maastricht is getroffen of als blijkt dat zo'n type aanval effectief is afgeslagen. De algemene crisisstructuren zijn door instellingen het afgelopen jaar als gevolg van de COVID-19 pandemie veelvuldig benut. In de begin periode (tot de zomer van 2020) was bij verschillende instellingen ICT aangehaakt in het crisismanagementteam van COVID-19. Omdat onderwijs en onderzoek vanuit huis werd uitgevoerd, waren er veel vragen over privacy maar ook over informatiebeveiliging rond ICT-producten. In de latere periode schoof ICT niet meer regulier aan bij het CMT-overleg.

Toegang tot incidentmelding
Een belangrijke taak van het crisisteam is het afhandelen van incidenten. Zonder een dekkend systeem van meldingen kan een crisisteam niet goed functioneren. Kijken we naar informatie over het 'melden van incidenten' op de websites van ho-instellingen (zie tabel 3.2a) dan zijn er totaal 23 instellingen, voornamelijk universiteiten en bekostigde hogescholen, die informatie geven over waar een incident kan worden gemeld. Er is nauwelijks informatie over de afhandeling. Websites die wel informatie over de afhandeling vermelden bieden vrijwel altijd ook de mogelijkheid een melding te doen. De melding kan gedaan worden over een datalek in de zin van AVG en soms in de zin van een ICT-beveiligingsincident. Wanneer expliciet wordt gesproken over beveiligingsincidenten worden vaak contactgegevens van het CERT gegeven. Ook hier is het goed mogelijk dat deze informatie op een andere wijze beschikbaar is voor medewerkers en studenten. Wel roept het de vraag op of de informatie goed vindbaar is op het moment dat een ho-instelling door een cyberincident is getroffen en in hoeverre de gekozen plaats en vindbaarheid bijdraagt aan de open cultuur (standaard 2) om te melden.

Tabel 3.2a Informatie over het melden van incidenten en de afhandeling (op websites) van universiteiten, hbo's en Rpho's (met totaal onderzochte instellingen).

	Universiteiten (18)	**Hogescholen (36)**	**Rpho's (58)**
Melden incidenten	10	10	3
Afhandelen incidenten	4	3	1

Wat betreft de afhandeling van incidenten blijkt uit de analyse van de jaarverslagen dat in totaal 17 ho-instellingen (15 bekostigde hogescholen en 2 universiteiten) hier enige informatie over heeft opgenomen. Er is verschil in wijze van rapporteren. Een hogeschool vermeldt alleen het registratiesysteem, anderen vermelden enkel incidenten die zijn aangemerkt als datalekken, en sommigen vermelden een totaal aantal (ernstige) incidenten waarbij wordt gespecificeerd hoeveel hiervan een datalek of een vermoeden daarvan betrof. Deze informatie is al met al sterk gedreven door de AVG wetgeving. De minister riep in dit verband in haar brief van 19 mei 2021 aan de Tweede Kamer[37] instellingen op hun cyberveiligheidsbeleid op te nemen in de jaarverslaglegging wanneer dit nog niet het geval is.

[37] Tweede Kamer, vergaderjaar 2020-2021, 31 288 en 26 643, nr 910.

Crisisteams voor andere dreigingen

Dat COVID-19 een grote impact heeft op het inschatten van de risico's en daarmee het inrichten van crisisteams blijkt uit de gegevens in de jaarverslagen. De aanpak van het crisismanagement (CMT) rond de pandemie is door een twaalftal instellingen (twee universiteiten en 10 bekostigde hogescholen) in het jaarverslag 2019 besproken. De instellingen gaan in op de samenstelling van het CMT, de frequentie waarin werd overlegd en op bespreekpunten zoals de impact op het primaire en ondersteunende proces. De COVID-19-CMT's zorgen ervoor dat de organisatie handelt in lijn met de door de (rijks)overheid afgegeven richtlijnen en denkt na over de postcorona-periode. In het kader van de COVID-19 monitor[38] heeft de inspectie met ho-instellingen gesproken over het crisismanagement. In deze gespreken gaven instellingen aan dat in de crisisafhandeling het mogelijk was snelle besluitvorming te realiseren waarbij veel geledingen uit de organisatie inclusief de medezeggenschap (ook indien dit niet verplicht is) werden betrokken. Dit heeft de inspectie ook geconstateerd over de crisisafhandeling van de cyberaanval bij de Universiteit Maastricht. Uit de COVID-19 monitor kwam naar voren dat er afgeschaald dient te worden – terug naar de reguliere organisatie – zodat niet te lang in de crisisorganisatie wordt geopereerd. Ook werd aangegeven dat het maken van duurzame beslissingen in een crisisperiode punt van aandacht is. Naast de instellingen die over een crisisteam op het vlak van cyber of COVID-19 rapporteerden, was er één instelling die de organisatie rond fysieke veiligheid (zoals branden) heeft opgenomen in het jaarverslag.

3.3 Stelsel hoger onderwijs

Definitie van de standaard voor het stelsel:

Op stelselniveau is er een risicoteam dat zicht heeft op (stelsel)risico's in het (hoger) onderwijs. In dat risicoteam zijn diverse disciplines vertegenwoordigd: privacy, onderwijslogistiek, cyber, onderwijskwaliteit, beleid, naleving. Bij incidenten binnen een ho-instelling is dit risicoteam eerste aanspreekpunt voor instellingen. Bij grotere incidenten functioneert het risicoteam ook als het crisismanagementteam. Indien relevant worden (interne/externe) toezichthouders op de hoogte gebracht door (het bestuur van) de instelling.

Sterktes

- Er zijn verschillende organisaties actief die tezamen over een enorme expertise beschikken.
- SURF organiseert tweejaarlijks een landelijke oefening gericht op de crisisorganisatie, waar steeds meer universiteiten, hogescholen en ook mbo-instellingen aan deelnemen.
- Na de aanval op de UM is in gezamenlijkheid SURF-SOC opgezet, die een specialistische partij inhuurt om mogelijke incidenten op het centrale onderwijsnetwerk te detecteren en is SURF aangewezen als computercrisisteam voor onderwijs en onderzoek om zo dreigingsinformatie van het NCSC voor de sector te kunnen ontvangen.

Zwaktes

- Er is geen coördinatie tussen organisaties op stelselniveau, waardoor er niet echt sprake is van een risicoteam dat zicht houdt op het stelsel.
- Niet alle ho-instellingen kunnen in dezelfde mate over dreigingsinformatie beschikken, enerzijds door de omvang – kleinere organisaties hebben niet altijd de menskracht in alle netwerken zelf vertegenwoordigd te zijn – en anderzijds doordat rpho's niet kunnen

[38] IvhO (2020) *Covid-19 monitor HO meting 3*. Utrecht: Inspectie van het Onderwijs. Zie: https://www.onderwijsinspectie.nl/onderwerpen/corona-onderzoeken/documenten/publicaties/2020/11/24/covid-19-monitor-ho-derde-meting

deelnemen aan de netwerken en informatiestromen die de bekostigde hogescholen en universiteiten benutten.
- Voor het onderwijs bestaat een meldingsplicht indien er sprake is van een (mogelijk) datalek als gevolg van een cyberincident bij de Autoriteit Persoonsgegevens. Informeren van andere toezichthouders en overheidspartijen over het optreden van een incident is aan het bestuur en de raad van toezicht van de ho-instelling.

Kansen
- Er is bereidheid tot samenwerking ook tussen universiteiten en hogescholen.
- In het bijzonder om met elkaar mee te denken nadat een groot cyberincident heeft plaatsgevonden; dit is alleen vooralsnog sterk afhankelijk van bestaande onderlinge relaties.
- Politieke druk vanuit WRR rapport en aandacht als gevolg van de COVID-19 pandemie voor de afhankelijkheid van de digitale infrastructuur voor het kunnen continueren van het hoger onderwijs.

Bedreigingen
- Rollen zijn vaak wettelijk bepaald, hetgeen samenwerking bemoeilijkt.
- Niet alle ho-instellingen zijn aangesloten bij risicoteams op stelselniveau – en ontvangen daarom geen actuele dreigingsinformatie.
- In Nederland is gekozen voor een decentrale structuur waarbij veel partijen betrokken zijn die bovendien verschillen voor vitale en niet-vitale sectoren. Daarmee kan er bij partijen die betrokken zijn bij de bescherming van de vitale sectoren informatie zijn over dreigingen gericht op specifieke organisaties in een niet-vitale sector (waaronder onderwijs) die de betreffende onderwijsinstelling niet bereikt.

Toelichting op de standaard

Cyberincidenten gerelateerd aan datalekken hebben een individuele oorsprong. Dat geldt niet noodzakelijk bij cyberaanvallen, zeker niet als een aanvaller van buiten de ho-instelling komt. Een aanval op één onderwijsinstelling kan daarmee de risicodetectie van anderen voeden. Bij de aanval in 2019 op de Universiteit Maastricht is dat ook gebeurd. De UM heeft specifieke informatie over de aanval – de IoC's (*Indicators of Compromise*) – via het SURF-CERT aan andere ho-instellingen beschikbaar gesteld om te voorkomen dat ook andere instellingen slachtoffer zouden worden. Bij een aanval op een instelling speelt vaak ook een stelselbelang. Ook kan er op stelselniveau relevante informatie, kennis en kunde aanwezig zijn die de individuele instelling kan helpen om te acteren. Tenslotte kan er sprake zijn van een aanval die verschillende instellingen treft of die nationale of gedeelde infrastructuren voor het onderwijs treffen. In al die gevallen kan een gezamenlijk risicoteam en een crisismanagementteam een belangrijke rol spelen. Daarom hebben we met instellingen gesproken over in hoeverre de functionaliteit van zo'n risicoteam landelijk of regionaal gewenst en aanwezig is.

De initiatieven op het stelselniveau gaan uit van de verantwoordelijkheid bij de bestuurders. Als een incident optreedt zijn zij aan zet om beslissingen te nemen. Dat blijkt ook uit de verschillende incidenten die bij instellingen hebben plaatsgevonden. De positie van het stelsel is vooral gericht op ondersteuning van instellingen daar waar opbouw van specialistische expertise gezamenlijk meerwaarde biedt. Dit is gericht op de voorkant van incidenten zodat de respons van instellingen kan verbeteren.

3.4 Bevindingen

Samenwerking tussen instellingen

Op diverse plekken in het hoger onderwijs is er kennis en kennisdeling over respons op en afhandeling van cyberincidenten. Die kennis wordt ook beschikbaar gesteld buiten de hoger onderwijssector. We zien weinig gebruik van elkaars expertise op

het moment dat zich daadwerkelijk een cyberincident voordoet. Uit het onderzoek bij de Universiteit Maastricht bleek dat de UM zelf een externe partij heeft ingehuurd om het forensisch onderzoek uit te voeren en bij te staan in het herstellen van de ICT-infrastructuur. In gesprekken kwamen enkele voorbeelden naar voren waarbij als gevolg van een gebrek aan goede ICT'ers, instellingen in gesprek zijn gegaan met andere instellingen in de buurt, om tijdelijk meer capaciteit te kunnen benutten. We hebben geen voorbeelden vernomen waarbij tijdens een crisisafhandeling expertise van anderen is ingezet. Dit in tegenstelling tot de aanpak van COVID-19. Op dat vlak is naar aanleiding van de overheidsmaatregelen op regionaal niveau afstemming geweest. Bijvoorbeeld over testfaciliteiten en de vraag hoe het openbaar vervoer meer gespreid kon worden belast. Instellingen gaven aan dat met de COVID-19 pandemie – meer dan bij de cyberaanval op de UM – instellingen allemaal op dezelfde wijze de crisis ervaarden.

SURF

Als bron voor informatie over risicodetectie op stelselniveau wordt door ho-instellingen in het bijzonder naar SURF gekeken. SURF geeft voorlichting over inrichtingsmogelijkheden van een risicoteam op instellingsniveau, met aandacht voor instellingsverschillen. Niet alleen binnen het hoger onderwijs, maar ook daarbuiten staat SURF bekend als een belangrijke speler met veel expertise. Partijen buiten het onderwijs geven aan dat SURF nauwe banden heeft met de wetenschap en zo eenvoudiger dan soortgelijke partijen in andere sectoren de nieuwste ontwikkelingen kent. Ook binnen de sector zijn partijen positief over SURF. In het bijzonder als platform om informatie uit te wisselen, bijvoorbeeld via congressen. Daarbij is er geen onderscheid tussen het hoger beroepsonderwijs en het wetenschappelijk onderwijs.

SURF-CERT

SURF heeft een centrale rol in de detectie van dreigingen die op het stelsel afkomen. SURF heeft een eigen *Computer Emergency Response Team*. SURF-CERT is sinds 24 januari 2020 door de minister van Justitie en Veiligheid aangewezen als één van de informatieknooppunten van niet-vitale infrastructuren die in nauw contact staat met Nationaal Cyber Security Centrum (NCSC)[39]. Door deze aanwijzing kan het Nationaal Cyber Security Center (NCSC) dreigingsinformatie delen met het hoger onderwijs. Het NCSC houdt de CISO /CERT van SURF op de hoogte van (actuele) veiligheidsrisico's. Vanuit de wet Wbni wordt deze dreigingsinformatie enkel met de zogenaamde vitale infrastructuren gedeeld. Ook communiceert het SURF-CERT informatie die binnen het onderwijsveld wordt verzameld bij incidenten naar het NCSC. Het onderscheid tussen vitale en niet-vitale infrastructuren wordt bekritiseerd, onder andere omdat informatie die over bedrijven in niet-vitale sectoren beschikbaar is bij het NCSC, niet zonder meer gedeeld wordt naar deze bedrijven. Door de aanwijzing van SURF-CERT kan onder voorwaarden relevante informatie wel met het hoger onderwijs worden gedeeld.

Via mailings kan het SURF-CERT instellingen op de hoogte brengen van mogelijke nieuwe dreigingen, bijvoorbeeld over een nieuw soort *phishing* mail die rondgaat. Instellingen melden na dergelijke informatie aan SURF terug of zij dit hebben aangetroffen. Op basis hiervan ontstaat een gedeeld beeld over de omvang. Met de aanwijzing van het SURF-CERT kan informatie vanuit het NCSC naar de sector hoger onderwijs worden gedeeld. In hoeverre daarmee het hoger onderwijs voldoende wordt bediend is in de komende tijd te bezien. Binnen de hoger onderwijssector lijkt zich eenzelfde fenomeen als tussen vitale en niet-vitale infrastructuren voor te doen:

[39] Dit is bepaald in de regeling aanwijzing computercrisisteams, Staatscourant 2020, 4410. Meer informatie over het NCSC is te vinden in paragraaf 2.3 betrokken actoren.

SURF-CERT kan over de dreigingsinformatie beschikken, maar niet alle onderwijsinstellingen zijn aangesloten bij SURF of bij SURF-CERT en ontvangen zodoende geen dreigingsinformatie. Alle grote bekostigde universiteiten en universitaire medische centra zijn bij SURF en het SURF-CERT aangesloten. De meeste bekostigde hogescholen zijn lid van SURF. Van de bekostigde hogescholen is 94 procent ook aangesloten bij SURF-CERT. Rpho's kunnen bijvoorbeeld als niet-bekostigde instelling klant maar geen lid worden van SURF. Dit betekent dat niet alle ho-instellingen in dezelfde mate aangesloten zijn op mogelijk relevante dreigingsinformatie die bij SURF beschikbaar komt. Dit geldt ook voor mbo-instellingen, niet alle bekostigde mbo-instellingen zijn namelijk lid van SURF.

Security Operations Center (SOC)

De (toegenomen hoeveelheid) dreigingsinformatie moet worden verwerkt. Daarnaast ontstond er naar aanleiding van de aanval op de UM bij verschillende instellingen de behoefte aan versterking van detectie en monitoring om zo (mogelijke) incidenten eerder in beeld te krijgen. Voor individuele instellingen is het niet of nauwelijks haalbaar voldoende gekwalificeerde mensen continu (24 uur per dag, zeven dagen per week) beschikbaar te hebben hiervoor. Daarom is er via SURF een gezamenlijk *Security Operations Center* (SOC) opgericht voor het hoger onderwijs. Het SURF-SOC is continu beschikbaar om op basis van signalen van een (mogelijk) incident in actie te komen. Een SOC detecteert cyberdreigingen pro-actiever om zo incidenten eerder op te kunnen sporen en eventuele aanvallen af te wenden of qua impact te beperken. In januari 2021 is het SURF-SOC gelanceerd. SURF heeft een overeenkomst met FOX-IT gesloten om security incident en event managementdiensten (SIEM) te leveren. Eind april 2021 was Universiteit Wageningen de eerste ho-instelling die aangesloten is op het SURF-SOC[40]. In eerste instantie sluiten de grote universiteiten en enkele grotere hogescholen aan. Met name de grotere universiteiten zijn vanuit meerdere perspectieven (zie paragraaf 2.1) mogelijk kwetsbaar voor cyberincidenten. De hogescholen die de inspectie sprak hebben eerst andere prioriteiten of wachten de ervaringen bij andere instellingen af. Uit onze gesprekken blijkt dat de capaciteit bij kleine onderwijsinstellingen dermate beperkt is, dat zij niet altijd kunnen aansluiten op organisaties zoals het SURF-SOC, die dreigingsinformatie delen.

Crisisoefeningen – OZON

In het onderwijs wordt sinds 2016 twee jaarlijks een gezamenlijk cyberoefening OZON uitgevoerd. Het opzetten, uitvoeren en evalueren van de oefening wordt door SURF gecoördineerd. Bij OZON gaat het om een gesimuleerd cyberincident dat uitmondt in een crisis om zo het crisismanagement van een onderwijsinstelling te testen. Er is in het verleden geoefend met een nagebootste cyberaanval waarna studenten tegen betaling cijfers konden ophogen (2016), een cyberaanval met een losgeldeis (2018) en een hack door een statelijke actor waarna vertrouwelijke gegevens van studenten worden aangeboden op internet (2021). Het aantal deelnemende onderwijsinstellingen is in de loop van de jaren toegenomen. In 2021 namen 65 instellingen deel; dit zijn niet alleen ho-instellingen ook enkele mbo-instellingen en ziekenhuizen participeren in de oefening. Deelname is mogelijk op verschillende niveaus: goud (operationeel, tactisch en strategisch niveau), zilver (tactisch en operationeel) en brons (operationeel niveau op kleiner scenario).

Lessen Universiteit Maastricht benut bij latere incidenten

De UvA en HvA huurden net als de UM een externe partij in om gebruik te maken van hun kennis over de aanvalsstrategie van de hackers, om de expertise in het

[40] 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)

uitvoeren van forensisch onderzoek en om het SOC van de UvA/HvA op korte termijn 24/7 te laten opereren[41]. Voor dit soort partijen is forensisch onderzoek corebusiness die zij dagelijks voor allerlei bedrijven doen. Bestuurders geven aan dat je zulke specialistische kennis die zelden nodig is, niet zelf moet organiseren maar moet inschakelen op het moment dat dit nodig is. Ook bij deze aanval is snel (aanvals)informatie die het CERT en SOC van de UvA/HvA hadden gevonden, via SURF-CERT gedeeld, zodat andere instellingen kunnen zoeken naar afwijkend gedrag door deze externe partij. Hoewel dit incident niet uitmondde in een gijzeling, speelden in de crisisafhandeling bij de UvA en HvA enkele kwetsbaarheden die ook bij de UM naar voren waren gekomen. Een daarvan is het beperkte zicht op de assets, in het bijzonder onvolledige informatie over de aanwezigheid van systemen en eigenaren van systemen. Dit hangt samen met een aanbeveling aan UvA en HvA die het COT[42] benoemt: maak keuzes hoe om te gaan met het dilemma tussen de mogelijkheden van beveiligingen en de praktische behoeften van docenten en studenten wat betreft gebruiksgemak (zie ook standaard 7).

Ook Hogeschool Inholland werd in 2021 getroffen door een hack. Inholland werd op 1 maart door het SURF-CERT geïnformeerd over data die in openbare bronnen was aangetroffen die mogelijk afkomstig zijn van de hogeschool. Het CERT van de hogeschool heeft na de melding vanuit SURF het forensisch onderzoek opgepakt en opgeschaald naar een crisisorganisatie met CMT waarin ook de directeur ICT, FG en bedrijfsjurist waren aangesloten. De groep medewerkers en studenten waar de melding van toepassing op was, werd aangeraden om wachtwoorden te wijzigingen. Later werd duidelijk dat het lek betrekking had op een selecte groep van accounts[43]. Net als bij andere incidenten is de hogeschool zelf verantwoordelijk voor het oplossen van het incident. Er was afstemming op stelselniveau, eerst doordat SURF Hogeschool Inholland informeerde over een mogelijk datalek en later informeerde SURF andere hogescholen met informatie uit het lopende onderzoek bij Inholland.

Betrekken Raad van Toezicht bij oefenen en incidenten

Hoewel RvT doorgaans bij een (grote) crisis worden aangesloten is dit lang niet overal een vast onderdeel van de crisisplannen. Bij crisisoefeningen – zoals OZON – is de RvT tot nog toe geen partij. Bij de afhandeling van de cyberaanval bij de Universiteit Maastricht was destijds ook de Raad van Toezicht betrokken. Ook werd contact met OCW en de Inspectie van het Onderwijs gelegd. Het bestuur heeft de RvT meegenomen in de belangrijke beslismomenten tijdens de afhandeling van de crisis. Omdat er kort voor het incident een scholingsdag op eigen verzoek voor de RvT was georganiseerd rond het thema ICT-security en privacy door de universiteit, had de RvT een beeld van de informatiebeveiliging binnen de organisatie en de mensen die hieraan werken. Of RvT-leden van andere (hoger) onderwijsinstellingen op het vlak van cyberveiligheid een beeld hebben van de risico's, incidenten die optreden en de wijze waarop de organisatie dit onderwerp aanpakt, hangt sterk af van de geagendeerde onderwerpen tijdens overleg tussen RvT en het bestuur. In één van de gesprekken kwam naar voren dat de voorzitter van het CvB het interview met de inspectie voor dit stelselonderzoek had besproken met de voorzitter van de RvT, mede omdat crisismanagement een aandachtsgebied is van betreffende RvT-voorzitter in zijn hoofdfunctie elders. In gesprekken met voorzitters van Raden van Toezicht van universiteiten en bekostigde hogescholen kwam naar voren dat zij de ontwikkelingen rondom cyberveiligheid met belangstelling volgen.

[41] 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)

[42] Zie voetnoot 41.

[43] Voor meer informatie zie: https://www.inholland.nl/voor-studenten-en-medewerkers/datalek-vragen-antwoorden/ (geraadpleegd op 19-7-2021)

Ze willen nagaan hoe ze kennis kunnen opbouwen om bij eventuele crises als gesprekspartner en/of controleur van het bestuur te kunnen optreden. Er is nadrukkelijk een wens om gezamenlijk kennis uit te wisselen om te weten wat de goede checkvragen zijn, en om te zien wat een goede handelwijze is als er zich een incident voordoet.

Extern toezicht

Zoals in paragraaf 2.1 aangegeven zijn er verschillende soorten cyberincidenten die voortkomen uit verschillende bronnen en gericht kunnen zijn op verschillend type data. Op het moment dat een cyberincident gerelateerd is aan persoonsgegevens komt de Autoriteit Persoonsgegevens (AP) in beeld. Instellingen zullen dan een vermoeden van datalek moeten melden.

Voor andere incidenten zijn er geen voorschriften ten aanzien van het toezicht in het onderwijsdomein. De vitale infrastructuren kennen dit soort voorschriften wel. Het Ministerie van Veiligheid en Justitie (VenJ) heeft naar aanleiding van het WRR rapport “Voorbereiden op digitale Ontwrichting” en het Cybersecuritybeeld Nederland 2020 samen met betrokken departementen een overzicht van de huidige wettelijke taken gemaakt[44]. Het overzicht gaat in op wettelijke verplichtingen, op mogelijkheden om te interveniëren in geval van een digitale dreiging of incident en op het delen van informatie in geval van een digitale dreiging, kwetsbaarheid of incident. De wettelijke verplichtingen gaan over zorgplichten en meldplichten in de vitale infrastructuren. Op grond van de Wbni is er bij een incident een meldplicht bij VenJ en kan er betrokkenheid zijn van de Inspectie Justitie en Veiligheid. Interventiemogelijkheden liggen veelal besloten in de sectorwetten. Het kan dan gaan om aanwijzingen in geval van een incident, maar ook om voorschriften ten aanzien van het waarborgen van de beheersbaarheid van risico’s indien een incident optreedt. Hierbij kunnen sectorale toezichthouders betrokken zijn.

Toezichthouders en ook beleidsdepartementen hebben door de sturingsfilosofie op cyberveiligheid in Nederland beperkt zicht op de dreigingen en incidenten in de eigen sector. De toegenomen aandacht mede naar aanleiding van grote(re) incidenten heeft ertoe geleid dat binnen de Inspectieraad, waarin alle toezichthouders verenigd zijn, het onderwerp cyberveiligheid afgelopen jaar op de agenda in prioriteit is toegenomen. Daarbij wordt ook gekeken hoe toezichthouders met meer technische kennis rond cyberveiligheid andere toezichthouders die sectorale kennis hebben kunnen bijstaan.

Onderwijsinstellingen hebben niet de verplichting om alle (cyber)incidenten bij de Inspectie van het Onderwijs te melden. Net als bij andere incidenten wegen besturen zelf af of ze actief incidenten melden. Bij grote aanvallen zoals de Universiteit Maastricht en dit jaar de Universiteit van Amsterdam en de Hogeschool van Amsterdam gebeurde dit wel. Signalen die de inspectie bereiken, door een onderwijsinstelling zelf of anderszins, kunnen voor ons aanleiding zijn om contact op te nemen met het bestuur. Indien mogelijk de kwaliteit van het onderwijs en/of de continuïteit van de organisatie in het geding is, kan worden besloten een onderzoek in te stellen. Dit geldt voor zowel universiteiten, bekostigde hogescholen als rpho’s.

Uitgangspunt van de Nederlandse overheid is dat er geen losgeld wordt betaald aan cybercriminelen. Zeker indien een instelling rijksbekostiging ontvangt zal bij een losgeldbetaling de uitgaven en de afweging om tot betalen over te gaan moeten worden verantwoord. De inspectie kijkt in het algemeen naar rechtmatige en doelmatige besteding van overheidsmiddelen. Ook ten aanzien van een

[44] Bijlage ‘Overzicht wet- en regelgeving cybersecurity’ bij TK, vergaderjaar 2020-2021, 26 643, nr 738.

losgeldbetaling komen deze vragen aan bod. Met het oog op het uitgangspunt van de Nederlandse overheid worden betalingen aan criminele organisaties en/of voor criminele activiteiten, zoals het afpersen voor toegang tot het onderwijs, als niet rechtmatig beschouwd. Die uitgaven kunnen wel doelmatig – in de zin van kostenefficiënt – zijn, namelijk om het onderwijs sneller en/of goedkoper dan via legaal herstel weer toegankelijk te krijgen. De uitkomst van doelmatigheid versus rechtmatigheid kan per hack aanval verschillen. Bij de grote incidenten die zich na de Universiteit Maastricht hebben voorgedaan in het hoger onderwijs is voor zover de Inspectie van het Onderwijs bekend geen sprake geweest van een losgeldeis.

4 Standaard 4: borgen risicomanagement

4.1 Instellingen hoger onderwijs

Definitie van de standaard voor instellingen:

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.

Sterktes

- Grote instellingen beleggen de verantwoordelijkheid voor het beheersen van cyberrisico's vrijwel altijd bij een apart persoon en/of eenheid in de organisatie; kleine instellingen beleggen de verantwoordelijkheid hiervan soms buiten de organisatie.
- De meeste ho-instellingen kennen al een goed uitgewerkte kwaliteitszorgcyclus, risico's worden daarin ook meegenomen.

Zwaktes

- Niet alle ho-instellingen hebben de verantwoordelijkheid voor cyberrisicomanagement in de organisatie belegd. Bij kleine instellingen wordt dit meestal veroorzaakt door de beperkte capaciteit.
    - Kleine instellingen kunnen door de overzichtelijke omvang van de digitale omgeving soms vertrouwen op enkele mensen met ICT-expertise. Echter de afhankelijkheid van één persoon kan de instelling kwetsbaar maken.
    - De urgentie van risicomanagement rond cybersecurity is bij sommige instellingen slechts bij een deel van de organisatie aanwezig, meestal de ICT en soms het CvB. De urgentie dringt niet altijd door tot in alle hoeken van de organisatie. Niet elke instelling heeft cyberrisico's opgenomen in beleidsplannen en het onderwerp heeft niet in alle bestuurlijke lagen de aandacht. Cyberrisico's worden door decentrale eenheden niet als hoog risico geprioriteerd.

Kansen

- De cyberaanval bij de UM heeft ervoor gezorgd dat risicomanagement rondom cybersecurity binnen ho-instellingen vaker op de bestuurstafel komt en sommige instellingen maatregelen hebben genomen om de beveiliging op te schroeven.
- Bij ho-instellingen met een goed uitgewerkte kwaliteitszorgcyclus, is inbedding van cyberrisico's in bestaande verbeterprocessen goed mogelijk.
- De acute dreiging van COVID-19 heeft geleid tot veel aandacht voor risicomanagement door alle lagen van de organisatie heen – en kan dienen als goed voorbeeld.

Bedreigingen

- De ICT-inrichting van grote universiteiten is vanwege de omvang en de decentrale ICT-inrichting onoverzichtelijker dan van kleine hogescholen. Sommige universiteiten hebben eigen ICT-diensten binnen de organisatie, door bijvoorbeeld specialistische ICT behoeften binnen het primaire proces. Hierdoor is het voor de centrale ICT-dienst moeilijker een totaalbeeld van de organisatie te behouden.
- Wanneer cyberincidenten op de achtergrond verdwijnen – of er meer acute dreigingen zoals COVID-19 aanwezig zijn – wordt het beheersen van cyberrisico's mogelijk niet langer als urgent aangemerkt en het risico mogelijk ten onrechte laag ingeschat.
- Risicomanagement wordt een papieren oefening wanneer instellingen enkel streven naar verantwoording door (jaar)verslaglegging en risico-evaluaties niet worden opgevolgd door acties.

Toelichting op de standaard

Standaard 4 – borgen van het risicomanagement – kan gedefinieerd worden als *alle systematische acties die nodig zijn om ervoor te zorgen dat het risicomanagement*

voldoet aan voldoende kwaliteitseisen. De acties die nodig zijn voor het borgen van het risicomanagement moeten systematisch zijn, omdat een risico-inschatting op geen één moment hetzelfde is. Dreigingen, de omgeving en wetgeving veranderen continu, waardoor de soorten risico's, de beoordeling van de impact van de risico's en de mogelijke gevolgen ook continu veranderen. Risicomanagement detecteert en anticipeert op de veranderingen en gebeurtenissen op een gepaste en tijdige manier, zodat de maatregelen doeltreffend en doelmatig blijven. Daarom moet risicomanagement een cyclisch, iteratief en terugkerend proces zijn.

Vastleggen verantwoordelijkheden cyberrisicomanagement in de organisatie

De eerste voorwaarde voor het borgen van risicomanagement die uit standaard 4 volgt is dat instellingen functionarissen moeten aanwijzen die verantwoordelijk zijn voor het identificeren en beoordelen van cyberrisico's, en dat deze verantwoordelijkheden belegd moeten worden binnen de gehele organisatie (zie ook de tien bestuurlijke principes die vastgelegd zijn voor gemeentelijke bestuurders[45]). Lijnmanagers kunnen verantwoordelijk gemaakt worden voor risicomanagement door afspraken met ze te maken over de risicobereidheid van de organisatie. Lijnmanagers zijn tevens verantwoordelijk voor de maatregelen en rapportage daarover. De kennis en verantwoordelijkheid van proces- en systeem eigenaren, zoals de *Chief Information Security Officer* (CISO), Functionaris Gegevensbescherming (FG) en Controller als onafhankelijke adviseurs, kunnen gebruikt worden.

Informatie-uitwisseling cyberrisico's binnen de organisatie

De risico-inschattingen en afwegingen moeten tevens kunnen leiden tot maatregelen om de eventuele impact van de cyberrisico's te verkleinen. Dit betekent dat de mensen met het mandaat om maatregelen te nemen, moeten spreken met de functionarissen die verantwoordelijk zijn voor het monitoren en evalueren van de risico's. Om structurele informatie uitwisseling over cyberrisico's te garanderen en tot maatregelen over te gaan wanneer dat nodig is, zullen instellingen overlegstructuren moeten vastleggen tussen de juiste mensen binnen de organisatie. Dit betekent dat de lijn en frequentie van het gesprek is vastgelegd en de lijn door de hele organisatie heen gaat (centraal en decentraal), het CvB goed contact heeft met ICT-functionarissen (CIO, CISO), en dat er directe betrokkenheid is van decanen en onderwijs/onderzoeksdirecteuren van andere organisatieonderdelen (vestigingen, faculteiten, vakgroepen, onderzoeksgroepen).

Integreren cyberrisicomanagement in alle werkprocessen van de organisatie

De laatste voorwaarde voor het borgen van risicomanagement die uit standaard 4 volgt is dat historische en actuele informatie over cyberrisico's die prioriteit hebben, tijdig, duidelijk en beschikbaar moet zijn, en periodiek uitgewisseld moet worden. Risicomanagement werkt dan ook alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Het bemachtigen van de meest recente informatie over relevante risico's kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek/paragraaf krijgen in alle bestuurlijke documenten (zie ook IBD, 2019). De aandacht voor cyberrisico's moet dan ook worden vastgelegd en uitgewerkt in kwaliteitszorgcycli (bijvoorbeeld: informatie-beveiligingsbeleid) – waarmee wordt voorkomen dat de risico's worden geregeerd (of genegeerd) door de waan van de dag en waardoor de afhandeling van risico's wordt geëvalueerd en leidt tot verbetering in lopende processen.

[45] De Informatie Beveiligingsdienst (IBD) van de VNG heeft in 2019 tien bestuurlijke principes op een rij gezet voor gemeentelijke bestuurders. Zie: https://www.informatiebeveiligingsdienst.nl/product/de-10-bestuurlijke-principes-voor-informatiebeveiliging/ (geraadpleegd op 19-7-2021)

4.2 Bevindingen

Vastgelegde verantwoordelijkheid cyberrisicomanagement

Uit de gesprekken blijkt dat grote instellingen de verantwoordelijkheid voor cyberrisicomanagement vaak bij een apart persoon en/of aparte eenheid in de organisatie hebben belegd. Wanneer deze verantwoordelijkheden belegd zijn, vinden er veelal ook structurele gesprekken plaats tussen bestuur en ICT. Bekostigde universiteiten hebben bijvoorbeeld vaak een CvB-lid dat bedrijfsvoering in portefeuille heeft, waar informatiebeveiliging ook bij hoort. De CISO rapporteert aan de CIO en heeft een directe lijn, ook in het geval van een cyberincident of crisis, naar het CvB-lid met ICT in portefeuille. De CISO/CIO heeft periodiek, bijvoorbeeld maandelijks, een gesprek met CvB-lid en is periodiek, bijvoorbeeld ieder kwartaal, aangesloten bij een overleg met het gehele CvB en de decanen, over de investeringsagenda en risico's. De CISO is in de organisatiestructuur bij grote instellingen op verschillende plekken gepositioneerd: bij de bestuurs-staf of in de centrale ICT-afdeling. De verantwoordelijkheid voor cyberveiligheid kan bij instellingen in zowel de centrale en decentrale delen van de organisatie belegd zijn. Zo geeft een hogeschool aan dat het lijnmanagement bestaat uit een netwerk van contactpersonen in de verschillende faculteiten. Iedere faculteit is verantwoordelijk voor de informatiebeveiliging van eigen processen. Het CvB heeft periodieke gesprekken met faculteits- en dienstdirecteuren waarvan informatiebeveiliging één van de onderwerpen is. Sommige bekostigde universiteiten hebben eigen ICT-diensten binnen de organisatie door bijvoorbeeld specialistische behoeften binnen het primaire proces als intensieve high performance computing eisen (werken met simulaties en grote datasets). Hierdoor is het voor de centrale ICT-dienst mogelijk moeilijker een totaalbeeld van de organisatie te behouden.

Er zijn kleine instellingen die de verantwoordelijkheid voor risicomanagement rond cybersecurity apart binnen – of buiten – de organisatie hebben belegd. Een kleine bekostigde instelling geeft aan kleinschalig te zijn, waardoor de lijntjes kort zijn. Toch hebben zij vastgelegd wie verantwoordelijk is voor ICT-beveiliging en wanneer structurele bijeenkomsten tussen bestuur en hoofd-ICT plaatsvinden en wat er besproken moet worden. Een kleine bekostigde universiteit geeft aan geen aparte specialisten te hebben op HRM of op ICT, zij heeft ICT bij een bedrijf in de regio ondergebracht, waardoor het onderwerp duidelijk is belegd. Wanneer een instelling de ICT volledig uitbesteedt, is het echter nog steeds essentieel dat het bestuur op de hoogte blijft van de (top) cyberrisico's binnen de organisatie.

Niet vastgelegde verantwoordelijkheid cyberrisicomanagement

Uit de gesprekken blijkt dat grote instellingen de verantwoordelijkheid voor risicomanagement op het vlak van cyberveiligheid niet altijd bij een apart persoon en/of aparte eenheid in de organisatie hebben belegd. Een grote bekostigde universiteit geeft aan dat de ICT-afdeling – en daarmee ook risicomanagement rondom cybersecurity – niet apart belegd is binnen de organisatie. De universiteit geeft zelf aan dat het eigenlijk vreemd is dat bij de faculteitsbureau's ICT niet apart belegd is naast een hoofd HR en een hoofd Financiën. Deze laatste bedrijfsvoeringstaken hebben daarmee binnen een faculteit een duidelijke probleemeigenaar. Ook een grote rpho geeft aan dat er geen aparte risicomanager is, maar dat de borging in de organisatie moet zitten, in de open cultuur – 'iedereen is een *security* en *privacy officer*'. Het vergt investering in de organisatie zodat dit ook door alle mensen zo wordt ervaren. Er is echter wel een CIO en een *Security Officer*.

Uit de gesprekken blijkt dat kleine instellingen de verantwoordelijkheid voor risicomanagement rond cyberveiligheid ook niet altijd bij een (apart) persoon of (aparte) lijn in de organisatie hebben belegd. Voor sommige instellingen werkt dit goed, echter niet voor alle. Een middelgrote bekostigde hogeschool heeft gekozen om geen integraal risicomanager aan te stellen, omdat dat mogelijk alleen een papieren zekerheid is. In plaats daarvan beleggen ze de verantwoordelijkheden zo veel mogelijk in de bestaande lijn. Een kleine rpho geeft aan dat de verantwoordelijkheid niet specifiek belegd is en dat er geen rapportagestructuur is. Zij geeft aan dat dit niet nodig is vanwege de kleinschaligheid en het kleine aantal veranderingen. Er is één persoon betrokken bij ICT-ontwikkelingen die ook aan het bestuur rapporteert. De medewerkers van de ICT-afdeling van een kleine hogeschool geven ook aan dat het bestuur de verantwoordelijkheid voor cybersecurity bij niemand heeft belegd. De ICT-afdeling wordt volgens hen vrijwel enkel gezien als dienstverlener. Incidenten worden gemeld bij het bestuur, maar het is geen structureel onderdeel van de bedrijfsvoering. Het belang van cyberveiligheid wordt volgens de ICT-afdeling beaamd door medewerkers, maar is secundair aan het onderwijs (zie ook standaard 1).

De informatie op de websites van ho-instellingen lijkt te suggereren dat ICT vaak, maar niet altijd, een eigenstandig onderdeel is binnen de organisatie. Eenendertig van de 54 bekostigde ho-instellingen hebben een organogram op de website staan, waarvan de meerderheid vermeldt waar in de organisatie de centrale ICT-afdeling zich bevindt. Twaalf van de 58 rpho's hebben op de website een organogram staan, waarvan bij de helft een ICT-afdeling vermeldt. Wanneer instellingen ICT vermelden in de organogram is de meest voorkomende structuur: College van Bestuur → Diensten / Staf → ICT afdeling. Regelmatig vormt ICT samen met facilitaire zaken een gezamenlijk organisatieonderdeel, bij universiteiten soms met de bibliotheekdiensten. Bij sommige instellingen is er onderscheid tussen de ICT en informatiebeveiliging zichtbaar in de organogram. Bij sommige universiteiten is er een apart expertisecentrum voor ICT, dat vaak ook buiten de instelling op het gebied van ICT(veiligheid) opdrachten heeft, advies geeft of onderdeel is van bredere netwerken. Er is geen informatie te vinden over een decentrale indeling van de ICT-afdeling bij instellingen.

Integratie cyberrisicomanagement bij besturen na cyberaanval Universiteit Maastricht

Uit de gesprekken komt naar voren dat de cyberaanval bij de UM in december 2019 ervoor heeft gezorgd dat risicomanagement rondom cybersecurity binnen ho-instellingen vaker op de bestuurstafel komt. Sommigen zeggen dat voor het risicomanagement de situatie bij de UM echt een gamechanger is geweest, waardoor het nu (wel) op de agenda van het College van Bestuur (CvB) staat. Ook geeft een instelling aan dat het incident bij de UM heeft geholpen om het onderwerp breder in de organisatie op tafel te krijgen. Het incident heeft ervoor gezorgd dat sommige instellingen concrete maatregelen hebben genomen om de beveiliging op te schroeven, zoals (overweging van) de invoering van multi-authenticatie, het maken van de juiste back-ups, controleren van de compartimentering van het netwerk en van de firewall.

Integratie cyberrisicomanagement: alleen in de werkprocessen van de ICT-afdeling

Uit de gesprekken blijkt echter ook dat de urgentie van risicomanagement rond cybersecurity bij een deel van de organisatie aanwezig is, meestal de ICT en soms het CvB, maar dat de urgentie niet doordringt tot in alle hoeken van organisatie – cyberrisicomanagement (b)lijkt niet altijd onderdeel te zijn in beleidsplannen en er is niet altijd aandacht in alle bestuurlijke lagen van de organisatie. De ICT-afdeling van

een kleine rpho geeft aan dat zij als dienstverlener wordt gezien en onderwijs leading is. Door onbegrip over wat er op ICT-vlak speelt, komen maatregelen voor cybersecurity niet aan bod in beleidsplannen. Een grote universiteit geeft aan dat cyberveiligheid niet in de top 10 van risico's in de begrotingen en jaarplannen staat van de verschillende faculteiten en diensten. Wanneer cyberrisico's door decentrale eenheden – met uitzondering van de ICT-afdeling en CvB – niet als hoog risico geprioriteerd worden, ontstaat het risico dat maatregelen die centraal ingezet worden niet in de hele organisatie worden doorgevoerd. Het risico op cyberincidenten blijft ondanks de inzet van centraal bestuur en ICT-afdeling onverminderd hoog bestaan.

Kwetsbaarheden in het risicomanagement door instellingsverschillen
Uit de gesprekken blijkt dat zowel kleine als grote instellingen kunnen verschillen in hoeverre zij het risico op cyberincidenten hoog inschatten en in hoeverre de risico's zijn meegenomen in de inrichting van hun organisatie en systemen. Een kleine rpho geeft aan dat ze weten dat het systeem op dit moment niet waterdicht is, maar dat ze daar iets aan gaan doen. Cyberrisico's worden wel geïdentificeerd, maar leiden niet tot een blijvende aanpak bij deze instelling. Een andere kleine maar bekostigde instelling geeft aan dat zij door de overzichtelijke omvang van de digitale omgeving, én door de inzet van een bevlogen ICT'er, de cybersecurity juist goed op orde heeft. Echter, door de afhankelijkheid van één persoon is de instelling toch kwetsbaar, wanneer deze persoon bijvoorbeeld plotseling vertrekt. De ICT-inrichting van universiteiten is vanwege de grootte en de decentrale inrichting soms een stuk onoverzichtelijker dan van kleine hogescholen. Ook hier zijn er verschillen in de hoeveelheid aandacht voor risicomanagement rond cybersecurity. Een grote bekostigde universiteit geeft aan dat slechts twee faculteiten cybersecurity hebben opgenomen als risico, terwijl het risico op een incident voor een universiteit hoog is. Daarentegen geeft een andere grote bekostigde universiteit aan dat de decentrale organisatie geen gevecht oplevert over investeringen in ICT en dat kritische vragen vanuit andere organisatieonderdelen een onderdeel is van het spel van het verdelen van middelen.

Cyberrisico's niet in de top van risicoafwegingen
De meeste ho-instellingen kennen al een goed uitgewerkte kwaliteitszorgcyclus, risico's worden daarin ook meegenomen. Inbedden van cyberrisico's in bestaande verbeterprocessen binnen instellingen is daarom goed mogelijk. Zoals uit de gesprekken blijkt worden cyberrisico's bij het bestuur vooral geagendeerd tijdens het gesprek met de ICT verantwoordelijken en minder vanuit de andere overlegstructuren. Om na te gaan of cyberrisicomanagement is geïntegreerd in alle werkprocessen – zoals kwaliteitscycli – van de instellingen hebben we ook bekeken of instellingen cyberrisico's meenemen in de jaarverslagen. Het aantal bekostigde instellingen dat informatie over cyberveiligheid heeft opgenomen in de jaarverslagen is relatief hoog, wat aangeeft dat er aandacht voor is (zie figuur 6.2a op pagina 77). Hoewel het onderwerp cyberveiligheid aan bod komt in de jaarverslagen, noemen lang niet alle instellingen voorbeelden van borgingsmaatregelen. Het blijft bijvoorbeeld enkel bij de constatering dat het risico ten aanzien van informatiebeveiliging toeneemt, als gevolg van het toenemende risico van cybercrime en de toenemende digitalisering. Daarnaast is de hoeveelheid aandacht voor cyberveiligheid in de jaarverslagen vertekend door de wet AVG die 25 mei 2018 is ingegaan. Instellingen hebben het veelal over de acties die ze hebben uitgevoerd om aan de AVG-wetgeving te voldoen en gaan verder niet in op andere vormen van cyberrisico's.

Wanneer voorbeelden van cyberincidenten op de achtergrond verdwijnen – of er meer acute dreigingen zoals COVID-19 aanwezig zijn – wordt

cyberrisicomanagement mogelijk niet als urgent ervaren en het risico mogelijk ten onrechte laag ingeschat. In vergelijking tot de aandacht voor COVID-19 en andere externe bedreigingen ontvangt cyberveiligheid bijvoorbeeld minder aandacht in de jaarverslagen. De acute dreiging van de pandemie verlangt directe maatregelen op het moment dat de jaarverslagen over 2019 werden gepubliceerd. Bovendien werd het gehele hoger onderwijs getroffen door deze gebeurtenis. Dit laat zien dat risico-inschatting sterk beïnvloed wordt door de waargenomen urgentie van de dreiging. Andere externe bedreigingen – zoals werkdruk, ongewenst gedrag, ziekteverzuim – ontvangen vrijwel altijd aandacht bij wo-instellingen in de jaarverslagen. Echter, bij hbo-instellingen is de aandacht voor COVID-19 hoger dan voor andere externe dreigingen. De acute dreiging van COVID-19 heeft geleid tot veel aandacht voor risicomanagement door alle lagen van de organisatie heen – en kan dienen als goed voorbeeld voor risicomanagement rond cyberveiligheid.

4.3 Stelsel hoger onderwijs

Definitie van de standaard voor het stelsel:

Ook op stelselniveau is risicomanagement een cyclisch, iteratief en terugkerend proces: de actoren binnen en buiten de hoger onderwijssector wegen en prioriteren de aandacht voor diverse dreigingen. Er is aandacht voor structurele samenwerking en kennisuitwisseling zodat de maatregelen doeltreffend en doelmatig zijn.

Sterktes

- Verschillende partijen in het bijzonder instellingsoverstijgende hebben risico's op de agenda staan, zoals toezichthouders, OCW, Platform IV-HO, SURF.
- Gesprekken tussen besturen van instellingen bevorderen de informatie-uitwisseling over risico's en mogelijke gezamenlijke maatregelen. Met name bij bekostigde instellingen is de interesse voor uitwisseling bij besturen toegenomen.
- Binnen het platform IV-HO en SURF is al veel aandacht voor instrumenten en inhoud van risicomanagement. Dit helpt instellingen risicomanagement gericht op cyber vast te leggen in hun werkprocessen.

Zwaktes

- De autonomie van instellingen vormt een risico voor het borgen van informatie-uitwisseling op stelselniveau. Risicomanagement en bedrijfsvoering worden gezien als aangelegenheid van individuele instellingen.
- Raden van Toezicht hebben weinig kennis over cybersecurity, mogelijke instrumenten en gebruikte normen. Niet veel Raden van Toezicht besteden aandacht aan cyberdreigingen in hun verslaglegging.
- Er is weinig samenwerking tussen inspecties en overheidsdepartementen op het gebied van cyberveiligheid. Op het gebied van toezicht zijn de verantwoordelijkheden voor cyberveiligheid in het hoger onderwijs niet vastgelegd.

Kansen

- Zicht op verschillende individuele risicoprofielen en de vergelijking van cyberweerbaarheid tussen instellingen kan een beeld geven van de risico's voor het gehele stelsel. Structurele verslaglegging in jaarverslagen kunnen hierbij helpen.
- Alle betrokkenen lijken zich bewust van de noodzaak om ook landelijk tot een meer iteratief proces te komen.
- Een samenwerking tussen toezichthouders – waardoor expertises cyberveiligheid en specifieke kennis over het onderwijsveld uitgewisseld kunnen worden – zou voor de hand liggen, bijvoorbeeld in de vorm van een werkgroep. Hierdoor kan de cyberweerbaarheid van het hoger onderwijs tot eenzelfde volwassenheid/niveau komen als bijvoorbeeld vitale sectoren.

Bedreigingen

- De verantwoordelijkheden voor het structureel analyseren van de cyberrisico's voor het hele stelsel is echter bij niemand in het stelsel vast belegd. Gebrek aan sturing en coördinatie kan leiden tot te laat detecteren van risico's en kan ertoe leiden dat iedereen het eigen wiel moet uitvinden.
- OCW kan middels wetgeving instellingen sturing geven, bijvoorbeeld door richtlijnen te maken voor cyberveiligheid – met de kanttekening dat het risicomanagement geen papieren oefening moet worden. De roep om wet/regelgeving kan namelijk leiden tot borging op papier en niet tot meer veiligheid.

Toelichting op de standaard

Op stelselniveau kunnen we standaard 4 – borgen van het risicomanagement – definiëren als *borgen van de risico's*. Er zijn zowel partijen binnen als partijen buiten het onderwijs op één of andere manier betrokken bij de veiligheid van ho-instellingen, of bij cyberveiligheid in de samenleving (zie ook standaard 5). Stelselpartijen zullen de cyberrisico's voor het hoger onderwijs kunnen borgen door systematische acties in te richten. Omdat een risico-inschatting op geen één moment hetzelfde is, moet ook op stelselniveau de aandacht voor cyberrisico's een cyclisch, iteratief en terugkerend proces zijn.

Vastleggen verantwoordelijkheden in het stelsel

De voorwaarden voor het borgen van cyberrisico's voor de instellingen gelden ook voor andere partijen in het hoger onderwijsstelsel. Ten eerste moeten partijen identificeren welke risico's het niveau van een individuele instelling overstijgen – en dus risico's voor het hele stelsel zijn. Vervolgens kan het vastleggen van verantwoordelijkheden rond cyberrisicomanagement binnen de verschillende partijen in de sector ervoor zorgen dat het cyberrisicomanagement beter geborgd is. Daarbij is tevens van belang te onderkennen wie stelselpartijen zijn en wie niet. Binnen het stelsel zou duidelijk moeten zijn wie verantwoordelijk is voor maatregelen op stelselniveau en wie over deze maatregelen rapporteert aan welke partijen en wie het geheel vervolgens evalueert.

Informatie-uitwisseling cyberrisico's binnen het stelsel

Ook voor het stelsel geldt dat een vaste lijn van informatie-uitwisseling ten goede komt aan de borging van risico's die instellingen overstijgen. Om ten behoeve van de cyberveiligheid doelmatige en doeltreffende maatregelen in te kunnen zetten, is de meest actuele informatie nodig en zal de informatie bij de juiste partijen beschikbaar moeten zijn. Om te zorgen voor de noodzakelijke relevante informatie-uitwisseling, zullen ook binnen het stelsel de lijn en frequentie van het gesprek – tussen de juiste partijen – vastgelegd moeten worden. Dit kan bijvoorbeeld bereikt worden door partijen binnen en buiten het onderwijsstelsel structureel te laten samenwerken en kennis uit te wisselen. Bij standaarden 2 en 5 gaan we dieper in op de huidige manier van samenwerken en informatie-uitwisseling.

Integreren cyberrisico's in alle werkprocessen van het stelsel

Ook binnen het stelsel volgt uit standaard 4 dat de aandacht voor cyberrisico's vastgelegd dient te worden in de werkprocessen van organisaties binnen het stelsel hoger onderwijs. Het bemachtigen van de meest recente informatie over relevante risico's, kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek krijgen in bestuurlijke documenten. Door cyberrisico's mee te nemen in kwaliteitszorgcycli wordt voorkomen dat de risico's worden geregeerd (of genegeerd) door de waan van de dag en waardoor de afhandeling van cyberrisico's worden geëvalueerd in samenhang met andere afwegingen en leiden tot verbetering in lopende processen.

4.4 Bevindingen

Vastleggen verantwoordelijkheden in het stelsel

Risicomanagement is bij uitstek een bedrijfsvoeringsthema dat in het hoger onderwijs zowel voor het bekostigde als niet-bekostigde onderwijs bij de verantwoordelijkheid van de instelling zelf ligt. De instellingen zijn autonoom in hun functioneren. Vanuit OCW worden geen richtlijnen gegeven over de inrichting hiervan, enkel over de verantwoording. Wanneer je de cyberveiligheid vanuit het stelsel beziet, ligt het voor de hand dat de verantwoordelijkheid voor instellingsoverstijgende risico's of individuele risico's die niet (voldoende) door een organisaties eigenstandig te beheersen zijn, in het stelsel ook bij specifieke gremia zouden moeten worden belegd. De vraag rijst bij wie in het stelsel hoger onderwijs – of in het stelsel van informatiebeveiligingsorganisaties – de verantwoordelijkheid ligt om actuele dreigingen binnen het stelsel te identificeren en instellingen te informeren over deze actuele en potentiële risico's. Moet daarbij het hoger onderwijs als geheel worden bediend of is er onderscheid tussen verschillende soorten ho-instellingen gerelateerd bijvoorbeeld aan het risicoprofiel? Uit onze gesprekken in het stelsel blijkt dat verschillende partijen instellingsoverstijgende risico's op de agenda hebben staan, zoals toezichthouders, OCW, Platform IV-HO, SURF. Alle betrokkenen lijken zich bewust van de noodzaak om ook landelijk tot een meer iteratief proces te komen. De verantwoordelijkheden voor het structureel analyseren van de cyberrisico's voor het hele stelsel is echter bij niemand in het stelsel vast belegd (zie ook alinea Extern toezicht hieronder), waarschijnlijk omdat instellingen zelf verantwoordelijk zijn voor hun bedrijfsvoering. Gebrek aan sturing en coördinatie van verantwoordelijkheden voor cyberrisicomanagement kan leiden tot te laat detecteren van risico's en ertoe leiden dat iedereen het eigen wiel moet uitvinden.

Informatie-uitwisseling cyberrisico's tussen besturen

Vanwege de autonomie van ho-instellingen was bedrijfsvoering voorheen in beperkte mate een gezamenlijk gespreksonderwerp, bijvoorbeeld tussen universiteitsbesturen, met uitzondering van de code goed bestuur waarin principes met elkaar zijn vastgelegd. Uit gesprekken met de koepelorganisatie voor universiteiten – VSNU – blijkt dat het onderwerp bedrijfsvoering na de hack op de Universiteit Maastricht wel op de agenda is gekomen van de gezamenlijke overleggen tussen universiteitsbesturen. Gesprekken tussen besturen van instellingen bevordert de informatie-uitwisseling over risico's en mogelijke gezamenlijke maatregelen. We krijgen vanuit onze gesprekken met instellingen niet het idee dat er behoefte is aan afstemming met bijvoorbeeld één uitvoeringspraktijk, wel is er behoefte aan (meer) uitwisseling. Voorheen vond deze uitwisseling vooral op operationeel en tactisch niveau plaats tussen CIO's. Daarbij was niet de koepel maar SURF de netwerkpartij. Met name bij bekostigde instellingen is de interesse voor uitwisseling bij bestuurders toegenomen.

Informatie-uitwisseling cyberrisico's op stelsel- en landelijk niveau

Zoals te lezen is bij de andere standaarden zijn er verschillende stelselinitiatieven om dreigingsinformatie op een efficiënte manier met elkaar (ho-instellingen) te delen (e.g., SOC, SURF-CERT bij standaard 3). Er is zelfs landelijke aansluiting: het SURF-CERT is voor uitwisseling van actuele dreigingen aangesloten bij NCSC. Sommige instellingen besluiten zelfstandig aan te sluiten bij landelijke *taskforces*. Eén van de universiteiten waarmee we gesproken hebben, geeft bijvoorbeeld aan dat deze diensten (aparte ICT-afdelingen voor gespecialiseerd onderzoek/grote datasets, simulaties ten behoeve van onderzoek) zijn betrokken bij de *taskforce* informatiebeveiliging. Wegens het besef van urgentie van het onderwerp is hoofd-ICT van een kleine bekostigde instelling bijvoorbeeld aangesloten bij landelijke netwerken van ICT-managers, zoals SURF, HBO-CSC, en COMIT. Niet alle

instellingen zijn echter betrokken bij landelijke- of stelselinitiatieven. Risicomanagement wordt namelijk gezien als decentrale aangelegenheid. Ook heerst er een informele cultuur, waardoor partijen niet lijken te willen – of kunnen – formaliseren. Een voorbeeld hiervan is de verstrengeling tussen het SURF lidmaatschap (informele structuur) met SURF netwerken zoals SURF-CERT of -SOC (formele structuren).

Integreren cyberrisico's in alle werkprocessen van het stelsel
Binnen het platform IV-HO en SURF is veel aandacht voor instrumenten en inhoud van risicomanagement. Dit helpt instellingen risicomanagement gericht op cyber vast te leggen in hun werkprocessen. Dit is steeds meer geïntegreerd binnen de afzonderlijke partijen in het onderwijsveld, maar nog niet structureel in gezamenlijke werkprocessen. Wanneer verschillende partijen met elkaar overlegstructuren, werkgroepen, of bestuurlijke documenten vastleggen, kunnen risico's bijvoorbeeld makkelijker met de juiste personen gecommuniceerd worden (e.g., SURF, NCSC), bestuurders van instellingen de risico's met regelmaat met elkaar uitwisselen (e.g., Platform IV-HO, koepels), wetgeving aangepast worden (e.g., OCW), en kunnen toezichtstaken op de meest urgente risico's afgestemd worden (RvT, of inspectie(s)). Het platform lijkt zich met name te richten op samenwerking op operationeel niveau, waarbij de ervaring binnen het platform voor andere veiligheidsrisico's dan cyber op dit moment groter is. Hiermee is het effectief voor aangesloten, vaak al actieve, instellingen, maar krijgen we de indruk dat de verdiensten en mogelijkheden enigszins buiten het zicht van besturen en koepelorganisaties blijven.

Intern toezicht: Regulering cyberveiligheid heeft voor en nadelen
Uit ons gesprek met de Raden van Toezicht van de universiteiten en hogescholen blijkt dat meerdere RvT's weinig kennis hebben over cybersecurity, mogelijke instrumenten en gebruikte normen. In enkele raden is specialistische kennis aanwezig als gevolg van de werkkring van één van de leden. De minister[46] heeft ho-instellingen opgeroepen het veiligheidsbeleid, waaronder cyberveiligheid, op te nemen in de jaarverslaglegging en structureel met hun Raden van Toezicht te bespreken. Het positieve hieraan is dat er structurele aandacht wordt gegeven aan het onderwerp doordat het onderwerp wordt geïntegreerd in werkprocessen. Echter, om te komen tot een aanvaardbaar risiconiveau is rapportage over het onderwerp in het jaarverslag niet genoeg – de evaluaties zouden moeten leiden tot prioritering van risico's en gepaste maatregelen. Een dergelijke keuze zou structurele gesprekken kunnen voeden over het risicoprofiel van individuele ho-instellingen. Ook kan verslaglegging ervoor zorgen dat ho-instellingen beter vergeleken kunnen worden. Echter, eerst zal nagedacht moeten worden hoe vastgesteld kan worden wat de cyberweerbaarheid van een ho-instelling is. Zicht op verschillende individuele risicoprofielen en de vergelijking van cyberweerbaarheid tussen instellingen kan een beeld geven over de risico's voor het gehele stelsel.

OCW kan middels wetgeving instellingen sturing geven, bijvoorbeeld door richtlijnen te maken voor cyberveiligheid – met de kanttekening dat het risicomanagement geen papieren oefening moet worden. De roep om wet/regelgeving kan namelijk leiden tot borging op papier en niet tot meer veiligheid. Organisaties die behoren tot de vitale infrastructuren hebben een wettelijk vastgelegde zorgplicht; deze aanbieders behoren adequate maatregelen te nemen voor de beveiliging van hun netwerk- en informatiesystemen. Een zorgplicht in het onderwijs zou mogelijk een aanleiding voor het bestuur en de RvT binnen het onderwijs kunnen zijn om het informatiebeveiligingsbeleid van instellingen te controleren. Tijdens onze gesprekken

[46] Tweede Kamer, vergaderjaar 2020-2021, 31 288 en 26 643, nr 910.

met instellingen en (cyber)partijen uit het stelsel bleek dat met name actoren die verantwoordelijk zijn cyberveiligheid (waaronder CISO's, integraal veiligheidskundigen, technisch experts) voorstanders zijn van enige regulering. Volgens hen ontstaat er dan een startpunt om afwegingen binnen en buiten instellingen structureler bespreekbaar te maken.

Extern toezicht: het is niet duidelijk welke verantwoordelijkheid toezichthouders hebben

Verschillende toezichthouders hebben cybersecurity op de agenda staan. Er is echter nog weinig samenwerking tussen inspecties en overheidsdepartementen op het vlak van cyberveiligheid en het gezamenlijk monitoren en aanpakken van risico's. Binnen de Inspectieraad is het onderwerp cyberveiligheid ook onderdeel van gesprek. Op dit moment is er veel expertkennis over cyberveiligheid aanwezig bij Inspectie van Justitie en Veiligheid en Agentschap Telecom. Echter, zij zijn niet betrokken bij het toezicht op het (hoger) onderwijs, noch betrokken in specifieke samenwerkingsverbanden of kennisuitwisseling rond cyberveiligheid met andere inspecties, zoals de Inspectie van het Onderwijs. Organisaties uit sommige vitale sectoren zijn verplicht een periodieke doorlichting te ondergaan. Zo kijkt het Agentschap Telecom bij dienstverleners van energie en digitale infrastructuur of de organisatie passende en evenredige technische en organisatorische maatregelen neemt. Een samenwerking tussen toezichthouders – waardoor expertises uitgewisseld kunnen worden – zou voor de hand liggen, bijvoorbeeld in de vorm van een werkgroep. De samenwerking zou een stimulans kunnen zijn om tot eenzelfde volwassenheidsniveau te komen als de vitale sectoren.

5 Standaard 5: aandacht ketensamenwerking

5.1 Instellingen hoger onderwijs

Definitie van de standaard voor instellingen:

Partners en leveranciers kunnen op afhankelijke wijze aantonen dat deze partijen aan de geldende eisen voldoen.

Sterktes

- Instellingen zijn bereid en gewend om met derden samen te werken, er is een blik naar buiten en medewerkers zijn gericht op delen.
- Er zijn veel informele contacten tussen met name bekostigde instellingen om kennis te delen.

Zwaktes

- Binnen sommige instellingen zijn afspraken niet duidelijk of afwezig of worden niet nageleefd.
- Er is verschil in volwassenheid tussen instellingen, wat de samenwerking bemoeilijkt.

Kansen

- Binnen instellingen zijn vaak zeer veel goede voorbeelden te vinden van samenwerking met derden.
- Security wordt steeds vaker onderdeel van het inkoopproces en van samenwerkingsafspraken.
- Er wordt al veel onderzoek verricht binnen instellingen. Die kennis kan niet alleen ten gunste van derden maar ook van de eigen organisatie benut worden.

Bedreigingen

- Eigenwijze professionals willen graag zo veel mogelijk handelingsvrijheid en voelen zich beknot door vaste regels voor inkoop en samenwerking.
- Zekere binnen grote instellingen zijn er conflicterende eisen en behoeftes.
- Voorlopers willen niet belemmerd worden door achterblijvers.

Toelichting op de standaard

Deze standaard richt zich op de samenwerking met partners en leveranciers, het maken van afspraken en het onderling afleggen van verantwoording. Waarbij ook blijvend gecontroleerd wordt of aan de afspraken is voldaan. Wij interpreteren de standaard breed: cyberveiligheid is gediend met brede afspraken en afstemming tussen alle partijen die betrokken zijn bij het onderwijs. Daarmee kijken we in dit onderzoek breder dan een keten met leveranciers en beschouwen ook samenwerkingspartners die onderwijs verzorgen.

Een ho-instelling is geen geïsoleerde eenheid. Instellingen opereren in een netwerk van partijen: gemeente, landelijke overheid, beroepsgroepen, regionale verbanden, de onderwijskolom, werkgevers, koepels, politiek. Binnen het netwerk is sprake van autonomie. Instellingen bepalen hun eigen koers binnen de gegeven kaders. De grenzen van de instelling en de invloedsfeer van opleidingen en instellingen zijn relatief duidelijk en stabiel. Dat geldt ook binnen bestaande samenwerkingsafspraken: bijvoorbeeld als de keten het gezamenlijk aanbieden van onderwijs omvat of de samenwerking in een onderzoeksinstituut. In fysieke zin zijn die grenzen van oudsher ook duidelijk: onderwijs wordt gegeven in een gebouw waar studenten toegang toe krijgen. Op lokaal niveau worden (bijvoorbeeld binnen de veiligheidsdriehoek) afspraken gemaakt over veiligheid, waarbij verantwoordelijkheden historisch duidelijk zijn gegroeid. Door haar open karakter is het hoger onderwijs goed voorbereid op het samenwerken met derden en heeft

daarmee ook een stevig startpunt als het om cyberweerbaarheid gaat. Digitalisering heeft aan die ketensamenwerking wel een dimensie toegevoegd doordat de grenzen en verantwoordelijkheden vervagen.

Een instelling is ook een keten met interne leveranciers
Binnen de keten van het stelsel, kunnen we de instelling beschouwen als een zelfstandig systeem, een eigenstandige keten. Binnen die instellingsketen bestaan ook interne leveranciers en klanten, en worden afspraken gemaakt en verantwoordelijkheden belegd. Ook daar geldt: afspraken, afstemming en vertrouwen is nodig. Cyber krijgt in toenemende mate ook een plaats op de bestuurstafel en daar hoort ook de afstemming met interne leveranciers en dienstverleners bij. Die meer zakelijke aanpak kan ook tot wederzijdse helderheid leiden: ICT-afdelingen zijn dan niet alleen de interne dienstverlener, maar worden ook meer in positie gebracht om de veiligheid te kunnen garanderen, ook als dat ten koste gaat van de autonomie van andere interne partijen.

5.2 Bevindingen

Er wordt veel samengewerkt, maar de verschillen zijn groot
Alle instellingen noemen vormen van ketensamenwerking in de gesprekken die we hebben gevoerd, op hun websites en in de jaarverslagen (zie tabel 5.2a op pagina 67). Uit de gesprekken blijkt ook dat die samenwerking sterk verschilt:

- Van zeer ad hoc en reactief (er is een actuele vraag die om een antwoord vraagt, er wordt een nieuw contract afgesloten), tot zeer actief, structureel en langdurig.
- Van uiterst beperkt in omvang (een enkele leverancier) tot zeer intensief (meerdere partijen, meerdere landelijke en internationale netwerken).

De mate van samenwerking hangt van een paar factoren af:

- Logischerwijs hangt de mate van samenwerking deels af van de **omvang** van de instelling: een kleine instelling met een of enkele opleidingen heeft noch de noodzaak, noch de mankracht om zeer uitgebreide netwerken te onderhouden.
- Een tweede factor is de visie die men heeft op **uitbesteding**: er zijn instellingen die bij voorkeur zo veel mogelijk intern organiseren en ontwikkelen. Zij kiezen daar bewust voor: korte lijnen, snel handelen, veel maatwerk. Die keuze betekent ook een zeker risico, je bevindt je relatief op een eiland. Er zijn ook instellingen die juist bewust uitbesteden; zij betogen dat de externe leverancier het beste in staat is om de veiligheid van hun product te waarborgen, bovendien hoeft de instelling dan minder gespecialiseerd personeel te werven en in dienst te houden.
- Een derde factor is de **bekostiging**. Met name kleine en niet-bekostigde instellingen maken een kostenafweging: levert de investering in deze samenwerking meer op dan de energie die ik er in stop. Daarnaast zijn de bekostigde instellingen zowel via de koepels als via SURF sterker geneigd om informatie uit te wisselen en met elkaar samen te werken. Naast een kostenafweging, speelt soms ook een concurrentiebelang een rol bij het minder intensief uitwisselen. Tenslotte worden niet-bekostigde instellingen ook minder en minder actief betrokken in de bestaande netwerken en missen daardoor informatie en aansluiting.

Tabel 5.2a Voorbeelden van ketensamenwerking (bron: gesprekken, websearch, jaarverslagen)

Soort samenwerking	Schaal van de samenwerking
Uitwisseling van personeel, zoals het gezamenlijk gebruik van functionaris gegevensbescherming.	**Bilateraal**
Gebruik van standaard verwerkersovereenkomsten	**Stelsel HO**
Gebruik van inkoop via met name SURF, inclusief de periodieke controle op de inkoopvoorwaarden	**Stelsel HO**
Kleine instellingen die samenwerken, met grotere instellingen (in de regio of binnen het domein)	**Bilateraal**
Uitwisseling van ervaringen, signalen en best practices op het niveau van ICT-verantwoordelijken (managers, directeuren, CISO)	**Bilateraal, bestaande clusters van samenwerking, stelsel HO**
Bestuurlijk overleg: binnen netwerken van bestuurders wordt kennis uitgewisseld	**Stelsel HO, regionaal**
Samenwerking met MKB en gemeente om cyberweerbaarheid te vergroten en de wirwar aan informatie op een duidelijke en concrete manier bij de partijen te krijgen.	**Lokaal, regionaal**
Samenwerking tussen onderwijsinstellingen rondom alle veiligheidskwesties binnen een stad of regio	**Lokaal, regionaal**
Gebruikersgroep specifieke onderwijssoftware pakketten	**Multi-lateraal**

Inbesteden of uitbesteden: lokale keuzes

Met name kleinere instellingen geven aan graag te kiezen voor uitbesteding van diensten en ICT. Hen ontbeert de kennis en de capaciteit om alles in huis te organiseren. Ook kiezen zij relatief vaak voor cloud-diensten. De vereisten die zij stellen zijn niet anders dan bij grote instellingen: veiligheid en betrouwbaarheid staat voorop. Bij het uitbesteden is het vaak lastig om te bepalen wat een betrouwbare partij is en of de diensten die geleverd worden ook voldoende veilig zijn. Kleine instellingen kiezen daarbij vaak voor een bekende partij of leverancier: ofwel een partij die al eerder (delen van) de ICT voor hen verzorgde, ofwel een ‘grote naam’. Voordeel van de eerste categorie is volgens de gesprekspartners de snelheid van dienstverlening en de mate waarin je als kleine afnemer invloed kunt hebben op de kwaliteit van het gebodene. Grote aanbieders zullen niet snel met een kleine afnemer in gesprek gaan over specifieke wensen, de mate waarin privacy beschermd is of hoe de cyberweerbaarheid van het product gewaarborgd wordt. De leveringsvoorwaarden van de grote leveranciers zijn daarin dwingend. Een enkele instelling kiest er bewust voor de volledige ICT in eigen huis te houden, inclusief de ontwikkeling van eigen tools.

Voor grotere instellingen geldt dat er relatief veel interne capaciteit beschikbaar is; er wordt veel intern beheerd, er is een eigen security afdeling en soms ook een eigen SOC, er is een professionele inkoop afdeling met specifieke ICT-expertise. Maar ook grote instellingen kopen veel producten in: financiële producten, HRM producten, producten voor studentegegevens, leeromgevingen. Daarmee neemt de afhankelijkheid van de kwaliteit van externe leveranciers ook toe.

Beoordelen van leveranciers: standaardisering en samenwerking

Instellingen noemen zelf diverse manieren om de kwaliteit van leveranciers te beoordelen. In toenemende mate wordt gebruik gemaakt van standaard contracten en wordt ICT bij de inkoop betrokken. Diverse instellingen noemen ook dat security steeds vaker actief onderdeel is van het inkoopproces. Daarnaast worden door veel instellingen jaarlijkse updategesprekken gevoerd met leveranciers; vaak gaat het dan om de grotere leveranciers van bijvoorbeeld software. Soms zijn deze gesprekken vooral netwerkend bedoeld en om op de hoogte te blijven, soms ligt de

focus ook nadrukkelijk op security. Kleine hogescholen noemen ook dat zij meer volgend zijn op de grotere hogescholen, bijvoorbeeld in de aanschaf van hun leeromgeving.

Wie is verantwoordelijk voor de veiligheid van ingekochte diensten en software?
Een terugkerende vraag is die van de verantwoordelijkheid: hoe ver reikt de verantwoordelijkheid van een bestuur voor de veiligheid van het ingekochte? Hoe houdt een instelling zicht op het hele gehele pallet aan software en diensten dat wordt ingekocht centraal en decentraal? Hoe vaak en hoe intensief moet je je leveranciers controleren en welke vragen zou je dan moeten stellen? Complicerend is daarbij dat er ook veel wordt samengewerkt, bijvoorbeeld binnen onderzoeksprojecten. Passen je inkooprichtlijnen dan wel op de vereisten van de subsidiegever? Hoe pas je een vereiste van open science toe binnen je eigen security beleid? Hoe blijf je volgen waar alle data wordt opgeslagen en wie er toegang heeft tot je systemen? Die vragen zijn deels technisch, maar deels ook principieel en horen daarom ook mede op de bestuurstafel. Het belang om hierover in gesprek te zijn tussen ho-instelling en leveranciers bleek bij het Blackbaud incident waar onder andere de TUDelft in 2020 mee werd geconfronteerd. Hoewel partijen voorwaarden over privacy en informatiebeveiliging hadden afgesproken en deze leverancier over het algemeen de zaken goed op orde heeft, bleek een back-up bestand met persoonsgegevens op een projectserver te staan die bij de software leverancier niet langer in beeld was. Aangezien de data met persoonsgegevens toebehoorden aan Nederlandse universiteiten is er ook bij de universiteit een verantwoordelijkheid om periodiek controles uit te (laten) voeren of verklaringen over de effectiviteit van maatregelen op te vragen bij leveranciers (zie verder standaard 6).

Ketensamenwerking bij een hack: als instelling doe je veel zelf
Als je als onderwijsinstelling een incident hebt, dan staat je in principe vooral zelf aan de lat om het probleem op te lossen. Naast de kennis die binnen de instelling aanwezig is, is er ook binnen SURF (CERT) capaciteit beschikbaar om bijstand te verlenen. Ook kan een instelling kiezen om een commerciële partij in te huren. Uit de gesprekken die wij hebben gevoerd blijkt dat de betrokkenheid van het NCSC na een incident binnen het hoger onderwijs beperkt is. SURF informeert het NCSC over het incident en kwetsbaarheden.

Krachten bundelen op inhoud, maar wat is het leereffect intern?
Interessant zijn enkele initiatieven, zowel van hbo- als van wo-instellingen om kenniscentra op het gebied van cyberveiligheid op te zetten. Die initiatieven bestaan doorgaans uit een combinatie van faculteiten, opleidingen, onderzoeksgroepen binnen één of soms meerdere instellingen. Uit de websearch blijkt niet wat de bijdrage van deze onderzoeksgroepen is voor de cyberweerbaarheid van het hoger onderwijs zelf. Met andere woorden: komt de opgedane kennis en kunde wel in voldoende mate te gunste van de eigen instellingen?

Voorbeeld: Cyber Security Academy
Dit is een initiatief van de Universiteit Leiden, de Technische Universiteit Delft en De Haagse Hogeschool en is tot stand gekomen met steun van de Gemeente Den Haag. Als partner verzorgen docenten onderwijs aan een specifieke doelgroep van professionals werkzaam in de publieke of private sector betrokken bij de organisatie en aanpak van vraagstukken op het terrein van (cyber) security die ofwel kennis hebben op bestuurlijk/juridisch vlak of op het gebied van ICT.

5.3 Stelsel hoger onderwijs

Definitie van de standaard voor het stelsel:

Op stelselniveau is er overleg over de kwaliteit en betrouwbaarheid van leveranciers van diensten en kan er gecoördineerd actie ondernomen worden om problemen op te lossen. Waar nuttig wordt gebruik gemaakt van gezamenlijke inkoop.
Er is sprake van een duidelijke en eenduidige rol- en verantwoordelijkheidsverdeling. De verschillende partijen in het veld kennen elkaars rol en weten welke maatregelen ze nemen om risico's tot een acceptabel niveau terug te dringen.

Sterktes

- Er is al veel samenwerking op het gebied van inkoop en aanbesteding, met name via SURF.
- Er wordt zeer veel informatie uitgewisseld en gezamenlijk opgetrokken, tussen instellingen, al dan niet binnen SURF verband.

Zwaktes

- Het lokale belang en de wens om autonoom tot de beste keuze te komen wint van het algemene belang. Niet iedereen is goed aangesloten bij het collectief.
- Er wordt een groot beroep gedaan op de verantwoordelijkheid van individuele instellingen. Daarmee worden instellingen deels overvraagd; voorlopers kunnen niet op eigen kosten en in eigen tijd achterblijvers op sleeptouw nemen, achterblijvers komen niet op eigen kracht verder.

Kansen

- Gezamenlijkheid kan leiden tot betere kwaliteit, doorzettingsmacht tegen grote leveranciers en kostenbesparing.
- Er is een toenemend besef dat cyber een stelselbreed probleem is dat stelselbrede samenwerking vraagt.

Bedreigingen

- Er zijn veel partijen actief, zowel binnen de onderwijs- als binnen de cyberkolom. Het is niet altijd duidelijk wie doorpakkingsmacht heeft, welke kaders er benut worden en gelden en bij wie je moet zijn.

Toelichting op de standaard

Tijdens het onderzoek naar de cyberaanval op de UM hebben we drie elementen geïdentificeerd die we binnen dit stelselonderzoek in de gesprekken nader hebben onderzocht: cyber is geen onderwerp dat op één enkel bordje is te plaatsen, binnen het onderwijs is er sprake van een gedistribueerde verantwoordelijkheid voor een veelheid van processen en de verbinding tussen de werelden van cyber en onderwijs.

5.4 Bevindingen

SURF speelt een belangrijke rol, verwachtingen zijn hoog

Uit de gesprekken komt duidelijk naar voren dat SURF een belangrijke rol speelt op diverse gebieden, het is het centrale punt waaruit diverse vormen van ketensamenwerking ontstaan en worden samengebracht. Uit de gesprekken blijkt dat het takenpakket van SURF en de onderliggende netwerken divers en omvangrijk zijn. Daarmee is niet gezegd dat het pakket ook dekkend is:

- Enkele taken zijn niet belegd bij SURF en/of passen niet bij haar taak(opvatting)
- Niet iedereen is op dezelfde wijze aangesloten bij SURF
- Het is onduidelijk wat je precies wel en niet kunt en moet afnemen

Veel gesprekspartners zien in SURF een 'hoeder van het stelsel'. Gevraagd naar wat dat precies betekent en of die verwachting realistisch is, zijn de antwoorden even divers en omvangrijk: gesprekspartners veronderstellen een dekking van taken en aansluiting op SURF-diensten die door andere gesprekken weer ontkend wordt. Met

name niet-bekostigde instellingen maar ook enkele kleinere bekostigde instellingen geven aan minder aansluiting bij SURF en de onderliggende netwerken te hebben. Daarnaast zijn niet alle bekostigde instellingen en rpho's in de zelfde mate aangesloten op de informatievoorziening vanuit SURF. Dat betekent dat er nu een verschil is tussen instellingen binnen het stelsel in de manier waarop zij op deze centrale spil in de keten zijn aangesloten.

Niet iedereen is lid van SURF

SURF is een coöperatie met ruim 100 leden. Dit zijn alle bekostigde Nederlandse universiteiten en umc's, de meeste bekostigde hbo- en verschillende mbo-instellingen en diverse onderzoeksinstellingen waaronder NWO- en KNAW-instituten. Een handvol bekostigde instellingen is geen lid van SURF. Geen enkele rpho is lid van SURF, met uitzondering van de Politieacademie. Wie geen lid is, heeft daarmee ook niet de beschikking over de informatie of de templates en andere diensten van SURF. Een enkele gesprekspartner gaf aan geen lid te zijn van SURF, maar wel lid te zijn van een mailingslijst of een special interest group van SURF. Instellingen met zowel een bekostigd als een niet-bekostigd deel, zijn via de bekostigde tak lid van SURF, waarmee zij wel kunnen profiteren van de voordelen van het lidmaatschap.

Coöperatieve samenwerking wordt gewaardeerd, maar kan niet alles oplossen

SURF is een netwerkorganisatie met een ledenstructuur. Via verschillende acties, evenementen, special interest groups en mailing list werkt ze aan de kennisuitwisseling en -bevordering. De kracht van SURF zit hem volgens de meeste van onze gesprekspartners in de open en informele cultuur: de wereld is klein, mensen weten elkaar goed te vinden en op diverse niveaus zijn er overlegstructuren. Zo is er het universitaire CISO overleg, dat ook door diverse instellingen wordt genoemd als belangrijke plek om het gesprek over dreigingen met elkaar te voeren. Ook wordt veel gebruik gemaakt van de standaard verwerkingsovereenkomsten. SURF is volgens veel van de gesprekspartners goed in staat om de vragen vanuit het veld te vertalen in concrete producten. Ook pikt ze signalen van knelpunten op. Een DPIA op google diensten die door enkele leden is uitgevoerd, leidde bijvoorbeeld vervolgens tot een gecoördineerde actie richting de leverancier. Als grootste risico wordt door enkele gesprekspartners genoemd dat er relatief veel vrijheid in deze wijze van samenwerking bestaat; SURF ziet het niet als haar taak haar leden aan te spreken op bijvoorbeeld de inrichting van haar informatiebeveiliging of om dwingende kaders te ontwikkelen of afspraken over inkoop, het gebruik van leveranciers of bepaalde standaarden af te dwingen.

Koepels zien voor zichzelf een bescheiden rol

De drie koepelorganisaties in het hoger onderwijs zien voor zichzelf op het domein van cyberveiligheid een relatief bescheiden rol. Dat heeft twee oorzaken: bedrijfsvoering en daarmee informatiebeveiliging is primair een verantwoordelijkheid van het instellingsbestuur. Belangrijker nog voor VSNU en VH is het feit dat SURF een goed functionerend netwerk is waar dit zijn plek heeft. Desalniettemin heeft de cyberaanval op de UM ook impact gehad op het gesprek binnen de koepels en tussen besturen: is er aanvullende inzet nodig om de cyberweerbaarheid van de sector als geheel te verbeteren? Voor de VSNU en de VH heeft dit geresulteerd in afspraken over de verplichte deelname aan de SURF-audit en binnen VSNU verband in de afspraak om deze audit door externen te laten uitvoeren. Ook is er binnen de VH en de VSNU gesproken over een streefniveau van volwassenheid, dat gezien mag worden als basisniveau voor elke instelling. De NRTO sluit meer aan op de vraag vanuit haar leden. Aangezien die vraag niet uniform is, is er vanuit deze koepel geen directe actie om tot meer samenwerking te komen op het gebied van bijvoorbeeld inkoop en informatieuitwisseling.

NCSC en SURF-CERT: informatie-uitwisseling komt verder op gang
Het NCSC en SURF kennen een lange geschiedenis van samenwerking. Sinds begin 2020 is SURF een aangewezen CERT. Voor de AVG en Wbni was er al ruime tijd informele uitwisseling van informatie tussen SURF (CERT) en NCSC. Beide wetten hebben tijdelijk geleid tot het minder goed (mogen) delen van informatie. De aanwijzing van SURF-CERT als computercrisisteam onder de Wbni creëert inmiddels de formele mogelijkheden om deze informatie (zoals persoonsgegevens) te delen. Na het incident bij de UM is besloten dat NCSC wel het hoger onderwijs op de hoogte brengt, mochten er dreigingen of kwetsbaarheden zijn. Uit onze gesprekken blijkt dat enkele instellingen en ketenpartijen wel op de hoogte zijn van deze afspraak, maar dat informatie nog niet altijd (tijdig) bij instellingen terecht komt.

Informatie over dreigingen en incidenten is veelrichtingsverkeer
NCSC is een kennisautoriteit, die sectorspecifieke CERTs kan ondersteunen om zo goed mogelijk hun werk te doen. NCSC heeft ook informatie van de sectorspecifieke CERTs nodig; die hebben generieke informatie over bijvoorbeeld kwetsbaarheid in kritieke processen en vertalen die informatie naar NCSC. Er is dus sprake van veelrichtingsverkeer. In de gesprekken die we hebben gevoerd, worden onderstaande informatiestromen genoemd. Niet alle stromen worden in alle gesprekken genoemd en zijn ook zeker niet bij alle gesprekspartners bekend:

- NCSC deelt informatie met SURF vanuit nationaal detectie netwerk en risico-detectie over mogelijke kwetsbaarheden, zoals *Indicators of Compromise* (IoC's);
- SURF informeert op haar beurt het NCSC op basis van informatie van haarzelf en instellingen;
- NCSC informeert rechtstreeks bij getroffen instellingen naar specifieke eigenschappen van een incident;
- Binnen bestaande verbanden (zoals het overleg van universitaire CISO's) zijn er ook korte lijnen;
- instellingen maken ook gebruik van de informatie die beschikbaar is bij commerciële partijen en beveiligingswebsites.

Versnipperde informatievoorziening
Alle gesprekspartners geven aan dat het van essentieel belang is om over de meest actuele informatie over dreigingen en zwakheden te beschikken. SURF faciliteert het CERT dat wordt gevormd door de CERTs van instellingen die erbij zijn aangesloten. Niet alle bekostigde instellingen zijn bij SURF-CERT aangesloten of beschikken over een eigen CERT. Rpho's zijn in het geheel niet aangesloten en hebben dus altijd te maken met een informatieachterstand. Dat vormt een risico voor de weerbaarheid van het stelsel als geheel. Tegelijkertijd is het ook begrijpelijk dat er prudent met informatie wordt omgegaan, een CERT en ICT-security werkt op basis van vertrouwensrelaties. Binnen een CERT is altijd spanning over het informeren tussen elkaar. Wel of niet vertellen over die ene situatie waarin het 'net niet fout is gegaan'. Er is ook geen doorzettingsmacht om organisaties te dwingen te delen of bepaalde maatregelen te nemen. Rpho's zijn zelf aangewezen op het achterhalen van informatie via leveranciers, het bijhouden van websites zoals van het NCSC en via informele contacten met specialisten werkzaam in andere bedrijfstakken. Het Digital Trust Center (DTC) dat als partij vanuit de Rijksoverheid informatiepunt is voor bedrijven in niet-vitale sectoren, is bij de rpho's die de inspectie heeft gesproken onbekend.

Kracht van gezamenlijkheid is groot

In de gesprekken hebben we diverse voorbeelden (zie tabel 5.4a) gehoord van de kracht van gezamenlijkheid. Die gezamenlijkheid doorkruist soms de traditioneel bestaande scheidslijnen in het hoger onderwijs.

Tabel 5.4a: diverse samenwerkingsvoorbeelden

	Typering samenwerking
Overleg universitaire CISO's en HBO-CISO overleg	Het U-CISO is een overleg van alle universitaire CISOs. Dit overleg staat enigszins los van SURF, het contact voor security vanuit SURF sluit bij het overleg van de universitaire CISO's aan. Het HBO-CISO overleg is in wording, een eerste overleg stond gepland ten tijde van ons onderzoek. Beide overleggen zijn georganiseerd langs de functionele lijn (de CISO) en er zijn gescheiden overleggen voor hbo- respectievelijk wo-instellingen. Voor niet-bekostigde instellingen bestaat een dergelijk overleg niet. Deze overleggen zijn duidelijk gepositioneerd langs de klassieke scheidslijn hbo - wo en bekostigd - niet-bekostigd.
SCIPR en SCIRT	SCIPR staat voor SURF Community voor Informatiebeveiliging en Privacy. Informatiebeveiligers en privacy officers maken deel uit van deze community. Ze ontwikkelen onder andere in gezamenlijkheid leidraden die leden kunnen gebruiken binnen hun eigen instelling.
SURF-SOC	Het SURF-SOC is een initiatief van enkele wo-instellingen om een gezamenlijk SOC in te richten. Het is een dienst die kan worden afgenomen van SURF. De Universiteit Wageningen was de eerste instelling die SURF-SOC afneemt.
Gebruikersoverleg OSIRIS	Elke instelling heeft een eigen overeenkomst met OSIRIS (een veelgebruikt administratiesysteem) met eisen en ook eigen SLA's. Daarnaast is er een strategische gebruikersoverleg. Dit collectief is mogelijk omdat er veel gebruikers van OSIRIS zijn in het hoger onderwijs. Er wordt een gezamenlijk test/audit op het systeem van OSIRIS gedaan, dat gaat zowel om de cloud versie als de on premise versie. De uitkomsten worden gedeeld met de leden. Zo worden de kosten gedeeld en wordt geprofiteerd van gezamenlijke inzichten.
Privacy test online diensten	Een hogeschool en een universiteit hebben een onderzoek ingesteld naar aanleiding van zorgen over het gebruik van meta-data door een leverancier. De resultaten van dit onderzoek zijn voor advies aan de Autoriteit Persoonsgegevens voorgelegd. Uiteindelijk heeft dit onderzoek geleid door een gezamenlijke actie voor het hele onderwijsveld vanuit SURF en SIVON, gericht op een oplossing van deze zwakheden, maar ook een hernieuwde discussie over het gebruik van onder andere cloud diensten en de afhankelijkheid van grote multinationals.

6 Standaard 6: controleren en evalueren

6.1 Instellingen hoger onderwijs

Definitie van de standaard voor instellingen:

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).

Sterktes

- Er is bij instellingen een grote bereidheid tot leren en verbeteren. Diverse instellingen werken planmatig aan veiligheidsbeleid, bijvoorbeeld vanuit een integraal veiligheidsplan of vanuit een informatiebeveiligingsaanpak.
- Er bestaan informele en formele structuren die gericht zijn op het controleren en evalueren van beleid, waaronder ook ICT-beleid.

Zwaktes

- Controle en evaluatie vinden plaats, maar leiden niet altijd tot de nodige verbeteringen. Instellingen verantwoorden zich niet publiek over informatiebeveiliging.
- Verbinding tussen alle actoren en belangen binnen een instelling is lastig, ICT evaluatie wordt vaak als een losstaand onderdeel gezien.
- Kleine instellingen beschikken niet over alle expertise.

Kansen

- De SURF-audit is een mooi en uitgebreid instrument. Dit zou nog beter gebruikt kunnen worden en verbonden moeten worden met de lokale verbetercyclus.
- Aan de bestuurstafel wordt steeds vaker cyberveiligheid geëvalueerd, als integraal onderdeel van instellingsbeleid
- Door diverse cyberincidenten in de media zijn instellingen meer doordrongen van de noodzaak van integrale controle en evaluatie, waarbij ICT vast onderdeel is van de PDCA cyclus.

Bedreigingen

- Controle leidt tot minder openheid en vergroot het risico op een papieren werkelijkheid.
- Risico's binnen instellingen strijden voortdurend om voorrang: cyberrisico's worden onderkend maar zijn relatief onzichtbaar, en halen meestal niet de top vijf van hoogste prioriteiten.

Oppassen voor blinde vlekken

Elke organisatie kent informele en formele verbanden en afspraken, het onderwijs niet uitgezonderd. Zowel informele als formele verbanden kunnen blindheid veroorzaken. In het informele gaat informatie verloren vanwege het open en vrijblijvende karakter van deze relatie, het onsystematische. In het formele gaat informatie verloren vanwege het vastomlijnde karakter van deze relatie, waardoor er te weinig ruimte is voor het onverwachte en het onvoorspelbare. Formele afspraken bieden een systematische basis van een doelgerichte PDCA (*plan, do, check, act*) cyclus (zie ook standaard 4). Informele circuits helpen daarbij om juist open te blijven staan voor het onverwachte. Idealiter zijn het informele en het formele met elkaar verbonden: ze voeden elkaar.

Een optimaal cyclisch proces dat past bij de complexe problematiek en de gedistribueerde verantwoordelijkheid

Als er wel checks zijn, maar de *act* ontbreekt, ofwel de follow-up van verbeterpunten laat te wensen over, dan ontstaan kwetsbaarheden. Om tot acties te komen helpt het om door de verschillende lagen van de organisatie heen

verantwoordelijkheden aan te wijzen. Door de wijze van organisatie in het hoger onderwijs, met veel verantwoordelijkheid voor decentrale eenheden, zijn de evaluatierollen vaak verspreid belegd. Hierdoor ontstaat het risico dat scherpte verloren gaat bij het doorgeven van informatie aan de verschillende lagen.

6.2 Bevindingen

Heroverweging eigen informatiebeveiliging na cyberaanval Universiteit Maastricht

Voor vrijwel alle instellingen die we hebben gesproken geldt dat de cyberaanval op de UM aanleiding is geweest om nog eens kritisch te kijken naar het interne systeem van controle en evaluatie. Daarbij speelde telkens de vraag: hebben wij zelf de kwetsbaarheden die bij de UM zijn aangetroffen voldoende in het vizier, zetten we onze middelen wel goed in en zijn onze informatiebeveiligingsdoelen nog wel passend? Die evaluatie heeft tot verschillende aanpassingen op het gebied van evalueren en controleren geleid:

- Versneld invoeren van reeds voorgenomen acties. Bijvoorbeeld snellere investeringen, snellere inrichting van een SOC, versnelde werving van netwerkbeheerders
- Intensiveren of aanscherpen van lopende beleid: een aantal instellingen heeft op basis van de analyse van de UM hun beveiligingsbeleid aangepast. Netwerksegmentering was dan bijvoorbeeld al geregeld, maar wordt nog verder en scherper geïmplementeerd
- Nieuwe maatregelen: de casus UM heeft enkele instellingen ook geholpen om intern nieuwe maatregelen door te voeren, zoals tweefactor authenticatie
- Herijken van de volledige PDCA cyclus en de positie van ICT daarbinnen: enkele instellingen gaven aan dat de hack bij de UM aanleiding was geweest om nog eens kritisch naar de bestaande procedures te kijken.

Zoektocht naar inrichting en afstemming

Er rijzen tijdens de gesprekken verschillende vragen over de optimale inrichting van een cyclisch controle en evaluatie proces. Er wordt in het hoger onderwijs veel gecontroleerd en geëvalueerd, maar komt dat bijvoorbeeld ook voldoende bij elkaar op de juiste plek? Moet er een IT-auditor komen? Wat is überhaupt de rol van de audit afdeling? Wat is de rol van de accountant en wat mogen we van die controles verwachten? Hoe actief moet de RvT sturen op controle en evaluatie? Welke plek nemen de CISO en de FG in? Wie is er verantwoordelijk voor de follow-up? Zijn alle partijen wel betrokken in elke fase van de PDCA cyclus? Geen van de gesprekspartners gelooft in een waterdichte PDCA cyclus, in de zin dat je nooit dingen zult missen. Wel horen we elementen waarin veel geïnvesteerd wordt om die cyclus zo sluitend en effectief mogelijk te maken:

- Een goede procedure, waar duidelijke verbinding is tussen bedrijfsvoering en onderwijs
- Met voldoende aandacht voor sturing en opdrachtgeverschap van bovenaf en
- Met een actief informerende rol voor de (cyber)experts op de werkvloer

Evaluaties en volwassenheidsniveau

Uit de gesprekken blijkt dat met name grote instellingen aangeven dat zij evaluaties uitvoeren ten behoeve van risicomanagement rond cybersecurity. De evaluaties nemen verschillende vormen aan. Een grote universiteit geeft bijvoorbeeld aan drie verschillende audits uit te voeren: 1) inhuren van een ethische hacker, 2) een interne audit door de eigen IT-auditor, en 3) een externe audit door een groot accountancy bedrijf. Ook nemen meerdere instellingen deel aan de landelijke cybercrisisoefening (OZON van SURF, zie ook standaard 3). Een grote bekostigde hogeschool kijkt nadrukkelijk naar de NIHO, het normenkader van SURF. Voor de

evaluaties gebruikt een rpho niet de SURF-normen, maar de ISO normering 27.001 als kapstok, inclusief ISMS, information security management systeem, wat bestaat uit strategisch en operationeel beleid. Drie instellingen geven in de gesprekken aan eigen audits te hanteren die meer passend zijn bij het eigen volwassenheidsniveau c.q. uitgebreider zijn dan de SURF-audit, omdat ze deze eigenlijk te beperkt vinden. Deze instellingen hebben al een lange traditie van stevige ICT-audits. Andere instellingen geven aan de SURF-audit weer te uitgebreid te vinden, zij staan eigenlijk nog aan het begin van een echte PDCA cyclus.

Kennis en kunde ontwikkelen

Meerdere Raden van Toezicht geven aan geregeld de evaluatiegegevens te bespreken in hun vergadering of in hun audit commissie. Anderen geven aan dit nog niet structureel te doen, maar wel de ambitie hebben. Uit alle gesprekken blijkt dat het goed kunnen interpreteren van de evaluatiegegevens nog een hele kunst is. Veel gesprekspartners geven aan dat het lastig is om het goede gesprek te voeren over dit onderwerp; maar weinigen kennen de technische finesses in voldoende mate en kunnen ‘reguliere’ dreigingen onderscheiden van ‘ernstige’ dreigingen. Dat is problematisch voor hen die een controlerende en sturende taak hebben, zoals het College van Bestuur en de Raad van Toezicht, van hen wordt verwacht keuzes te maken en te prioriteren. Een CISO of een integraal veiligheidsmanager kan het bestuur daarbij helpen. Enkele ICT’ers geven aan dat hun vak niet alleen technisch is, maar dat je ook de skills moet hebben om de bestuurder op de juiste manier te informeren en in beweging te zetten om te doen wat nodig is. Een ICT’er maakt afwegingen over de ernst van risico’s: wat heeft de CvB’er nodig, wat niet. Het CvB moet op haar beurt kritische vragen stellen. De meeste gesprekspartners geven aan dat het afgelopen jaar ook op het gebied van de eigen kennis en kunde, en het stellen van de juiste vragen, voortgang is geboekt. Ze geven echter ook aan dat er nog veel afhangt van persoonlijke affiniteit. Dat laatste wordt door alle gesprekspartners als ongewenst gezien; het vrijblijvende en ad hoc karakter van de PDCA rondom cyberveiligheid vindt men niet meer van deze tijd. Die ontwikkeling is dan ook snel gegaan blijkt uit de gesprekken.

Beproeven van de informatiebeveiliging in de praktijk

Naast een (uitgebreide) audit zijn er verschillende instellingen die op soms beperkte schaal de praktijk van hun informatiebeveiliging beproeven. Daarbij wordt pentesting[47] het meeste genoemd. Een universiteit gaf aan sinds enkele jaren jaarlijks pentesting via een “red team” oefening te houden. Een derde partij probeert dan als ethisch hacker het netwerk binnen te dringen. Deze universiteit overweegt om de volgende test als “purple team” oefening te houden. Naast het aanvallende (rode) team is er dan een “blue team” dat evalueert of de universiteit de juiste acties neemt om de aanval tegen te houden.

Wel of niet opschalen

Met name de verantwoordelijken voor ICT geven aan dat ze constant afwegingen maken over de ernst van alle actuele dreigingen, zodat er op tijd aandacht en maatregelen opgeschaald en afgeschaald kunnen worden. Ze moeten kiezen welke informatie er aan het beslisniveau moet worden doorgegeven. Zeker bij grote instellingen zijn er dagelijks kleinere incidenten en signalen. De vraag voor de instellingen wanneer en hoe deze moeten worden opgeschaald en om generieke actie vragen. Ook in de monitoring van incidenten moeten er keuzes gemaakt

[47] Handmatige controle waarbij men zo diep mogelijk wil binnendringen in een systeem om zwakke plekken te vinden en de gevolgen hiervan te kennen. Men gebruikt de zwakke plekken om nog wat dieper in het systeem te komen. Doel van de test is niet om zoveel mogelijk zwakke plekken te vinden. Dat gebeurt wel bij een vulnerability scan. (uit: P. Oldengarm & L. Holterman (redactie) *Cybersecurity Woordenboek. Van cybersecurity naar Nederlands.* 2e druk. Den Haag Cyberveilig Nederland. Zie: www.cyberveilignederland.nl/woordenboek (geraadpleegd 26 juli 2021))

worden volgens de gesprekspartners; je kunt zeker als je niet goed in de materie zit gemakkelijk overweldigd worden door de veelheid aan informatie en de verkeerde conclusies trekken.

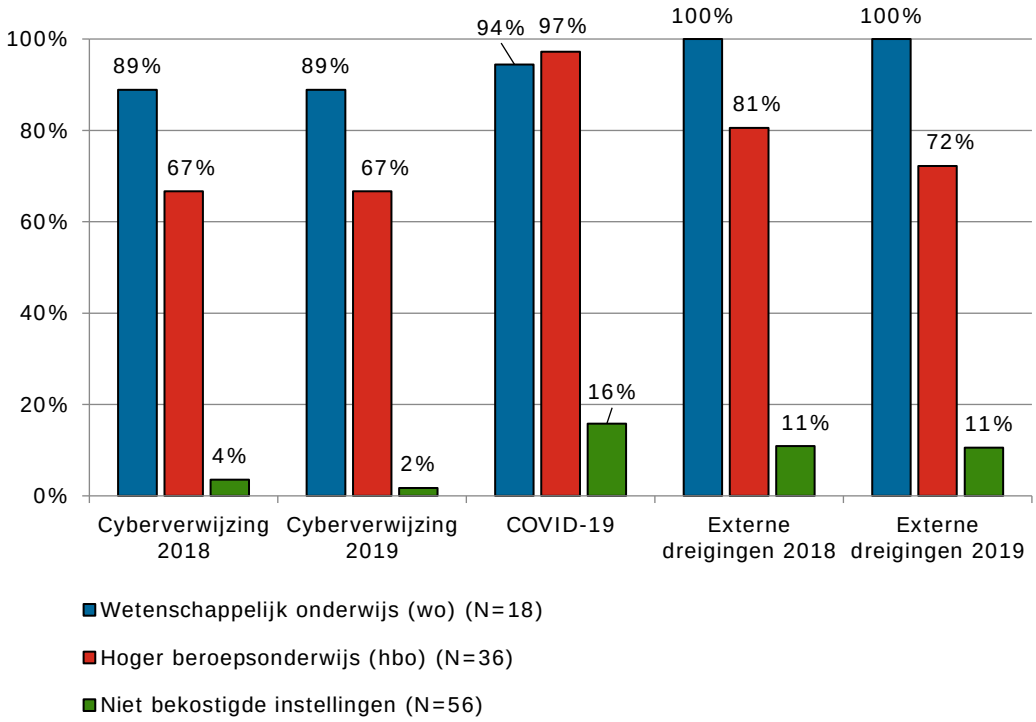
Cyber in decentrale management rapportages

Bij de grotere instellingen is de PDCA cyclus geformaliseerd en worden periodiek, maar in elk geval jaarlijks gesprekken gevoerd tussen het College van Bestuur en de verantwoordelijk directeuren op basis van managementrapportages. Die rapportages bevatten doorgaans ook een risico-paragraaf met een top vijf van risico's, alsmede een paragraaf met verbeterpunten, lopende acties en dergelijke. Die gesprekken vinden zowel plaats met stafdirecties als met onderwijsdirecties of faculteiten/decanen. Soms is ICT of cybersecurity een vast onderdeel van een dergelijke managementrapportrage, meestal is het format echter open en minder sturend. Een overweging voor een meer open format is het beperken van de administratieve last: alleen bij afwijkingen of risico's krijgt een onderwerp een plek in de rapportage. Uit de gesprekken blijkt dat niemand het belang van cyber ontkent, maar dat het onderwerp cyber niet vaak onderdeel is van de managementrapportages van onderwijsdirecties of faculteiten, tenzij daar vanuit het CvB soms specifiek naar is gevraagd. 'Echte' onderwijsonderwerpen blijven de boventoon voeren: de agenda van overleggen is vaak vol en is primair gericht op onderwerpen die het onderwijsproces direct raken. Sommige gesprekspartners noemen een separaat bedrijfsvoeringsoverleg, andere geven aan dat bedrijfsvoering als breed onderwerp altijd op de agenda staat van bijvoorbeeld een directeurenoverleg of een stafhoofdenoverleg. In die gevallen komt cyber al vaker op de agenda, maar lang niet altijd structureel (zie ook standaard 4). De managementrapportages van de verantwoordelijke ICT directie omvat uiteraard wel altijd het onderwerp cybersecurity.

Publieke verantwoording

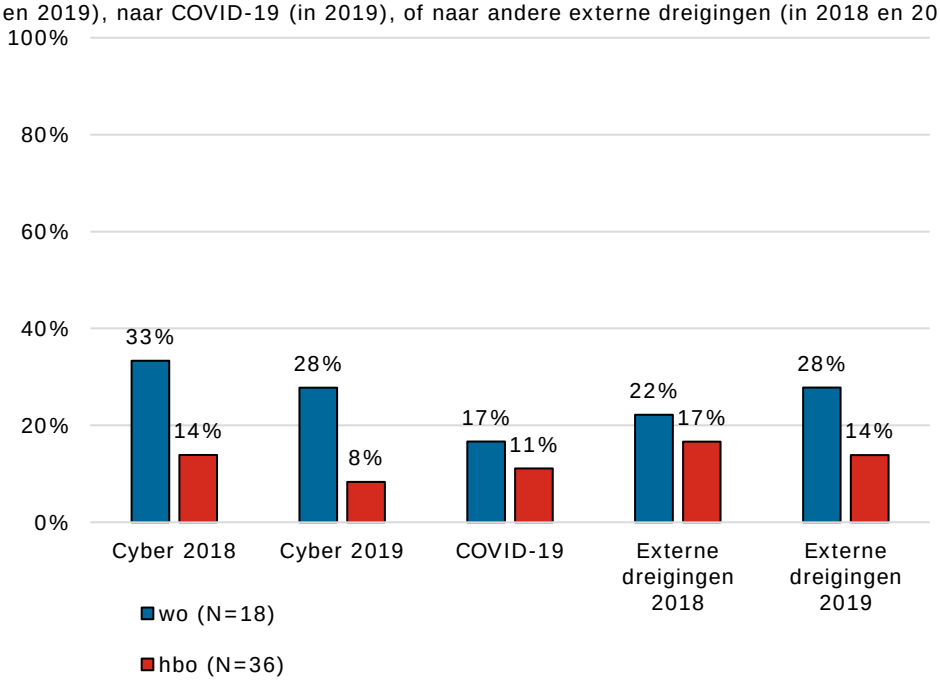
Bij een goed functionerende PDCA cyclus hoort ook het afleggen van verantwoording over gesignaleerde risico's en de ondernomen acties om deze te adresseren. Jaarverslagen zijn bij uitstek het openbare verantwoordingsdocument voor instellingen. In de jaarverslagen geven bijna alle bekostigde universiteiten en het merendeel van de bekostigde hogescholen aandacht aan cyberveiligheid als onderdeel van de bedrijfsvoering (zie figuur 6.2a). Daar tegenover staat dat vrijwel geen van de rpho's in hun verslag van werkzaamheden aandacht geven aan cyberveiligheid. Voor zowel jaarverslagen als de verslagen van werkzaamheden is het niet verplicht om iets op te nemen over cyberveiligheid. Desondanks geeft de uitkomst van deze analyse een beeld van de mate van aandacht die er is voor dit onderwerp als onderdeel van de bedrijfsvoering (zie standaard 4). Dat neemt niet weg dat ook instellingen die hier niets over vermeld hebben in hun jaarverslaglegging bezig kunnen zijn geweest met bewustwording bij het bestuur.

Figuur 6.2a Aandacht voor cyberveiligheid versus corona en externe dreigingen in de jaarverslagen. Het percentage bekostigde instellingen in het wo (N=18) en hbo (N=36) en rpho's (N=56) dat in de jaarverslagen verwijst naar cyberveiligheid (2018 en 2019), COVID-19 (2019) en naar andere externe dreigingen (2018 en 2019).



De RvT is verantwoordelijk voor het interne toezicht en legt in een aparte passage in het jaarverslag verantwoording af voor de controle en evaluatie die hij in een jaar heeft uitgevoerd. De passages van de RvT uit de jaarverslagen van 2018 en 2019 bevatten echter weinig informatie over cyberveiligheid (zie figuur 6.2b). De RvT's rapporteren veel over werkdruk gerelateerde onderzoeken en interventies, en als het over informatiebeveiliging gaat dan is het doorgaans AVG gerelateerd. Eén RvT vermeldt: "Iedere vier maanden ontvangt de Raad van Toezicht rapportages van de afdeling Interne Audits waarin verslag wordt gedaan van de bevindingen van de uitgevoerde audits naar de naleving van (interne) regelgeving. Tevens ontvangt de Raad van Toezicht de periodieke rapportages over integrale veiligheid waarin onder meer een overzicht is opgenomen van incidentenmeldingen op het gebied van ICT, brand en ongevallen."

Figuur 6.2b Het percentage bekostigde instellingen in het wo (N=18) en hbo (N=36) dat in de passage van de Raad van Toezicht in de jaarverslagen verwijst naar cyberveiligheid (in 2018 en 2019), naar COVID-19 (in 2019), of naar andere externe dreigingen (in 2018 en 2019).



6.3 Stelsel hoger onderwijs

Definitie van de standaard voor het stelsel:

Er is een landelijk dreigingsbeeld voor risico's in het onderwijs. Er is zicht op de mate waarin instellingen en het stelsel als geheel is voorbereid op risico's, hoe risico's worden afgehandeld en er wordt geëvalueerd welke aanpassingen op stelselniveau nodig zijn om escalatie en herhaling te voorkomen.

Sterktes

- SURF maakt een dreigingsbeeld onderwijs en onderzoek en deelt dit actief met haar leden en de buitenwereld.
- SURF heeft een goed uitgewerkt normen- en toetsingskader dat voor alle instellingen beschikbaar is en gebruikt kan worden.

Zwaktes

- De deelname aan de audits is nog niet volledig. Er is onvoldoende transparantie over de cyberweerbaarheid van het stelsel als geheel. Het landelijk beeld geeft geen specifieke informatie over instellingen.

Kansen

- Recente incidenten hebben de aandacht voor cyber duidelijk vergroot.
- VH en VSNU hebben afspraken gemaakt met haar leden over de deelname aan de SURF-audit. De gegevens van de survey en de audit bieden in potentie informatie over de kwetsbaarheden in het stelsel en op welke punten aandacht, aanscherping of kennis nodig is.
- Bij diverse toezichthouders is behoefte aan meer zicht op stelselrisico's.

Bedreigingen

- Focus op controle en evaluatie vermindert de aanwezige openheid en bereidheid tot delen.
- Gestructureerde controles kunnen blindheid veroorzaken voor onverwachte dreigingen.

- Het is niet duidelijk wie aanspreekbaar is op de uitkomsten van de landelijke evaluaties en wie verbeteringen moet doorvoeren en opvolgen. Er zij veel actoren, waardoor niemand ‘eigenaar’ is.

Grensoverstijgend controleren en evalueren
Cybersecurity is een onderwerp dat de grenzen en de verantwoordelijkheid van de individuele instelling overstijgt. Dit geldt ook voor controleren en evalueren. Om als instelling goed te kunnen controleren en evalueren, zijn landelijke normen nodig, is vergelijking met anderen en een benchmark noodzakelijk en is externe expertise vaak onontbeerlijk. Daarnaast is cyberveiligheid bij uitstek een onderwerp dat ook op stelselniveau speelt: hoe veilig is het (hoger) onderwijs als geheel? SURF speelt een belangrijk rol bij het beantwoorden van die vraag door haar jaarlijkse dreigingsbeeld en de SURF-audit.

Controleren en evalueren om het lerend vermogen van het stelsel als geheel te vergroten
Het uiteindelijke doel van controleren en evalueren op stelselniveau is het lerend vermogen van het stelsel als geheel te bevorderen. Het is belangrijk om aan te tekenen dat – zie ook standaard 5 over ketensamenwerking – het stelsel wat ons betreft hier tamelijk groot is: niet alleen de wo-instellingen, niet alleen het hoger onderwijs, maar het onderwijs als geheel en de cyberveiligheid ‘community’ als geheel en die delen samen. Daarom zijn we ook juist in dit onderzoek op zoek: hoe werkt die samenwerking op het gebied van controleren en evalueren, waar kan het lerend vermogen vergroot worden en wat leert het stelsel als geheel van incidenten als de hack bij de UM?

6.4 Bevindingen

Bekendheid dreigingsinformatie
Veel gesprekspartners verwijzen naar het cyberdreigingsbeeld dat SURF jaarlijks publiceert en de onderliggende survey waarop dit dreigingsbeeld is gebaseerd. Gevraagd naar de evaluatie-instrumenten die door SURF beschikbaar worden gesteld, noemen gesprekspartners vaak de survey. Een enkele keer wordt ook expliciet naar de SURF-audit verwezen. In sommige gesprekken blijken bestuurders en ICT’ers niet direct op de hoogte van het verschil tussen de survey en de audit. Dat verschil blijkt er wel te zijn; het dreigingsbeeld is geen benchmark of ranking, het geeft geen inzicht in absolute zin over de weerbaarheid van het stelsel als geheel, noch van het volwassenheidsniveau per onderwerp. Het dreigingsbeeld geeft (op basis van zelfinschatting van respondenten aan de survey) een overzicht van onder andere incidenten en van de type investeringen in weerbaarheid die door instellingen worden gedaan. Het dreigingsbeeld is daarmee een uitstekend startpunt voor degene die zich afvraagt wat de trends zijn als het gaat om cyberdreigingen in het onderwijs.

Inschatting cyberweerbaarheid van het stelsel als geheel
Het cyberdreigingsbeeld 2020[48] van SURF geeft een overzicht van de grootste risico’s die het stelsel als geheel bedreigen. In het cyberdreigingsbeeld 2020 is de score voor cyberweerbaarheid van 6,5 iets hoger dan die van 6,3 uit 2019. SURF stelt daar zelf over in haar dreigingsbeeld: “Op basis van deze uitkomsten kunnen we stellen dat er, ondanks enige vooruitgang, bij onderwijs- en onderzoeksinstellingen nog genoeg ruimte is voor verdere verhoging van de cyberweerbaarheid”. Onze gesprekspartners bevestigen de conclusie uit het

[48] 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)

cyberdreigingsbeeld. Enerzijds zijn ze behoorlijk tevreden over hoe dingen in het hoger onderwijs geregeld zijn, anderzijds noemen ze nog veel punten die echt om verbetering vragen. Daarbij hebben we ICT'ers gesproken die uitgesproken kritisch waren over het volwassenheidsniveau van de sector als geheel in vergelijking met bijvoorbeeld banken, maar ook experts die juist uitgesproken positief waren over de positie van het hoger onderwijs in vergelijking met bijvoorbeeld gemeentes en andere onderwijssectoren. We horen uit de gesprekken terug dat er door de toegenomen aandacht ook sprake is van een steviger kritische reflectie en een aanscherping van de eigen interne normen. De overall score is daarom volgens hen vooral een indicatie. De gesprekspartners geven ook aan dat de score is gebaseerd op een geaggregeerde zelf-inschatting; die inschatting wordt gemaakt op basis van de kennis en kunde van vaak een enkele persoon op basis van de aan die persoon beschikbare informatie. Bovendien wordt hij ingevuld voor de instelling als geheel en kan dat latente zwakheden daarmee verbloemen. Daarmee is de inschatting niet onbelangrijk, maar heeft niet de betrouwbaarheid als die van een externe audit of benchmark op alle organisatieniveaus. Dat mag overigens ook niet als diskwalificatie worden gezien van de inschatting of van het dreigingsbeeld. Het is een mooi voorbeeld van transparantie binnen de sector en de wil om verantwoording af te leggen van haar inspanningen. Het is een noodzakelijk element van het geheel van controle en evaluatie op stelselniveau.

Bekendheid normenkader

SURF heeft een normenkader voor informatiebeveiliging in het hoger onderwijs (NIHO) ontwikkeld. Het toetsingskader vult het normenkader aan door te beschrijven wat de vereisten zijn om aan een bepaald volwassenheidsniveau te voldoen. Onderwijsinstellingen kunnen daarmee de informatiebeveiliging van de universiteit of hogeschool beoordelen, voor de instelling als geheel of voor afzonderlijke afdelingen. Het normen- en toetsingskader vormt de basis van de tweejaarlijkse SURF-audit-benchmark waaraan instellingen kunnen deelnemen. In de gesprekken met instellingen wordt geregeld naar dit normenkader verwezen, het biedt instellingen houvast als het gaat om informatiebeveiliging. Hoewel het kader wel breed bekend is, is het niet bij alle instellingen volledig bekend noch komt uit de gesprekken met instellingen het beeld naar voren dat de inhoud van alle clusters gesneden koek is voor de gesprekspartners. Veel ICT'ers verwijzen er uit eigen beweging naar, binnen kleinere instellingen is het vaak minder bekend, bij bestuurders vaak in mindere mate en bij rpho's is het kader vrijwel onbekend.

Instellingen kunnen vrijwillig kiezen om deel te nemen aan de SURF audit op basis van het SURF toetsingskader. De resultaten van die audit worden gepubliceerd in een benchmark. De benchmark geeft individuele onderwijsinstellingen inzicht in de eigen scores ten opzichten van andere ho-instellingen. De baseline waaraan instellingen zouden moeten voldoen wordt bepaald door de aanbevolen volwassenheidsniveaus. De volwassenheidsniveaus worden op hun beurt weer mede bepaald door de risico's die het cyberdreigingsbeeld[49] identificeert. De niveaus lopen van 1 tot 5, waarbij 4 bijvoorbeeld staat voor een maatregel die van zo groot belang is dat een regelmatige toetsing (PDCA-cyclus) noodzakelijk is, en 3 voor een maatregel die basaal is en daardoor niet kan ontbreken – of in het cyberdreigingsbeeld geclassificeerd is als belangrijk. Alle andere maatregelen krijgen in ieder geval volwassenheidsniveau 2[50].

[49] Het Cyberdreigingsbeeld (zie voetnoot 48) is gebaseerd op een survey onder medewerkers van onderwijs- en onderzoeksinstellingen en op publieke bronnen. In de survey vraagt SURF onder andere welke risicofactoren volgens de SURF-doelgroep het belangrijkste zijn, welke incidenten hebben plaatsgevonden en wat de weerbaarheid van de instellingen is.

[50] Voor meer informatie over het normenkader voor de SURFaudit en volwassenheidsniveaus, zie: https://www.surf.nl/normenkader-surfaudit-audit-je-informatiebeveiliging (geraadpleegd op 19-7-2021)

Van normenkader naar toetsingskader
Het normenkader is verder uitgewerkt in een toetsingskader. Met dit kader kunnen instellingen een self-assessment uitvoeren of een audit (laten) uitvoeren. Daartoe zijn er vijf volwassenheidsniveaus uitgewerkt op basis van het volwassenheidsniveau van de NBA[1]. SURF licht deze volwassenheidniveaus op de volgende manier toe:

1. Beheersmaatregelen zijn niet of slechts gedeeltelijk vastgesteld en/of worden op een inconsistente manier uitgevoerd en zijn sterk afhankelijk van individuen.
2. Beheersmaatregelen bestaan en worden op een gestructureerde en consistente, maar informele manier uitgevoerd.
3. Beheersmaatregelen zijn gedocumenteerd en worden op een gestructureerde en formele manier uitgevoerd. Uitvoering van de maatregelen is aantoonbaar, getest en effectief.
4. De effectiviteit van beheersmaatregelen wordt periodiek beoordeeld en indien nodig verbeterd. Deze beoordeling is gedocumenteerd.
5. Een bedrijfsbreed risico- en beheersprogramma voorziet in continue en effectieve beheersing en aanpak van risico's.

Resultaten van de SURF-audit

De laatste benchmark dateert van 2019. Het rapport is in 2020 verschenen[51]. Aan deze SURF-benchmark namen 9 universiteiten en 24 hogescholen deel. Er hadden zich meer instellingen opgegeven om deel te gaan nemen (namelijk 12 universiteiten en 26 hogescholen). Ten opzichte van de vorige benchmark nam vooral het aantal deelnemende hogescholen toe. De resultaten van deze benchmark zijn op basis van een self-assessment door instellingen. Gemiddelde score van de deelnemende instellingen lag op 2,3. In 2017 was de waarde 2,4. Er is dus sprake van een geringe daling. Ook hier geldt de kanttekening die in de gesprekken is gemaakt: met toenemende kennis neemt ook de interne kritische blik toe. Geaggregeerd kunnen de scores op deze SURF-audit ook een beeld schetsen van de cyberweerbaarheid van het stelsel als geheel, maar die mogelijkheid ontbreekt tot nu toe vanwege de niet volledige deelname en de verschillende manieren waarop instellingen met de audit omgaan. Juist ook op stelselniveau is een betrouwbare inschatting van de weerbaarheid nodig, omdat het antwoord kan bieden op vragen die tijdens onze gesprekken worden gesteld: Welke specifieke elementen vragen nationale aandacht? Waar scoort het hoger onderwijs goed en kan zij hulp bieden aan anderen (onderwijs)sectoren en waar heeft zij wellicht hulp nodig van anderen? De informatie die nodig is om te bepalen of dat ook zo is, is potentieel met de SURF-audit aanwezig. Daartoe moeten echter drie problemen worden opgelost, zo blijkt uit onze gesprekken:

1. Zorgdragen voor een betrouwbare en vergelijkbare beoordeling.
2. Zorgdragen voor eigenaarschap op stelselniveau, niet alleen op de inhoud maar ook op voortdurende verbetering, zonder daarbij over de individuele verantwoordelijkheid van besturen heen te stappen.
3. Zorgdragen voor transparantie over de uitkomsten naar belanghebbenden – waarbij goed nagedacht moet worden over de betekenis van transparantie op de wil om uit te wisselen.

Landelijke afspraken over volwassenheidsniveau

In de VSNU en de VH is afgesproken dat alle bekostigde instellingen deelnemen aan de SURF-audit en dat zij ten minste volwassenheidsniveau 3 nastreven. Daarnaast is binnen VSNU verband afgesproken dat alle universiteiten in 2020 een externe audit laten uitvoeren op basis van het SURF-toetsingskader. Daarbij is afgesproken dat indien men zelf al een externe audit heeft laten uitvoeren, men de resultaten van

[51] 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)

deze eigen audits vertaalt en plot naar een score op volwassenheidsniveau op het SURF-normenkader. In VH verband is afgesproken dat alle bekostigde hogescholen uiterlijk in 2021 op basis van het normenkader het volwassenheidsniveau bepalen via een self-assessment en eventueel onderling peer review toepassen. Rpho's kennen een dergelijke gezamenlijke afspraak niet. In onze gesprekken wordt geregeld naar deze afspraken verwezen en werd het belang van zulke landelijke afspraken onderstreept. Een streefniveau voor volwassenheid is volgens het overgrote deel van de gesprekspartners niet vrijblijvend, het is niet iets dat je als instelling zelf bepaalt maar een zaak van collectief belang. Bij het doorpraten over wat die afspraken inhielden, bleek er wel onduidelijkheid over de exacte aard van de afspraak: wanneer wordt welk volwassenheidniveau verwacht en wat houdt dat volwassenheidsniveau eigenlijk in?

Volwassenheidsniveau 3 als tussenstap

Cyberweerbaarheid is op alle fronten een strijd met een voortdurend veranderende en verbeterende vijand en een voortdurende veranderende interne werkelijkheid, blijkt uit alle gesprekken. Een volwassenheidsniveau van 3 betekent daarom voor enkele instellingen al een forse opgave die niet direct gerealiseerd is. Zonder expliciet te verwijzen naar de volwassenheidsniveaus, geven diverse gesprekspartners ook aan dat juist de geïntegreerde risico-aanpak essentieel is om cybercriminelen een stap voor te blijven. Daarmee is niveau 3 niet een eindstation, de gesprekspartners noemen ook elementen die horen bij niveau 4 en 5. De gesprekken onderstrepen ook de kracht van niveau 2: met het streven naar stevig risicomanagement mag de kracht van het informele corrigerende vermogen niet worden weggegooid. Complicerend is dat in de gesprekken enkele bestuurders aangeven dat een weerbaarheidsniveau 5 niet voor het onderwijs is weggelegd, wat de vraag oproept of iedereen wel eenzelfde beeld heeft van wat de niveaus inhouden en of er wel sprake is van een gezamenlijk ambitieniveau.

Specifiek toezicht op cybersecurity in het onderwijs

Er is geen toezichthouder die specifiek toezicht houdt op de cyberweerbaarheid van het hoger onderwijs. Er is ook geen wettelijk voorschrift voor bedrijfsvoering in het algemeen, noch voor specifiek cyberveiligheid; de bedrijfsvoering valt onder de verantwoordelijkheid van de individuele instellingen en haar bestuur. De overheid is terughoudend in het geven van inrichtingsaanwijzingen, laat staan in het in detail voorschrijven van normen en kaders voor bedrijfsvoering. Voor bekostigde onderwijsinstellingen geldt wel dat de continuïteit van onderwijs en onderzoek gewaarborgd moet zijn (artikel 9.9a, 10.3e en 11.7a WHW) en dat de besteding van middelen rechtmatig en doelmatig moet zijn (artikel 9.8 lid 1f, 10.d lid 2f en 11.6 lid 1f WHW). Ook rpho's moeten de continuïteit van onderwijs waarborgen om de bevoegdheid graden te verlenen niet te verliezen. Buiten die artikelen heeft de onderwijsinspectie geen handhavingsgronden op instellingsniveau[52]. Wel kan de inspectie thematisch stelselonderzoek doen naar de kwaliteit van het hoger onderwijsstelsel als geheel.

Moet het toezicht meer specifiek naar cyberweerbaarheid kijken?

Via de koepels maar met name via SURF is er – zo betogen ook de meeste gesprekspartners – al voldoende zicht op het gebruik van ICT en de cyberweerbaarheid. De rol van het externe toezicht is in diverse gesprekken aan de orde geweest – zowel met instellingen als met andere belanghebbenden. De vraag was: moet de overheid steviger (kunnen) ingrijpen bij problemen met de cyberweerbaarheid binnen instellingen of in het stelsel als geheel? De meeste instellingen hebben geen behoefte aan een steviger toezicht, bij echt ernstige

[52] Zie paragraaf 1.3 voor uitgebreidere uiteenzetting.

verstoringen kan op basis van de WHW al een onderzoek worden ingesteld. Inhoudelijk geloven de gesprekspartners meer in het oplossen via de formele en informele mogelijkheden die SURF biedt. Er wordt wel een kwetsbaarheid gesignaleerd door enkele gesprekspartners: vanwege het coöperatieve netwerkkarakter zal SURF niet ingrijpen in geval van omissies op het niveau van (groepen) van instellingen, in de mate waarin een toezichthouder dat zou doen. Binnen SURF staat leren van elkaar en ondersteuning bij issues hoog op de agenda, maar SURF heeft niet de opdracht noch het mandaat om in te grijpen als er zich een ernstig incident voordoet. Op de vraag of dat een probleem is, wordt door instellingen doorgaans ontkennend geantwoord. Het zelfcorrigerend vermogen binnen het hoger onderwijs is zo groot en de kaders via SURF zo duidelijk dat dit afdoende werking heeft. Een extra toezichtslaag zou daar vooral bureaucratie aan toevoegen. Wel erkennen enkele gesprekspartners dat die insteek een mogelijke blinde vlek impliceert; binnen SURF of haar communities is er wellicht kennis van zwakheden waarop niet of indirect wordt geacteerd. Maar overwegend wordt dat risico als zeer klein ingeschat door de gesprekspartners bij instellingen, maar ook door andere gesprekspartners.

Toezicht op cybersecurity in andere sectoren

We hebben ook gesprekken gevoerd met enkele andere toezichthouders om te zien waar geleerd kan worden van andere sectoren.

Het *agentschap telecom* (AT) valt onder het Ministerie van Economische zaken en houdt toezicht op:

- Vitale dienstverleners Telecom (Energie en digitale Infra);
- Digitale service providers (DSP's): online marktplaats, online zoekmachine, clouddienst;
- Netbeheerders.

Het AT is één van de toezichthouders op de Wbni. Alle partijen die onder het toezicht van de AT vallen, hebben meldplicht bij een incident. De medewerkers van het AT hebben allen een achtergrond in of expertise op het terrein van cyber en/of ICT. AT voert systeemtoezicht uit op basis van een open norm: nemen bedrijven passende en evenredige technische en organisatorische maatregelen? De toezichtsrelatie gaat uit van een open omgang met elkaar, waarbij rechtvaardig behandelen en een leercultuur van belang zijn. Om bedrijven daarbij te stimuleren voert AT gesprekken, maar kan ook (ICT) audits uitvoeren.

De *Inspectie Gezondheidszorg en Jeugd* (IGJ) heeft sinds de eerste gesprekken over het elektronisch patiëntdossier aandacht voor informatiebeveiliging. Sinds 2017 houdt men actief toezicht op e-health, zowel vanuit het perspectief van fabrikanten als van zorgaanbieders. Onderwerpen die aan de orde komen in dat toezicht zijn:

- *Goed bestuur en verantwoord innoveren*: Het bestuur van de zorgaanbieder moet 'in control' zijn, ook op het gebied van e-health.
- *Invoering en gebruik van e-health-producten en –diensten*: De zorgaanbieder moet bij invoering en gebruik van e-health-producten en -diensten zorgen voor goede voorwaarden.
- *Patiëntparticipatie*: De patiëntenzorg wordt steeds afhankelijker van e-health. Daarom is het belangrijk dat de zorgaanbieder de cliëntenraad raadpleegt over het beleid.
- *Samenwerken in het netwerk en elektronisch vastleggen en uitwisselen van gegevens*: e-health kan andere vormen van samenwerken mogelijk maken tussen zorgverleners.
- *Informatiebeveiliging en continuïteit*: De groeiende afhankelijkheid van ICT vraagt erom dat de organisatie zorgt voor de continuïteit.

In de zorg bestaat in tegenstelling tot het onderwijs een wettelijke basis (Wet kwaliteit, klachten en geschillen zorg) t.a.v. informatiebeveiliging. Het toetsingskader bestaat uit een aantal normen en daarbij horende toetsingscriteria, die zijn gebaseerd op wet- en regelgeving en 'veldnormen' die beroepsorganisaties van zorgverleners hebben opgesteld. De voor de zorg sectorale standaard voor informatiebeveiliging is vastgelegd in NEN normen[53], die zijn gebaseerd op de internationale ISO standaarden. Daarnaast is in 2018 vanuit de koepelorganisaties de Zorg-CERT opgericht om zorginstellingen te ondersteunen op het gebied van cybersecurity en t.b.v. het uitwisselen van informatie. Alle zorgaanbieders zijn daarbij aangesloten onafhankelijk van aard of omvang (groot klein, publiek of privaat, ziekenhuis of huisarts).

Europese ontwikkelingen en aanbevelingen gezamenlijk inspectiebeeld vitale sectoren

De *Inspectie Justitie en Veiligheid* (IJenV) is voor de vitale sectoren de coördinerende toezichthouder voor cyberveiligheid. Onder coördinatie van de IJenV hebben de gezamenlijke toezichthouders op vitale processen een samenhangend inspectiebeeld[54] uitgebracht (zie ook paragraaf 2.4). Naast het in kaart brengen van de ontwikkelingen rond het toezicht in vitale sectoren wordt ook vooruit gekeken. In Europees verband is gestart met de herziening van de NIB-richtlijn, waarbij de verwachting is dat het aantal vitale sectoren uitgebreid zal worden en het toezicht daarmee zal toenemen. Het samenhangende inspectiebeeld schetst vier aandachtspunten die ook van toepassing zijn op het toezicht in het onderwijs. Deze aandachtspunten zijn:

1. Aandacht én inhoud. Er is bewustzijn. Gezien de ontwikkelingen is het nodig voortdurend aandacht te houden bij vitale organisaties, beleidsdepartement en toezicht. Cyberveiligheid is niet van de ICT afdeling alleen maar verdient brede aandacht ook ten aanzien van de impact van nieuwe technologie.
2. Meer samenhang in het beeld. Dit eerste beeld kan geen conclusies trekken ten aanzien van het generieke kader. Sectorale verschillen blijven bestaan en zorgen ook voor verschillende risico's. Het veld is voor het toezicht jong, daarom is samenwerking tussen toezichthouders belangrijk om waar mogelijk van elkaar te leren.
3. Ontwikkelingen toezicht. In het kader van de verschillende ontwikkelingen, Europees en nationaal, zou het goed zijn als toezichthouders processen en werkwijzen op elkaar aansluiten. Dit maakt het mogelijk kennis en mensen uit te wisselen en resultaten over sectoren heen te vergelijken. Tevens wordt aandacht gevraagd voor de diverse wetgevingsinitiatieven zodat er uitvoerbare en handhaafbare praktijk komt die aansluit bij de al bestaande, al dan niet sectorale, toezichtpraktijken.
4. Professionaliseer het toezicht verder. De toezichthouders op vitale sectoren geven aan dat toezicht op cybersecurity niet zomaar aan de bestaande programmering is toe te voegen. Dit vraagt om kennis en expertise die nog niet bij alle toezichthouders aanwezig is.

[53] Dit betreft de NEN 7510 Informatiebeveiliging in de zorg, die is afgeleid van de ISO 27.001. Deel 1 stelt eisen aan het informatiebeveiligingsmanagementsysteem en deel 2 bevat richtlijnen voor beheersmaatregelen. Zie: www.webtoolnen7510.nl (geraadpleegd op 19-7-2021)

[54] 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)

7 Standaard 7: geld investeren in informatiebeveiliging

7.1 Instellingen hoger onderwijs

Definitie van de standaard voor instellingen:

Er worden voldoende middelen beschikbaar gesteld om de onderkende risico's op een adequate manier te behandelen.

Sterktes

- Instellingen hebben veel beleidsvrijheid in het alloceren van hun bekostiging.
- ICT afdelingen zijn goed in staat om hun vraag te articuleren.

Zwaktes

- De investeringen van kleine instellingen in cyberbeveiliging zijn mogelijk niet toereikend.
- Grote instellingen doen (steeds meer) investeringen – maar het is onduidelijk of deze toereikend zijn voor de betreffende instelling.

Kansen

- ICT en primair proces raken steeds meer met elkaar verbonden. Daarmee is ICT niet alleen een 'kostenpost'.
- Incidenten hebben geleid tot een gevoel van urgentie, waardoor noodzakelijke investeringen hoger op de lijst komen te staan.

Bedreigingen

- Investeringen in preventie van cyberrisico's zijn vaak onzichtbaar en daarmee minder goed te verdedigen.
- Er ontbreekt een benchmark voor de omvang van investeringen en maatregelen.

Wat is voldoende?

Deze standaard spreekt over de beschikbaarheid van voldoende middelen. Bij elke investeringsvraag die zich voordoet, moeten besturen zich de vraag stellen: hoeveel geld is nodig en kan ik dat geld ook aan andere zaken besteden? Bij investeringen in ICT geldt bovendien dat deze tamelijk onzichtbaar blijven, de impact op het primaire proces is lang niet altijd zichtbaar. Zo lang het om nieuwe laptops of andere verbeteringen gaat, is de afweging doorgaans wat eenvoudiger dan wanneer het om meer ongrijpbare investeringen in cyber gaat. Bij het spreken over deze standaard hebben we dan ook telkens de vraag aan de gesprekspartners gesteld: wat is voldoende en aan welke norm meet je dat dan af? Is er überhaupt een norm te geven en wordt er bij investeringen ook een businesscase gemaakt om tot een kosten-baten afweging te kunnen komen? En als die afweging er is, hoe weeg je dan het belang en de impact en de financiële schade van een hack?

Over welke middelen en maatregelen hebben we het: ICT, onderwijs, risicomanagement?

ICT is onlosmakelijk verbonden geraakt met het primaire onderwijsproces. Zelfs al worden alle lessen nog klassikaal en op locatie verzorgd, dan zijn er altijd nog financiële, administratieve en onderzoeksystemen waar medewerkers en studenten van afhankelijk zijn. In de praktijk is ook het onderwijs steeds meer afhankelijk van ICT: online lessen, video-calls, samenwerking met partijen in binnen- en buitenland. Maar ook bijvoorbeeld complexe apparatuur die onderdeel uitmaakt van het lokale netwerk. Daarom kijken we bij deze standaard naar de grenzen van investeringen: kun je nog wel spreken van investeringen in ICT als apart gespreksonderwerp en ingestoken vanuit investeringsvoorstellen die door ICT afdelingen worden gedaan? Hoe pakken instellingen dit vraagstuk op? Worden investeringsvoorstellen integraal afgewogen, bijvoorbeeld in een bedrijfsvoeringsoverleg, of wordt er gewerkt met

separate budgetten – naar bedrijfsvoeringsonderwerp of naar organieke eenheid? Mag je dan bijvoorbeeld van faculteiten ook investeringen vragen in cyberweerbaarheid? En wat doen instellingen aan investeringen in het verbeteren van het risicomanagement, de PDCA en de audits? Investeren in maatregelen gaat feitelijk over het investeren in elk van de zes overige standaarden, waar zet je op in? Omdat ICT op veel vlakken zo voorwaardelijk is voor de continuïteit van onderwijs en onderzoek, is de balans tussen diverse investeringen daarom telkens onderwerp van gesprek geweest in dit onderzoek.

Hoe weet je of een maatregel adequaat is?
Om te kunnen bepalen of een maatregel adequaat is, moet je daar uiteraard zicht op hebben. Zoals bij standaard 6 (evalueren en controleren) besproken, vraagt dat om een sluitende PDCA-cyclus. Bij deze standaard kijken we niet of die bestaat, maar wel of uitkomsten van interne evaluaties uiteindelijk leiden tot keuzes in investeringen. Het is een kwestie van *put your money where your mouth is*: als uit alles blijkt dat cyberdreigingen een groot risico zijn, maar niemand is bereid te investeren in maatregelen, dan heeft het risicomanagement en het evalueren geen zin gehad. Als er andersom vanuit een gevoel van urgentie veel geld in beveiliging wordt gepompt, zonder een afweging of de investeringen nuttig zijn, dan is er mogelijk geen sprake van doelmatige besteding van middelen. We interpreteren adequaat dus als: op basis van gedegen evaluaties, passend binnen het risicomanagement en leidend tot doelmatige uitgaven.

7.2 Bevindingen

Investeringsruimte voor informatiebeveiliging
In alle gevallen is het bestuur (het College van Bestuur of de directie van een rpho) verantwoordelijk voor het geheel aan investeringen, waaronder ICT. Doorgaans is er een centrale ICT dienst of een ICT directie, soms is het een ICT afdeling binnen een centrale directie met een eigenstandig budget waarbinnen gehandeld wordt, doorgaans als resultaat van een meerjarenbegroting. Binnen deze begroting heeft informatiebeveiliging vaak een eigen plek. Deze begrotingen worden vertaald in jaarplannen, waarover geregeld gesprekken worden gevoerd met het CvB. Met name universiteiten hebben een complexere bestuursstructuur, waarbij de decaan op facultair niveau verantwoordelijkheid draagt en over eigen middelen beschikt. Binnen die bevoegdheid valt vaak ook een eigen ICT afdeling en een eigen ICT budget. Een centrale ICT dienst kijkt in die gevallen doorgaans mee met investeringen, adviseert of deze in lijn zijn met het instellingsbeleid, begeleidt bij aanschaf etc. Daarnaast vindt er overleg plaats tussen CvB en faculteiten over hun investering, waaronder over ICT. Hoewel de ICT directie ook binnen grote universiteiten dus een stevige sturende stem heeft, is er ook veel lokale ruimte. Veel gesprekspartners geven daarbij wel aan dat die ruimte voor wat betreft informatiebeveiliging minder groot is geworden of zelfs ontbreekt. Binnen hogescholen heeft de centrale ICT dienst vaak al van oudsher een meer sturende rol. Lokale ICT budgetten komen daar nauwelijks voor.

Grote instellingen nemen maatregelen op basis van evaluaties en recente cyberincidenten
Grote instellingen voeren evaluaties uit ten behoeve van risicomanagement rond cybersecurity, om deze vervolgens te verwerken in strategisch en operationeel beleid. Zo geeft een bekostigde universiteit aan dat de prioriteiten op basis van de uitkomsten van de audits uitgewerkt worden in beleid en procedures. Instellingen schatten het risico op cyberdreigingen hoger in, door recente incidenten in het hoger onderwijs, en zetten dit om in concrete maatregelen. Zo zetten grote universiteiten

in op het opzetten van een SOC (zie ook standaard 3) en investeren instellingen in verschillende technische borgingsmaatregelen zoals permanente monitoring.

Grote instellingen investeren in mensen en tools om de veiligheid te bevorderen

Uit de gesprekken blijkt dat grote instellingen investeringen in mankracht en in techniek doen ten behoeve van risicomanagement rond cybersecurity. Een grote universiteit investeert bijvoorbeeld in de juiste mensen op de juiste plek in de organisatie, uitbreiding in FTE's voor een CISO en een aparte FG, aanschaffen van de juiste tools zodat je goed kunt monitoren en risico's tijdig kunt signaleren of *phishing* mails kunt blokkeren. Ook rpho's investeren in technologie; ze plaatsen firewalls en passen websites aan om die omgeving zo dicht mogelijk te maken, laptops zijn voorzien van *preboot encryption* en de instelling wil *multifactor authentication* invoeren. Een andere rpho geeft aan gebruik te maken van licenties van Microsoft. Deze instelling geeft aan dat zo'n platform beter is toegerust om alle nieuwe technieken bij te houden en in te zetten.

Kleine instellingen schatten hun risico's lager in en de investeringen zijn kleiner

Uit gesprekken blijkt dat kleine instellingen ook verschillende investeringen doen ten behoeven van het cyberrisicomanagement, maar in mindere mate dan grote instellingen. De prioriteit van het risico op cyberincidenten wordt door een aantal kleine instellingen lager ingeschat. Met name risico's die samenhangen met privacy (zoals datalekken) zijn bij deze instellingen uitgangspunt voor het risicomanagement. Een kleine hogeschool geeft aan dat zij het risicoprofiel van zichzelf lager inschat dan van een universiteit, omdat het onderzoek op een universiteit interessanter is voor kwaadwillenden. Een andere instelling geeft aan dat het gespreksonderwerp informatiebeveiliging geen prioriteit heeft gekregen afgelopen jaar, door coronacrisis (ICT-dienst heeft veel taken erbij gekregen door online onderwijs) en door wisselingen in het personeel en in het bestuur. Ook op het gebied van borging van het risicomanagement door middel van cyclische evaluaties en structurele monitoring van het netwerk lijken kleine instellingen minder maatregelen uit te voeren (zie standaard 3 en 6 voor een verdere uitwerking en voorbeelden). Het monitoren van het netwerk op cyberrisico's zoals een hack of *phishing* mails wordt door een kleine rpho (nog) door de ICT medewerker van de instelling zelf uitgevoerd en gebeurt niet automatisch. Ook oefent deze instelling niet specifiek op het vlak van cyberveiligheid.

Kleine instellingen investeren ook in techniek

Tot slot kiezen verschillende kleine instellingen net als grote instellingen voor verschillende technische investeringen ten behoeven van de verbetering van cyberveiligheid. Een kleine bekostigde hogeschool geeft aan voor de segmentatie en de toegang van de systemen risico's te minimaliseren. Accounts van studenten, medewerkers en gasten zijn qua infrastructuur gescheiden. Niet iedereen krijgt zomaar een account met volledige rechten (cursisten) en leveranciers krijgen minder toegang tot systemen dan voorheen. Een rpho geeft aan nog geen segmentatie te hebben, maar wel van plan te zijn dit door te voeren. Ook geven ze aan dat de monitoring uitgebreid moet worden. Een rpho geeft aan dat ze door de kleine omvang, strategisch kiezen voor gebruik van SURF. SURF is als partij omvangrijker, treedt op voor veel onderwijsinstellingen en is daarmee gelijkwaardiger in het gesprek naar grote leveranciers.

Er wordt geïnvesteerd in weerbaarheid

Hoewel het niet mogelijk is om de omvang van de investeringen exact weer te geven, kunnen we uit de gesprekken en de jaarverslagen (zie tabel 7.2a) wel

opmaken dat er door instellingen in de afgelopen jaren enorm veel geïnvesteerd is en waar die investeringen op gericht zijn. Het is niet duidelijk of de investeringen en maatregelen die instellingen nemen toereikend zijn voor de individuele instelling. Uit gesprekken blijkt dat instellingen niet direct een antwoord hebben op de vraag welk percentage van de totale investeringen binnen een instelling aan ICT besteed moet of mag worden. Evenmin is het duidelijk welk percentage van de totale ICT begroting aan cyberveiligheid besteed moet worden. Een benchmark voor de omvang van investeringen ontbreekt. Instellingen geven aan dat een exact kostenplaatje ook ingewikkeld is. Investeringen zijn vaak een optelsom van centrale en decentrale uitgaven, en zijn niet duidelijk af te bakenen naar specifieke kostenposten. Maatregelen variëren van specifiek technische ICT uitgaven tot uitgaven op het terrein van bijvoorbeeld leermiddelen, personeel en campagnes.

Tabel 7.2a: voorbeelden van maatregelen genoemd in jaarverslagen

Type maatregel	**Genoemde maatregel/investering**
Updates hardware, software en netwerk	Vernieuwing van het datacenter Verbeterde procedures patches van werkplekken en servers Up to date maken/houden van apparatuur en software De servers vernieuwd en het ICT-systeem met internet, computers en telefonie geïntegreerd Onderhoud centraal uitbesteed aan één externe partij De firewall opnieuw uitgebreid met nieuwe functionaliteit, waarmee onder andere ‘verdacht gedrag’ kan worden waargenomen Voorbereidingen getroffen voor de vervanging van het ‘hart’ van de netwerkinfrastructuur, de zogenaamde backbone Realisatie beheersbare mobiele werkplekomgeving in 2020 Verouderde systemen worden geactualiseerd Investeren in digitale onderzoeksinfrastructuur Het aantal ICT-toepassingen vermindert gestaag. De organisatie wordt daardoor op dit gebied minder kwetsbaar
Zonering	Is het ICT-netwerk van […] voor het belangrijkste deel gezoneerd. Dat betekent dat beveiligingsincidenten beter te isoleren (per zone) zijn en niet doorwerken in de hele infrastructuur. Hiermee is de informatie in studenten- en medewerkersapplicaties aanmerkelijk beter beveiligd tegen cyberaanvallen
Authenticatie en toegang	Oplossingen voor authenticatie (waaronder “multi factor authenticatie”) en gebruikersautorisatie
AVG	Aanschaf van applicatie voor privacy impact assessments
Spam/phishing	Structurele maatregelen getroffen om spam en phishing tegen te gaan
Backup beleid	Redundant uitvoeren van alle applicaties en data, en data in de cloud Verbeterde procedures voor backups
Monitoring	Nieuwe virus en ransomware monitoring Monitoring netwerkverkeer Monitoren afwijkend verkeer Continue monitoring en hoogwaardige digitale beveiliging Pilot gestart voor een Security Operations Center (SOC). Het SOC zal bestaan uit specialisten van verschillende teams met veel security-kennis. Implementatie van een security monitoring dienst waarmee veiligheidsrisico’s real time worden gedetecteerd

Type maatregel	Genoemde maatregel/investering
Kennis en gedrag	Aantoonbare kennis en vaardigheden van het ICT personeel Voortdurende investeringen om kennis en bewustzijn medewerkers en studenten op een hoger plan te brengen Vaardigheden ICT personeel Personeel en leiderschap binnen ICT wordt verder opgeleid en ontwikkeld.
Evaluatie en advies	Een externe adviseur voerde een 'health' check uit, waaruit blijkt dat enkele punten nog verbeterd moeten vervolgonderzoek uitgevoerd naar deze status. Mede naar aanleiding van een rapport door een accountant is besloten om nog intensiever te investeren in implementatie en toepassing van de AVG op alle niveaus en in alle geledingen van de instelling, en te anticiperen op de komst van de nieuwe privacy-verordening Implementatie adviezen informatiebeveiliging SURF

Cyberveiligheid (basis)maatregelen en autonomie van onderwijs en onderzoek

In het Cybersecuritybeeld Nederland (CSBN) wordt aandacht gevraagd voor de basismaatregelen die op orde moeten zijn, maar nog regelmatig ontbreken. De acht basismaatregelen volgens het NCSC[55] komen overeen met verbeterpunten die uit diverse evaluaties van incidenten in de afgelopen periode naar voren zijn gekomen en met de investeringen die door een deel van de instellingen al is gedaan of is voorgenomen. De basismaatregelen zijn:

- Installeer updates
- Zorg dat elke applicatie en elk systeem voldoende loginformatie genereert
- Pas multifactor authenticatie toe
- Maak regelmatig back-ups van uw systemen en test deze
- Segmenteer netwerken
- Bepaal wie toegang heeft tot uw data en dienst
- Versleutel opslagmedia met gevoelige bedrijfsinformatie
- Controleer welke apparaten en diensten bereikbaar zijn vanaf het internet en bescherm deze

Uit de gesprekken en uit tabel 7.2a komt naar voren dat verschillende van deze maatregelen onderdeel van het informatiebeveiligingsbeleid zijn of thans worden besproken binnen ho-instellingen. Desondanks zien we dat bij verschillende cyberincidenten ook na de Universiteit Maastricht een aantal van deze maatregelen niet volledig was ingebed in de organisatie. Dat maakt het stelsel kwetsbaar en roept de vraag op waarom hier niet steviger op gestuurd wordt, zoals wel binnen de vitale sectoren het gebruik is. Netwerksegmentatie bijvoorbeeld is van belang om een aanvaller te verhinderen eenvoudig door het netwerk en tussen systemen te kunnen bewegen. In het bijzonder wanneer er sprake is van meerdere decentraal beheerde netwerken of systemen, is het van belang alle verbindingen (alsmede het toegestane netwerkverkeer daarop) tussen het centrale en decentrale beheer in kaart te hebben. Met betrekking tot apparaten en diensten bereikbaar vanaf het internet, is een assessment van belang met daarbij een compleet overzicht binnen de ICT omgeving van de ho-instelling. Dit geldt zowel in het kader van monitoring als bij het reageren op een incident. Zonder een totaaloverzicht duurt een onderzoek naar mogelijk geraakte (gecompromitteerde) systemen en diensten aanzienlijk langer, waarmee de periode tot een incident onder controle is langer duurt. Omdat

[55] 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)

netwerken, apparaten en diensten steeds wijzigen, vraagt dit om een blijvend gesprek tussen verantwoordelijken over de te nemen maatregelen binnen de instelling.

Ook de basismaatregel die gebruikers rechtstreeks treft – multifactor authenticatie – is nog niet overal gemeengoed zo blijkt uit onze gesprekken. Op afstand werken via een VPN-verbinding was bij verschillende ho-instellingen ook voor COVID-19 mogelijk. Bij verschillende ho-instellingen hebben gebruikers via enkel een gebruikersnaam en wachtwoord toegang. Bij deze instellingen wordt multifactor authenticatie (zoals via een token of biometrisch identificatie naast een wachtwoord) beperkt ingezet bijvoorbeeld voor het ICT beheer. Uit alle evaluatie- en adviesrapporten die we tijdens dit onderzoek hebben geraadpleegd, blijkt dat dit geen houdbare praktijk is. Het gebruik van multifactor authenticatie voorkomt dat een aanvaller toegang tot een account verkrijgt na een geslaagde phishing aanval. Indien het gebruik van multifactor authenticatie nog beperkt wordt ingezet, wordt aangeraden in ieder geval te zetten op sterke wachtwoorden en daarmee gepaard gaand beleid. Dit laatste betreft onder ander de duur dat een wachtwoord geldig blijft en het periodiek controleren of een gebruiker toegangsrechten nodig heeft. Die keuzes raken gebruikers, dat blijkt uit alle gesprekken. Maar alle gesprekspartners geven aan dat het gezamenlijke belang van een goede beveiligde omgeving ook best wat van een eindgebruiker mag vragen. Die eindgebruiker heeft tenslotte ook baat bij de continuïteit van onderwijs en onderzoek. In de ervaring van veel instellingen, valt het uiteindelijk wel mee met de weerstand; eenmaal gewend aan bijvoorbeeld het gebruik van een extra token, verstomt het commentaar meestal. Wel is soms een incident nodig om het bewustzijn een zet te geven dat die extra stap ook van de eindgebruiker mag worden verwacht als onderdeel van zijn of haar professionaliteit.

7.3 Stelsel hoger onderwijs

Definitie van de standaard voor het stelsel:

Er worden voldoende middelen beschikbaar gesteld om de onderkende risico's op een adequate manier te behandelen. Dat impliceert dat er regelmatig op basis van een risico-inventarisatie wordt bepaald of er op stelselniveau voldoende middelen beschikbaar zijn voor informatiebeveiliging en of er binnen de bekostiging van instellingen voldoende middelen besteed (kunnen) worden aan beveiliging en preventie.

Sterktes

- De lump sum bekostiging biedt veel ruimte voor lokale accenten.

Zwaktes

- In het bepalen van de bekostiging wordt beveiliging niet apart opgenomen.
- Er is geen businesscase gemaakt op stelselniveau: wat zijn de kosten op stelselniveau en wat zijn de risico's van niet investeren?

Kansen

- Cybersecurity wordt door iedereen als belangrijk gezien en op diverse dossiers zien we dat de discussie over noodzaak en kosten wordt gevoerd.

Bedreigingen

- Echt goede beveiliging is enorm duur. Voor individuele instellingen kan losgeld betalen toch financieel aantrekkelijk blijven terwijl de stelselkosten daarvan potentieel enorm zijn.

Toelichting op de standaard

Ook op stelselniveau kunnen investeringen en maatregelen bijdragen aan het risicomanagement van instellingen. Niet alleen de instellingen zelf, maar ook andere organisaties in het onderwijsveld kunnen op basis van een risico-inventarisatie

bepalen of er op stelselniveau voldoende middelen beschikbaar zijn voor informatiebeveiliging. De bekostigde instellingen ontvangen een bedrag van de overheid en zijn zelf verantwoordelijk voor een doelmatige besteding van dat geld. De vraag is of binnen de bekostiging van instellingen voldoende middelen besteed (kunnen) worden aan cyberveiligheid en preventie van cyberdreigingen.

7.4 Bevindingen

Geen aparte aandacht voor ICT en cyberweerbaarheid in de bekostiging

Onderwijsbekostiging vindt plaats volgens het lump sum principe, en kent daarom geen specifieke toedeling voor bedrijfsvoering. Extra kosten voor ICT, beveiliging of bijvoorbeeld deelname aan een SOC moeten door instellingen uit deze lump sum worden gefinancierd. Instellingen geven aan dat dat tot nu toe telkens lukt, maar dat met name de laatste stap naar meer zekerheid een stevige extra investering vraagt. Die investering, bijvoorbeeld in een 24/7 SOC kan meer betaalbaar worden als hij vanuit gezamenlijkheid wordt gedaan. Toch blijft het een feit dat de inzet op security volgens alle gesprekspartners stevige investeringen vraagt.

Generieke investeringen en maatregelen

In veel gesprekken wordt benadrukt dat informatiebeveiliging een lokale verantwoordelijkheid is. Uit de achtergrondinformatie over diverse incidenten komt echter ook een beeld naar voren van een aantal systemische knelpunten die vragen om generieke maatregelen die door het hele stelsel kunnen of misschien wel moeten worden opgepakt. Vanuit SURF worden diverse generieke maatregelen opgepakt die, bij voldoende deelname een wezenlijke bijdrage kunnen leveren aan de cyberweerbaarheid van het stelsel. Enkele voorbeelden worden veel genoemd in de gesprekken en worden elders uitgebreider beschreven:

1. Het SURF-SOC: al voor het cyberincident bij de Universiteit Maastricht was het initiatief genomen om te komen tot een gezamenlijk security operations center. Het SURF-SOC is een dienst die instellingen kunnen afnemen. Deelname is tot nu toe relatief beperkt. Het SOC is interessant voor instellingen die zelf geen eigen SOC kunnen of willen opzetten
2. Het SURF-CERT: deze dienst biedt 24/7 ondersteuning en monitoring op cyberincidenten. Instellingen kunnen continu contact opnemen met dit CERT bij incidenten. Vanwege de aanwijzing van het CERT beschikt het onderwijs in principe over actuele informatie over dreigingen.
3. Cybersave yourself: deze materialen worden door veel instellingen gebruikt voor bewustwordingscampagnes
4. SURF internet: in dit netwerk zit al veel veiligheid ingebouwd.

Welke investeringen en maatregelen zijn landelijk, welke regionaal en welke lokaal?

Initiatieven tot investeringen en maatregelen komen in het ho doorgaans van onderop, er is een sterke vraagsturing. Voor een deel zorgt die vraagsturing dus ook voor ad hoc beleid. Een incident als bij de universiteit Maastricht geeft plots een enorme impuls aan lokale initiatieven. SURF is de partij die ook de lange lijn probeert vorm te geven. Zo dateerden de initiatieven om tot een gezamenlijk SOC te komen al van voor de cyberaanval op de UM. Vervolgens wordt de deelname aan het SOC weer aan de individuele instelling overgelaten. Dat bedreigt het draagvlak onder het SOC (bij onvoldoende deelname is het mogelijk geen duurzaam initiatief) en vergroot de kwetsbaarheid van het stelsel als geheel. Een verplichte deelname aan het SOC zou direct een enorme impuls geven aan de cyberweerbaarheid van het stelsel als geheel. Er lijkt in de gesprekken wel een zekere weerstand tegen het landelijk opleggen van dergelijke maatregelen, vanuit de behoefte aan autonomie. De stap van autonomie naar vrijblijvendheid is echter snel gezet. Uit de gesprekken blijkt dat het geen sinecure is om tot een landelijke oplossing te komen. Zowel

volwassenheidniveaus als omvang als visie als budgetten zorgen voor een wel heel ongelijksoortige uitgangspositie. Met name kleine instellingen geven aan de investeringen niet zelf te kunnen dragen. Hoewel grote instellingen aangeven dit probleem te herkennen en zelfs op fronten solidair zijn door kennis en kunde te delen, mag volgens hen niet verwacht worden dat zij de benodigde investeringen voor kleinere partijen gaan doen.

Wat betekent het niet betalen van losgeld?
Als het gaat om ‘investeringen’ dan is een terugkerende vraag die van het betalen van losgeld. Op dat front zijn er duidelijke overheidsvoorschriften: losgeldbetaling is onwenselijk aangezien dat het verdienmodel van hackers in stand houdt en losgeldbetaling is onrechtmatig omdat het een betaling van (gemeenschaps)geld aan criminelen is. Daarmee is een hack ook meteen het probleem van een individueel bestuur. Op lokaal niveau kan de afweging er namelijk anders uitzien; het betalen van losgeld kan een ‘voordelige’ optie zijn, afgezet tegen de kosten van de totale herbouw van een systeem. Bovendien is het bestuur verantwoordelijk voor de continuïteit van onderwijs en onderzoek en de betaling van losgeld is op het eerste gezicht een manier om snel over te kunnen gaan tot de orde van de dag. Geen enkele gesprekspartner geeft overigens aan zoiets een eenvoudige of bedrijfseconomische keuze te vinden, maar het houdt veel bestuurders en toezichthouders wel bezig. Wat als het mij gebeurt en onze systemen liggen drie maanden plat? Om deze keuze zo veel mogelijk te voorkomen, moet er sprake zijn van solidariteit in het stelsel. Kosten voor preventie en voor het oplossen van een hack moeten in gezamenlijkheid gedragen kunnen worden.

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 leidinggevenden. 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 bedrijfsvoeringaspecten 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 crisisafhandeling 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 en 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 achtneming 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/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 Terrorisme bestrijding 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 computercrisisteams*, 4410.

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

Bijlage I: Lijst van gesproken organisaties en gesprekspartners

Onderstaande partijen hebben wij gesproken in het kader van de netwerkanalyse om inzicht te krijgen in de stelselactiviteiten en verantwoordelijkheden rond cyberveiligheid in het hoger onderwijs.

- Agentschap Telecom
- Inspectie Gezondheidszorg en Jeugd
- Inspectie Justitie en Veiligheid
- Nationaal Coördinator Terrorismebestrijding en Veiligheid
- Nederlands Cybersecurity Center
- NRTO
- Platform Integraal Veilig Hoger onderwijs (IV-HO)
- SURF
- Vereniging Hogescholen (VH)
- Vereniging Universiteiten (VSNU)
- Vereniging van Toezichthouders van Hogescholen (bekostigd)
- Voorzitters Raden van Toezicht WO

Onderstaande universiteiten, hogescholen en rechtspersonen voor hoger onderwijs hebben wij gesproken om een indruk te krijgen van de aanpak van cyberveiligheid bij hoger onderwijsinstellingen en de uitdagingen waar ho-instellingen voor staan. Bij de keuze van instellingen is nadrukkelijk gekeken naar diversiteit, zodat met zowel omvangrijke als kleine instellingen uit het bekostigd en niet-bekostigd onderwijs is gesproken. De TU Delft, UvA en HvA hebben wij (ook) gesproken in het kader van cyberincidenten die zich voordeden bij deze instellingen. Van de Hogeschool InHolland is na het gesprek informatie ontvangen over het cyberincident dat zich bij hen voordeed.

- Christelijke Hogeschool Ede
- Hogeschool van Amsterdam
- Hogeschool ArtEZ
- Hogeschool InHolland
- Hogeschool Leiden
- NCOI
- Nederlandse Academie voor Beeldcreatie
- Nyenrode Businessschool
- Technische Universiteit Delft
- Technische Universiteit Eindhoven
- Theologische Universiteit Apeldoorn
- TMO Fashion
- Radboud Universiteit
- Universiteit van Amsterdam

Bijlage II: Lijst van afkortingen

AP	Autoriteit Persoonsgegevens
ARBO	Arbeidsomstandigheden
AT	Agentschap Telecom
AVG	Algemene Verordening Gegevensbescherming
BHV	bedrijfshulpverlening
BIO	Baseline Informatiebeveiliging Overheid
CBS	Centraal Bureau voor de Statistiek
CvB	College van Bestuur
CERT	Computer Emergency Respons Team
CIO	Chief Information Officer
CIP	Centrum informatiebeveiliging en privacybescherming
CISO	Chief Information Security Officer
CMT	Crisis Management Team
COMIT	Coördinerend Overleg Informatie Technologie
COT	Instituut voor Veiligheids- en Crisismanagement
CSBN	Cybersecuritybeeld Nederland
CSIRT	Computer Security Incident Response Team
CSR	Cyber Security Raad
DPIA	Data Protection Impact Assessment
DSP	Digitale Service Provider
DTC	Digital Trust Center
FG	Functionaris Gegevensbescherming
FTE	Fulltime-equivalent
HvA	Hogeschool van Amsterdam
hbo	hoger beroepsonderwijs
HBO-CSC	Coördinerend overleg van CIO's en/of ICT-directeuren
ho	hoger onderwijs
HRM	humanresourcemanagement
IBD	Informatie Beveiligingsdienst
IGJ	Inspectie Gezondheidszorg en Jeugd
IJenV	Inspectie Justitie en Veiligheid
IoC's	Indicators of Compromise
ISMS	information security management systeem
ISO	Internationale Organisatie voor Standaardisatie
ICT	Informatie- en Communicatietechnologie
IV-HO	Platform Integraal Veilig Hoger Onderwijs
KNAW	Koninklijke Nederlandse Akademie van Wetenschappen
LDS	Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden
MKB	midden en klein bedrijf
MTO	Medewerkers Tevredenheidsonderzoek
NCP	Nationaal Crisis Plan
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NEN	Nederlandse Norm (Stichting Koninklijk Nederlands Normalisatie Instituut)
NBA	Nederlandse Beroepsorganisatie voor Accountants
NIB	netwerk- en informatiebeveiliging (richtlijn)
NIHO	Normenkader voor informatiebeveiliging in het hoger onderwijs
NRTO	Nederlandse Raad voor Training en Opleiding
NWO	Nederlandse Organisatie voor Wetenschap RvT Raad van Toezicht
OCW	Ministerie van Onderwijs, Cultuur en Wetenschap

OZON	Oefening Zonder Officiële Naam
PDCA	Plan Do Check Act
PSA	Psychosociale arbeidsbelasting
ROC	regionaal opleidingscentrum
Rpho	Rechtspersoon voor hoger onderwijs
RI&E	Risico-inventarisatie en -evaluatie
RvT	Raad van Toezicht
SCIRT	SURFnet Community van Incident Response Teams
SIEM	Security Incident en Event Management
SIVON	Samen Inkopen Voor Onderwijs Nederland
SLA	Service Level Agreement
SOC	Security Operations Center
TUDelft	Technische Universiteit Delft
UM	Universiteit Maastricht
UvA	Universiteit van Amsterdam
VenJ	Ministerie van Veiligheid en Justitie
VH	Vereniging Hogescholen
VPN	Virtual Private Network
VSNU	Vereniging van Universiteiten
Wbni	Wet beveiliging netwerk- en informatiesystemen
WHW	Wet op het hoger onderwijs en wetenschappelijk onderzoek
wo	wetenschappelijk onderwijs
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.