Ministerie van Onderwijs, Cultuur en Wetenschap

>Retouradres Postbus 16375 2500 BJ Den Haag

De voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Op 9 september jl. heb ik uw Kamer het tweede deel van het rapport van de Inspectie van het Onderwijs (hierna: Inspectie) gezonden inzake het onderzoek naar cyberdreigingen in het hoger onderwijs.[1] Dit stelselonderzoek is het vervolg op het instellingsonderzoek naar aanleiding van de ransomware-aanval op de Universiteit Maastricht op 23 december 2019. In deze brief geef ik mijn beleidsreactie op het nu uitgebrachte tweede deel van het rapport van de Inspectie. Ik sta stil bij de stappen die de sector reeds heeft genomen, maar vooral ook bij de stappen die nog nodig zijn om de digitale weerbaarheid van de hoger onderwijs- en onderzoekssector te vergroten. Vanzelfsprekend is de verhoging van de weerbaarheid ook in andere sectoren van belang. Ik schets daarom ook de voornemens in het middelbaar beroepsonderwijs en in de

[1] Kamerstuk 'Binnen zonder kloppen- digitale weerbaarheid in het hoger onderwijs'| 15-09-2021.

onderzoekssector. Voor primair en voortgezet onderwijs verwijs ik naar de brief van de minister voor Basis- en Voortgezet Onderwijs en Media.[2]

Datum 28 september 2021

Betreft Digitale weerbaarheid in het hoger onderwijs en onderzoek en in het middelbaar beroepsonderwijs

Hoger Onderwijs en Studiefinanciering
Rijnstraat 50
Den Haag
Postbus 16375
2500 BJ Den Haag
www.rijksoverheid.nl

Onze referentie
29517143

Inspectierapport

De Inspectie heeft een themaonderzoek ingesteld met als hoofdvraag: *"Hoe kan het stelsel hoger onderwijs, met in het bijzonder besturen van hoger onderwijs-instellingen, handelen om de weerstand tegen cyberdreigingen te vergroten en zo de goede voortgang en kwaliteit van het onderwijs en onderzoek te waarborgen?"*

Het onderzoek richt zich op het bestuurlijk handelen rondom cyberveiligheid, waarbij de continuïteit van onderwijs en onderzoek het belangrijkste uitgangspunt is. Doordat de WHW geen nadere invulling geeft van dit bestuurlijk handelen maakt de Inspectie ook in dit tweede deel van het rapport gebruik van de binnen de overheid breed gebruikte zes BIO-standaarden.[3] Aan de zes standaarden heeft de Inspectie zelf een zevende toegevoegd, te weten: 'geld investeren in informatiebeveiliging'.

De Inspectie concludeert dat er op het gebied van cyberveiligheid in het hoger onderwijs veel gebeurt, maar er zeker nog belangrijke stappen nodig zijn om de digitale weerbaarheid te vergroten. Zo kan het hoger onderwijsstelsel, met in het bijzonder besturen van hoger onderwijsinstellingen, de weerstand tegen cyberdreigingen vergroten en zo de goede voortgang en kwaliteit van het onderwijs en onderzoek waarborgen door ten eerste een integrale benadering van cyberveiligheid te omarmen. Verder moet continu gemonitord worden zodat een lerend systeem ontstaat. De Inspectie concludeert als derde dat het expliciteren

[2] Kamerbrief 'Digitalisering in het funderend onderwijs' | 24-09-2021.

[3] De BIO (De Baseline informatiebeveiliging Overheid) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Het is gebaseerd op internationale standaarden, de ISO-normen 27001 en 27002. Deze zijn als verplicht te gebruiken standaarden opgenomen op de pas-toe-of-leg-uit-lijst op het forum standaardisatie. De zes BIO-standaarden zijn 1. Vergroten bewustzijn, 2. Veilige en open cultuur, 3. Inrichten risicoteam, 4. Borgen risicomanagement, 5. Aandacht ketensamenwerking, 6. Controleren en evalueren.

van eigenaarschap binnen het stelsel nodig is. Samenwerken en informatie-uitwisseling zijn essentieel omdat geen enkele partij alleen cyberveiligheid op een gewenst niveau kan brengen. Traditionele onderverdelingen (hogeschool-universiteit; bekostigd-onbekostigd; grotere-kleinere instellingen) zijn daarbij in het kader van cyberveiligheid niet relevant. De overheid moet tot slot regie nemen door met de sector een door allen gedeeld normenkader en ambitieniveau vast te stellen. En door te zorgen dat de sector goed is aangesloten op netwerken om ook op internationaal niveau informatie te delen.

Belangrijke stappen gezet in de sector, maar ook aanvullende maatregelen nodig

In alle sectoren binnen en buiten het onderwijs zien we een aanzienlijke stijging in de aard en omvang van cyberaanvallen waardoor de dreiging per saldo toeneemt.[4] Het is niet alleen een probleem van de onderwijssector, maar een nationaal en internationaal probleem. Hoewel cyberaanvallen niet te voorkomen zijn, zeker niet in een open systeem dat onderwijs en onderzoek per definitie vormen, zijn de maatregelen erop gericht aanvallen af te weren en, als dan toch een aanval plaatsvindt, de gevolgen te beperken.

Ikzelf heb zeer recent met de verschillende koepels gesproken over de verhoging van de weerbaarheid tegen cyberdreigingen. Bij alle partijen bestaat een gedeeld gevoel van urgentie om extra maatregelen te treffen en grote overeenstemming over de richting en het doel dat we willen bereiken. Vanzelfsprekend is soms differentiatie nodig -instellingen zijn niet gelijk qua grootte en risicoprofiel- maar deze differentiatie doet niets af aan de gedeelde urgentie en het gedeelde eindbeeld.
Hieronder ga ik nader in op de te nemen maatregelen. Kernelementen zijn dat elke instelling in het MBO en HO aan een vooraf afgesproken streefdoel voldoet, dat elke instelling wordt aangesloten op een mechanisme om 24/7 dreigingen te monitoren en dat elke instelling zich periodiek (ook) extern laat auditen. Zoals gezegd is maatwerk daarbij noodzakelijk. In het eerste kwartaal van 2022 wil ik met de sectoren een plan van aanpak met een kalender wanneer dit voor elke instelling gerealiseerd kan zijn. Verder draag ik zorg voor voldoende informatie (loketfunctie) vanuit het NCSC en de veiligheidsdiensten over dreigingen, en voor aansluiting op relevante internationale ontwikkelingen op het terrein van digitale weerbaarheid.

Ik heb uw Kamer eerder geïnformeerd over de verschillende maatregelen die zijn getroffen om cyberdreigingen zo veel mogelijk te weerstaan.[5] Ik heb dat gedaan aan de hand van de volgende indeling:

1. Welke maatregelen treffen instellingen ten aanzien van het vergroten van bewustzijn inzake cyberdreigingen.

---

[4] SURF 'Cyberdreigingsbeeld 2019/2020 onderwijs en onderzoek'.

[5] Kamerbrieven: 'Onderzoek naar cyberaanval Universiteit Maastricht en maatregelen cyberveiligheid' | 03-07-2021, 'Cyberveiligheid in het hoger onderwijs-en onderzoeksveld' | 19-05-2021 en 'Cyberveiligheid in het onderwijs' | 14-02-2020.

2. Welke maatregelen treffen zij om hun risicomanagement te borgen.
3. Welke maatregelen zijn getroffen om de aandacht voor ketensamenwerking te vergroten.

Naar aanleiding van het rapport van de Inspectie voeg ik aan die indeling maatregelen toe om:

4. De sturing van en in het stelsel te verbeteren.
5. Het toezicht te verbeteren.

Vergroten bewustzijn
Vele instellingen investeren al geruime tijd, zoals ook de Inspectie aangeeft, in het verbeteren bij medewerkers en studenten van het bewustzijn van de risico's van cyberdreigingen door het aanbieden van trainingen, campagnes, brochures en grootschalige oefeningen zoals de crisisoefening OZON van SURF. Hierbij is de rol van bestuurders essentieel. Vele besturen agenderen het onderwerp, bespreken het intern en treffen maatregelen om het bewustzijn over cyberrisico's te vergroten. Het is daarbij van belang dat bestuurders hier zowel op centraal (instellings-)niveau als op decentraal niveau (faculteits- of opleidingsniveau) aandacht voor vragen en een open en veilige cultuur bevorderen waarin medewerkers zich vrij voelen om niet alleen incidenten, maar ook (potentiële) risico's proactief te melden, zodat op dreigende risico's adequaat kan worden gereageerd. Het rapport van de Inspectie benoemt vele voorbeelden van maatregelen die verschillende instellingen al genomen hebben en andere kunnen navolgen.

Het is echter essentieel dat in élke instelling en in alle lagen van de instelling maatregelen worden genomen om medewerkers en studenten bewust te maken van cyberdreigingen. Ik wil daarom afspraken maken zodat elke instelling, groot én klein, bekostigd én onbekostigd, dergelijke maatregelen neemt. Samen met de koepels, waaronder uitdrukkelijk ook de NRTO, wil ik dit najaar afspraken maken hoe vooral ook kleinere instellingen en de niet bekostigde instellingen geholpen kunnen worden met maatregelen om het bewustzijn in alle lagen van de instelling te vergroten.

Borgen risicomanagement
De instellingen hebben inzake hun risicomanagement, zoals ik in eerdere brieven heb uiteengezet, reeds verschillende maatregelen getroffen. Cruciaal is het opzetten van een gezamenlijk Security Operations Center (SOC) onder SURF. Een belangrijk onderdeel van dit SOC is de 24/7 monitoring van netwerken en signalering van dreigingen om cyberincidenten te voorkomen. Naast het SURFsoc

bestaat het SURFcert.[6] SURFsoc en SURFcert zijn van groot belang om de cyberweerbaarheid te vergroten. Onder regie van SURF worden dreigingsinformatie en mitigerende maatregelen direct gedeeld met andere instellingen, zodat zij preventieve maatregelen kunnen treffen om zichzelf extra te beschermen. Bij de recente hacks is dit ook gebeurd, waarvan andere instellingen hebben kunnen profiteren.

In overleg met de VSNU, de VH, de MBO-raad en SURF wil ik verkennen hoe we alle instellingen kunnen stimuleren en aanmoedigen om deel te nemen aan een SOC oplossing, aangezien vrijwillige deelname van individuele instellingen aan een dergelijke oplossing blinde vlekken mogelijk maakt en de kwetsbaarheid van het stelsel als geheel vergroot. Het is niet reëel, gezien de vereiste investeringen en vereiste capaciteit, ook van SURF, om binnen enkele jaren elke instelling aangesloten te hebben op een SOC oplossing. Ik wil in het eerste kwartaal van 2022 een overzicht van de noodzakelijke (financiële, personele, capacitaire) vereisten en een kalender wanneer welke instelling kan worden aangesloten. Voor het onbekostigd onderwijs bezie ik met de NRTO hoe de niet-bekostigde instellingen aangesloten kunnen worden op informatieverstrekking ten aanzien van dreigingen.

Om risicomanagement goed in te richten, is een adequaat systeem van preventie en respons belangrijk maar niet voldoende. Ook een gedeeld normenkader is noodzakelijk. De hoger onderwijsinstellingen maken bij hun audits gebruik van het SURFaudit Toetsingskader Informatiebeveiliging Hoger Onderwijs, een risico-gebaseerd model waarin wordt gerefereerd aan maatregelen uit de ISO-27002.[7] De mbo-instellingen kennen een vergelijkbare methodiek op basis van het Volwassenheidsmodel informatiebeveiliging van de NBA (de Koninklijke Nederlandse Beroepsorganisatie van Accountants). In navolging van de aanbeveling van de Inspectie zal ik met de koepels tot afspraken komen over dit gedeeld normenkader en over de stappen die gezet moeten worden om elke instelling aan het afgesproken volwassenheidsniveau (normering) te laten voldoen.[8] De instellingen hebben aangegeven dat zij over de verschillende clusters gemiddeld volwassenheidsniveau 3 gerealiseerd willen hebben, waarbij

---

[6] SURFcert- het SURF Computer Emergency Response Team is een schakelorganisatie binnen met het Landelijk Dekkend Stelsel (LDS). Het LDS is een stelsel waarin publieke en private partijen kennis en informatie met elkaar uitwisselen, en waarmee het NCSC dreigingsinformatie kan delen. Aangesloten zijn bijvoorbeeld CERTs, OKTTs (sectorale en regionale samenwerkingsverbanden), sectorale en regionale samenwerkingsverbanden en het Digital Trust Center (DTC).

[7] Normenkader informatiebeveiliging hoger onderwijs kent zes clusters met elk een eigen volwassenheidsniveau. In de laatste SURFaudit van 2019 was de gemiddelde score van alle instellingen op de zes onderdelen 2,3. Het afgesproken ambitieniveau is 3.

[8] Het toetsingskader vult het normenkader aan. Dit beschrijft wat de vereisten zijn om aan een bepaald volwassenheidsniveau te voldoen. Per onderdeel zijn er zijn vijf verschillende volwassenheidsniveaus: 1. Initieel/ ad hoc; 2. Herhaalbaar, maar informeel; 3. Gedocumenteerd, formeel en aantoonbaar; 4. Beheerst en meetbaar; 5. Continue verbetering.

sommige instellingen op basis van hun risicoprofiel ook een hoger volwassenheidsniveau kunnen nastreven. Ook hier wil ik in het eerste kwartaal van 2022 een plan van aanpak met de sector hoe en wanneer elke instelling aan dit volwassenheidsniveau voldoet.

Naast een adequaat systeem van preventie en respons en een duidelijk normenkader zijn er vele technische maatregelen die instellingen kunnen nemen om risico's op cyberaanvallen te verkleinen of de gevolgen te beperken. Sommige instellingen nemen deze maatregelen ook op in hun jaarverslagen. In het Cybersecuritybeeld Nederland (CSBN) wordt aandacht gevraagd voor de basismaatregelen die op orde moeten zijn voor een minimumniveau van digitale veiligheid, maar die nog regelmatig ontbreken, niet alleen in de onderwijssector.[9] Deze basismaatregelen 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.[10] Het gaat hierbij onder andere om het toepassen van multifactor authenticatie, het segmenteren van netwerken, het regelmatig maken van back-ups en testen van systemen, bijvoorbeeld met de inzet van 'ethische hackers' en het bepalen van wie toegang heeft tot data en diensten.

De Inspectie signaleert in het rapport dat, ondanks dat een deel van deze basismaatregelen onderdeel is van het informatiebeveiligingsbeleid van hoger onderwijsinstellingen, een aantal ook niet (volledig) is ingebed in elke organisatie. Dat maakt het stelsel kwetsbaar. Daarom roep ik instellingen op om naast het zorgvuldig inrichten van risicomanagement, deze basisregels, voor zover dit niet het geval is, zoveel mogelijk toe te passen en hierover in hun jaarverslag te rapporteren. In mijn overleggen met de koepels zal ik ook meenemen hoe deze basismaatregelen, door de instellingen zorgvuldig kunnen worden toegepast, met inachtneming van de diversiteit en het verschil in risicoprofiel tussen instellingen.

<u>Aandacht voor ketensamenwerking</u>
Bij een effectieve bestrijding van cyberrisico's is samenwerking en continue kennis-en informatiedeling over risico's nodig. De instellingen maken hier al veel werk van. Zo hebben de Hogeschool van Amsterdam en de Universiteit van Amsterdam begin juli jl. een leerevaluatie cyberaanval uitgebracht, getiteld 'Aanval afgeslagen'.[11]

---

[9] Cyber Security Beeld Nederland 2021 | 28-06-2021.

[10] NCSC (2021) 'Handreiking cybersecuritymaatregelen. Stap voor stap naar een digitaal veilige organisatie'. Den Haag: Nationaal Cyber Security Centrum. Ministerie van Justitie en Veiligheid.

[11] L*eerevaluatie cyberaanval* HvA en UvA *'Aanval afgeslagen'* door het COT- Instituut voor Veiligheids- en Crisismanagement | 06-07-2021.

Ook in internationaal verband is kennis- en informatiedeling relevant. In Europees verband speelt bijvoorbeeld de herziening van de NIS-2-richtlijn.[12] Deze Europese richtlijn kan, afhankelijk van nadere Europese besluitvorming, ook voor de hoger onderwijssector voorschriften gaan bevatten. In samenspraak met de sector en waar nodig in samenwerking met andere beleidsdepartementen en toezichthouders, zal ik zorgdragen dat de sector voorbereid is op dergelijke internationale ontwikkelingen en aangehaakt op relevante kennis-en informatiedeling. Dit geldt ook voor de informatievoorziening uit de EU en (ten aanzien van dreigingen) vanuit het NCSC, de AIVD en de MIVD zodat instellingen over alle relevante informatie en expertise beschikken om een goed totaalbeeld van de risico's te krijgen.

Sturing van en in het stelsel
De hoger onderwijssector kenmerkt zich door institutionele autonomie. Dit betekent dat de sector een grote mate van vrijheid heeft om zelf een visie op veiligheid en deelaspecten van veiligheid op te stellen, veiligheidsrisico's te monitoren, een normenkader vast te stellen en instrumenten te ontwikkelen. Die autonomie is een groot goed en de verantwoordelijkheid voor de aanpak van cybersecurity moet ook primair, zoals ook de Inspectie aangeeft, bij de instellingen blijven liggen. De overheid heeft een belangrijke faciliterende en aanjagende verantwoordelijkheid. Daartoe behoort ook een financiële verantwoordelijkheid. De Inspectie signaleert dat cybersecurity door instellingen als essentieel wordt gezien, maar dat er ook discussie wordt gevoerd over noodzaak en kosten. Op basis van een risico-inventarisatie bepalen instellingen of er voldoende middelen beschikbaar zijn. Instellingen geven aan dat dit tot nu toe wel het geval is, maar onderstrepen ook dat met name de stap naar meer zekerheid en weerbaarheid een stevige extra investering vraagt.
Substantiële investeringen, zoals ook de Cyber Security Raad heeft gevraagd in zijn recente advies aan het kabinet, zijn echter aan een volgend kabinet.[13]
Gezien het belang van cyberveiligheid wil ik twee maal per jaar met de koepels bestuurlijk overleg voeren om de stand van zaken rondom cyberveiligheid op te maken en voortgang van maatregelen te evalueren. De benodigde investeringen in informatiebeveiliging zullen daarvan ook onderdeel uitmaken.

Toezicht op cyberveiligheid
Audits zijn een belangrijke informatiebron om de aanpak van cyberveiligheid te monitoren, zowel op het niveau van de instelling als voor het stelsel als geheel. Zowel interne als externe audits worden door instellingen gebruikt om meer inzicht te krijgen in de eigen informatiebeveiliging en privacy-maatregelen.
Zo doen alle hoger onderwijsinstellingen mee aan de tweejaarlijkse SURFaudit benchmark. Dit is een assessment dat inzicht geeft in de mate waarin instellingen de informatiebeveiliging onder controle hebben en waar verbetering nodig is. Het sectorbeeld dat zo tot stand komt, wordt gepubliceerd in een benchmark. Het

[12] Netwerk-en informatie systemen. Deze richtlijn bevat voorschriften voor de vitale infrastructuur met betrekking tot cybersecurity eisen.

[13] CSR advies 'Nederlandse Digitale Autonomie en Cyber Security' | 14-05-2021

MBO kent een soortgelijke benchmark, de benchmark IBP-E.[14] Een vast onderdeel in deze benchmark is peer review waarbij de mbo-instellingen elkaar beoordelen of externe partijen hiervoor inschakelen.

Alle universiteiten hebben afgelopen jaar ook een externe audit laten uitvoeren op de informatiebeveiliging en hebben afgesproken dit tweejaarlijks te herhalen.

Ik vind het van belang dat alle instellingen in het hoger en middelbaar beroepsonderwijs, naast het gebruik van eigen, interne audits en zelf-assessments, zich laten toetsen door middel van externe audits. Het belang van cyberveiligheid op het ongestoord verloop van het onderwijs en onderzoek rechtvaardigt dat. Ik maak daarom dit najaar met de koepels afspraken hoe we audits en monitoring vorm gaan geven en hoe we kunnen verzekeren dat elke instelling periodiek extern geaudit wordt.

Voor toezichthouders is niet precies duidelijk welke verantwoordelijkheid ze op het gebied van cyberveiligheid hebben, geeft de Inspectie aan. Met de Inspectie bekijk ik welke maatregelen nodig zijn om hier duidelijkheid te verschaffen, ook in relatie tot bovengeschetste Europese ontwikkelingen.

NWO en KNAW
Het rapport van de Inspectie heeft onderzoek gedaan naar de digitale weerbaarheid in het hoger onderwijs. De inspectie benadrukt in haar rapport, en ik onderschrijf dat van harte, het belang van samenwerking in de hele keten. Voor het hoger onderwijs zijn de instituten van NWO en de KNAW een belangrijke partner. Daarom vind ik het belangrijk om, ondanks het feit dat zij buiten de scope van dit onderzoek vallen, ook met NWO en de KNAW in gesprek te gaan. Zo kunnen we nader bepalen wat de aanbevelingen uit het Inspectierapport voor hen kunnen betekenen en hoe ik deze onderzoeksinstituten verder kan ondersteunen in hun cyberveiligheid. Waar nodig en opportuun kunnen de acties die hieruit voortkomen gelijktijdig worden opgepakt met de acties in het hoger onderwijs. Eerder heb ik u in de Kamerbrief van 19 mei jl. geïnformeerd over de inspanningen van deze organisaties op het gebied van cyberveiligheid. Naast de individuele audits en maatregelen zijn zowel de NWO als de KNAW goed aangesloten bij SURFcert. Ook zullen zij zich aansluiten bij SURFsoc.

Middelbaar beroepsonderwijs
Zoals eerder in deze brief beschreven, gelden veel van de maatregelen zowel voor het hoger als middelbaar beroepsonderwijs. Zo wordt er in het MBO al veel samengewerkt onder de coördinatie van saMBO-ICT. Ook worden voorbereidingen getroffen om instellingen te laten aansluiten op SURFsoc of een andere SOC oplossing. Ik heb u hierover in de beantwoording van de vragen naar aanleiding van de hack bij ROC Mondriaan eerder bericht[15]. Verbetering is evenwel nodig. Dit

[14] https://www.sambo-ict.nl/netwerken/informatiebeveiliging/framework-ibp/

[15] Zie ook kamerstukken met kenmerk 2021D34616 en 2021D34263.

blijkt al uit de constatering dat de helft van de instellingen in het MBO het ambitieniveau nog niet heeft gehaald. Zoals ik hierboven aangaf, is de rol van de bestuurders en de aandacht die dit onderwerp krijgt binnen de instelling van groot belang. Ik ben daarom, net als in het hoger onderwijs, ook met de koepels in het MBO in gesprek over hoe we de digitale weerbaarheid in deze onderwijssector kunnen vergroten. Ik trek daarbij zoveel mogelijk gezamenlijk op met het hoger onderwijs.

Tot slot

Het onderwijs is door zijn open karakter kwetsbaar. Tegelijkertijd is openheid een kernwaarde van hoogwaardig onderwijs. Een open leer-en werkomgeving is een voorwaarde voor goed onderwijs, excellent onderzoek en kennisdeling. De voordelen van digitalisering, die door de coronacrisis in een versnelling is geraakt, (internationale) samenwerking en open science zijn evident. Het is belangrijk om deze kernwaarde niet uit het oog te verliezen. Evenzeer is het van belang te blijven realiseren dat 100% veiligheid onmogelijk is.

Het verhogen van de digitale weerbaarheid van de onderwijssector is niettemin noodzakelijk en gebaat bij een integrale aanpak van veiligheid waarin een afweging wordt gemaakt tussen kernwaarden, bedreigingen en de te beschermen belangen. Daarbij moeten ook kosten en baten van veiligheidsmaatregelen tegen elkaar worden afgewogen. Ook moet het duidelijk zijn welke verantwoordelijkheden individuele instellingen zelf kunnen invullen, waar ze in gezamenlijkheid kunnen optreden om de kennis en expertise van alle ketenpartners optimaal te benutten en waar aanvullende coördinatie of ondersteuning vanuit de overheid nodig is. Met de hier voorgenomen maatregelen onderstrepen de sector en ik de urgentie en het gezamenlijk streven om de digitale weerbaarheid van de sector te verhogen.

De minister van Onderwijs, Cultuur en Wetenschap,

Ingrid van Engelshoven