Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

31 288 Hoger Onderwijs-, Onderzoek- en Wetenschapsbeleid

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1189

BRIEF VAN DE MINISTER VAN ONDERWIJS, CULTUUR EN WETENSCHAP

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 24 april 2025

De digitale dreiging is groot en divers, en neemt toe. Dit geldt voor de hele samenleving, waaronder ook in het onderwijs. We zien steeds meer dat digitale risico's complex en onderling met elkaar verbonden zijn. Onderwijs- en onderzoeksinstellingen (hierna: instellingen) zijn dan ook niet alleen op zichzelf doelwit van cyberaanvallen, maar kunnen tevens een tussenstap zijn naar cyberaanvallen in het bredere digitale ecosysteem.

Dat ook het onderwijs doelwit is bleek eens te meer toen in januari van dit jaar de TU Eindhoven te maken kreeg met een cyberaanval en in de daaropvolgende dagen tevens het netwerk van SURF doelwit werd van DDoS-aanvallen. Door effectief ingrijpen bleven de gevolgen van deze aanvallen gelukkig beperkt.[1] Dit verdient waardering. Het effectief optreden laat zien dat instellingen zich bewust zijn van de cyberdreiging en zich inspannen voor het versterken van de cyberweerbaarheid. Hieraan is in de afgelopen jaren hard gewerkt langs de lijnen van de bestuurlijke afspraken met mijn ministerie.

Tegelijkertijd zie ik dat de cyberdreiging, ook in de richting van het onderwijs, permanent is en blijvend in beweging. Het is essentieel dat de instellingen nu en in de toekomst goed voorbereid zijn op de risico's die de cyberdreiging met zich meebrengt en dat zij hier, als onderdeel van het bredere digitale ecosysteem, blijvend op inzetten. Ik heb daarom besloten om gebruik te maken van mijn bevoegdheid om het hbo en wo onder de komende Cyberbeveiligingswet (hierna: Cbw) te brengen. Hiermee zorg ik dat de cyberweerbaarheid in het hbo en wo wettelijk wordt verankerd en de digitale risico's duurzaam worden beheerst. In deze brief licht ik dit besluit nader toe.

[1] Kamerstuk 31 288, nr. 1176

kst-31288-1189
ISSN 0921 - 7371
's-Gravenhage 2025

Ik schets in deze brief het dreigingsbeeld voor het onderwijs. Vervolgens ga ik in op de voortgang die de afgelopen jaren is geboekt om de cyberweerbaarheid in het vervolgonderwijs te verhogen. Ik licht toe hoe de in 2021 aangekondigde en in 2022 gemaakte bestuurlijke afspraken door de instellingen met overtuiging zijn opgepakt. Vervolgens licht ik mijn keuze toe om het hbo en wo onder de reikwijdte van de Cbw te brengen, inclusief de daarbij behorende tijdpaden en de overwegingen die hieraan ten grondslag liggen. Tot slot benoem ik welke stappen er gezet worden in de sectoren die niet door mij onder de Cbw gebracht worden, namelijk het mbo, het niet-bekostigd onderwijs en enkele onderzoeksinstellingen.

Dreigingsbeeld

Eind oktober vorig jaar berichtte de NCTV in het Cybersecuritybeeld Nederland 2024 dat de digitale dreiging voor Nederland onverminderd groot en voortdurend aan verandering onderhevig is.[2] In dit rapport is nadrukkelijk gewezen op de turbulente geopolitieke tijden waarin statelijke actoren hun cyberactiviteiten intensiveren, hun capaciteit verbreden en een bredere gereedschapskist inzetten om hun belangen te behartigen. Daarnaast is Nederland met haar hoogwaardige kenniseconomie en als voorloper op het gebied van bepaalde technologieën, een aantrekkelijk doelwit voor kwaadwillenden. Zij kunnen kennis daarover (proberen te) ontvreemden. Verder maakt het bredere digitale ecosysteem waarin organisaties zich bevinden het complexer om mogelijke risico's in kaart te brengen. Alle digitale processen, sectoren en organisaties zijn potentieel interessant voor actoren. Organisaties die op het eerste gezicht geen doelwit lijken, kunnen namelijk ook als opstap naar andere, mogelijk interessantere, doelwitten fungeren. Het kabinet zet daarom als onderdeel van het regeerprogramma en de Nederlandse Cybersecuritystrategie breed in op het verhogen van de cyberweerbaarheid in heel Nederland. Onderdeel hiervan is de inwerkingtreding van de Cbw.

Waar de NCTV een Cybersecuritybeeld van Nederland opstelt, stelt SURF het cyberdreigingsbeeld onderwijs en onderzoek op.[3] In dit dreigingsbeeld spreekt SURF van een wapenwedloop tussen cybercriminelen en verdedigingsmaatregelen die naar verwachting zal versnellen maar in essentie niet zal veranderen. Een nog alertere en flexibelere aanpak van cybersecurity is noodzakelijk. Het is daarom van belang dat onderwijsinstellingen blijven samenwerken en zich doorlopend blijven inzetten op het versterken van de cyberweerbaarheid van hun organisaties.

1. Voortgang huidige maatregelen

Met de bestuurlijke afspraken uit 2021 hebben de onderwijsinstellingen in het vervolgonderwijs de digitale weerbaarheid verhoogd.[4] Hierin zijn concrete maatregelen vastgelegd voor versterking van de cyberweerbaarheid.[5] Aan de hand van deze bestuurlijke afspraken en aanvullende investeringen[6], zetten de instellingen sinds 2021 langs drie lijnen in op maatregelen: (1) vergroten van het bewustzijn over risico's, (2) vergroting van de gehele systeemvolwassenheid door toepassing van een gedeeld

---

[2] Cyberdreigingsbeeld Nederland 2024: turbulente tijden, onvoorziene effecten
[3] Cyberdreigingsbeeld 2014–2024 Onderwijs en onderzoek
[4] Kamerstuk 31 288, nr. 922
[5] Deze maatregelen zijn uiteengezet in de Kamerbrief «Verhogen digitale veiligheid onderwijs en onderzoek» l14 juli 2022 (Kamerstukken 35 925 VIII en 26 643 en 32 761, nr. 190)
[6] Hierbij gaat het om in totaal € 25 miljoen euro in het mbo tot in 2027. Voor hbo en wo gaat het om € 19 miljoen in 2023 aflopend naar € 8 miljoen structureel vanaf 2027.

toetsingskader[7] en een meer risicogebaseerde werkwijze en (3) versterking van de ketensamenwerking.[8]

De sectorbeelden die het vervolgonderwijs jaarlijks opstelt laten over de hele linie zien dat er aantoonbare stappen voorwaarts zijn gezet. Hieronder licht ik dit kort toe en noem ik een aantal voorbeelden van concrete maatregelen.

Vergroten bewustwording en bestuurlijke commitment

Als onderdeel van de maatregelen omtrent cyberveiligheid die in 2021 met de bekostigde instellingen zijn afgesproken wordt vol ingezet en samengewerkt op het vergroten van het bewustzijn, kennis en kunde bij zowel studenten en medewerkers als bij bestuurders en toezichthouders. Niet alleen binnen de instellingen maar ook in SURF-verband wordt gewerkt aan verhoging van de bewustwording, kennisdeling en het effectief van elkaar leren. Dit wordt bijvoorbeeld gedaan door gezamenlijke ontwikkeling van instrumenten, diensten en activiteiten zoals de crisisoefening OZON van SURF[9] met instellingen uit het mbo, hbo en wo.[10]

Systeemvolwassenheid

Het is van belang dat instellingen voorbereid zijn op risico's en dreigingen, deze detecteren en adequaat kunnen reageren als incidenten zich voordoen. Alle onderwijsinstellingen hanteren inmiddels hetzelfde toetsingskader van SURF voor de monitoring van de stand van de informatiebeveiliging en streven naar een vastgesteld volwassenheidsniveau van 3 volgens het NBA Volwassenheidsmodel. Doordat de startsituatie voor de deelsectoren en instellingen verschillend is, blijven er tempo- en niveauverschillen bestaan. De ontwikkeling wordt door alle instellingen periodiek extern gemonitord op basis van de SURFaudit benchmark. Deze harmonisatie in de werkwijze vergroot het lerend vermogen van de sector. Ook is afgesproken dat alle instellingen beschikken over een passende Security Operations Center (SOC)-oplossing voor monitoring en passende opvolging. Inmiddels zijn alle universiteiten, bijna alle hbo-instellingen en een groot deel van de mbo-instellingen op een SOC-oplossing aangesloten.

Verantwoording en versterking ketensamenwerking

Om de stand van zaken rondom cyberveiligheid op te maken en de voortgang van de maatregelen te evalueren is verantwoording naar elkaar en naar de samenleving van belang. Vanaf 2024 is een rapportage over genomen maatregelen ten aanzien van digitale veiligheid een vast onderdeel van de jaarverslagen. De handreiking «verantwoording cybersecurity in jaarverslagen» die onderwijskoepels in samenwerking met SURF hebben opgesteld biedt handvatten bij de verslaglegging van de verantwoording omtrent cybersecurity in de risicoparagraaf in de jaarverslagen.[11]

---

[7] Hiervoor wordt het SURFaudit Toetsingskader Informatiebeveiliging gebruikt, gebaseerd op de internationale ISO-standaard 27001 en het Volwassenheidsmodel Informatiebeveiliging van de Nederlandse Beroepsorganisatie van Accountants (NBA).

[8] Kamerstuk 31 288, nr. 922

[9] https://www.surf.nl/diensten/ozon-en-nozon

[10] https://www.surf.nl/themas/cybersecurity

[11] https://sec.surf.nl/asset/handreiking-verantwoording-cybersecurity-in-jaarverslagen/

Op instellingsniveau voeren alle instellingen onafhankelijke externe audits uit. De governance binnen instellingen is geregeld via periodieke interne verantwoording met een portefeuillehouder informatiebeveiliging in het college van bestuur en het faculteitsbestuur. Op sectorniveau bespreken instellingen onderling hun auditresultaten, spreken zij elkaar aan op en helpen elkaar bij achterliggende progressie, gebruik makend van de ondersteuningsstructuur van SURF. Ten behoeve van de bestuurlijke afspraken voert mijn ministerie tweemaal per jaar een bestuurlijk overleg met Universiteiten van Nederland (UNL), de Vereniging van Hogescholen (VH), de MBO-raad en SURF. Hierbij wordt het sectorbeeld van het voorgaande jaar gepresenteerd en de sectorale voortgang van de maatregelen geëvalueerd.

Ook de Nederlandse organisatie voor Wetenschappelijk Onderzoek (NWO), de Koninklijke Nederlandse Akademie van Wetenschappen (KNAW) en de Nederlandse Raad voor Training en Opleiding (NRTO) zijn betrokken bij deze bestuurlijke overleggen en werken verder aan het verhogen van hun cyberveiligheid, en de kennisuitwisseling met de onderwijskoepelorganisaties. Voor het niet-bekostigd onderwijs investeert de NRTO, de brancheorganisatie waarvan een groot deel van de niet-bekostigde instellingen lid is, in maatregelen om de digitale weerbaarheid van de niet-bekostigde instellingen te verhogen. Dit doen zij door onder andere het creëren van bewustzijn en het faciliteren van trainingen voor hun leden. Daarnaast wordt de aanwezigheid van cyberveiligheidsprocessen onderdeel van het NRTO-keurmerk dat nodig is om lid te worden en te blijven van de NRTO.

Samenwerking en kennisdeling binnen de onderwijssector blijft van groot belang. Er wordt in de gehele keten, inclusief bijvoorbeeld software- en examenleveranciers, intensief samengewerkt. Zo zijn er binnen de sectoren en in SURF-verband samenwerkingsovereenkomsten afgesloten en zijn er verschillende samenwerkingsverbanden waarin kennis en best practices met elkaar worden gedeeld. De kennisdeling via het SURF Security Expertise Centrum (SEC) is hier een mooi voorbeeld van.[12]

2. Aanwijzing instellingen in het hbo en wo onder de cyberbeveiligingswet

Een belangrijk element van de kabinetsinzet om de cyberweerbaarheid in Nederland te vergroten is de Nederlandse Cybersecuritystrategie en de implementatie van de EU-Richtlijn NIS2 in de Cyberbeveiligingswet (Cbw), die de Minister van Justitie en Veiligheid coördineert. Het voorstel voor de Cbw wordt op korte termijn bij uw Kamer ingediend. In de concepttekst van dit wetsvoorstel is, in lijn met de NIS2-richtlijn[13], de mogelijkheid opgenomen voor de Minister van Onderwijs, Cultuur en Wetenschap om na overleg met de Minister van Justitie en Veiligheid hbo- en wo-instellingen als essentiële of belangrijke entiteit als bedoeld in de Cbw aan te wijzen en daarmee onder de reikwijdte van de Cbw te brengen.[14] Zoals ik in het begin van deze brief aangeef, zal ik hiertoe overgaan en de hbo- en wo-instellingen onder de toepasselijkheid van deze wet brengen. Ik licht dit besluit hieronder nader toe.

---

[12] https://sec.surf.nl/

[13] De NIS2-richtlijn geeft lidstaten de mogelijkheid om te bepalen dat deze richtlijn van toepassing is op «onderwijsinstellingen, met name wanneer zij kritieke onderzoeksactiviteiten verrichten».

[14] Het besluit om het hoger onderwijs als essentiële of belangrijke entiteit als bedoeld in de Cbw aan te wijzen is nog niet genomen en volgt tijdens de nadere uitwerking.

De toenemende digitale dreiging die ook het onderwijs raakt, zoals toegelicht aan de hand van het dreigingsbeeld, blijft onverminderd zorgelijk. Het maakt de noodzaak voor een gezamenlijke en duurzame aanpak des te dringender. Gezien deze ontwikkelingen, de bestuurlijke afspraken cyberweerbaarheid en het staande beleid ten aanzien van kennisveiligheid bij hbo- en wo-instellingen, heb ik in de afgelopen periode intensief overleg gevoerd met alle betrokken stakeholders over de toenemende digitale dreiging en een effectieve aanpak voor de verdere versterking van de cyberweerbaarheid. Met VH, UNL, MBO-raad, SURF en JenV heb ik veelvuldig gesproken over de impact van het onder de Cbw brengen voor de sectoren en hoe die zich verhoudt tot het staande beleid om via bestuurlijke afspraken te werken aan versterking van de cyberweerbaarheid. Hierbij is ook gesproken over de door de instellingen geschetste uitvoeringslast volgend uit de Cbw. Zij geven aan zorgen te hebben over negatieve gevolgen die een aanwijzing als bedoeld in de Cbw volgens hen gaat hebben voor de cyberweerbaarheid gezien dit tijd en inzet vraagt van instellingen om zich hierop voor te bereiden. Deze overleggen stonden nadrukkelijk in het teken van het vormen van een zo compleet mogelijk beeld om alle aspecten zo goed mogelijk in kaart te hebben ten behoeve van de besluitvorming.

Uit deze gesprekken volgt voor mij het beeld dat de inhoudelijke normen in de Cbw, voor een groot deel aansluiten bij de wijze waarop het vervolgonderwijs langs bestuurlijke afspraken werkt aan het verhogen van de cyberweerbaarheid. Zij zien hier zelf met intern toezicht en onafhankelijke audits op toe. Dit vind ik een belangrijk gegeven omdat de instellingen daarmee de stevig opgebouwde basis van de afgelopen jaren en de inhoudelijke stappen die zij reeds zetten met onder meer een goede inrichting van risicomanagement verder kunnen vervolgen. Tegelijkertijd zijn er ook verschillen, bijvoorbeeld als het gaat om aanvullende monitoring en evaluatie op de genomen maatregelen, de bestuurlijke aansprakelijkheid en het externe onafhankelijke toezicht. Ook deze zaken zijn van invloed op de instellingen en dit kan per instelling sterk verschillen.

Dit alles overwegende – de impact van de Cbw maar ook het belang van een brede en duurzame beheersing van cyberrisico's gezien de toenemende digitale dreiging – heb ik, na overleg met de Minister van Justitie en Veiligheid, besloten om de bekostigde hbo- en wo-instellingen onder de Cbw te brengen. Hiermee komt er een wettelijke plicht om passende en evenredige maatregelen te treffen om de risico's voor de beveiliging van de netwerk- en informatiesystemen te beheersen (zorgplicht)[15], een meldplicht van significante incidenten, recht op bijstand en advies van een Computer Incident Response Team (CSIRT) bij dreigingen en incidenten, een registratieplicht, en onafhankelijk extern toezicht op de naleving van genoemde plichten.

Hoewel de hbo- en wo-instellingen zich al jarenlang fors inspannen voor het versterken van de cyberweerbaarheid, ben ik me terdege bewust van het feit dat het onder de Cbw brengen van deze instellingen nieuwe verplichtingen met zich meebrengt. Ik vind het dan ook essentieel dat de instellingen voldoende tijd krijgen om zich voor te bereiden op de toepasselijkheid van de Cbw. Om die reden wil ik de plichten die uit de Cbw volgen, met inbegrip van het toezicht op de naleving daarvan, alsook het recht op bijstand door een CSIRT, gefaseerd in laten gaan. De meldplicht en registratieplicht, inclusief het toezicht daarop, en het wettelijke recht op bijstand door een CSIRT wil ik gelijk laten ingaan met

[15] Organisaties worden in het kader van bovenbedoelde zorgplicht o.a. verplicht beleid te hebben met betrekking tot het uitvoeren van risicoanalyses.

de inwerkingtreding van de Cbw.[16] De zorgplicht en het daarbij behorende toezicht wil ik later laten ingaan. Deze fasering heeft twee redenen welke ik hieronder nader toelicht.

In samenspraak met de Minister van Justitie en Veiligheid heb ik geconcludeerd dat het van belang is dat de meldplicht, de registratieplicht, het toezicht op de naleving van die plichten én het recht op bijstand door een CSIRT zo snel als mogelijk ingaan. Dit biedt onder meer een wettelijke basis voor informatiedeling met alle relevante partijen in geval van dreigingen en incidenten. Dit geldt zowel voor informatieverstrekking aan en door onderwijsinstellingen via het CSIRT, als het onderling delen van relevante informatie tussen CSIRT's. Nu geldt reeds dat SURFcert bij significante incidenten in contact staat met andere relevante actoren (waaronder andere CSIRT's). Ik ga met SURF in gesprek over wat nodig is om de wettelijke taak als CSIRT onder de Cbw op een goede wijze te kunnen uitvoeren.

De tweede reden voor de gefaseerde invoering is dat de hbo- en wo-instellingen, in tegenstelling tot de entiteiten die rechtstreeks onder de wet gaan vallen, minder tijd hebben gehad om zich voor te bereiden en te voldoen aan de eisen in het kader van de zorgplicht in de wet. Bovendien hebben de instellingen mij nadrukkelijk hun zorg meegegeven dat de wet nieuwe verplichtingen met zich meebrengt waarop zij nog niet zijn ingericht. Ik neem deze zorgen serieus. Door de zorgplicht en het toezicht daarop later in te laten gaan wil ik de instellingen nadrukkelijk de tijd geven om zich zorgvuldig voor te kunnen bereiden en toe te werken naar het voldoen aan de eisen die in het kader van de wettelijke zorgplicht aan de instellingen worden gesteld. Ik hecht zeer aan het inbouwen van voldoende tijd vanuit het oogpunt van uitvoerbaarheid.

Ik ben met de instellingen in gesprek over wat de aanwijzing als bedoeld in de Cbw betekent voor de huidige bestuurlijke afspraken met de mbo-, hbo- en wo-instellingen. Via deze bestuurlijke afspraken is er inmiddels een zeer belangrijke basis gelegd door alle sectoren en ik ben ervan overtuigd dat het hbo en wo hier bij het gaan voldoen aan de wetgeving profijt van zullen ondervinden. Ik wil deze bestuurlijke afspraken in samenspraak met de sectoren, inclusief het mbo, hernieuwen zowel qua ambitie, inhoud als tijdspad zodat deze aansluiten onder meer de zorgplicht die volgt uit de Cbw en zodat op een realistische en uitvoerbare wijze kan worden toegewerkt naar de toepasselijkheid van de Cbw. Voor het mbo geldt dat deze sector niet zal worden aangewezen onder de Cbw. Wel vind ik het belang dat ook het mbo blijft werken aan het verhogen van de cyberweerbaarheid en dat dit waar mogelijk in samenwerking kan binnen SURF-verband en met het hbo en wo. Daarom wil ik ook het mbo betrekken bij dit gesprek over vervolging van de bestuurlijke afspraken. Verderop in de brief ga ik nader in op het mbo.

De komende periode werk ik dit en het besluit om de hogescholen en universiteiten als essentiële of belangrijke entiteiten als bedoeld in de Cbw aan te wijzen nader uit. Dit doe ik onder andere met de beoogde toezichthouder (Inspectie voor het Onderwijs) en het beoogde CSIRT (SURFcert), de Minister van JenV en uiteraard de universiteiten en hogescholen. Hierbij zal ik ook kijken naar welke financiële implicaties er zijn verbonden aan de uitvoering van de Cbw. Hier moet immers bij inwerkingtreding van de wet duidelijkheid over zijn. Over de voortzetting van de bestuurlijke afspraken en de precieze uitwerking van de aanwijzing ben ik voornemens uw Kamer later dit jaar te informeren.

---

[16] Het kabinet streeft naar inwerkingtreding van de Cbw in Q3 2025.

3. Verhogen cyberweerbaarheid mbo

Ondanks het feit dat er vanuit het kennisveiligheidsbeleid geen aanleiding is om mbo-instellingen onder de Cbw te brengen is een verdere versterking van de cyberweerbaarheid voor het mbo nodig.

De mbo-instellingen hebben de afgelopen jaren ambitieus ingezet op het verhogen van de cyberweerbaarheid. De urgentie heeft zich vertaald in een gezamenlijke en breed gedragen aanpak waar we de komende jaren op voort kunnen bouwen. Binnen het programma Cyberveiligheid mbo realiseren de mbo-instellingen tot en met 2027 gezamenlijke initiatieven.[17] Bijvoorbeeld door het opzetten van een cyberrisicopool, de aandacht voor cyberethiek binnen de opleidingen of het werken met een «CISO as a service» dat als voorbeeld dient voor andere sectoren.[18] Dat geeft vertrouwen in de toekomst.

Tegelijkertijd betekent het door aanwijzing onder de Cbw brengen van de universiteiten en hogescholen dat de brede samenwerking binnen het gehele vervolgonderwijs in SURF-verband potentieel anders vormgegeven moet gaan worden. Bij de positionering van SURFcert als wettelijk aangewezen CSIRT voor de hogescholen en universiteiten heb ik oog voor de huidige dienstverlening van SURFcert aan mbo-instellingen.

Ik vind het van belang dat de mbo-instellingen zich met dezelfde energie van de afgelopen jaren blijven inzetten om de cyberweerbaarheid te verhogen. Toegankelijk onderwijs voor de hele beroepskolom blijft hierbij de inzet. In de gesprekken met de onderwijskoepels blijf ik daarom oog houden voor een versterking van de onderlinge samenwerking, gericht op het verhogen van de cyberweerbaarheid van het gehele vervolgonderwijs.

4. Tot slot

Het vergroten van de cyberweerbaarheid is een doorlopend proces en het blijft onverminderd van belang dat met de sectoren verder wordt gebouwd aan een veilige digitale omgeving. Dit met als doel om de continuïteit, de toegankelijkheid en kwaliteit van onderwijs en onderzoek te borgen. Door de ingezette koers en de huidige inspanningen en investeringen van de instellingen afzonderlijk én gezamenlijk, zijn aantoonbare vorderingen geboekt op de maatregelen die in 2021 zijn afgesproken. Ik ga er vanuit dat de instellingen ook de komende jaren met elkaar de noodzakelijke stappen zullen blijven zetten, zowel de instellingen die aan de Cbw moeten voldoen als de overige instellingen. Ik blijf dit nauwlettend volgen en hierover met de sectoren in gesprek. Later dit jaar informeer ik uw Kamer over de nadere uitwerking van de aanwijzing van het hbo en wo als essentiële of belangrijke entiteiten als bedoeld in de Cbw en het vervolg van de bestuurlijke afspraken met het mbo, hbo en wo. Ook blijf ik uw Kamer bij relevante ontwikkelingen informeren.

De Minister van Onderwijs, Cultuur en Wetenschap,
E.E.W. Bruins

[17] https://mbodigitaal.nl/programmas/programma-cyberveiligheid-mbo/
[18] https://mbodigitaal.nl/2025/01/cyberrisicopool-cooperatie-maakt-compensatie-schade-mogelijk/