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

Ministerie van Onderwijs, Cultuur en Wetenschap

>Retouradres Postbus 16375 2500 BJ Den Haag

Datum 24 juni 2026

Betreft Voortgang aanpak cyberweerbaarheid in het vervolgonderwijs

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

Contactpersoon

Onze referentie
63949335

Bijlagen

In deze brief informeer ik uw Kamer over de voortgang van de aanpak voor verhoging van de cyberweerbaarheid in het vervolgonderwijs. Het digitale dreigingslandschap wordt steeds diverser en onvoorspelbaarder. Technologische ontwikkelingen, zoals die van generatieve Artificial Intelligence (AI), gaan razendsnel en er is een grote verscheidenheid aan aanvallen door statelijke actoren, cybercriminelen en andere kwaadwillenden.[1] Ook onderwijsinstellingen zijn doelwit van deze cyberaanvallen, of vormen een tussenstap naar aanvallen in het bredere digitale ecosysteem.[2] Het is daarom van belang voor Nederland en voor de sectoren dat de instellingen in het vervolgonderwijs goed voorbereid zijn op deze cyberdreiging. Dit is niet alleen nodig om

[1] NCTV | Cybersecuritybeeld Nederland 2025
[2] Dreigingsbeeld Nederland 2024: turbulente tijden, onvoorziene effecten (NCSC

ongewenste overdracht van kennis en technologie tegen te gaan (kennisveiligheid) maar ook vanwege de bescherming van (privacygevoelige) gegevens waar deze voor de instellingen, hun studenten en medewerkers cruciaal zijn voor het primaire proces van onderwijs en onderzoek.

De mbo-instellingen, hogescholen en universiteiten werken al langere tijd aan de verhoging van hun cyberweerbaarheid.[3] Daarbij zetten zij goede stappen om cyberaanvallen zoveel mogelijk voor te zijn en om adequaat te reageren als een aanval niet kan worden voorkomen. Dit is geen eenvoudige opgave. Cyberincidenten zijn nu eenmaal onvermijdelijk, ook in het onderwijs, waardoor digitale veiligheid doorlopende aandacht vraagt. Bovendien zijn digitale risico's complex en met elkaar verbonden. Dit laat bijvoorbeeld ook de recente cyberaanval op Instructure, de leverancier van onderwijsplatform Canvas, zien.[4]

Via deze brief informeer ik uw Kamer specifiek over de nadere uitwerking van de aanwijzing van de bekostigde hogescholen en universiteiten als entiteiten zoals bedoeld in de Cyberbeveiligingswet (hierna: Cbw). Uw Kamer is op 24 april 2025 geïnformeerd over het besluit om de bekostigde hogescholen en universiteiten onder de reikwijdte van deze wet te brengen, vanwege het belang van een brede en duurzame beheersing van cyberrisico's.[5] Daarmee komt er voor deze instellingen een registratieplicht, een meldplicht van significante incidenten en het recht op bijstand en advies door een Computer Security Incident Response Team (CSIRT) bij dreigingen en incidenten en komt er op termijn een wettelijke zorgplicht voor het nemen van passende en evenredige beveiligingsmaatregelen.[6] Ik zet dit beleid voort en tref hiervoor momenteel de voorbereidingen. Ook informeer ik uw Kamer via deze brief over de stappen die worden gezet in het mbo en de afspraken die ik maak met het mbo.

1. Uitwerking aanwijzing hogescholen en universiteiten als entiteiten zoals bedoeld in de Cyberbeveiligingswet (Cbw)

Cyberbeveiligingsregeling hoger onderwijs
Om de bekostigde hogescholen en universiteiten onder de reikwijdte van de Cbw te brengen werk ik momenteel aan een sectorspecifieke ministeriële regeling waarin de aanwijzing van deze instellingen als zogenoemde *belangrijke* entiteiten zal zijn opgenomen. Deze Cyberbeveiligingsregeling hoger onderwijs bevat daarnaast een aantal andere onderdelen, namelijk de vaststelling van de drempelwaarden voor de meldplicht van significante incidenten en de aanwijzing van het CSIRT voor deze instellingen. Ook wordt via deze regeling het extern toezicht op de verplichtingen in de Cbw en de daaronder vallende regelgeving belegd bij de Inspectie van het Onderwijs.[7]

[3] Kamerstukken VIII, 2021/22, 35925, nr. 190
[4] Zie ook de beantwoording van de vragen van de leden El Boujdaini en Rooderkerk over het bericht 'Studenten gewaarschuwd voor phishing na hack softwarebedrijf' (2026Z09749), die gelijktijdig met onderhavige brief aan uw Kamer is verzonden.
[5] *Kamerstukken II* 2024/25, 31288, nr. 1189
[6] CSIRT: Computer security incident response team, dat onder meer tot taak heeft om bijstand en advies te verlenen bij cyberdreigingen, kwetsbaarheden en incidenten.
[7] Op grond van artikel 15, derde lid, Cbw is de Minister van OCW voor instellingen van hoger onderwijs, die zijn aangewezen als belangrijke entiteit of essentiële entiteit, de bevoegde autoriteit. Op grond van artikel 15, zesde lid, onderdeel a, Cbw heeft de bevoegde autoriteit de taak om te zorgen voor de bestuursrechtelijke handhaving van het bepaalde bij of krachtens de Cbw. Ik ben voornemens om op grond van artikel 68, eerste lid, Cbw ambtenaren van de Inspectie van het Onderwijs te belasten met het toezicht op de naleving van de verplichtingen in de Cbw en de daarop gebaseerde regelgeving door deze instellingen.

Een ontwerp van de Cyberbeveiligingsregeling hoger onderwijs is sinds 12 juni jl. te raadplegen in het kader van de openbare internetconsultatie.[8]

Ik vind het van belang dat de aanwijzing van de instellingen onder de Cbw en de verplichtingen die daaruit voortvloeien uitvoerbaar zijn voor zowel de instellingen zelf, alsook voor de Inspectie van het Onderwijs als de beoogde toezichthoudende instantie, en SURFcert als het beoogde CSIRT. Bij het opstellen van de wet- en regelgeving is naast uitvoerbaarheid ook proportionaliteit een belangrijk uitgangspunt en is er nadrukkelijk oog voor de administratieve last die entiteiten ervaren als gevolg van de wet- en regelgeving. Zo schrijft de Cbw een risicogebaseerde aanpak voor waarmee de instellingen eigen risico's dienen te identificeren en de ruimte hebben om op basis daarvan passende en evenredige beveiligingsmaatregelen te nemen. Bij de uitwerking van de aanwijzing in de sectorspecifieke regeling voor de hogescholen en universiteiten heb ik ook nadrukkelijk aandacht voor de uitvoerbaarheid en proportionaliteit. Daartoe betrek ik relevante stakeholders zoals de sectorverenigingen, SURF, Inspectie van het Onderwijs en experts bij deze uitwerking en vindt er vanuit mijn ministerie intensief overleg plaats met deze partijen.

Mijn streven is om de inwerkingtreding van de ministeriële regeling, en daarmee de aanwijzing van de hogescholen en universiteiten als belangrijke entiteit in de zin van de Cbw, zo snel mogelijk na inwerkingtreding van de Cbw te laten plaatsvinden.[9] Hieronder licht ik de uitwerking van de aanwijzing van de hogescholen en universiteiten per onderdeel nader toe.

Aanwijzing als 'belangrijke' entiteit
De Cbw geeft de mogelijkheid om de hogescholen en universiteiten onder de Cbw te brengen als ofwel essentiële entiteit ofwel belangrijke entiteit. De Cbw veronderstelt hierbij dat het proportioneel is om belangrijke entiteiten minder te belasten met administratieve lasten die volgen uit toezicht dan essentiële entiteiten vanwege hun omvang, de door hen verleende diensten en de sectoren waarin zij actief zijn. Ik kies ervoor om alle bekostigde instellingen in het hoger onderwijs als belangrijke entiteit onder de Cbw aan te wijzen en beschouw dit als passend voor de sector.[10] Gelet op de aard van de sector, die niet rechtstreeks onder de werking van de Cbw valt maar vanuit de mogelijkheid die de wet daartoe biedt, en gelet op de proportionaliteit van de uitvoeringslast voor de instellingen, ligt het niet in de rede om te kiezen voor het zwaarste toezichtsregime voor de onderwijssector. De aanwijzing als belangrijke entiteiten betekent dat de instellingen te maken krijgen met uitsluitend extern toezicht achteraf (ex-post) en niet met extern toezicht vooraf (ex-ante), zoals dat bij essentiële entiteiten wel het geval is.

Meldplicht en registratieplicht
Direct na hun aanwijzing als belangrijke entiteit onder de Cbw gaat voor de instellingen een registratieplicht en een meldplicht gelden. De registratieplicht verplicht de instellingen om zich in te schrijven bij het nationaal register van entiteiten.[11] Dit verloopt in de praktijk via het digitale portaal van het Nationaal Cyber Security Centrum (NCSC) van het ministerie van Justitie en Veiligheid.

[8] https://www.internetconsultatie.nl/cyberbeveiliging/b1]
[9] Het wetsvoorstel voor de Cbw ligt momenteel voor behandeling in de Eerste Kamer.
[10] Dit zijn de bekostigde hogescholen en universiteiten, zoals vermeld in de bijlage bij de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW), onder a tot en met i.
[11] Zoals bedoeld in artikel 43 Cbw.

Bij de meldplicht gaat het om het melden van significante incidenten bij het CSIRT en de bevoegde toezichthouder.[12] Om te bepalen wanneer er sprake is van een significant incident worden voor de instellingen criteria (drempelwaarden) vastgesteld. Aan de hand daarvan kunnen zij beoordelen of een incident significant is, en zodoende moet worden gemeld. Om tot heldere drempelwaarden te komen zijn bij de uitwerking de relevante stakeholders alsook experts vanuit de instellingen geraadpleegd. De drempelwaarden voor het melden van significante incidenten worden opgenomen in de ministeriële regeling.

Aanwijzing CSIRT (Computer Security Incident Response Team)
Direct na de aanwijzing hebben de instellingen vanuit de wet recht op bijstand en advies bij cyberdreigingen en incidenten door een als CSIRT aangewezen instantie. De aanwijzing van het CSIRT zal worden opgenomen in de ministeriële regeling. Het CSIRT heeft onder meer tot taak om belangrijke entiteiten in geval van dreigingen, kwetsbaarheden en incidenten vroegtijdig te waarschuwen, daarover informatie te verstrekken, en bijstand te verlenen. Ik ben, gelet op de bestaande kennis, expertise en ervaring van SURF en SURFcert (als huidig computercrisisteam voor het vervolgonderwijs), in vergevorderd gesprek met SURF over de uitoefening van de wettelijke taken van het CSIRT als bedoeld in de Cbw. Daarvoor zou door SURF een nieuwe privaatrechtelijke rechtspersoon opgericht dienen te worden bij wie de wettelijke taak door mij wordt belegd. De Comptabiliteitswet vereist dat in het geval van het doen oprichten van een privaatrechtelijke rechtspersoon, het voornemen daartoe voor voorhang wordt voorgelegd aan de Tweede en Eerste Kamer.[13] Deze procedure verwacht ik na de zomer te kunnen starten.

Voorbereiding op de zorgplicht
Met de aanwijzing onder de Cbw komt er op termijn ook een wettelijke zorgplicht voor de instellingen om, op basis van risicoanalyses, passende en evenredige maatregelen te treffen om de risico's voor de beveiliging van de netwerk- en informatiesystemen te beheersen, incidenten te voorkomen en de gevolgen van eventuele incidenten voor de afnemers van hun diensten te beperken. De sectorverenigingen Universiteiten van Nederland (UNL) en Vereniging Hogescholen (VH) hebben eerder hun zorgen geuit over de tijd, inzet en middelen die het vraagt van instellingen om te voldoen aan de nieuwe verplichtingen als gevolg van de aanwijzing als entiteit in de zin van de Cbw. Om die reden is door mijn voorganger, in samenspraak met de Minister van Justitie en Veiligheid, reeds besloten en in de Cbw geregeld dat de zorgplicht 36 maanden na de aanwijzing van de hogescholen en universiteiten van toepassing zal zijn. Deze gefaseerde aanpak biedt de instellingen tijd om zich zorgvuldig hierop voor te bereiden.[14]

De bekostigde hogescholen en universiteiten hebben de afgelopen jaren ingezet op het verhogen van de cyberweerbaarheid van de instellingen en hebben daar in lijn met de bestuurlijke afspraken en bijbehorende middelen een belangrijke basis voor gelegd. Aan de hand van deze bestuurlijke afspraken hebben de instellingen sinds 2021 gewerkt aan onder andere het vergroten van het bewustzijn over risico's, het vergroten van de

[12] Zoals bedoeld in artikel 25, tweede lid, Cbw,
[13] Artikel 4.7, eerste lid, onderdeel a van de Comptabiliteitswet.
[14] Voor de andere verplichtingen uit de Cbw, waaronder de meldplicht van significante incidenten en de registratieplicht, geldt dat die wel direct van toepassing zullen zijn na aanwijzing. Ook voor het in de Cbw geregelde recht op onder meer bijstand door het CSIRT bij dreigingen en incidenten geldt dat dit ten aanzien van de instellingen direct na aanwijzing van toepassing zal zijn.

gehele systeemvolwassenheid en de versterking van de ketensamenwerking. De instellingen blijven hier onverminderd op inzetten.

In voorbereiding op de aanwijzing en de wettelijke zorgplicht werken de bekostigde instellingen en SURF momenteel intensief samen aan de implementatie van de Cbw. Daarbij wisselen zij kennis uit over de belangrijkste stappen die nodig zijn voor succesvolle implementatie. Twee keer per jaar voer ik met de sector een bestuurlijk overleg over de voortgang van de implementatie van de Cbw en de voorbereiding op de zorgplicht.

Vanaf dit jaar ontvangen de hogescholen en universiteiten in totaal circa € 9 mln. structureel in hun lumpsum voor hun aanpak op cyberveiligheid. Om de sector verder tegemoet te komen investeert het kabinet tot en met 2031 € 80 miljoen om de instellingen[15] op weg te helpen bij hun uitdagingen op het vlak van (kennis)veiligheid en cyberweerbaarheid.[16] De middelen worden via de rijksbijdrage beschikbaar gesteld en kunnen ook worden aangewend voor voorbereidingswerkzaamheden rond de Cbw. Hierna verwacht ik dat de hogescholen en universiteiten in staat zijn om de kosten voor deze uitdagingen te kunnen financieren uit de bestaande middelen van de lumpsum.[17]

Ik gebruik de komende periode om met de relevante stakeholders en experts in gesprek te gaan over de nadere uitwerking van de zorgplicht in de ministeriële regeling, in aanvulling op wat hierover is opgenomen in het Cyberbeveiligingsbesluit. Mijn vertrekpunt hierbij is om zoveel mogelijk aan te sluiten bij bestaande werkwijzen en normen in de onderwijssector. Dit draagt bij aan de uitvoerbaarheid en beoogde proportionaliteit. In het kader van de ministeriële regeling is de regeldruk voor de instellingen als gevolg van de nieuwe verplichtingen in kaart gebracht. De uitkomsten hiervan zijn opgenomen in het ontwerp van de regeling dat ter internetconsultatie voorligt. Bij de uitwerking van de zorgplicht bij ministeriële regeling breng ik ook daarvan de regeldruk in kaart.

Extern toezicht
Het onafhankelijk extern toezicht op de naleving van de verplichtingen in de Cbw en de daarop gebaseerde regelgeving beleg ik bij de Inspectie van het Onderwijs. Het toezicht op de Cbw wordt voor de inspectie een nieuwe, eigenstandige aan hen opgedragen taak. De inspectie bereidt zich hier momenteel op voor en heeft aangegeven hierin samen met de hogescholen en universiteiten op te willen trekken. Bij de inrichting van het toezicht wordt er rekening gehouden met de hiervoor genoemde gefaseerde aanpak, wat betekent dat er gedurende de eerste 36 maanden vanaf de aanwijzing nog geen sprake zal zijn van extern toezicht op de zorgplicht in het kader van de Cbw.

Niet-bekostigd onderwijs
De versterking van cyberweerbaarheid is ook in de niet-bekostigde onderwijssector van belang. Aanwijzing van de niet-bekostigde entiteiten onder de Cbw wordt tegelijkertijd niet passend geacht vanuit de nadruk die in de NIS2-richtlijn in dit verband wordt gelegd

[15] Ook de kennisinstellingen maken aanspraak op de middelen uit de 80 mln, om in te zetten op cyberveiligheid.
[16] Zoals aangekondigd in mijn Beleidsbrief Onderwijs Cultuur en Wetenschap 2026-2030, 24 april 2026, Kamerstuk 36800-VIII, nr. 148
[17] De kosten als gevolg van de Cbw voor de uitvoering door SURFcert als het beoogde CSIRT en de Inspectie van het Onderwijs als de beoogde toezichthoudende instantie komen uit op € 5,9 miljoen structureel en zijn gedekt vanuit de middelen op de begroting van het Ministerie van Onderwijs, Cultuur en Wetenschap voor het hbo en wo.

op kritieke onderzoeksactiviteiten en vanuit het oogpunt van proportionaliteit. Voor het niet-bekostigd onderwijs investeert de NRTO, de brancheorganisatie van de niet-bekostigde instellingen, in maatregelen om de digitale weerbaarheid van haar leden te verhogen. Dit doet zij door onder andere het creëren van bewustzijn en het faciliteren van trainingen voor haar leden. De NRTO-audit verplicht de leden jaarlijks de basisscan "cyberweerbaarheid" van het Nationaal Cyber Security Centrum (NCSC) uit te voeren. Daarnaast heeft NRTO een samenwerking met Samen Digitaal Vaardig waarbij de leden worden voorzien van relevante informatie vanuit onder andere de NCSC.

2. Verhoging cyberweerbaarheid mbo

Vanzelfsprekend is ook voor het mbo een verdere verhoging van de cyberweerbaarheid en bescherming van (privacy)gevoelige gegevens nodig. De sector mbo zal niet onder de werking van de Cbw vallen omdat met betrekking tot onderwijsinstellingen vanuit de NIS2-richtlijn, en daarmee ook de Cbw, de nadruk ligt op instellingen die kritieke onderzoeksactiviteiten verrichten. Hieronder beschrijf ik hoe de aanpak in het mbo vorm krijgt.

Bestuurlijke afspraken tot aan 2027 voor het mbo

Het mbo heeft sinds de gemaakte bestuurlijke afspraken in 2021 fors ingezet op een verbetering van de cyberveiligheid. Onder de vlag van mbo-digitaal is het programma Cyberveiligheid mbo inmiddels vier jaar bezig en zijn er verschillende tastbare resultaten geboekt.[18] De bestuurlijke afspraken met de mbo-instellingen blijven in elk geval tot aan het eind van het programma in 2027 van kracht en we scherpen de ambities hierin aan. Over de voortgang houd ik nauw contact met de sector via het reguliere bestuurlijk overleg dat ik voer met de vertegenwoordigers van de mbo-instellingen, de hogescholen en de universiteiten.

Op basis van de bestuurlijke afspraken werken de mbo-instellingen gezamenlijk aan de verhoging van de cyberbeveiliging langs drie lijnen: (1) vergroten van het bewustzijn over risico's, (2) vergroting van de gehele systeemvolwassenheid door toepassing van een gedeeld toetsingskader en een meer risico gebaseerde werkwijze en (3) versterking van de ketensamenwerking.

Om het bewustzijn te vergroten zijn de afgelopen jaren op een groot deel van de mbo-instellingen verschillende oefeningen uitgevoerd. Onder andere door de inzet van red-teaming[19], pentesten, mystery guests en crisisoefeningen wordt er blijvend gewerkt aan het bewustzijn en het lerend vermogen van de instellingen. De ambities rond de systeemvolwassenheid scherpen we aan met de afspraak dat de mbo-sector in 2029 gemiddeld op een minimaal volwassenheidsniveau van 3 uit komt.[20] Voor individuele mbo-instellingen kan dit niveau een jaar later, voor 2030, worden bereikt. Om op dit volwassenheidsniveau te komen, wordt er veel van de instellingen gevraagd. Dit blijkt onder meer uit de resultaten van de eerste ronde externe security audits.[21] De organisatie en de governance op cyberbeveiliging scoort binnen de mbo-instellingen naar verwachting. Echter, op het gebied van de risicomanagement en identiteits- en toegangsbeheer zijn nog flinke stappen nodig. Een gezamenlijke inzet onder de vlag van

[18] https://mbodigitaal.nl/programmas/programma-cyberveiligheid-mbo/praatplaat-cyberveiligheid/#:~:text=Met%20de%20praatplaat%20over%20cyberveiligheid,van%20cyberveiligheid%20in%20het%20mbo
[19] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/oefenen-en-kennisdelen/gereedschapskist-red-teaming/
[20] https://sec.surf.nl/surfaudit-toetsingskader-informatiebeveiliging/
[21] https://mbodigitaal.nl/2026/04/resultaten-en-bevindingen-eerste-ronde-security-audits/

mbo-digitaal, in de keten en gebruik makend van de ondersteuningsstructuur van SURF, is hierbij belangrijk.

Gezamenlijke ambitie voor het mbo na 2027
Om weerstand te kunnen bieden aan de toenemende cyberdreiging, zullen de mbo-instellingen hun gezamenlijke inzet, vanuit het fundament van zelfregulering, moeten blijven continueren. Om dit concreet handen en voeten te geven en een vervolg te geven aan de activiteiten uit het huidige programma, heeft de mbo-sector het initiatief genomen een cyberweerbaarheidspool op te zetten.[22] Binnen deze pool maken de mbo-instellingen afspraken over hun inzet en resultaten op het gebied van cyberveiligheid en worden ter ondersteuning van alle mbo-instellingen centraal voorzieningen ingericht.

Mocht het voorkomen dat een mbo-instelling het slachtoffer wordt van een hack, dan ondersteunen de instellingen elkaar door middel van deze pool. Op basis van heldere spelregels kan dat, indien noodzakelijk, ook in financiële zin. De cyberweerbaarheidspool dient zo meerdere doelen: alle instellingen committeren zich aan heldere ambities en verantwoorden zich naar elkaar op basis van scherpe afspraken, er worden gezamenlijk diensten en voorzieningen ingericht en de instellingen staan voor elkaar klaar op het moment dat het nodig is. Het streven is deze cyberweerbaarheidspool in oktober 2027 te starten. Ik steun deze ontwikkeling van harte en ben voornemens afspraken over deze pool ook op te nemen in de bestuurlijke afspraken voor na 2027.

De samenhang met de aanpak in het hbo en wo blijft de komende periode essentieel. Daarom zal de in de Cyberbeveiligingsregeling hoger onderwijs opgenomen meld- en zorgplicht voor hogescholen en universiteiten, ook het uitgangspunt zijn voor de aanpak in het mbo als het gaat om cyberweerbaarheid. Na de beoogde wettelijke aanwijzing van SURFcert als CSIRT voor de hogescholen en universiteiten, blijft de dienstverlening door SURFcert aan de mbo-instellingen in stand.

Tot slot
De digitale dreigingen nemen toe en dit raakt ook het onderwijs. Het is essentieel dat de instellingen in het vervolgonderwijs nu en in de toekomst goed voorbereid zijn op de risico's die de cyberdreiging met zich meebrengt en dat zij, als onderdeel van het bredere digitale ecosysteem, blijvend inzetten op verhoging van de cyberweerbaarheid. Samenwerking tussen de sectoren is hierin van belang. Ik ga er vanuit dat de instellingen de komende jaren de noodzakelijke stappen hierop blijven zetten. Ik blijf dit nauwlettend volgen en informeer uw Kamer bij relevante ontwikkelingen.

De minister van Onderwijs, Cultuur en Wetenschap,

Rianne Letschert

[22] https://mbodigitaal.nl/programmas/programma-cyberveiligheid-mbo/incidenten-herstellen/cyberrisicopooling/