Universiteiten van Nederland

Vereniging Hogescholen

MBO Raad

SURF

Aan De heer dr. E.E.W. Bruins,
Minister van Onderwijs, Cultuur en Wetenschap
Postbus 16375
2500 BJ DEN HAAG

i.a.a. De heer D.M. van Weel,
Minister van Justitie en Veiligheid
Postbus 20301
2500 EH DEN HAAG

&

Tweede Kamer der Staten-Generaal

Datum 1 mei 2025

Doorkiesnummer persoonsgegeven

Email persoonsgegeven

Onderwerp **Reactie op kabinetsvoornemen tot aanwijzen onderwijsinstellingen onder de NIS2-richtlijn**

Ons kenmerk VH-25.5544.persoonsgegeven

Bijlage(n) brieven van 8 april 2024 en 14 februari 2025

Geachte minister Bruins,

Net als het kabinet achten wij het van evident belang het onderwijs en onderzoek zeer goed te beveiligen. Daarom hebben wij in de afgelopen jaren, als hogescholen en universiteiten tezamen met de mbo-sector en SURF, intensief samengewerkt met het ministerie van OCW om te werken aan formele bestuurlijke afspraken die gericht zijn op het versterken van de cyberweerbaarheid van de onderwijssector. We hebben aangetoond dat het mogelijk is om deze weerbaarheid snel en stevig te verbeteren zonder de noodzaak van dwingende, bureaucratische en kostbare wetgeving waar de sector al te veel mee te maken heeft. Om die reden hebben we als onderwijsinstellingen bezwaar tegen het voornemen geuit in uw brief aan de Tweede Kamer van 24 april 2025 (TK 31.288 nr. 1189) om universiteiten en hogescholen aan te wijzen onder de nog bij het parlement in te dienen Cyberbeveiligingswet. De onderwijsinstellingen behoren niet tot de kritische sectoren waarvoor de Europese NIS2-richtlijn is beoogd en die via deze wet in Nederland wordt geïmplementeerd.

Zoals wij in eerdere brieven aan de minister van OCW en de minister van JenV hebben aangegeven (bijgevoegd in bijlage) hebben wij in kaart gebracht en met beide ministeries gedeeld dat de invoering van deze wet de instellingen in het hoger onderwijs onterecht zal belasten met veel nieuwe administratieve verplichtingen die het feitelijke doel onnodig zullen belemmeren: het verbeteren van de veiligheid. Op beide brieven hebben wij nimmer een reactie van u of uw collega van JenV ontvangen.

Nieuwe maatregelen ter implementatie van de Europese NIS2-richtlijn die onderwijsinstellingen, SURF en de onderwijsinspectie moeten nemen, vergen veel tijd voor voorbereiding en implementatie, terwijl er op dit

moment al een aangetoond goed werkend systeem van maatregelen en aanpak in werking is dat periodiek extern geaudit en aangescherpt wordt. De uitwerking van de nieuwe wet is op dit moment ook nog eens op veel punten onduidelijk, waardoor niet alleen het risico op dubbele maatregelen en inefficiëntie groot is, maar ook het risico op niet functionerende onderlinge afhankelijkheden die de veiligheid juist verslechteren in plaats van verbeteren.

Aanwijzing van onderwijsinstellingen onder NIS2 is door de Europese Commissie niet voor niets nadrukkelijk optioneel gemaakt en is dus geen verplichting voor de lidstaten. Een keuze door Nederland om bij invoering van de Cyberbeveiligingswet het hoger onderwijs ook direct onder (delen van) deze wet te stellen, wijkt niet alleen af van een aantal ons omringende landen, maar creëert bovendien een situatie waarbij de termijnen die zijn gesteld voor implementatie nu volstrekt onhaalbaar zijn. De minister van EZK heeft de TO2-instellingen afgelopen jaar helder gemaakt dat zij niet onder de wet aangewezen zullen worden. Een wet die overigens al meerdere keren is uitgesteld, vanwege de complexiteit van implementatie, blijkend uit eerdere kabinets-brieven. Uit het overleg met uw ministerie ontstond nadrukkelijk de indruk dat het hoger onderwijs eveneens niet onder deze wet zou gaan vallen. Door uw ministerie is niet op daadwerkelijke voorbereiding voor implementatie ingezet. Zelfs in deze fase laat u in uw brief nog in het midden of sprake zal zijn van een aanwijzing als 'essentiële' ofwel 'belangrijke' entiteit; een verschil dat ook belangrijke consequenties heeft.

De NIS2-richtlijn stelt (ook) dat de lidstaten, voor sectoren die onder de regels komen te vallen, de noodzakelijke financiële middelen beschikbaar moeten stellen voor de systeemwijzigingen die de wetgeving met zich meebrengt. De kosten voor invoering van de NIS2-richtlijn zijn zeer hoog (de Europese Commissie raamt zelf de extra kosten op 22% van de huidige budgetten). Tegelijkertijd heeft dit kabinet juist drastisch bezuinigd op de budgetten van de onderwijsinstellingen. Uit de 1e suppletoire OCW-begroting naar aanleiding van de Voorjaarsnota 2025 (TK 36725-VIII) blijkt bovendien dat het kabinet de instellingsbudgetten van mbo-instellingen, hogescholen en universiteiten nog eens structureel met 7,6 miljoen euro extra kort om de NIS2-kosten van de Onderwijsinspectie en SURF te vergoeden. Dit maakt het des te moeilijker voor instellingen om de nieuwe verplichtingen te bekostigen. Ze moeten immers zelfs de extra rekening betalen. De beoogde nieuwe toezichtstaak door de Inspectie van het Onderwijs in de zin van de (nog niet bij het parlement ingediende) Cyberbeveiligingswet, is bovendien nog niet getoetst op haalbaarheid, laat staan dat de instellingen en SURF zich hierop hebben kunnen voorbereiden. Recent schreef u nog aan de Tweede Kamer te streven naar: “een vermindering van de administratieve lasten en het beleggen van verantwoordelijkheden waar ze primair thuishoren” (TK 31.288 nr. 1185). Wij constateren het omgekeerde.

Zoals aangegeven hebben hogescholen en universiteiten grote bezwaren tegen het via de Cyberveiligheidswet aanwijzen van het hoger onderwijs onder de NIS2-richtlijn. Het veroorzaakt onnodige bureaucratie terwijl het hoger onderwijs daar niet ‘veiliger’ door wordt. Bovendien zet het de samenwerking in SURF-verband, onder andere met het mbo, onder druk, en moet tijdens de implementatieperiode capaciteit en middelen verdeeld worden over die bureaucratische regels enerzijds en onze cyberveiligheid anderzijds. Mocht u, ondanks onze serieuze bezwaren, het hoger onderwijs desondanks onder deze wetgeving willen brengen, dan vragen we om:

- Deze hoe dan ook niet voor 2029 van kracht te laten worden, of zoveel later tot volstrekte duidelijkheid bestaat over de regelgeving waaraan voldaan moet worden, zodat er voldoende tijd is voor een zorgvuldige voorbereiding van de implementatie en wij tussentijds zonder veiligheidsrisico’s en zonder schade voor onderwijs en onderzoek onze inspanningen kunnen voortzetten, juist om onze veiligheid te blijven borgen. Alleen dan biedt dit instellingen, de inspectie en SURF de ruimte om de noodzakelijke maatregelen in te voeren.

- Voldoende budget ter beschikking te stellen aan instellingen en SURF om invoering binnen dit tijdsbestek mogelijk te maken en ruimte te bieden voor duidelijke afspraken waarmee voortgebouwd kan worden op het goedwerkende systeem van samenwerking dat SURF en de onderwijsinstellingen in de afgelopen jaren hebben ontwikkeld en zo te waarborgen dat óók de samenwerking met de mbo- en TO2-instellingen die niet onder de NIS2-regels worden aangewezen, niet belemmerd wordt.
- In de noodzakelijke sectorale uitwerking bovendien rekening te houden met een normstelling die past bij het risiconiveau van het onderwijs, zodat de wetgeving geïmplementeerd kan worden in de context van het hoger onderwijs.

Wij hopen op een constructief gesprek over realistische en haalbare afspraken in de geest van de veiligheidsdoelstelling die beoogd is met de NIS2-richtlijn en de verdere samenwerking op dit gebied.

Met vriendelijke groet,

Namens de universiteiten,

persoonsgegeven

De heer prof. dr. C.F. van den Berg
Voorzitter vereniging Universiteiten van Nederland

Namens de hogescholen,

persoonsgegeven

De heer mr. Maurice Limmen
Voorzitter Vereniging Hogescholen

Namens de mbo-instellingen,

persoonsgegeven

De heer Adnan Tekin
Voorzitter MBO Raad

Namens de coöperatie SURF,

persoonsgegeven

De heer drs. Ron Augustus
Voorzitter Raad van Bestuur SURF

Universiteiten van Nederland

Vereniging Hogescholen

MBO Raad

Aan

De heer D.M. van Weel
Minister van Justitie en Veiligheid
Postbus 20301
2500 EH Den Haag

De heer Dr. E.E.W. Bruins
Minister van Onderwijs, Cultuur en Wetenschap
Postbus 16375
2500 BJ Den Haag

Datum 14 februari 2025
Telefoon persoonsgegeven
E-mail

Onderwerp **NIS2- richtlijn hoger onderwijs**

Geachte heer Van Weel,
Geachte heer Bruins,

Naar aanleiding van het Commissiedebat over Online Veiligheid en Cybersecurity van 5 februari 2025, waarin de minister van Justitie en Veiligheid in antwoord op het kamerlid Michon-Derkzen aangeeft bij de Minister van Onderwijs, Cultuur en Wetenschap te bepleiten de onderwijssector onder de NIS2-richtlijn aan te wijzen, willen wij graag het volgende onder uw aandacht brengen.

Nederlandse universiteiten, hogescholen en mbo-instellingen streven naar een open en veilig leer- en onderzoeksklimaat. Open, omdat kwalitatief hoogwaardig onderwijs en onderzoek simpelweg niet mogelijk zijn zonder samenwerking van mensen en organisaties rondom nieuwe inzichten. Veiligheid is daarnaast een voorwaarde om deze kwaliteit te bereiken. Een uitstekende beveiliging van de digitale infrastructuur van instellingen is daarvoor randvoorwaardelijk en staat dan ook al jaren hoog op de agenda van alle instellingen. Er is een stevige, en op de sector geënte aanpak geïmplementeerd om de cyberweerbaarheid te waarborgen en door te ontwikkelen. Deze aanpak omvat bestuurlijke afspraken met het ministerie van OCW, sectorbrede volwassenheidsambities, frequente externe audits, grootschalige oefeningen met tevens aandacht voor ketens en leveranciers, detectie via SOC's en respons via Computer Emergency Response Teams (CERT) inclusief SURFcert: het sectorale onderwijs-CERT binnen het Landelijk Dekkend Stelsel. De sector legt hierover regelmatig verantwoording af aan het ministerie van OCW. Daarnaast is er een sectorspecifiek landelijk expertisecentrum (SURF), bij wet is er bestuurlijke verantwoordelijkheid en toezicht, en er is samenwerking met bedrijven en overheid. Via een kortcyclische verbeteraanpak worden ambities en bestuurlijke afspraken steeds geoptimaliseerd. Hierover voeren instellingen regelmatig het bestuurlijke gesprek met OCW, zo ook in deze periode.

De NIS2-verordening van toepassing verklaren zal de voorwaartse beweging verstoren. De vormvereisten onder de wet wijken zodanig af van de huidige bewezen aanpak, dat de beschikbare middelen niet meer aan

Vereniging Universiteiten van Nederland

Lange Houtstraat 2
Postbus 13739
2501 ES Den Haag

Tel +31 70 302 14 00
E-mail post@unl.nl
Web universiteitenvannederland.nl

KvK 40480226
IBAN NL61 INGB 0001 5964 15
BTW NL007088784B01

het verder versterken van cyberweerbaarheid besteed kunnen worden, maar noodgedwongen aan andere, niet noodzakelijk bétere, wijzen van verantwoording en governance.

Wat betekent dit concreet? We noemen enkele voorbeelden, maar niet limitatief.

- De NIS2-regelgeving zou van de onderwijssector eisen om bestaande en goedwerkende, geïntegreerde structuren voor toezicht en verantwoording te stoppen, en daarvoor andere structuren in te richten. Concreet zal bijvoorbeeld onder de NIS2 een extra toezichthoudend orgaan moeten worden benoemd dat binnen de kaders van de NIS2 middels meerdere nieuwe inspecties de informatiebeveiliging van onderwijsinstellingen toetst, bestuurders aanspreekt en middels dwang indien nodig instellingen verbeteringen laat doorvoeren. Hoe dit orgaan zich moet verhouden tot de Raden van Toezicht, bestuurders en organisatie van de instellingen is onduidelijk. Dit vereist in de praktijk onder meer het overboord zetten van de bewezen goedwerkende externe auditsystematiek en het in plaats daarvan opzetten en uitwerken van een nieuwe inspectiemethode die voor de instellingen en in de hele sector ook in de praktijk een nieuwe manier van werken zal betekenen waarvan het effect op korte en middellange termijn op zijn zachtst gezegd onzeker is. Daar waar in de huidige systematiek in een aantal jaren een uitstekende samenwerking en weerbaarheid is opgebouwd die bewezen effectief is, zouden de instellingen, zonder noodzaak, teruggeworpen worden op een nog te ontwikkelen systeem waar de sector zich opnieuw op moet gaan inrichten. We achten dit niet proportioneel, mede gelet op het feit dat het hier niet om een kritische sector gaat, en zeer risicovol.
- Een nieuwe vorm van bestuurdersverantwoordelijkheid vastleggen zou vereist zijn conform de NIS2 maar brengt de facto geen verbetering, wel meer bureaucratie. Bestuurders zijn al wettelijk verantwoordelijk én aansprakelijk. De portefeuille cybersecurity is formeel belegd bij een van de bestuursleden. Hierop worden zij aangesproken door de Raad van Toezicht (RvT) waar het externe toezicht is belegd. Er zijn afspraken over periodieke rapportage en agendering bij de RvT's en het onderwerp staat veelvuldig op de agenda van het overleg van voorzitters RvT met OCW. Invoeren van een nieuwe systematiek van toezicht kost onnodig veel tijd en geld. Bovendien blijft het toezicht conform de WHW gelden en dus zouden onder NIS 2 dubbele toezichtrollen ontstaan
- Instellingen werken op basis van een auditkader passend bij het risicoprofiel van de sector. Dit is gebaseerd op de geldende internationale standaarden voor informatiebeveiliging. Dit kader wordt sectorbreed toegepast en heeft geleid tot een breed begrip, werkwijze en taal voor informatiebeveiliging. De sector komt daarmee tot snelle en adequate informatie-uitwisseling (binnen en buiten de sector) en ontwikkeling van informatiebeveiliging hetgeen ook blijkt uit de stijgende scores op de externe audits die periodiek worden uitgevoerd. Het opnieuw eigen maken, implementeren en auditen van het NIS2 kader doet deze jarenlange investering teniet en vraagt een complete herijking, met alle risico's van dien.

Met deze selectie aan voorbeelden willen wij duidelijk maken dat aanwijzing geen recht zou doen aan het werkelijke doel: de sector optimaal cyberweerbaar maken en houden in de toekomst.

Het bewustzijn van de bredere weerbaarheidsopgave in Nederland en het mede-verantwoordelijkheidsgevoel hiervoor is evenwel ook in de onderwijssector groot. Met het ministerie van OCW zijn dan ook opvolgende bestuurlijke afspraken over cyberweerbaarheid voorbereid waarin er specifiek op gelet is dat de sector aansluit op belangrijke weerbaarheidseisen uit de NIS2-regelgeving, zoals risicomanagement. Ook zijn passende oplossingen voor meld- en zorgplicht opgenomen, voor onmiddellijke en brede informatiedeling en voor het nog beter expliciteren van de bestuurlijke verantwoordelijkheid, Net als bij de vergelijkbare TO2-instellingen, die onder het ministerie van EZ vallen, en *niet* aangewezen worden, zou dit ruimschoots moeten volstaan, en proportioneel zijn met het oog op de niet-kritische status en de inhoudelijke belangen in onderwijs en onderzoek.

Universiteiten van Nederland

Vereniging Hogescholen

MBO Raad

Alle instellingen hebben zich vanuit deze intrinsieke motivatie bestuurlijk gecommitteerd aan de nieuw te maken bestuurlijke afspraken, mits de NIS2-regelgeving niet van toepassing zal zijn. Als de sector wél aangewezen wordt, moet er veel veranderen aan zaken die niet met feitelijke weerbaarheid te maken hebben, veranderingen die naar verwachting geen verbeteringen zijn. Onder die omstandigheden zal er substantieel budget- en capaciteitstekort zijn en veel onnodige bureaucratie.

Het overgaan naar een nieuw kader zou een groot aantal investeringen uit de afgelopen jaren teniet doen en de verdere voortgang verhinderen, die de instellingen individueel en collectief nastreven. De zorg hierover in onze sector is groot, zowel bij bestuurders alsook bij CIO's en CISO's. De instellingen hebben hierover ook al eerder een brief gestuurd aan de minister van OCW, die verantwoordelijk is voor het wel of niet aanwijzen van hoger-onderwijsinstellingen onder de NIS2. U treft hierbij voor de volledigheid een kopie van deze brief.

Tot slot, en samenvattend. Universiteiten, hogescholen en mbo-instellingen zijn ervan overtuigd dat de weg naar een optimale cyberweerbaarheid aan dient te sluiten op de huidige aanpak en bestuurlijke afspraken. Nieuwe wetgeving is disproportioneel en schadelijk voor onderwijs en onderzoek, en gaat stagnatie of teruggang in veiligheid, meer bureaucratie en veel hogere kosten opleveren, waarvoor geen budget of capaciteit beschikbaar is. Graag gaan we hierover op korte termijn met u in gesprek.

Hoogachtend,

persoonsgegeven

Mevrouw dr. M.M.N. Ummelen
Bestuurlijk Trekker Integrale Veiligheid en Cyberveiligheid Universiteiten van Nederland

persoonsgegeven

De heer prof.dr. C.F. van den Berg
Voorzitter vereniging Universiteiten van Nederland

persoonsgegeven

Mevrouw dr. Angelien Sanderman
Bestuurlijk Trekker Cyberveiligheid Vereniging Hogescholen

Universiteiten van Nederland

Vereniging Hogescholen

MBO Raad

persoonsgegeven

De heer mr. Maurice Limmen
Voorzitter Vereniging Hogescholen

persoonsgegeven

Mevrouw Mirjam Koster
Bestuurlijk Trekker Cyberveiligheid MBO Raad

persoonsgegeven

De heer Adnan Tekin
Voorzitter MBO Raad

Universiteiten *van* Nederland

Vereniging Hogescholen

De heer prof. dr. R.H. Dijkgraaf
Minister van Onderwijs, Cultuur en Wetenschap
Postbus 16375
2500 BJ DEN HAAG

Cc: SBF-leden

Datum	8 april 2024	*Uw kenmerk*	
Telefoon	persoonsgegeven	*Ons kenmerk*	UNL 24025U
E-mail		*Bijlagen*	-

Onderwerp **Verzoek vrijstelling NIS2-richtlijn**

Geachte heer Dijkgraaf,

Via deze brief willen wij verzoeken om universiteiten en hogescholen niet aan te wijzen onder de herziene Network and Information Security (NIS2) richtlijn. Graag brengen we een aantal inzichten en zorgen onder uw aandacht ter ondersteuning van dit verzoek.

De NIS2-richtlijn is in het leven geroepen om kritische infrastructuur te beschermen. De universiteiten en hogescholen erkennen volledig het belang hiervan. Hoewel bescherming van kennis en informatie ook voor universiteiten en hogescholen van cruciaal belang is, vallen zij echter -met reden- niet onder de definitie van kritische infrastructuur blijkens de Europese richtlijn. Aanwijzing is dan ook niet vereist, maar een keuze die de minister kan maken. Als die keuze inderdaad gemaakt zou worden, heeft dat naar onze verwachting een onevenredig grote impact op de sector, terwijl het de vraag is of een aanwijzing wel substantieel meerwaarde zal brengen ten opzichte van de serieuze stappen en resultaten die momenteel al aantoonbaar geboekt worden in informatieveiligheid; en waarvoor alle instellingen zich ook in de toekomst maximaal zullen blijven inspannen.

Maatschappelijke taken in relatie tot NIS2
De maatschappelijke taak van universiteiten en hogescholen is het geven van hoogwaardig onderwijs, het verrichten van onderzoek van wereldniveau en het realiseren van maatschappelijke impact, om daarmee te bouwen aan een sterke kennissamenleving. Zo dragen de instellingen bij aan een krachtige samenleving waarmee Nederland internationaal een vooraanstaande positie behaalt en behoudt. De netwerk- en informatiesystemen van hogescholen en universiteiten zijn ingericht om te kunnen voldoen aan deze maatschappelijke taak. De taken en ook de risico's in het hoger onderwijs verschillen echter fundamenteel van die in de kritieke infrastructuren die de NIS2-richtlijn beoogt te beschermen.

Informatiebeveiliging in het HO: ambities en resultaten
Het belang van informatieveiligheid, cyberweerbaarheid, kennisveiligheid wordt in de HO-sector volledig onderschreven. Er is al veel in geïnvesteerd en deze inspanningen worden krachtig voortgezet. Dit vertaalt zich ook in meetbare resultaten.
Voor informatiebeveiliging en cyberweerbaarheid hanteren alle hoger onderwijsinstellingen een formeel en voor de sector passend toetsingskader, gebaseerd op standaarden van de Internationale Organisatie voor Standaardisatie (ISO). Dit kader, ook wel SURF-normenkader, is de basis voor periodieke formele externe

Vereniging Universiteiten van Nederland
Lange Houtstraat 2
Postbus 13739
2501 ES Den Haag
Tel +31 70 302 14 00
E-mail post@unl.nl
Web universiteitenvannederland.nl
KvK 40480226
IBAN NL61 INGB 0001 5964 15
BTW NL007088784B01

audits. Er is een sectorbrede minimumambitie vastgesteld, en op basis van de audits worden systematische en continue verbeterprocessen gevolgd. Er wordt verantwoording afgelegd in Raden van Toezicht, jaarverslagen en er vindt halfjaarlijks Bestuurlijk Overleg plaats over de voortgang.

De HO-sector, veelal via het coöperatief platform van SURF, loopt al vele jaren voorop in deze ontwikkelingen, onder meer door het organiseren van centrale expertise in bijvoorbeeld het gezamenlijke Computer Emergency Response Team voor onderwijs en onderzoek, het SURFcert, met daarin security-experts van aangesloten instellingen en SURF. Ook door verschillende incidenten, zoals de cyberaanval aan de Universiteit Maastricht in 2019, is het bewustzijn van risico's en het belang van weerbaarheid op alle niveaus onverminderd hoog. Met nog steeds groeiende focus investeren instellingen in zowel in technische als organisatorische maatrelen om de digitale weerbaarheid te blijven vergroten en ook toetsbaar te maken. Het heeft een hoge prioriteit op de bestuurlijke agenda van alle instellingen, van de sector als geheel en van partners in de samenwerkingsketens.

Huidige informatiebeveiliging in relatie tot vorm en opbrengst NIS2
De nieuwe NIS2-richtlijn schrijft specifieke vormen van zorgplicht, meldplicht en toezicht voor, die in veel facetten lijken op hetgeen er al in het HO gebeurt, maar de specifieke vormvereisten vergen grote veranderinspanningen ten opzichte van het hele huis aan procedures die op dit moment al in positie en uitvoering zijn, met goede resultaten.
In de huidige situatie zorgen instellingen reeds voor passende beveiligingsmaatregelen, waaronder basismaatregelen zoals multifactor authenticatie, netwerksegmentering, detectie (d.m.v. SOC/SIEM) en awareness programma's. Zij testen de cyberweerbaarheid periodiek door middel van o.a. zogenaamde Pentests. Informatie over pogingen tot inbreken of andere risico's worden gemeld en gedeeld binnen het hechte netwerk van specialisten via de platforms van SURF. Bij cyberaanvallen biedt SURFcert ondersteuning en advies aan de Incident Respons Teams bij de instellingen. Het SURFcert is onderdeel van het Landelijk Dekkend Stelsel van het Nationaal Cyber Security Centrum (NCSC). Op het gebied van cyberweerbaarheid blijken de getroffen maatregelen grote dreigingen te hebben kunnen afweren. Naast de toegenomen cyberweerbaarheid is dat waarneembaar in de positieve trend ten aanzien van de audit scores. Naast de interne toezicht maatregelen in de instellingen hebben ook Raden van Toezicht het onderwerp hoog op de agenda staan.

Het is de vraag welke meerwaarde andere vormvereisten onder aanwijzing van de wetgeving zullen hebben. De extra inspanningen en investeringen om hieraan te kunnen voldoen zullen echter groot zijn, niet alleen aan de zijde van de instellingen, maar het zal ook veel vragen van uw ministerie en de inspectie. De administratieve lastendruk zal er (contrair aan alle goede intenties) door toenemen, terwijl alle HO-instellingen deze energie liever steken in het verder brengen van de cyberweerbaarheid zelf, bijvoorbeeld door zowel dit jaar als volgend jaar weer een aantoonbare volgende sprong in het volwassenheidsmodel te maken voor informatiebeveiliging en kennisveiligheid. Er is veel goede energie in de instellingen op deze onderwerpen en de actuele resultaten hopen we u in juni tijdens het BO te presenteren.

Verwachte gevolgen NIS2 voor (internationale) samenwerking in onderwijs en onderzoek
Een andere vorm van impact van NIS2 voor het hoger onderwijs en onderzoek is die op het onderwijs en onderzoek. Afhankelijk van de gevolgen van de wetgevingsvereisten kan er verandering nodig zijn in het gebruik van specifieke diensten, systemen of technologie die vereist zijn voor het aanbieden van onderwijs of het samenwerken in onderwijs en onderzoek, passend bij de maatschappelijke taken. Deze impact kan groot zijn als in Nederland de instellingen worden aangewezen voor de NIS2, maar in overige landen niet. In de afgelopen maanden is gebleken dat hier nog geen eenduidig beeld over bestaat, maar ook dat de ons omringende landen naar verwachting niet de hele HO-sector zullen gaan aanwijzen. Mochten de Nederlandse instellingen op dit moment wél aangewezen worden, dan is de impact op Europese en internationale samenwerking onderwijs en onderzoek ongewis. Ook het ICTU-impactrapport geeft hier geen helderheid over.

Universiteiten *van* Nederland

Vereniging Hogescholen

Consequenties van aanwijzing in het kort

Mochten universiteiten en hogescholen onder de NIS2-richtlijn gaan vallen dan betekent dit substantiële extra financiële en operationele lasten voor de instellingen, terwijl de meerwaarde aan (extra) veiligheid naar verwachting gering zal zijn. De Europese Commissie schat dat de uitgaven voor ICT-beveiliging voor organisaties in de jaren na de invoering van het nieuwe NIS-kader met maximaal 22% zullen stijgen. Voor universiteiten en hogescholen zou dit een onevenredige lastenverzwaring zijn. Naast de financiële impact is het uitdagend om de juiste mensen aan te trekken in verband met schaarste op de arbeidsmarkt in zijn algemeenheid maar zeker voor de cybersecurity experts. Dit gaat ten koste van andere noodzakelijke investeringen waarin bestuurlijke keuzes moeten worden gemaakt. Ook deze extra investeringen kunnen leiden tot een slechtere internationale concurrentiepositie van Nederlandse instellingen ten opzichte van landen waar de NIS2 niet van toepassing wordt verklaard. De NIS2-richtlijn is immers niet verplicht voor hoger onderwijsinstellingen en ook buiten Europa gelden andere richtlijnen.

Ter afsluiting

De Nederlandse universiteiten en hogescholen onderschrijven het belang van digitale weerbaarheid en zijn hierover met uw ministerie in goed en constructief overleg waarbij over en weer vertrouwen is uitgesproken in de stappen die gezet zijn en worden. Extra regulering door middel van NIS2-wetgeving lijkt niet in verhouding te staan tot deze positieve, constructieve dialoog. Het doet ook geen recht aan de ontwikkeling waarbij de instellingen in de afgelopen jaren hebben laten zien hun verantwoordelijkheid ten aanzien van informatiebeveiliging/cybersecurity zeer serieus te nemen en ook oog te hebben voor de veranderende geopolitieke verhoudingen die in het onderwerp kennisveiligheid samenkomen. Onderzoek naar de ontwikkelingen van het kennisveiligheidsbeleid van instellingen laat zien dat ook hier grote stappen worden gezet.

Wij verzoeken u daarom vriendelijk om de Nederlandse universiteiten en hogescholen niet aan te wijzen onder de NIS2-richtlijn, rekening houdend met onze unieke positie en de mogelijke negatieve gevolgen van dergelijke regelgeving voor onze instellingen. Wij staan open voor verdere discussies en zijn bereid om samen te werken met uw ministerie om voortdurend te verkennen welke stappen de veiligheid van netwerk- en informatiesystemen kunnen waarborgen zonder afbreuk te doen aan onze kernmissies.

Wij danken u bij voorbaat voor uw begrip en aandacht.

Hoogachtend,

persoonsgegeven

Nicole Ummelen
Bestuurlijk Trekker Cyber Security /
Bestuurlijk trekker Integrale Veiligheid UNL

persoonsgegeven

Jopie Nooren
Portefeuillehouder Integrale Veiligheid VH