Beleidskompasformulier voor **internetconsultatie**

Instructie voor gebruik:

Dit is het formulier voor de beantwoording van de Beleidskompasvragen ten behoeve van internetconsultatie. Per 29 maart 2023 worden bij nieuwe internetconsultaties de antwoorden op de vragen van het Beleidskompas gepubliceerd. Let op dat dit formulier op enkele punten afwijkt van het reguliere Beleidskompasformulier, aangezien dit formulier terugblikt op de stappen voorafgaand aan de consultatie.

Alle tekstvakken in het formulier dienen te worden ingevuld en vragen mogen niet worden verwijderd. Indien het voorstel een technische wijziging betreft of om een andere reden beleidsarm is, kan bij de vragen die niet van toepassing zijn worden volstaan met het invullen van "n.v.t.".

Verwijder de cursief gedrukte tekst na beantwoording van de vragen.

Titel:

(Vul hier de publicatietitel van de internetconsultatie in)

Cyberbeveiligingsregeling hoger onderwijs

∞ Wie zijn belanghebbenden en waarom?

Toelichting

Hulpvragen

- Wie zijn direct of indirect belanghebbenden bij het betreffende vraagstuk?

Voor de nationale implementatie van de NIS2-richtlijn in de Cyberbeveiligingswet (hierna: Cbw) is het ministerie van Justitie en Veiligheid (hierna: JenV) het coördinerende ministerie. Vanuit hun rol nemen ze regie op alle ministeriele regelingen. Het ministerie van Onderwijs, Cultuur en Wetenschap (hierna: OCW) werkt de sectorspecifieke eisen uit in de Cyberbeveiligingsregeling hoger onderwijs.

De direct belanghebbenden zijn de bekostigde instellingen voor hoger onderwijs, zoals opgenomen in de bijlage onder a tot en met i van de WHW, aangezien deze instellingen binnen de reikwijdte van de Cbw vallen.

De indirecte belanghebbenden zijn de koepels in de sector hoger onderwijs. De Inspectie van het Onderwijs (hierna: IvhO) zal toezicht houden op de naleving van de verplichtingen uit de Cbw, het Cbb en de Cyberbeveiligingsregeling hoger onderwijs. Het Computer Security Incident Response Team (hierna: CSIRT), zal ondersteuning leveren aan de bekostigde instellingen voor hoger onderwijs die als belangrijke entiteiten onder de wet vallen.

- Wie beschikken er over relevante kennis over en ervaring met het vraagstuk?

Onder andere koepelorganisaties, SURF en Inspectie van het Onderwijs beschikken over de relevante kennis.

- Op welke wijze zijn belanghebbenden tot nu toe in de verschillende fasen van het beleidstraject betrokken?

Het wetsvoorstel en het besluit zijn eerder in internetconsultatie geweest. Belanghebbenden hebben hierop kunnen reageren. Belanghebbenden, SURF en Inspectie van het Onderwijs zijn door afstemming betrokken bij het opstellen van deze regeling. Vanuit de regierol die JenV heeft, worden via gezamenlijke overleggen de regelingen van alle vakdepartementen besproken en de voortgang bewaakt met oog op inwerkingtreding en uniformele regeling.

1. Wat is het probleem?

Toelichting

Hulpvragen

a) Wat is het probleem?

De NIS2-richtlijn verplicht tot het implementeren van regels over de beveiliging van netwerk- en informatiesystemen van essentiële en belangrijke entiteiten (de zorgplicht) en de daarvoor benodigde governance binnen de entiteiten. Daarnaast wordt er een meldplicht voor significante incidenten bij de daarvoor aangewezen Computer Security Incident Response Teams (CSIRTs) ingesteld en wordt toezicht en handhaving op de voorgenoemde regels ingevoerd. Deze regels zijn omgezet in het voorstel voor de Cyberbeveiligingswet (Cbw) en het Cyberbeveiligingsbesluit (Cbb), de Algemene Maatregel van Bestuur onder de Cbw. Daarin zijn een aantal grondslagen opgenomen voor het stellen van nadere regels voor de verschillende essentiële en belangrijke sectoren (en eventueel voor subsectoren en entiteiten. Als gevolg van het besluit om bekostigde hoger onderwijsinstellingen onder de reikwijdte van de Cyberbeveiligingswet te laten vallen, moeten deze instellingen per ministeriële regeling worden aangewezen. In het Cbb is een aantal grondslagen opgenomen om per ministeriële regeling nadere regels te stellen. Deze zien toe op het aanwijzen van een ander CSIRT dan het Nationaal Cyber Security Centrum (NCSC), het stellen van nadere regels voor de zorgplicht en het opnemen van sectorspecifieke drempelwaarden voor de meldplicht. Dit moet uitgewerkt worden in een sectorspecifieke ministeriële regeling. Tevens moet er per regeling een toezichthouder worden aangewezen.

b) Wat zijn de oorzaken van het probleem?

Zie antwoord op vraag 1a Met het vaststellen van de NIS2-richtlijn, de opvolger van de NIS1-richtlijn, betekent dit dat de wetgeving nationaal wordt geïmplementeerd om de cyberbeveiliging in alle lidstaten te versterken, inclusief de sector onderwijs aangezien deze wordt aangewezen. Ondanks dat de sector onderwijs geen onderdeel was van de NIS1-richtlijn, hebben zowel de hbo- als wo-instelling zich al jarenlang ingespannen voor het versterken van de cyberweerbaarheid. Het onder de Cbw brengen van deze instellingen brengt derhalve nieuwe verplichtingen met zich mee. Hierdoor krijgt het onderwijsveld te maken met nieuwe wet- en regelgeving met betrekking tot cyberbeveiliging en de daaruit voortvloeiende vereisten.

c) Wat is de omvang van het probleem?

Zie antwoord op vraag 1a

d) Wat is het huidige beleid en wat heeft de evaluatie opgeleverd?

In 2021 zijn bestuurlijke afspraken gemaakt met de sector waarin concrete maatregelen zijn vastgelegd voor versterking van de cyberweerbaarheid. Aan de hand van deze bestuurlijke afspraken en aanvullende investeringen 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 toetsingskader en een meer risico gebaseerde werkwijze; en
(3) versterking van de ketensamenwerking.

Ten behoeve van de bestuurlijke afspraken voerde OCW tweemaal per jaar een bestuurlijk overleg met UNL, de VH en de MBO-raad. Hierbij wordt het sectorbeeld van het voorgaande jaar gepresenteerd en de sectorale voortgang van de maatregelen geëvalueerd. De sectorbeelden die het vervolgonderwijs jaarlijks opstelt laten over de hele linie zien dat er aantoonbare stappen voorwaarts zijn gezet.

e) Wat gebeurt er als de overheid niets doet (Nuloptie)? Wat rechtvaardigt overheidsinterventie?

Als de overheid niets doet (nuloptie), zijn er geen verplichte kaders voor het duurzaam beheersen van cyberrisico's door onderwijsinstellingen terwijl ook zij kwetsbaar zijn voor de toenemende en permanente digitale dreiging. Om deze risico's te beperken en de cyberweerbaarheid te vergroten, is overheidsinterventie gerechtvaardigd. De Europese NIS2-richtlijn biedt lidstaten de mogelijkheid om onderwijsinstellingen, vooral wanneer zij kritieke onderzoeksactiviteiten uitvoeren, onder de regelgeving te brengen. In Nederland wordt dit vormgegeven via de Cybersecuritystrategie en de implementatie van NIS2 in de Cyberbeveiligingswet (Cbw), onder coördinatie van de minister van Justitie en Veiligheid. In de concepttekst van deze wet is voorzien dat de minister van Onderwijs, Cultuur en Wetenschap, in overleg met Justitie en Veiligheid, hbo- en wo-instellingen kan aanwijzen als essentiële of belangrijke entiteiten. Dit maakt het voor deze instellingen verplicht om cyberrisico's structureel te beheersen en versterkt zo de digitale veiligheid van het onderwijs.

2. Wat is het beoogde doel?

Toelichting

Hulpvragen

a) Wat zijn de beleidsdoelen?

Met de implementatie van de Cbw worden algemene eisen gesteld aan de organisaties die onder het toepassingsbereik vallen. Echter, verschillende sectoren vallen onder de wet en moeten aan deze eisen voldoen. Om ervoor te zorgen dat deze eisen duidelijk en toegespitst zijn op de betreffende sectoren, worden deze eisen in de regelingen sectorspecifiek gemaakt. Met de onderhavige regeling worden de eisen die voortvloeien uit onder andere de zorgplicht en meldplicht nader uitgewerkt. Dit omvat het nader uitwerken van de drempelwaarden voor het melden van significante incidenten, het nader uitwerken van de aanwijzing van het CSIRT en het feit dat de IvhO zal toezien op de naleving van de wet.

b) Aan welke duurzame ontwikkelingsdoelen (sustainable development goals, SDG's) en brede welvaartsuitkomsten dragen de doelen bij?

n.v.t.

3. Wat zijn opties om het doel te realiseren?

Toelichting

Hulpvragen

a) Wat zijn kansrijke aangrijpingspunten om het doel te realiseren?

De Cbw, de Cbb en de sectorspecifieke regeling resulteren in een wettelijke verankering die aansluit op de doelen die zijn gesteld in de Cybersecuritystrategie 2022-2028 van het NCSC. Het doel wordt bereikt door onder meer plichten op te leggen aan entiteiten, zoals de verplichting tot het treffen van passende en evenredige maatregelen en het melden van significante cyberincidenten. Naast deze plichten zijn er ook rechten voor de belangrijke entiteiten in het bekostigde hoger onderwijs, zoals het recht op bijstand vanuit de CSIRT. Dit zijn aangrijpingspunten om de sector hoger onderwijs als geheel digitaal weerbaarder te maken en om de digitale veerkracht te verhogen. Dit is vooral belangrijk nu er sprake is van toenemende complexiteit in het dreigingsbeeld.

De implementatie van de Cbw en het verhogen van digitale weerbaarheid zullen de basisprincipes vormen om een effectieve barrière te creëren tegen vele verschillende aanvallen van kwaadwillenden in de digitale omgeving.

b) Wat zijn, gegeven de aangrijpingspunten, kansrijke beleidsopties?

Zie 3a

c) Wat is de beleidstheorie (doelenboom) per kansrijke beleidsoptie?

n.v.t.

4. Wat zijn de gevolgen van de opties?

Toelichting

Hulpvragen

a) Wat zijn de verwachte gevolgen per beleidsoptie?

Met de implementatie van de Cbw en de onderliggende wetgeving wordt het doel bereikt om organisaties te stimuleren tot het verhogen van hun digitale weerbaarheid. Dit heeft als gevolg dat de organisaties die onder het toepassingsbereik van de wet vallen een verhoging in regeldrukeffecten zien. Dit is vanwege de investeringen en inspanningen die gedaan moeten worden om aan de verplichtingen te voldoen, denk hierbij aan o.a. de zorgplicht en de meldplicht.
Daarnaast zullen er toezichts- en handhavingskosten plaatsvinden voor de bevoegde autoriteit in het toezien op de wet, hiervoor zal de IvhO een UHT uitvoeren om dit ook voor de regeling verder in kaart te brengen. Verder zullen ook uitvoeringseffecten en -kosten ontstaan voor het aangewezen CSIRT.

b) Welke verplichte toetsen zijn van toepassing en wat zijn daarvan de uitkomsten (voor zover bekend)?

Deze regeling wordt uitgezet voor openbare internetconsultatie, parallel zal het traject van de uitvoeringstoets en algemene toets regeldruk plaatsvinden.

5. Wat is de voorkeursoptie?

Toelichting

Hulpvragen

a) Wat is het voorstel?

Voor het traject om de NIS2-richtlijn te implementeren kent deze wet drie lagen: de Cbw, het Cbb en de Cyberbeveiligingsregeling hoger onderwijs. De wet en het besluit zijn al in een internetconsultatie geweest en bevinden zich in een verder stadium van het proces. Dit werd vanuit de coördinerende rol van het ministerie van JenV begeleid en geregeld. Nu zijn de vakdepartementen aan de beurt om een sectorspecifieke regeling op te stellen die de vereisten uit de wet en het besluit nader uitwerken.

De nader uitgewerkte eisen die in de Cyberbeveiligingsregeling hoger onderwijs worden opgenomen, moeten worden geconsulteerd met het veld. Hierdoor krijgt het veld de mogelijkheid om input te leveren aan bijvoorbeeld de drempelwaarden voor het melden van een significant cyberincident.

b) Hoe houdt het voorstel rekening met:

- doeltreffendheid en doelmatigheid;
- uitvoerbaarheid voor alle relevante partijen (inclusief doenvermogen, regeldruk en handhaving);
- brede maatschappelijke impact?

Deze regeling betreft een nadere uitwerking van het reeds bij de Tweede Kamer ingediende wetsvoorstel, waarvoor een beleidskompas is ingevuld. De inhoudelijke keuzes die aan de basis van deze regeling liggen, zijn reeds gemaakt in het kader van dat wetsvoorstel. Met de inwerkingtreding van de Cbw, zal deze naar verwachting een stevige impuls geven aan de versterking van de digitale weerbaarheid van Nederland. Dit gebeurt door organisaties, op wie de wet van toepassing is, te verplichten cyberbeveiligingsmaatregelen te treffen en ernstige incidenten te melden.
Dit betekent dat de belangrijke entiteiten in het hoger onderwijs hun digitale weerbaarheid op orde moeten hebben.
Bij de uitwerking van deze regeling is rekening gehouden met de regeldruk en de uitvoerbaarheid.

c) Wat zijn de risico's en onzekerheden van dit voorstel?

n.v.t.

d) Hoe ziet de voorgenomen monitoring en evaluatie eruit?

n.v.t.