vewin vereniging van waterbedrijven in Nederland

Ministerie van Justitie en Veiligheid via
internetconsultatie.nl

Datum	:	1 juli 2024
Onderwerp	:	Reactie Consultatie NiS2/Cbw
Ons kenmerk	:	96378/MB
Voor informatie	:	Mariëlle Basten
		basten@vewin.nl
		070 3490 883
Bijlage(n)	:	-

Geachte heer, mevrouw,

Inleiding
Op 21 mei 2024 is een consultatie gestart voor de implementatie van de Europese richtlijnen 2022/2555 (hierna genoemd: NiS2) en 2022/2557 (hierna genoemd: CER). De Europese Unie verplicht de lidstaten op grond van het Verdrag betreffende de Werking van de Europese Unie om richtlijnen te implementeren in nationale wetgeving. U heeft ervoor gekozen om de NiS2 te implementeren in de Cyberbeveiligingswet (hierna genoemd: Cbw) en de CER in de Wet weerbaarheid kritieke entiteiten (hierna genoemd: Wwke).

Vewin heeft twee zienswijzen ingediend voor zowel de Cbw als de Wwke. Deze zienswijze van Vewin betreft de Cbw. Aangezien de Cbw voor de drinkwatersector een essentiële wet is, maakt Vewin graag gebruik van deze consulatie.

Algemene opmerkingen vooraf
De drinkwatersector is in het algemeen positief over de NiS2 en het voorliggende wetsvoorstel ter implementatie van de NiS2 in de Cbw. Het doel van de NiS2-richtlijn is "*om een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie te bereiken, teneinde de werking van de interne markt te verbeteren.*" Dit ziet Vewin terug in het wetsvoorstel en de Memorie van Toelichting (hierna genoemd: MvT).

Vewin heeft een aantal algemene aandachtspunten die wij graag met u delen.

Samenhang Cyberbeveiligingswet en de Wet weerbare kritieke entiteiten
Vewin wil als eerste aandachtspunt de samenhang tussen de Cbw en de Wwke benoemen. In de MvT beperkt de Cbw zich tot netwerk- en informatiesystemen, inclusief de fysieke omgeving. De Wwke richt zich op natuurlijke en door de mens veroorzaakte risico's die negatieve gevolgen kunnen hebben voor de verlening van essentiële diensten. Beide wetsvoorstellen kennen een zorgplicht, een meldplicht en een eigen toezichtregime.

Voor de effectiviteit, de doelstelling, de omvang en aard van de NiS2-richtlijn is het belangrijk dat de verplichtingen uit de Cbw, Wwke en sectorale wet- en regelgeving zoveel mogelijk op elkaar worden afgestemd en uitwerking van de vereisten uit de Cbw plaatsvindt in lagere sectorale wet- en regelgeving. Voor Vewin is het belangrijk dat één integraal kader blijft bestaan voor de drinkwatersector en aansluiting wordt gezocht bij bestaande planvorming. Daarnaast pleit Vewin

dat één loket voor alle meldplichten wordt ingericht om dubbele verplichtingen en lastendruk tegen te gaan.

Ook pleit Vewin ervoor om in lagere regelgeving expliciet vast te leggen dat bij entiteiten die onder beide wetten vallen, het toezicht op de naleving van de verplichtingen uit de Cbw, Wwke en Drinkwaterrichtlijn[1] zo wordt ingericht dat dit plaatsvindt op basis van één overkoepelende en integrale risicoanalyse en één pakket aan (aanvullende) maatregelen.

Uitbreiding reikwijdte zorgplicht en meldplicht
De reikwijdte van de zorgplicht en de meldplicht wordt met de NiS2 uitgebreid van netwerk- en informatiesystemen die gebruikt worden voor de essentiële dienstverlening, naar alle netwerk- en informatiesystemen die entiteiten gebruiken voor hun werkzaamheden of dienstverlening, inclusief de fysieke omgeving.

Vewin is blij dat een risicogerichte benadering expliciet is opgenomen in het voorliggende wetsvoorstel. Vewin ziet graag dat deze risicogerichte benadering en aanpak ook als uitgangspunt wordt gehanteerd bij de nadere uitwerking van de zorgplicht en meldplicht in lagere sectorale wet- en regelgeving en de inrichting van het toezicht.

Eén centraal meldloket
Vewin adviseert de wetgever om één centraal meldloket in te richten van waaruit meldingen kunnen worden doorgezet naar de toezichthouder en het computer security response team (hierna genoemd: CSIRT) met als doel de lastendruk tegen te gaan.

Borgen van vertrouwelijke informatie:
Artikel 65 lid 1 en 2 van het concept wetvoorstel luidt

1. De bevoegde autoriteit, het centrale contactpunt, het CSIRT en Onze Minister kunnen elkaar, de bevoegde autoriteit, bedoeld in artikel 60, de bevoegde autoriteit van een andere lidstaat van de Europese Unie die op grond van artikel 8 van de NIS2-richtlijn als zodanig is aangewezen in het nationale recht van die lidstaat, een andere toezichthoudende autoriteit die krachtens Unierecht of nationaal recht ter uitvoering van Unierecht is aangewezen of ingesteld en de Europese Commissie vertrouwelijke gegevens verstrekken, doch uitsluitend voor zover:
   a. dat noodzakelijk is ter uitvoering van hun taken uit hoofde van deze wet;
   b. de verstrekking beperkt blijft tot die vertrouwelijke gegevens die noodzakelijk zijn en verstrekking evenredig is aan het doel van die verstrekking;
   c. de vertrouwelijkheid van die vertrouwelijke gegevens is gewaarborgd;
   d. de veiligheids- en commerciële belangen van de betrokken entiteit worden beschermd.

Vewin vraagt zich af wat wordt verstaan onder 'vertrouwelijke' gegevens? En onder welke voorwaarden kunnen deze gegevens tussen de in het artikel opgenomen bevoegde autoriteit, het centrale contactpunt, het CSIRT, de Minister en de Europese Commissie worden uitgewisseld?

[1] De Drinkwaterrichtlijn is geïmplementeerd in het Drinkwaterbesluit.

Een zorgpunt is of de vertrouwelijkheid van informatie bij rapportageverplichtingen vanuit de lidstaten aan de Europese Commissie, voldoende kan worden gewaarborgd. In de Europese Unie is de transparantie en openbaarmaking van documenten geregeld in Verordening (EG) 1049/2001.[2] Deze verordening gaat uit van het principe dat een zo ruim mogelijke toegang tot documenten wordt gewaarborgd.

Op basis van Europese regelgeving en een uitspraak van het Hof van Justitie[3], is er een aanzienlijk risico dat als een beroep wordt gedaan op het openbaar maken van documenten en/of gegevens, informatie over de vitale infrastructuur die in Nederland als vertrouwelijk wordt aangemerkt, (bijvoorbeeld locaties van winputten), alsnog openbaar moet worden gemaakt.

Vewin wil voorkomen dat de situatie zoals hierboven omschreven kan ontstaan en informatie die in Nederland als vertrouwelijk wordt gekwalificeerd, in verband met rapportageverplichtingen aan de Europese Commissie, alsnog openbaar gemaakt moet worden. Het verzoek van Vewin is om in het wetsvoorstel en/of de MvT nader in te gaan hoe de vertrouwelijkheid van informatie van essentiële entiteiten zal worden gewaarborgd.

Vewin wil de wetgever wijzen op de mogelijkheid van de Europese wetgever om deze vertrouwelijke documenten op voorhand aan te merken als 'TOP SECRET", "SECRET".[4] Dit maakt het voor de Europese Commissie eenvoudiger om vertrouwelijke informatie uit Nederland te beschermen tegen openbaarmaking. Vewin vraagt zich af of hiermee in alle gevallen de vertrouwelijkheid in Europees verband kan worden gewaarborgd.

Specifieke aandachtspunten en implementatieproces

Zorgplicht

In het wetsvoorstel is over de zorgplicht opgenomen: "Iedere essentiële entiteit en belangrijke entiteit neemt passende en evenredige technische, operationele en organisatorische maatregelen om de risico's voor de beveiliging van de netwerk- en informatiesystemen, die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruikt, te beheersen. Ook neemt zij deze maatregelen om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van haar diensten en voor andere diensten te beperken."

Vewin onderschrijft het uitgangspunt dat de drinkwaterbedrijven zelf verantwoordelijk zijn voor het vaststellen welke maatregelen passend en evenredig zijn om de risico's, waarmee zij geconfronteerd kunnen worden, beheersbaar te houden. De drinkwatersector vindt het cruciaal dat kan worden aangesloten bij en voortgeborduurd op de bestaande systematiek, werkwijzen en normenkaders die worden gehanteerd voor reeds bestaande wettelijke verplichtingen. Het is de taak van de toezichthouder om vervolgens te beoordelen of de genomen maatregelen voldoende zijn om de risico's te mitigeren en/of de weerbaarheid van de drinkwaterbedrijven voldoende is

[2] Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie.

[3] [3] HvJ EU 28 november 2013, Case C-576/12 P, ECLI:EU:C:2013:777 (*Jurašinović tegen de Raad*) r.o. 45.

[4] Artikel 9(1) Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie.

gewaarborgd. Een risico-gebaseerde aanpak zou daarbij het uitgangspunt moeten zijn. De drinkwatersector heeft zelf de meeste kennis van haar systemen en risico's.

Meldplicht
Vewin pleit ervoor dat een proportionele en risico-gebaseerde drempelwaarde voor de meldplicht van significante incidenten wordt vastgesteld. Dit heeft te maken met de lastendruk die de meldplicht met zich meebrengt. SMART geformuleerde drempelwaarden kunnen daarbij helpen om eventuele discussies in de praktijk tussen entiteiten, CSIRT's of toezichthouders te voorkomen.

Vewin wil graag bij de totstandkoming van de AMvB worden betrokken en meewerken aan de totstandkoming en/of vaststelling van de parameters om de drempelwaarde(n) voor de meldplicht te bepalen. Dit is voor de drinkwatersector essentieel, omdat zij beschikt over de kennis om te beoordelen of de continuïteit van de essentiële dienstverlening en leveringszekerheid in gevaar komt of dreigt te komen.

Wat Vewin opvalt is dat in artikel 42 lid 2 is gekozen om informatie over vrijwillige meldingen van (bijna-) incidenten van een essentiële entiteit die tevens een kritieke entiteit is onder de Wwke, door te zetten naar de toezichthouder. Wanneer het Computer Security Incident Respons Team (CSIRT) vrijwillige meldingen gaat doorzetten naar de toezichthouder onder de Wwke, zal de bereidheid bij bedrijven om vrijwillig te melden aanzienlijk afnemen. Vewin pleit ervoor om het aan de bedrijven zelf over te laten of zij de toezichthouder willen informeren. Het systeem van vrijwillig melden moet gericht blijven op leren en verbeteren in een vertrouwelijke setting.

Informatieverstrekking online registratievoorziening en nationale register
In artikel 45 van het wetsvoorstel is opgenomen dat een essentiële, belangrijke entiteit en een entiteit die domeinnaamregistratiediensten verleent, via een daarvoor opgezet mechanisme (online registratievoorziening) informatie (adres- en contactgegevens, telefoonnummers IP-bereiken, bij AMvB genoemde gegevens etc.) verstrekt voor het nationale register.

Voor onze sector zijn waarborgen vanuit het Rijk rondom de digitale en fysieke beveiliging van de online registratievoorziening en het nationale register van belang, omdat in dit online registratievoorziening/register zeer veel vertrouwelijke informatie van zeer veel bedrijven wordt opgeslagen; dit brengt een groot en potentieel cyberrisico met zich mee. Ook is nu onduidelijk wie toegang heeft en/of krijgt tot deze data?

Toezicht en handhaving
Vewin is het eens dat de wetgever heeft gekozen voor behoud van sectoraal toezicht dat wordt belegd bij het vakdepartement, het ministerie van IenW. Gezien de juridische samenhang tussen de Cbw en Wwke pleit Vewin voor een risico-gebaseerde samenhangende aanpak in het toezicht op de uitvoering van de verplichtingen uit beide wetten.

Governance
Vewin heeft een aantal aandachtspunten met betrekking tot de governance.

Definitie:
Vewin pleit ervoor om in de begripsbepaling van het wetsvoorstel een definitie op te nemen wie worden bedoeld met de 'leden van het bestuur'. Nu is onduidelijk of daaronder ook de (leden van) de Raad van Commissarissen en/of Dagelijks Bestuur vallen?

Beveiliging toeleveringsketen
In paragraaf 5.3.4 van de MvT wordt ingegaan op de beveiliging van de toeleveringsketen[5]. Het gaat dan ook over beveiliging gerelateerde aspecten met betrekking tot de relaties tussen de entiteit en haar rechtstreekse leveranciers of dienstverleners.

Vewin vraagt zich af hoever deze verantwoordelijkheid reikt? Beperkt de zorgplicht van de entiteit zich alleen tot de partij waarmee ze zelf een overeenkomst aangaat of gaat deze verantwoordelijkheid verder? Hoe wordt voorkomen dat leveranciers van de kernfunctionaliteit, waaraan de entiteit behoefte heeft en die veilig moet blijven, zich onttrekken aan hun verantwoordelijkheid door een schil van tussenpartijen te gebruiken die de relatie met de entiteit onderhouden? Vewin heeft behoefte aan meer duiding van de zorgplicht op dit punt. Hier kan invulling aan worden gegeven in een leidraad van de toezichthouders.

Kennis en vaardigheden Bestuur
Daarnaast onderschrijft Vewin dat bestuursleden een cruciale rol spelen in het neerzetten van een sterke cyberweerbaarheidscultuur binnen hun entiteit, en zelf over voldoende kennis en vaardigheden moeten beschikken om cybersecurity risico's te (kunnen) identificeren, en de risicobeheerspraktijken en gevolgen daarvan te kunnen beoordelen.

Vewin is echter van mening dat van bestuursleden -gezien hun positie, rol en verantwoordelijkheden-, mag worden verwacht dat zij ervoor zorgen dat ze beschikken over de kennis en vaardigheden die nodig is om te voldoen aan de eisen uit de Cbw. Door heel specifiek voor te schrijven hoe entiteiten hieraan invulling moeten geven -aantoonbaar door het overleggen van een certificaat-, gaat de wetgever in onze ogen te ver.

Vewin pleit ervoor om in het wetsvoorstel geen specifieke eisen op te nemen over hoe hieraan het beste invulling kan worden gegeven. Het past in onze ogen beter om suggesties hierover een plek te geven in de MvT en de wijze waarop hieraan invulling wordt gegeven over te laten aan de entiteit zelf. In lijn met het voorgaande is het dan aan de toezichthouder om hierover eventuele nadere afspraken te maken met de entiteit en te beoordelen of het bestuur aan deze vereisten heeft voldaan.

---

[5] Artikel 21 lid 2, onderdeel d en lid 3 NIS2 richtlijn en artikel 23 Cbw.

Ons kenmerk: 96378/MB

Kennisniveau in relatie tot bestuursaansprakelijkheid

Vewin vindt het wenselijk dat in paragraaf 5.4 van de MvT meer context wordt gegeven over verwachtingen met betrekking tot het (vereiste) kennisniveau van bestuurders en hoe dit zich verhoudt tot de bestuurdersaansprakelijkheid. Wanneer beschikken bestuurders bijvoorbeeld over voldoende kennis en vaardigheden en op basis waarvan wordt dat getoetst? En mag en kan de bestuurder bijvoorbeeld leunen op of delegeren aan een (gecertificeerd) CISO?

Inzet handhavingsinstrumentarium

De Cbw hanteert voor essentiële entiteiten twee bestuursrechtelijke handhavingsinstrumenten, te weten: een last onder bestuursdwang en/of een bestuurlijke boete. Daarnaast kan een bevoegde autoriteit ook bij de (burgerlijke) rechter een verzoek tot schorsing van een bestuurslid indienen en/of een verzoek tot schorsing van de certificering of vergunning van een essentiële entiteit. Het juridisch handhavingsinstrumentarium om naleving van de Cbw te effectueren is uitgebreid (bestuursrecht, privaatrecht en strafrecht) en daarom vindt Vewin het wenselijk dat in de toelichting meer duidelijkheid wordt gegeven over de inzet van dit instrumentarium (wanneer wat wordt ingezet).

Wij stellen het op prijs als deze zienswijze en onze positie wordt betrokken bij de totstandkoming van de Cbw.

Met vriendelijke groet,

drs. J.H. de Groene
Directeur