UNIE VAN WATERSCHAPPEN

Bijlage
CBCF 23-77

Agendapunt
17.12

Update diverse ontwikkelingen informatieveiligheid

In deze mededeling vindt u een update over vier onderwerpen, namelijk de Europese richtlijnen NIS2 en CER, de externe audit op informatiebeveiliging en privacy van dit najaar, de omgang met applicaties uit landen met een offensief cyberprogramma (appbeleid) en een uitnodiging voor de bestuurlijke cybertafel van de overheidsbrede cyberoefening in november a.s..

1. Update Europese richtlijnen NIS2 en CER

De nieuwe Netwerk- en Informatiebeveiliging Richtlijn (NIS2, ook bekend als NIB2)[1] en de Critical Entities Resilience (CER)[2] worden per 18 oktober 2024 van kracht. De waterschappen moeten op dat moment voldoen aan deze twee richtlijnen. Momenteel worden deze richtlijnen omgezet in Nederlandse wetgeving. In het vierde kwartaal van dit jaar zal de conceptwet in consulatie gebracht worden.
Onder de NIS2 moet ook voldaan worden aan toezicht, meldplicht en zorgplicht. Hier wordt momenteel vorm aan gegeven door o.a. de ministeries van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en Infrastructuur en Waterstaat (IenW). Het is op dit moment nog onduidelijk welke partij de toezichthouder wordt voor de waterschappen.

Afvalwater in NIS2 en CER

In de NIS2 en CER staat afvalwater benoemd als sector waarvoor de Europese richtlijnen gaan gelden. In de NIS2 is afvalwater een essentiële entiteit. In de CER wordt afvalwater benoemd als kwetsbare infrastructuur. Dit betekent dat in de Nederlandse wetgeving mogelijk zal worden vastgesteld dat afvalwater een nationaal vitaal proces is. In de CER zal dit betekenen dat waterschappen moeten worden gezien als kritieke entiteiten en dienen te voldoen aan de eisen volgend uit de CER richtlijn. Voor de NIS2 geldt dat de informatiebeveiliging van het afvalwaterproces moet voldoen aan de in de richtlijn gestelde eisen.
Na de zomer start het proces voor herijking van de vitale afvalwatersector. De vorige herijking vond plaats in 2018-2019. De conclusie was toen dat het proces niet ‘vitaal’ was. Belangrijkste reden is hiervoor dat er geen grote aantallen chronisch zieken of doden zullen vallen na een cyberaanval. We hebben wel toen aangegeven dat we het proces afvalwater zeer serieus nemen en alle veiligheidsmaatregelen zullen nemen die we noodzakelijk achten. Het is verplicht om de herijking van het afvalwater proces als vitale infrastructuur om de vijf jaar te herzien. Deze herijking zal gedaan worden door IenW en de Unie met betrokkenheid van waterschapsmedewerkers uit het primaire proces afvalwater.

Invulling sectorale CSIRT door CERT-WM

De Nederlandse overheid (ministerie van Justitie en Veiligheid) wil invulling geven aan de NIS2 met een stelsel van landelijke en sectorale CSIRT’s (Computer Security Incident Response Teams). Het idee is dat één van die CSIRT’s de sector ‘water’ gaat bedienen. Vanuit het gezamenlijke programma “versterken cyberweerbaarheid in de watersector”, onder regie van IenW, is een onderzoek gestart naar de mogelijkheden van een CSIRT voor de watersector. Hierbij wordt gedacht om het bestaande CERT-WM uit te bouwen en daarmee mogelijk te positioneren als het CSIRT voor de watersector. We zijn hierover in gesprek met IenW. Hier zijn collega’s vanuit de waterschappen en het programma Informatieveiligheid & Privacy (IV&P) van het Waterschapshuis (hWh) bij betrokken.

---

[1] De NIS2 richt zich op risico's die netwerk- en informatiesystemen bedreigen, zoals cyberbeveiligingsrisico's, en moet bijdragen aan een hoger niveau van informatieveiligheid bij organisaties. De NIS2 is de opvolger van de eerste NIS-richtlijn die in 2016 in Nederland is opgenomen in de Wet beveiliging netwerk- en informatiesystemen (Wbni).

[2] De CER richt zich op de bescherming van publieke en private organisaties tegen fysieke risico's, zoals de gevolgen van misdrijven, sabotage en natuurrampen. Deze richtlijn gaat aanbieders van vitale processen beschermen door het verhogen van hun weerbaarheid en veerkracht. Hiermee blijft de continuïteit van de processen beter geborgd. De richtlijn richt zich op fysieke veiligheid en beveiliging van vitale processen.

Lobby voor meer duidelijkheid NIS2 richtlijn

Samen met het Interprovinciaal Overleg (IPO) en de Vereniging Nederlandse Gemeenten (VNG) heeft de Unie inbreng geleverd aan de Tweede Kamer voor het commissiedebat online veiligheid van 29 juni jl.[3] Dit is een vervolg op onze eerdere inbreng aan de Tweede Kamer op 5 april jl.[4] Dit heeft geleid tot een aangenomen motie met de oproep om medeoverheden zo snel mogelijk duidelijkheid te geven over de scope en focus van de NIS2-richtlijn. Hierover is op de website van de Unie een nieuwsbericht geplaatst: https://unievanwaterschappen.nl/motie-aangenomen-voor-meer-duidelijkheid-nieuwe-cyberrichtlijn/.
We zijn met IPO en VNG in contact om deze lobby door te zetten. We zetten in op helderheid, gezamenlijkheid en tijdigheid. Ook zijn we met IPO en VNG een actie gestart om de beschikbare informatie in kaart te brengen, om zo meer duidelijkheid te creëren. Dit zorgt hopelijk voor meer inzicht voor de waterschappen, terwijl we het Rijk blijven oproepen om meer duidelijkheid en informatie.

Voorbereiding op NIS2 en CER bij de waterschappen

Om tijdig te voldoen aan de NIS2 en CER kunnen de waterschappen zich alvast voorbereiden door te werken aan de aandachtspunten op gebied van informatieveiligheid bij het eigen waterschap. De verbeterpunten uit de vorige en aankomende audit vormen een goede indicatie voor waar de waterschappen hun werkzaamheden op kunnen richten.
Indien aan volwassenheidsniveau 4 wordt voldaan, is het waterschap het beste voorbereid op de komst van de NIS2 richtlijn. De Cyber Security Implementatie Richtlijn (CSIR)[5] biedt ook goede handvatten voor goede informatiebeveiliging bij de waterschappen en in de keten.

2. Externe audit informatiebeveiliging en privacy

Als waterschappen hebben we de bestuurlijke ambitie gesteld om te voldoen aan volwassenheidsniveau 4 van de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG). Onderdeel van deze afspraak is deelname aan een externe audit. Dit najaar volgt er weer een externe audit op informatiebeveiliging en privacy (BIO/AVG). Deze audit wordt uitgevoerd door VKA en gecoördineerd vanuit het hWh.

Animatie ambitie volwassenheidsniveau 4

Het programma IV&P van hWh heeft een animatie gemaakt over volwassenheidsniveau 4 van de BIO. Deze animatie is bedoeld ter ondersteuning van de waterschappen bij het realiseren van deze ambitie. De animatie kan hier bekeken worden: https://youtu.be/vRonBBhyP8M.

3. Omgang met applicaties uit landen met een offensief cyberprogramma op zakelijke apparatuur (Appbeleid)

Recent hebben de waterschappen een standpunt vastgesteld over omgang met applicaties vanuit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen. Hierover is een ledenbrief verstuurd naar de waterschappen.[6] Vanuit de waterschappen hebben we aangegeven mee te denken met het Rijk over een lijst met onveilige applicaties en een afwegingskader. In oktober a.s. volgt een vervolgoverleg met het Rijk en de koepels over dit initiatief. Wanneer de lijst met onveilige applicaties (nu bestaande uit TikTok) uitgebreid wordt, zullen we de waterschappen hiervan op de hoogte brengen.

4. Bestuurlijke cybertafel 2023

Op woensdagmiddag 22 november 2023 wordt de bestuurlijke cybertafel ‘een cyberoefening in de waterketen’ georganiseerd in Amersfoort. Deze cybertafel is het vervolg op de eerdere edities uit 2021 en

[3] https://unievanwaterschappen.nl/meer-duidelijkheid-informatieveiligheid/
[4] https://unievanwaterschappen.nl/medeoverheden-vragen-het-rijk-om-meer-duidelijkheid-nieuwe-cyberrichtlijnen/
[5] https://www.cert-wm.nl/csir
[6] https://unievanwaterschappen.nl/unie-van-waterschappen-roept-waterschappen-op-tiktok-te-verbieden/

2022 en wordt georganiseerd door het programma ‘Versterken cyberweerbaarheid in de watersector’ van IenW.

Programma

Tijdens de bestuurlijke cybertafel zal een scenario doorgespeeld worden, gericht op de rol van de bestuurder. Dit wordt begeleid door experts van Fox-IT die ook de landelijke ‘ISIDOOR oefening’ begeleiden. Het programma begint vanaf 13.15 uur met een lunch en om 14.00 uur wordt gestart met een plenaire opening. Om 14.15 uur vindt het oefenscenario plaats en na een korte wrap-up zal om 16.00 uur geëindigd worden met een netwerkborrel.

Aanmelden voor de bestuurlijke cybertafel

Voorkennis is niet van belang, iedere bestuurder kan deelnemen. Doel van deze tafel is om van elkaar te leren en nieuwe inzichten op te doen die meegenomen kunnen worden in de eigen organisatie.
De bestuurlijke cybertafel is exclusief bedoeld voor bestuurders en directieleden in de watersector (waaronder waterschappen, gemeenten, provincies en drinkwaterbedrijven) om kennis te delen en met elkaar in gesprek te gaan over informatieveiligheid. Via dit formulier kunt u zich aanmelden voor de bestuurlijke cybertafel: link.