UNIE VAN WATERSCHAPPEN

BEZOEKADRES
Koningskade 40
2596 AA Den Haag
070 351 97 51
Nederland

POSTADRES
Postbus 93218
2509 AE Den Haag
Nederland

Aan de leden-waterschappen
Cc: belastingsamenwerkingen

datum	ons kenmerk	contactpersoon
15 december 2023	00122663/KTC	mw. N. de Keijzer
bijlage(n)	uw kenmerk	e-mail
2	-	nkeijzer@uvw.nl

betreft
Ontwikkelingen informatieveiligheid waterschappen

Geachte leden-waterschappen,

Op dit moment gebeurt er veel op het gebied van informatieveiligheid. Via deze ledenbrief wil ik u graag over twee belangrijke ontwikkelingen informeren: de Netwerk- en informatiebeveiligingsrichtlijn (NIB2, ook bekend als NIS2) en het onderzoek naar een sectoraal Computer Security Incident Response Team (CSIRT).

Netwerk- en Informatiebeveiligingsrichtlijn (NIS2)
De NIS2 is in november 2022 aangenomen door het Europees Parlement en de Raad van de EU. Deze richtlijn is bedoeld om de cyberveiligheid en de weerbaarheid van essentiële diensten in de EU-lidstaten te verbeteren. De NIS2 vergroot de reikwijdte van de eerste NIS richtlijn door meer sectoren te omvatten. Zo vallen de sectoren 'afvalwater' en 'overheidsdiensten' onder de bepalingen van de NIS2, waardoor de waterschappen zowel via het ministerie van Infrastructuur en Waterstaat (IenW) als via het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) onder de reikwijdte van de richtlijn komen te vallen. Daarnaast stelt de richtlijn strengere beveiligingsnormen en meldingsvereisten voor incidenten. Ook stelt de NIS2 de bestuursorganen verantwoordelijk voor het toezien op de uitvoering van de NIS2. Daarmee worden bestuurders aansprakelijk voor de weerbaarheid van hun organisatie.
De lidstaten hebben 21 maanden de tijd om de richtlijn om te zetten in nationale wetgeving. De datum waarop de NIS2 in werking treedt is 17 oktober 2024.

In Nederland wordt de Europese richtlijn op dit moment omgezet in nationale wetgeving in de vorm van een aanpassing van de Wet beveiliging netwerk- en informatiesystemen (Wbni) en lagere regelgeving. Dit gebeurt onder coördinatie van de minister van Justitie en Veiligheid. De Unie van Waterschappen en het programma Informatieveiligheid & Privacy van het Waterschapshuis hebben hierover contact met het ministerie van BZK als stelselverantwoordelijke voor de sector overheid en met het ministerie van IenW als verantwoordelijk ministerie voor weg- en waterbeheer (o.a. afvalwater).

Onlangs heeft de Unie van Waterschapen een brief van het ministerie van BZK over de implementatie van de NIS2 richtlijn ontvangen (bijlage 1). In deze brief wordt bevestigd dat de waterschappen onder de reikwijdte van de richtlijn vallen. Dit heeft de volgende consequenties:

1. *Toezicht en verantwoording*
   De NIS2 richtlijn verplicht dat onafhankelijk toezicht wordt uitgeoefend. Hiertoe wil het ministerie van BZK maximaal gebruik maken van bestaande toezichts- en verantwoordingsinstrumenten en waar nodig deze instrumenten versterken en optimaal op elkaar laten aansluiten. De Rijksinspectie Digitale Infrastructuur (RDI) gaat toezicht houden op het hele stelsel van informatieveiligheid voor de sector overheid en baseert zich daarbij mede op de informatie die voortkomt uit de bestaande verantwoordings- en toezichtstructuren.
   Ook al wordt er in de brief voornamelijk over de Eenduidige Normatiek Single Information Audit (ENSIA) van de gemeenten gesproken, voor de waterschappen geldt dat het ministerie de bestaande informatieveiligheid en privacy audit in beeld heeft als toezichts- en verantwoordingsinstrument.

2. *Meldplicht*
   De NIS2 richtlijn verplicht lidstaten om in nationale wet- en regelgeving te voorzien in een meldplicht bij cybersecurityincidenten 'met aanzienlijke gevolgen'. Er moet worden gemeld aan de toezichthouder en aan het eigen Computer Security Incident Response Team (CSIRT).
   In het geval van de waterschappen ligt het in de lijn der verwachting dat het bestaande Computer Emergency Response Team Watermanagement (CERT-WM) de rol van CSIRT, zoals bedoeld in de NIS2, gaat vervullen, ook gezien het feit dat het CERT-WM in 2020 bij ministeriële regeling in het kader van de Wbni aangewezen is. Randvoorwaarde hiervoor is wel dat het helder moet worden wat de exacte taken en verantwoordelijkheden van de sectorale CSIRT's onder de nieuwe wetgeving gaan worden. Tevens zal het CERT-WM, dat onder de paraplu van het Waterschapshuis valt, opdracht voor deze taakuitbreiding moeten krijgen.

3. *Zorgplicht*
   Voor overheden gaat een zorgplicht voor informatieveiligheid gelden. De bestaande Baseline Informatiebeveiliging Overheid (BIO) wordt wettelijk verankerd als sectoraal kader voor de gehele overheid onder NIS2. Toepassing van de BIO krijgt hiermee prioriteit binnen de overheid.

Meer informatie over de NIS2 is op 12 oktober jl. gedeeld via een webinar, dat u terug kunt kijken via de website Weerbare Digitale Overheid: https://www.weerbaredigitaleoverheid.nl/programma-onderdelen/sessie/259c8281/.
Binnenkort gaan een internetconsultatie en een Uitvoerbaarheidstoets Decentrale Overheden van start. De resultaten hiervan worden gepubliceerd en waar mogelijk verwerkt in de wetsvoorstellen. Zodra hier meer over bekend is, zullen we deze informatie met u delen en om uw medewerking vragen zodat al uw zorgen over de implementatie van de NIS2 richtlijn goed in de consultatie en uitvoerbaarheidstoets worden meegenomen.

Onderzoek sectoraal CSIRT
Als er sprake is van een dreiging of een incident in netwerk- en informatiesystemen van vitale aanbieders, onderdelen van het Rijk of digitale dienstverleners, dan zijn er computercrisisteams die hulp verlenen. Deze teams worden in de NIS2 aangeduid als Computer Security Incident Response Teams (CSIRT).

Het ministerie van IenW heeft de Unie van Waterschappen in september 2023 een brief gestuurd over de uitwerking van een businesscase voor een sectoraal CSIRT voor de gehele watersector, dat wil zeggen voor waterschappen, Rijkswaterstaat en drinkwaterbedrijven (bijlage 2). Samen met de sector zullen de haalbaarheid, wenselijkheid en randvoorwaarden voor een sectoraal CSIRT onderzocht worden. In dit sectorale CSIRT kunnen mogelijk de huidige taken van het CERT WM als wel de toekomstige taken, die benoemd worden in de NIS2 richtlijn, opgenomen worden.

Als de uitkomst van de businesscase positief is, er draagvlak is in de sector en de randvoorwaarden kunnen worden ingevuld zal de oprichting van een sectoraal CSIRT ter besluitvorming voorgelegd worden aan bestuurlijke gremia. De besluitvorming bij de waterschappen zal via de Werkgroep Bedrijfsvoering, Digitalisering en Dienstverlening (WBDD) en Commissie Bestuurszaken Communicatie en Financiën (CBCF) van de Unie van Waterschappen verlopen. Het Uitvoerend Overleg (UO) van het programma Informatieveiligheid & Privacy en zo nodig de Opdrachtgeverstafel van het Waterschapshuis zullen hierbij om advies worden gevraagd.

Op dit moment is de businesscase gestart. Hier zijn collega's vanuit de waterschappen en het programma Informatieveiligheid & Privacy van het Waterschapshuis bij betrokken. De ontwikkelingen rondom de businesscase worden besproken in het UO van het programma Informatieveiligheid & Privacy en het overleg van de Coördinatoren Informatieveiligheid Waterschappen (CIW) bij het Waterschapshuis. Op deze manier worden de Chief Information Security Officers (CISO's) en Information Security Officers (ISO's) van de waterschappen geïnformeerd en betrokken.

Ik hoop u hiermee voldoende geïnformeerd te hebben. Mocht u naar aanleiding van deze brief nog vragen over en/of opmerkingen bij de genoemde ontwikkelingen op het gebied van informatieveiligheid hebben, dan kunt u contact opnemen met mevrouw N. de Keijzer via de contactgegevens in het briefhoofd.

Met vriendelijke groet,

Meindert Smallenbroek
Algemeen directeur