Bijlage
CBCF 23-35b

Agendapunt
6

EINDRAPPORTAGE

Evaluatie Programma Versterken Cyberweerbaarheid in de Watersector

68594 – Vertrouwelijk – definitieve versie – 2 februari 2023

Hans Reterink, Niek Overgaauw, Noortje van Velthoven, Joost Christians, Luuk Stadhouders

Inhoudsopgave

Managementsamenvatting

Achtergrond programma Versterken cyberweerbaarheid in de watersector

In 2019 is het Ministerie van Infrastructuur en Waterstaat (IenW) gestart met het programma 'Versterken cyberweerbaarheid binnen de watersector'. Dit programma is mede voortgekomen uit hetgeen is afgesproken in het Bestuursakkoord Water (BAW) spoor 2. In het programma werken alle BAW-partijen (het Rijk, waterschappen, gemeenten en drinkwaterbedrijven) samen aan het vergroten van de cyberweerbaarheid van de watersector. Het programmaplan uit 2022 bestaat uit 26 projecten, opgesplitst naar verschillende thema's, instapniveaus en gebruikers. Elk project draagt er op eigen manier aan bij om cyberincidenten zoveel mogelijk te voorkomen en de gevolgen ervan te beperken.

Het programma wordt aangestuurd door een programmateam van IenW. Het programmateam wordt bijgestaan door een regiegroep, verantwoordelijk voor de aansturing op hoofdlijnen, en een klankbordgroep, die meedenkt op inhoud en uitvoering. Het programma heeft een planning tot eind 2022, waar ook het huidige BAW afloopt.

Gewenste richting voor het programma

Berenschot heeft het programma 'Versterken Cyberweerbaarheid binnen de watersector' geëvalueerd op drie aspecten: richting, inrichting en verrichting. De evaluatie richt zich daarmee enerzijds op het terugblikken op de programmadoelen, de werking van de programmastructuur en de bereikte resultaten, en anderzijds vooruitkijken naar verbeterpunten voor de ambitie en doelen en de gevolgen van nieuwe ontwikkelingen. De inzichten uit deze evaluatie dienen om te bepalen of voortzetting van het programma gewenst is en zo ja, met welke richting.

Hoofdbevindingen

De focus van het programma op uitvoering en de aansturing door het programmateam worden positief beoordeeld door betrokken partners. Benoemde succesfactoren voor het programma zijn de beschikbaarheid van de juiste kennis (in een domein waar goede kennis schaars is), beschikking over voldoende financiële middelen, een toegewijd programmateam, inbreng vanuit de sector en de wijze waarop management en de beleidskern van IenW het programma ondersteunen.

Verbeterpunten zijn het bestuurlijke commitment, de beperkt beschikbare capaciteit bij het programmateam en de sectorpartners en de borging van resultaten en kennis voor de langere termijn. De regiegroepleden hebben in de praktijk niet het juiste mandaat voor besluiten die impact hebben (zoals op gebied van financiën en toepassen van normenkaders) voor de betrokken organisaties. Dat is echter wel een uitgangspunt van het programma.

Gelet op de behoefte en de gewenste richting, is er vanuit de waterpartners meer aandacht gewenst voor de ontwikkeling van ketenmanagement en maatregelen op basis hiervan. Daarnaast spelen de ontwikkelingen op het gebied van wetgeving een bepalende rol. Waterpartners bereiden zich voor op onder meer de Europese NIB2-richtlijn, die een grote impact heeft op normen en richtlijnen en de scope van cyber voor de watersector. Om zowel op het vlak van ketenmanagement en wetgeving beter ondersteund te worden, verlangen verscheidene waterpartners vanuit IenW een meer sturende rol.

Aanbevelingen (advies)

De opgave voor cyberweerbaarheid in de watersector is groot en partners hebben behoefte aan ondersteuning. Het is daarom wenselijk om het programma voort te zetten. Het programma levert veel toegevoegde waarde voor de watersector en heeft zelfs ook uitstraling naar andere sectoren. Daarnaast liggen er ook een aantal opgaven om in de toekomst te kunnen voorzien in de behoeftes van de waterpartners en de externe ontwikkelingen.

- **Visie, richting en resultaten.** Voor de voortzetting van het programma is het van belang een kapstok te ontwikkelen, met een gezamenlijke visie en ambitie, SMART-programmadoelen en projectdoelstellingen. Het advies is om de scope hierbij beperkt te houden tot cyber en water, met een focus op Industriële Controle Systemen (ICS). Belangrijke additionele elementen zijn duidelijke afspraken over het eigenaarschap en borging van resultaten, door bijvoorbeeld in een vaste organisatie onder te brengen. Waterpartners hebben daarbij sterke behoefte aan activiteiten gericht op de ontwikkelingen rondom NIB2-richtlijn en de versterking van ketenanalyses - als mechanisme voor maatregelen.
- **Wettelijke kaders.** De projecten in het programma richten zich op het faciliteren van organisaties in de sector om weerbaarder te worden. Hier is een koppeling te leggen met de vereisten die vanuit de NIB2-richtlijn worden gevraagd. De projecten die ontwikkeld worden in het programma ondersteunen organisaties om de juiste maatregelen te nemen. Het programma kan daarnaast de implementatie van de NIB2-richtlijn ondersteunen door de IenW-beleidskern te voeden, zonder daarmee de beleidsverantwoordelijkheid van het departement over te nemen. Het programma is een uitvoeringsprogramma en deze keuze wordt ook door de deelnemers gewaardeerd, beleidsvorming en regelgeving is geen taak van het programma. Dit kan door de kennis en inzichten uit de uitvoeringspraktijk mee te geven in de vorming van beleid en regelgeving.
- **Advies governance en bemensing.** Versterk de governance vanuit elke deelsector. Wij werken in het rapport een aantal opties hiervoor uit, waaronder: een herbevestiging van de deelname vanuit de sectoren aan voortzetting van het programma in het BO Water, het opnemen van watersectorstuurgroepen in de governance van het programma, en het verkennen van de mogelijkheid tot het vormen van een bestuurlijke *coalition of the willing*. Het is daarnaast gewenst om te zorgen voor continuïteit en robuustheid van het programmateam door capaciteitsbehoud en -uitbreiding.

HOOFDSTUK 1

Inleiding

1.1 Achtergrond

Het Programma 'Versterken Cyberweerbaarheid in de Watersector' is mede voortgekomen uit hetgeen is afgesproken in het Bestuursakkoord Water (BAW) spoor 2. In het BAW hebben het Rijk, provincies, gemeenten, waterschappen en drinkwaterbedrijven afgesproken om samen te werken aan doelmatig waterbeheer. In een addendum van het BAW (BAW+) hebben zij ook afgesproken om de cyberweerbaarheid van de watersector te vergroten. Door samen te werken, willen de betrokken partijen ernstige cyberincidenten zoveel mogelijk voorkomen en – als er toch sprake is van een incident – de gevolgen ervan beperken. Hiertoe brengen zij dreigingen en (keten-)afhankelijkheden in kaart en treffen zij maatregelen om risico's voor de continuïteit van de dienstverlening te verkleinen. In dat kader worden ook activiteiten ontplooid rond kennis-ontwikkeling, kennisdeling en innovatie. Het Ministerie van Infrastructuur en Waterstaat, directoraat-generaal Water en Bodem (hierna: IenW DGWB) faciliteert het programma 'Versterken Cyberweerbaarheid in de watersector'. In het programma zijn de afspraken uit de BAW+ belegd, en wordt uitvoering gegeven aan verschillende projecten. Alle BAW-partijen zijn als waterpartners betrokken bij het programma en leveren met hun kennis en expertise input in projecten. Het programma wordt op grote lijnen aangestuurd door een regiegroep met vertegenwoordigers van de waterpartners. Een klankbordgroep denkt mee op inhoud en uitvoering. Het programmateam verzorgt de dagelijkse aansturing van het programma en de onderliggende projecten.

Het programma heeft een voorziene looptijd tot het einde van 2022, wanneer ook het huidige Bestuursakkoord Water afloopt. Het is vanuit IenW DGWB en het programma gezien, daarom van belang na te denken over het vervolg.

1.2 Vraag

Tegen de geschetste achtergrond is Berenschot gevraagd een evaluatie uit te voeren naar de opzet en het resultaat van het programma tot nu toe, en hoe het programma na 2022 het beste kan worden doorgezet. De vraag naar een externe evaluatie is geformuleerd door de regiegroep, als de opdrachtgever voor de evaluatie.

De hoofdvraag achter de evaluatie luidt als volgt:

'In hoeverre hebben de inrichting (programmastructuur en activiteiten) en verrichting (uitvoering) bijgedragen aan de gewenste richting (ambities en doelen) van het Programma Cyberweerbaarheid in de watersector en welke veranderingen zijn daarin gewenst voor het vervolg?'

Om tot het antwoord op de hoofdvraag te komen, zijn de volgende deelvragen geformuleerd:

1. Hoe is het programma nu ingericht en wat is desgewenst nodig?
2. Welke resultaten zijn tijdens het programma bereikt en welke wil je bereiken?
3. Hoe zullen nieuwe wet- en regelgeving en andere ontwikkelingen het programma beïnvloeden?

1.3 Aanpak

1.3.1 Onderzoekskader

Als basis voor het onderzoek is het *richten-inrichten-verrichten*-model gehanteerd. Het programma is gestart met een akkoord, opdracht en een plan (richten), daaromheen is een programma-structuur ingericht (inrichten) die projecten heeft aangestuurd en uitgevoerd (verrichten). Het vraagstuk rondom de evaluatie – het enerzijds terugblikken op de doelen, de werking van de programmastructuur en de bereikte resultaten, en het anderzijds vooruit te kijken naar verbeterpunten voor de ambitie en doelen en de gevolgen van nieuwe ontwikkelingen - is derhalve goed te duiden met dit model.

Figuur 1. Raamwerk voor het onderzoekskader: richten, inrichten en verrichten.

De afronding van de geplande programmatermijn is een geschikt moment om het net op te halen: hoe pakte de inrichting in de praktijk uit, hoe is het verrichten verlopen en hoe verhoudt zich dat tot de gewenste richting. Om vervolgens vooruit te kijken naar de resterende en toekomstige opgaven en het programma, de structuur en de activiteiten daarop bij te sturen.

Onze bevindingen, analyse en conclusies hebben wij, als onderzoekers, gebaseerd op de feitelijke informatie, gesprekken en werksessies, met bovenstaand raamwerk voor het onderzoekskader. In het onderzoekskader zijn aan de hand van het denkraam 'richten-inrichten-verrichten' de onderzoeksvragen geordend en aangevuld.

Ook zijn de vragen vertaald naar informatiebronnen: *op basis van welke informatie wordt de onderzoeksvraag geanalyseerd en beantwoord.* De twee type informatiebronnen die in dit onderzoek zijn gebruikt, zijn de bureaustudie en interviews. De bureaustudie is een studie van bestaande documenten met feitelijke informatie. Interviews zijn gesprekken met relevante gesprekspartners, waarbij beelden worden verkregen. Het onderzoekskader is voorgelegd aan het programmateam en na instemming gebruikt voor het verzamelen van informatie, het structureren van de bureaustudie, het opstellen van de interviewleidraad en het analyseren van de resultaten. Het onderzoekskader is bijgevoegd in Bijlage 1: Vraagstelling en onderzoekskader.

Proces en onderzoeksmethode

In het onderzoek maken we onderscheid tussen feiten en beelden.

Feiten

In het hoofdstuk hebben we het over feiten, wanneer we het hebben over informatie opgehaald uit documentenanalyse. Het programmateam heeft de documentatie voor de bureaustudie aangeleverd, zoals het programmaplan, flyers, verslagen van regiegroep, stuurgroep en klankbordgroep, kamerbrieven, etc.

Beelden

Als onderdeel van het onderzoek heeft Berenschot (groeps)interviews met betrokkenen georganiseerd, waaronder de klankbordgroep, regiegroep, projectleiders, projectmedewerkers, programmateam, stakeholders (zoals NCTV/NCSC) en betrokkenen van de waterpartners zoals waterschappen, RWS, drinkwaterbedrijven, gemeenten, provincies en het Ministerie van I&W. De lijst met gesprekspartners is in samenspraak met het programmateam opgesteld en gegroepeerd en door de regiegroep bijgesteld.

1.3.2 Begeleiding en ondersteuning onderzoek

Berenschot werd bij dit onderzoek ondersteund door het programmateam, dat in nauw contact staat met de regiegroep als opdrachtgever en begeleider voor de evaluatie. Gedurende het onderzoek heeft Berenschot structureel contact met het programmateam. Het programmateam heeft de documentatie voor de bureaustudie aangeleverd. Vervolgens is er nauw contact geweest over het vaststellen van het onderzoekskader, de interviewleidraad en gesprekspartners. De regiegroep heeft ook een bijdrage geleverd aan de lijst met gesprekspartners, door deze lijst bij te stellen. Alle contactgegevens van de gesprekspartners zijn door het programmateam aangeleverd.

In een validatiesessie van een dagdeel waarvoor meer dan twintig geïnterviewden zijn uitgenodigd (waaronder leden van de klankbordgroep, de regiegroep en het programmateam) zijn onze bevindingen getoetst en waar nodig bijgesteld op feitelijke onjuistheden. De bevindingen en aanbevelingen zijn in concept aan de regiegroep als opdrachtgever gepresenteerd. Tot slot zijn de definitieve bevindingen en aanbevelingen middels een conceptrapport aan het programmateam en de regiegroep voorgelegd. In deze fase heeft het programmateam en regiegroep de laatste opmerkingen/feedback kunnen geven, waarna wij het rapport definitief hebben gemaakt.

HOOFDSTUK 2

Bevindingen

2.1 Context en tijdlijn

Het programma Versterken Cyberweerbaarheid in de Watersector is in 2019 gestart. Het voegde drie bestaande sporen, en de bijbehorende projecten, samen:[1]

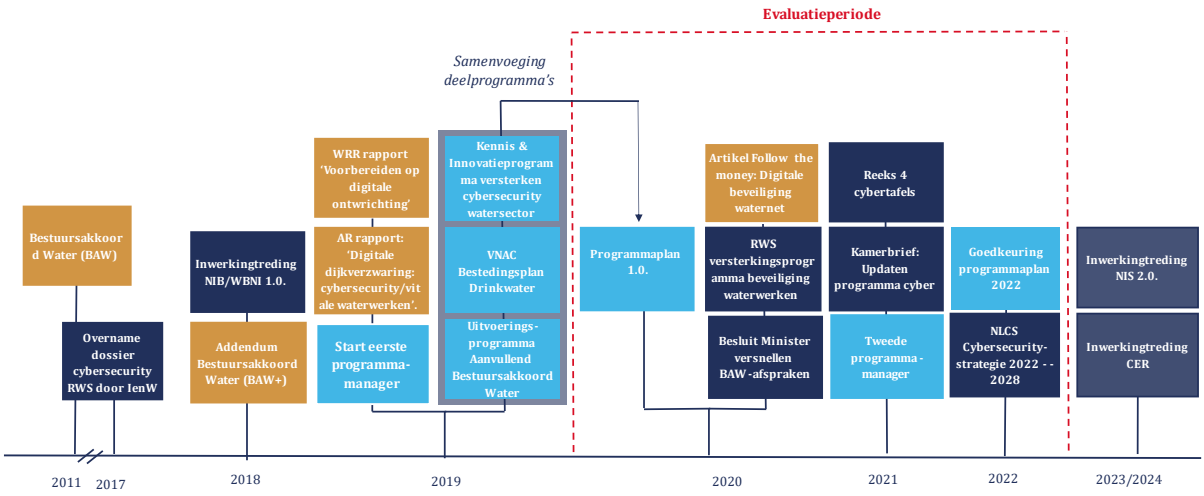
1. De aanvullende afspraken uit spoor 2 uit het Bestuursakkoord Water (BAW+).
2. Het Kennis- en Innovatieprogramma.
3. Het VNAC-bestedingsplan Drinkwater.

Het programmaplan 2019-2022 beschrijft verschillende aspecten van het programma, zoals het doel, de uitgangspunten, de governance en organisatie, projecten en aanpak, financiering en andere afspraken. Deze zaken zijn hieronder in de desbetreffende paragrafen nader beschreven.

Binnen het programma 'Versterken Cyberweerbaarheid in de Watersector' werken Rijk, waterschappen, provincies, gemeenten en drinkwaterbedrijven samen. Naast het programma zijn er nog andere trajecten die zich richten op het versterken van de cyberweerbaarheid in (delen van) de watersector.[2] Zo werkt Rijkswaterstaat in het eigen Versterkingsprogramma Cybersecurity aan implementatie van de aanbevelingen uit het Algemene Rekenkamer-rapport 'Digitale dijkverzwaring: Cybersecurity en vitale waterwerken'. IenW werkt momenteel aan de IenW Cybersecurity Strategie (2022-2026) in aansluiting op de Nederlandse Cybersecuritystrategie 2022-2028. De strategie van IenW beschrijft de cybersecurityaanpak en heeft als doel om IenW en de vitale sectoren waar IenW een verantwoordelijkheid heeft digitaal veiliger te maken.

Dit leidt tot de tijdlijn in het schema hierna. Hierbij zijn donkerblauwe blokken direct gerelateerd aan het programma zelf, lichtblauwe blokken geven belangrijke zaken in bemensing aan en lichtbruine blokken geven belangrijke externe documenten aan welke van invloed waren op het programma. De rode stippellijn geeft de evaluatieperiode aan: deze is gestart met het programmaplan 1.0 en eindigt in 2022.

[1] Digitale folder Programma Cyberweerbaarheid in de drinkwatersector, maart 2021.
[2] Harbers, M.G.J. (2022, 7 juni). Versterken Cyberweerbaarheid in de Watersector [Kamerbrief].



Figuur 2. Tijdlijn van en rond programma versterken cyberweerbaarheid in de watersector.

2.2 Richten – Ambities en doelen

2.2.1 Feiten

Het overkoepelende doel van het programma is het versterken van de cyberweerbaarheid in de watersector. Daarnaast beoogt het programma efficiënt en effectief projecten samen met de waterpartners uit te voeren en flexibiliteit te geven om in te spelen op veranderde omstandigheden.[3] Om hier invulling aan te geven, heeft het programmateam in eerste instantie vijftien projecten opgenomen in het programmaplan 2019-2022 (zie bijlage 1).

In oktober 2022 bestaat het programma uit 26 projecten/activiteiten geclusterd onder vijf specifieke en elkaar aanvullende thema's.[4] Er zijn 25 projecten opgenomen in het jaarplan 2022. Aan dit plan is daarnaast een extra project toegevoegd.[5] Elk thema heeft zijn eigen ambitie en doelen.[6] Onderstaand staat een overzicht opgenomen met de gehanteerde thema's en doelen. In bijlage 2 is in een overzicht opgenomen, welke projecten/activiteiten vallen onder welke categorie, wat het doel en de status is per project/activiteit.

Nr.	Thema's	Doelen
1	Trainen, Testen en Oefenen (TTO)	Impact van cyberincidenten minimaliseren door optimaal voorbereid te zijn. Identificeren van verbeterpunten voor de cyberweerbaarheid van organisaties. Organisaties en medewerkers van verschillende organisaties weten elkaar te vinden en het uitwisselen van kennis wordt gestimuleerd.

[3] Programmaplan 1.0. 2019.
[4] Thema two pager extern programma Cyberweerbaarheid watersector, Ministerie van Infrastructuur & Waterstaat, 2022.
[5] Handreiking proces Coördinated Vulnerability Disclosure (CVD) is een project dat niet staat opgenomen in de two pager, maar wel is behandeld met de werkgroep.
[6] Thema two pager extern programma Cyberweerbaarheid watersector, Ministerie van Infrastructuur & Waterstaat, 2022.

Nr.	Thema's	Doelen
2	Ketens en Risicomanagement (KR)	Inzicht hebben in de risico's die voor een organisatie relevant zijn: Classificeren van objecten (op basis van Business Impact). Uitvoeren van ketenanalyses. Inventariseren welke cybersecurityrisico's relevant zijn voor de organisatie.
3	Maatregelen en Implementatie (MI)	Organisaties optimaal ondersteunen bij het nemen van de (basis)maatregelen. En daarnaast instrumenten bieden voor het nemen van extra maatregelen die passen bij het risicoprofiel van de organisatie.
4	Monitoring en Detectie (MD)	Het optimaal inrichten van monitoring en detectie. Zo kunnen incidenten snel opgemerkt worden. De impact van incidenten kan op deze manier bovendien zo klein mogelijk worden gehouden.
5	Samenwerking en Expertise (SE)	De cybersecurityexpertise binnen de watersector verbeteren door het verstevigen van de samenwerking en het borgen van de kennis.

2.2.2 Beelden

In verschillende interviews is benoemd dat het goed is dat voor een *uitvoeringsprogramma* gekozen is. Men vindt de focus op uitvoering erg waardevol. De doelen en ambities van het programma zijn niet bij alle betrokkenen even goed bekend, zo blijkt uit de interviews. Ook zijn er verschillende opvattingen over het gewenste ambitieniveau van het programma. Sommige gesprekspartners redeneren vanuit de inhoudelijke opgave voor cyberweerbaarheid en vinden dat de doelen ambitieuzer zouden moeten zijn. Specifiek verlangen deze gesprekspartners een ontwikkeling naar ketenmanagement[7] en meer aandacht voor het formuleren en implementeren van ketenmaatregelen na het uitvoeren van ketenanalyses. Andere gesprekspartners redeneren vanuit de schaarse kennis en capaciteit bij sectorpartners voor deelname aan de activiteiten en geven aan dat een hoger ambitieniveau lastig haalbaar is.

Uit de validatiesessie met het programmateam en klankbordgroepleden kwam naar voren dat er behoefte is aan een 'kapstok' om het programma, en de activiteiten daarin, meer richting te geven. Die kapstok bestaat uit een overkoepelende visie en programmadoelen die kunnen worden vertaald naar doelstellingen op projectniveau.

[7] Bij ketens wordt dan gedacht aan een indeling van ketens die betrekking heeft op de hoofdprocessen van de waterpartners in een specifieke regio, aangevuld met ketens van afhankelijkheden op cybergebied, zoals kunnen bestaan tussen bv. besturing van systemen, de leveranciers van deze systemen en organisaties betrokken bij het omgaan met aanvallen en kwetsbaarheden zoals CERTS.

2.3 Inrichten – Programmastructuur en governance

2.3.1 Programma

Feiten

Het Ministerie van IenW verzorgt het programmamanagement en stelt het programmateam (nu drie medewerkers) beschikbaar. Het programmateam verzorgt de dagelijkse aansturing van het programma en de onderliggende projecten. Communicatie maakt hier onderdeel van uit. Het team heeft een communicatiestrategie uitgewerkt, gericht op interne en externe communicatie. De boodschap is vooral informerend van aard, over o.a. de resultaten van projecten of bijeenkomsten.[8] Een voorbeeld van externe communicatie is de maandelijkse nieuwsbrief die wordt verstuurd.

Het programmaplan 2019-2022 beschrijft de volgende uitgangspunten die leidend zijn voor het programma:[9]

- Het programma en de projecten zijn wendbaar; leereffecten moeten kunnen leiden tot tussentijdse aanpassingen in projectdoelstellingen.
- Projecten zijn innovatief.
- Planning en prioritering van projecten is gebaseerd op daadwerkelijke bijdrage aan de versterking cyberweerbaarheid (grootste kwetsbaarheden/dreigingen eerst).
- Projecten moeten leiden tot door de partners gewenste producten die toepasbaar zijn voor de verbetering van de cyberweerbaarheid.
- Er wordt gestreefd naar synergie en efficiency door bundelen van projectvoorstellen.
- Focus ligt op procesautomatisering gezien de potentiële risico's voor het maatschappelijk verkeer.
- Min. IenW zorgt voor het gehele programmamanagement, inclusief projectsecretariaat en de projectleiding (opstellen projectplannen, inkoopprocessen, opleveren projectresultaten), de watersectorpartners worden zoveel mogelijk ontlast bij het projectmanagement zodat zij hun schaarse tijd volledig kunnen inzetten als inhoudelijke experts en klankbordlid.
- Deelname aan projecten door partners is vrijwillig, maar niet vrijblijvend.
- Waar mogelijk is alliantievorming met andere sectoren en/of overheden gewenst.
- Het programma is tijdelijk van aard en stopt bij de décharge van het laatste project.

In het programmaplan 2019-2022 zijn vijftien, door de partners vastgestelde, projecten opgenomen (zie bijlage 1). In het programmaplan over 2019-2023 staat vermeld dat onder het programma geen nieuwe projecten worden geplaatst, alleen herdefiniëring is mogelijk na besluitvorming in de regiegroep. Het huidige programmateam geeft aan deze afspraak niet te herkennen, maar dat nieuwe activiteiten wel alleen na besluitvorming in de regiegroep worden gestart. Beleidsontwikkeling of toezicht op de kwaliteit van de cyberweerbaarheid in de partnerorganisaties is geen onderdeel van het programma.10

Het programma en de onderhangende projecten, zijn op alle partners - waterschappen, RWS, drinkwaterbedrijven, provincies en gemeenten - gericht. Het is afhankelijk van het type project, welke partner meer betrokken is/gebruikmaakt van. In oktober 2022 bestaat het programma uit 26 projecten (zie bijlage 2 voor een overzicht).

---

[8] Programmaplan Versterking Cyberweerbaarheid in de Watersector 2019-2022, p. 17.
[9] Programmaplan Versterking Cyberweerbaarheid in de Watersector 2019-2022, p. 13.
[10] Programmaplan Versterking Cyberweerbaarheid in de Watersector 2019-2022, p. 13.

De projecten zijn onderverdeeld in vijf thema's:

1. Trainen, Testen en Oefenen (TTO).
2. Ketens en Risicomanagement (KR).
3. Maatregelen en Implementatie (MI).
4. Monitoring en Detectie (MD).
5. Samenwerking en Expertise (SE).

Daarnaast worden de projecten onderscheiden in drie complexiteitsniveaus. Niveau 1 is voor organisaties die actiever willen samenwerken met de sector maar nog zoeken naar een invulling daarvan. Niveau 2 is voor organisaties die willen aansluiten bij sectorale samenwerking op het gebied van cybersecurity. En niveau 3 is voor organisaties die actief willen en kunnen bijdragen aan het vergroten van het kennisniveau binnen de watersector.

Beelden

In het algemeen wordt door de gesprekspartners de inrichting van het programma en het functioneren van het programmateam als positief beoordeeld. In een aantal interviews is specifiek waardering uitgesproken voor de opzet van het programma waarbij de nadruk ligt op de uitvoering in de praktijk. Hiermee wordt het programma gezien als koploper en een voorbeeld voor andere domeinen en ministeries. Daarbij komt wel naar voren dat door gesprekspartners een afhankelijkheid van de – nu sterke – invulling door het programmateam wordt ervaren, zowel op het gebied van kennis, professionaliteit en de energie die ze brengen.

De samenhang en complementariteit tussen activiteiten, zowel binnen als buiten het programma, wordt door gesprekspartners niet altijd herkend. Zij vinden dit echter niet onlogisch gezien de heterogeniteit van de sector: er zijn uiteenlopende taken, normen, technieken, cybervolwassenheidsniveaus, systemen en verschillende betrokken ministeries vanuit verschillende invalshoeken. Daarnaast geven gesprekspartners aan dat projecten en activiteiten voornamelijk zijn gericht op ontwikkeling (training/workshop), kennis (producten) en capaciteit. Daarbij ontbreekt een procedure waarin is vastgelegd hoe resultaten op langere termijn worden geborgd en opgevolgd. De gesprekspartners merken dat de resultaten van de activiteiten veel worden gebruikt door waterschappen en RWS.

Veel gesprekspartners geven aan er belang aan te hechten dat het programma vraaggestuurd wordt ingericht, oftewel dat de activiteiten aansluiten bij de behoefte van de doelgroepen. Toch vindt een aantal partijen het soms lastig om te formuleren waar 'vraag' naar is. Daarbij speelt mee, dat waar 'vraag' naar is, afhankelijk is van wie daarover wordt gesproken. Dit beide heeft mede te maken met de uiteenlopende volwassenheidsniveaus van sectorpartners.

2.3.2 Governance/bestuurlijk commitment

Feiten

In het programmaplan Versterking Cyberweerbaarheid in de Watersector 2019-2022 staat de governance omschreven. Deze bestaat uit een regiegroep en een klankbordgroep, zo nodig ad hoc aangevuld met andere gremia. Deze verschillende overlegstructuren worden hieronder nader beschreven.

Regiegroep

Het programma wordt aangestuurd door een regiegroep waarin alle partners van het BAW+ zijn vertegenwoordigd 'op senior niveau'.[11] Namens het Rijk nemen IenW en Rijkswaterstaat deel, en de waterschappen, provincies, gemeenten en drinkwaterbedrijven zijn vertegenwoordigd door hun koepels.[12] De regiegroep komt drie keer per jaar samen. Uitgangspunt is dat de regiegroepleden mandaat van hun organisatie of achterban hebben om beslissingen over het gehele programma te nemen. Naast het nemen van beslissingen, moeten leden uit de regiegroep ervoor zorgen dat afspraken in hun organisatie worden nagekomen. De regiegroep wordt voorgezeten door het afdelingshoofd Waterveiligheid van IenW en secretarieel ondersteund door het programmateam. De programmamanager neemt deel als opdrachtnemer.

Regiegroepleden moeten ervoor zorgen dat afspraken over inzet binnen projecten in hun organisaties worden nagekomen. Daarnaast dient de regiegroep als escalatietrede voor het programmateam. Besluitvorming over de aanpassing van het programma gebeurt door de regiegroep op advies van de programmamanager.[13]

Klankbordgroep

Net als bij de regiegroep zijn in de klankbordgroep alle leden van het BAW+ vertegenwoordigd. De NCTV en NCSC zijn hierbij aangesloten als agendalid en de programmamanager is voorzitter.

In het programmaplan is afgesproken dat de klankbordgroep vier keer per jaar bij elkaar komt. Doel van die besprekingen is om de programmamanager te adviseren over de uitvoering van het programma en onderliggende projecten. Daarnaast hebben de klankbordgroepleden de taak om de communicatie tussen de partnerorganisaties en programmamanager te verzorgen en nemen zij plaats in de begeleidingscommissies van individuele projecten.

Aanvullende overlegstructuren

In het programmaplan is opgenomen dat op ad-hocbasis aanvullende overleggen kunnen worden georganiseerd. Zo kan er een bestuurlijk overleg worden ingelast ter vergroting van het draagvlak. Het DT van IenW/DGWB, de Directeur-Generaal en de portefeuillehouder cybersecurity kunnen worden geïnformeerd over planning, voortgang, middelen en risico's. Tot slot kan de minister van IenW worden geïnformeerd, bijvoorbeeld ter voorbereiding van het BO Water (in het programmaplan Stuurgroep Water genoemd), het algemene overleg Water en Wetgevingsoverleg Water.

Financiële dekking

Ten tijde van het programmaplan 2019-2022 waren alle vijftien projecten binnen het programma bekostigd vanuit de VNAC-bestedingsplan Drinkwater voor IenW. In 2020 en 2021 is onderuitputting van het programmabudget gerealiseerd.[14] De resterende gelden zijn naar 2022 doorgeschoven, met hogere bestedingsruimte tot gevolg.

De hogere bestedingsruimte is echter lastig inzetbaar voor het vergroten van de capaciteit van het programmateam. Dit heeft te maken met de moeilijke procedures rondom inzet van inhuur en een fte-plafond.

---

[11] Programmaplan Versterking Cyberweerbaarheid in de Watersector 2019-2022, p. 8.
[12] Overzicht betrokkenen programma Versterken Cyberweerbaarheid in de Watersector, aangeleverd door programmateam.
[13] Programmaplan Versterking Cyberweerbaarheid in de Watersector 2019-2022, p. 9.
[14] Verslag regiegroep 7 juli 2021.

Beelden

Besturing

Uit de interviews komt naar voren dat bestuurders beperkt betrokken zijn bij het programma. Het uitgangspunt uit het programmaplan 2019-2022 dat regiegroepleden mandaat van hun organisatie of achterban hebben om beslissingen over het gehele programma te nemen, wordt in de praktijk ook zo ingevuld. Voor besluiten die duidelijk direct impact hebben op organisaties in de sector is, volgens sommigen, een groter mandaat nodig. Hierbij valt te denken aan besluiten met impact op deelnemende organisaties uit de sector, financiën of toepassing van normenkaders binnen organisaties. Binnen alle watersectoren zijn wél afstemgroepen (ook met bestuurders) die te maken hebben met cyber, deze worden soms ad hoc betrokken.

IenW

De ondersteunende rol van IenW wordt door gesprekspartners positief beoordeeld, desalniettemin kan de rol steviger worden ingezet. Vanuit de opgave geredeneerd is een meer sturende inbreng van IenW, vanuit de systeemverantwoordelijkheid, voor de hand liggend. Wat deze systeemverantwoordelijkheid precies inhoudt, is nog niet precies bekend onder de betrokkenen. Binnen IenW loopt momenteel een traject om dit verder uit te werken. Een voorbeeld waarop sturing is gewenst, is rondom het ketenmanagement. Het programma kan dit aanjagen door dit bestuurlijk te agenderen.

Klankbordgroep

Over de rol van de klankbordgroep bestaan verschillende beelden. Hun rol bij het formuleren van behoeftes, wordt wisselend ervaren. Sinds een half jaar bestaat de klankbordgroep uit een flink aantal nieuwe leden. Leden die langer deel uitmaken van de klankbordgroep krijgen een ervarener en actievere rol, dan nieuwe leden. Nieuwe leden zouden nog beter meegenomen kunnen worden in het proces om de verwachting en rol van de klankbordgroep waar te maken.

2.4 Verrichten – Projecten en resultaten

Feiten

Ten tijde van dit onderzoek waren tien van de zesentwintig projecten afgerond, terwijl vier projecten naar verwachting in 2022 zijn afgerond. Zeven worden naar verwachting in 2023 afgerond en voor vijf projecten is dit nog onduidelijk. Een overzicht van de voortgang per project staat opgenomen in bijlage 3. Hierin is voor elk project een korte omschrijving opgenomen.

Beelden

Gesprekspartners kijken in het algemeen positief naar de voortgang van projecten. De betreffende projecten worden door afnemers in principe goed beoordeeld. Succesfactoren die zijn benoemd zijn:

- Beschikbaarheid van de juiste kennis en expertise (in een domein waar goede kennis schaars is.
- Voldoende financiële middelen.
- Een toegewijd programmateam.
- Inbreng vanuit de sector en steun vanuit management en de beleidskern van IenW.

Ondanks de succesfactoren, constateren partners dat continue beschikbaarheid van resultaten op lange termijn niet goed zijn geborgd. Beschikbaarheid is sterk afhankelijk van het vervolg van het programma en de continuïteit van het programmateam. Beter zou zijn om resultaten van het programma onder te brengen in een meer vaste organisatievorm.

Randvoorwaarden die (nu nog) ontbreken, zijn prioriteit in bestuurlijk commitment en dedicated capaciteit vanuit sectororganisaties om aan de gezamenlijke opgave te werken. Tot slot wordt door betrokkenen de uitstraling van het programma op andere gebieden/sectoren benadrukt.

2.5 Ontwikkelingen

Feiten

Ontwikkelingen rondom cyberweerbaarheid binnen de watersector worden momenteel primair gezien als voortkomend uit Europees en nationaal beleid. Momenteel zijn er diverse lopende (Europese) wetgevingstrajecten al in een vergevorderd stadium. Dit betekent dat wet- en regelgeving in veel gevallen nog niet definitief is vastgesteld, maar dat men wel al een duidelijke richting kan identificeren en op hoofdlijnen kan inschatten wat de impact hiervan is. In Europees verband is het van belang om onderscheid te maken tussen twee typen wetgevingsinstrumenten:

Instrument	Toelichting
Europese Directive (Richtlijn)	Een Europese richtlijn is een wetgevingsinstrument waarbij vanuit de EU specifieke doelen worden vastgesteld. Deze doelen zijn niet rechtstreeks bindend voor burgers en organisaties binnen de EU, maar moeten door de lidstaten worden omgezet in nationale wetgeving. Hierbij hebben zij zelf de keuze om te bepalen hoe zij dit doen. De huidige NIS Directive is hier een voorbeeld van.
Europese Regulation (Verordening)	Een Europese verordening is een wetgevend instrument van de Europese Unie. Een verordening heeft een algemene strekking. Zij is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat. Ook is een verordening rechtstreeks van toepassing, wat betekent dat zij rechtstreeks recht schept dat in alle EU-lidstaten dezelfde kracht heeft als het nationale recht, zonder dat nationale instanties daarvoor iets hoeven te doen. Een voorbeeld van een verordening is de Algemene Verordening Gegevensbescherming (AVG).

De Europese Commissie (EC) heeft in de '*EU Cybersecurity Strategy*' beleid uitgewerkt dat de komende jaren – onder meer – in wet- en regelgeving vertaald zal worden, met als doel de weerbaarheid tegen digitale aanvallen en dreigingen te versterken. Recentelijk heeft ook Nederland in de '*Nederlandse Cybersecuritystrategie 2022-2028*' haar plannen om de Nederlandse digitale weerbaarheid te versterken vastgelegd. In beide strategische documenten is een duidelijke behoefte te zien aan meer regulering op het gebied van cyberweerbaarheid. In algemene zin, zien we op drie vlakken dat wet- en regelgeving zich ontwikkeld:

- Verbeteren bescherming kritische infrastructuur: er bestaat meer behoefte om aanbieders van vitale en essentiële diensten beter te reguleren en te beschermen. Hiervoor zien we dat zowel vanuit de EU als binnen Nederland wet- en regelgeving wordt ontwikkeld die erop gericht is om samenwerking te verbeteren. Een belangrijk instrument hiervoor is de NIB2-richtlijn, welke momenteel wordt aangeboden aan het Europees Parlement. Deze richtlijn vervangt de huidige NIB-richtlijn, welke in Nederland is geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen (Wbni). De Wbni is nu richtinggevend voor de cybersecurity in de watersector. De belangrijkste wijzigingen die in het huidige voorstel zijn terug te vinden, bestaan uit strengere eisen op het gebied van risicomanagement en het nemen van informatiebeveiligingsmaatregelen. Ook op nationaal niveau zien we diverse maatregelen die worden genomen om de bescherming van kritische infrastructuur verder te verbeteren. Zo wordt er steeds meer nadruk gelegd op het verbeteren van informatie-uitwisseling tussen verschillende partijen en het oefenen van cybercrises binnen Nederland en Europa.

Ook op nationaal niveau zien we een grotere roep om de cyberweerbaarheid sterker in wet- en regelgeving te verankeren. Dit zien we bijvoorbeeld terug in de plannen van de staatsecretaris om voor overheden een algemene zorgplicht in wet- en regelgeving vast te leggen die bijvoorbeeld de maatregelen uit de Baseline Informatiebeveiliging Overheid (BIO) verplicht.[15] Daar waar de BIO met name is gericht op meer generieke maatregelen inzake de bescherming van informatie(systemen) (voornamelijk IT), is er ook voor de operationele techniek (OT) een implementatierichtlijn ontwikkeld, namelijk de CSIR. De meest recente versie hiervan is versie 3 en vormt een aanvulling op de BIO.

- Verbeteren cybersecurity rondom producten, diensten en processen: met de introductie van de Cybersecurity Act (CSA), wordt er een Europees certificeringsstelsel geïntroduceerd voor de cybersecurity van ICT-producten, -diensten en -processen. Deze verordening is momenteel al in werking getreden, maar vergt nog nadere uitwerking door de diverse lidstaten. De verordening zal in combinatie met andere wet- en regelgeving veel impact hebben op de (verplichte) toepassing van bepaalde standaarden en certificeringen voor producten, diensten en processen. De specifieke vereisten worden de komende jaren vastgesteld.
- Versterken toezicht en ondersteuning: tot slot zien we de groeiende behoefte om beter toe te zien op naleving van wet- en regelgeving. In het voorstel voor de NIB2-richtlijn zien we al een sterkere positie rondom toezicht op de naleving van verplichtingen rondom cybersecurity. Daarnaast zien we dat het Agentschap Telecom de rol vervult van Nederlandse Nationale Cybersecurity Certificeringsautoriteit (NCCA). En dat de overheid meer regie pakt ten aanzien van het versterken van de cyberweerbaarheid door de doorontwikkeling van het Landelijk Dekkend Stelsel (LDS). Hiermee zal een meer gecentraliseerde aanpak ertoe moeten leiden dat informatie en kennis beter uitgewisseld kunnen worden.

Daarnaast zijn er ook nog diverse andere (strategische) beleidsdocumenten die mogelijk effecten hebben op het programma Cyberweerbaarheid in de Watersector, zoals de *Nederlandse digitaliseringsstrategie 2021* en de *I-strategie Rijk 2021-2025*. Voor deze evaluatie is een volledig overzicht van potentieel relevante beleidsdocumenten niet noodzakelijk om de belangrijkste ontwikkelingen in kaart te brengen. Nieuwe wet- en regelgeving heeft meestal ook gevolgen voor het toezicht van de naleving daarvan. De impact daarvan nemen we ook mee in de ontwikkelingen.

Impact op inrichting programma

De (aanstaande) wijzigingen in wet- en regelgeving zullen naar verwachting de komende jaren veel impact hebben, zeker ook op de watersector. Allereerst zullen meer organisaties verplicht zijn om de komende jaren verstrekkende maatregelen te nemen om de cyberweerbaarheid te verhogen. Wanneer het voorstel voor de NIB2-richtlijn is vertaald naar Nederlandse wet- en regelgeving zullen meer organisaties binnen de watersector worden aangemerkt als aanbieders van vitale diensten en kritieke infrastructuur (bijvoorbeeld organisaties rondom afvalwater en het openbaar bestuur).

Daarnaast kunnen de betrokken organisaties strengere maatregelen verwachten. Het huidige voorstel voor de NIB2-richtlijn bevat verschillende bepalingen die gericht zijn op verbeteren van de cyberweerbaarheid. Zo worden strengere eisen gesteld rondom risicomanagement, *supply chain security*, encryptie en kwetsbaarhedenmanagement. Ook verplichtingen inzake het rapporteren over de cyberweerbaarheid en incidenten zal stringenter worden. Op nationaal niveau zien we in de Nederlandse Cybersecuritystrategie 2022-2028 dat er ook diverse maatregelen worden genomen om de samenwerking te verbeteren.

[15] Zie kamerbrief BZK.

Ontwikkeling van het Landelijk Dekkend Stelsel (hierna: LDS) zal ervoor zorgen dat het delen van informatie tussen verschillende partijen binnen de keten verder wordt vormgegeven. Daarnaast zullen organisaties vaker en meer met elkaar oefenen.

Tot slot is het te verwachten dat de komende jaren verschillende standaarden en certificeringen worden ontwikkeld op basis van het cybersecurity certificeringsframework dat momenteel wordt ingericht en vormgegeven. Zoals te zien in onderstaande afbeelding worden momenteel zowel generieke, technische, als sectorale certificeringsschema's ontwikkeld waarmee zekerheid ten aanzien van IT-producten, -diensten en -processen kan worden geboden. Op de website van de Europese Commissie wordt daarbij expliciet verwezen naar het belang om weerbaarheid ten aanzien van kritieke diensten te verhogen, onder meer als gevolg van het opblazen van de Nord Stream-pijplijn.[16]

Beelden

Gesprekspartners zien dat NIB2 een grote impact op normen/richtlijnen gaat hebben en de scope voor de watersector verruimt. Dit heeft er o.a. mee te maken dat meer partijen en meer processen er onder vallen. Uiteindelijk leidt dit tot een grotere opgave voor de partners, die aangeven dat ze dit nu ook al niet goed kunnen bemensen.

Tegelijkertijd maakt de NIB2, dat gesprekspartners een andere (stevigere) rol vanuit IenW verwachten, rondom bijvoorbeeld voorbereiding en ondersteuning. Volgens gesprekspartners zou dit betekenen dat IenW ondersteuning biedt bij stroomlijnen, coördineren en implementeren van NIB2 en het gevolg ervan in de watersectoren.

[16] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6238

HOOFDSTUK 3

Advies

3.1 Adviesrichting en resultaten

Voortzetting programma

Het is zowel vanuit de behoeften van de waterpartners en vanuit de opgave geredeneerd zeer gewenst om het programma voort te zetten. Het programma levert veel toegevoegde waarde voor de watersector en heeft zelfs ook uitstraling naar andere sectoren. Het biedt ook efficiency gezien de beperkte beschikbaarheid van cyberexperts. Daarbij denken wij dat het het meest effectief is om de scope beperkt te houden tot cyber en water, met een focus op ICS, net zoals nu het geval is. Hoewel een succesvol programma altijd extra activiteiten aantrekt, zou het programma door een uitbreiding van scope te veel focus kwijtraken.

Gezamenlijke visie en ambitie als kapstok

Het is gewenst vanuit de opgave om een kapstok te hebben voor de richting van het programma om een gezamenlijke visie en ambitie voor de watersector te formuleren. Deze visie en ambitie kunnen worden uitgewerkt in SMART-programmadoelen en projectdoelstellingen. Per waterpartner kunnen de doelstellingen verschillen. Het programma kan zo worden doorgezet richting het formuleren en ondersteunen bij het implementeren van tactisch/operationele maatregelen in een PDCA-cyclus binnen organisaties in de watersector. Nu is veel gericht op kennis en inzicht. De impact van het programma op de versterking van cyberweerbaarheid kan vergroot worden door besluitvorming over de ontwikkeling en toepassing van instrumenten bij de sector zelf te beleggen.

Ketenanalyse

Ketenanalyse kan een krachtig instrument zijn voor een betere analyse van risico's. We adviseren om de ketenanalyses door te zetten zodat alle regio's en hoofdprocessen worden geanalyseerd. Vervolgens kunnen met de sector noodzakelijke maatregelen worden geïdentificeerd en de implementatie gevolgd.

3.2 Advies richting en wettelijke kaders

NIB2-richtlijn

De Europese NIB2-richtlijn en de Nederlandse implementatie daarvan in een 'Wbni2' zal veel impact hebben, ook op de watersector en daarmee het programma. Het programma kan hier een belangrijke rol in hebben door als uitvoeringsprogramma praktische handvaten te ontwikkelen voor de sector en daartoe de wettelijke ontwikkelingen te volgen. Daarnaast kan ze het effect van de wettelijke ontwikkelingen op de Nederlandse watersectoren inschatten, zonder daarmee uiteraard de verantwoordelijkheid van het departement over te nemen. Het programmateam kan de IenW-beleidskern voeden met kennis vanuit het programma en de waterpartners zodat de inzichten uit de uitvoeringspraktijk worden meegenomen in de vorming van beleid en regelgeving. In vervolg op NIB2 is het natuurlijk gewenst dat een dekkend en onderling consistent stelsel van wetgeving en normen ontstaat met beperkte overlap waar beleid, toezicht en uitvoering in de watersectoren congruent zijn en van hetzelfde normenkader uitgaan.

Dit is een verantwoordelijkheid die niet bij het programma ligt, maar bij de IenW-beleidskern.

3.3 Advies governance en bemensing

Vanuit de opgave en om organisaties effectief te helpen bij de impact van NIB2 is het gewenst om de governance, ook bestuurlijk, vanuit elke deelsector te versterken. Daartoe kunnen de volgende zaken behulpzaam zijn:

Herbevestiging door BO Water

Een herbevestiging van het voortzetten van het programma vanuit het BO Water. Ook is gewenst om het BO Water het ontwikkelen van een gezamenlijke visie en ambitie te laten ondersteunen, te besluiten tot het toevoegen van de watersectorstuurgroepen[17] en de governance van het programma en het mandaat van de regiegroep te verduidelijken. Door het bevorderen van deze afspraken kan IenW mede invulling geven aan de systeemverantwoordelijkheid.

Versterken besturing

Het is zowel vanuit de opgave, als voor draagvlak in management en bestuur gewenst om de governance vanuit de sectoren te versterken door een directe relatie van het programma te hebben met de watersectorstuurgroepen. Deze worden geïnformeerd over het programma, kunnen jaarplannen en eventuele maatregelen die de sector raken bekrachtigen en capaciteit vanuit de sector organiseren. De regiegroep en klankbordgroep worden ook behouden. De regiegroep kan de ontwikkeling van een gezamenlijke visie en ambitie ter hand nemen, samenhang in het programma bevorderen en de voortgang van het programma en projecten volgen en waar nodig bijsturen.

Coalition of the willing

Een verkenning van de mogelijkheid om een *coalition of the willing* van bestuurders te formeren die sponsorship kan invullen en als adviesraad kan fungeren.

Continuïteit programmateam

Ook is het gewenst om te zorgen voor continuïteit en robuustheid van het programmateam door capaciteitsbehoud en -uitbreiding.

Borging resultaten

Als laatste bevelen wij aan om borging en eigenaarschap van resultaten en de verantwoording daarover van het programma (en toegang daartoe vanuit water en andere domeinen) als vaste taak bij een vaste organisatie te beleggen, zodat de resultaten beschikbaar blijven.

[17] Stuurgroepen die een goede rol kunnen vervullen zijn bv.: Drinkwater: stuurgroep Beveiliging en Crisismanagement (BCM); Waterschappen: Commissie Bestuurszaken, communicatie en Financien (CBCF) & Werkgroep Bedrijfsvoering Digitalisering en Dienstverlening (WBDD).

BIJLAGEN

Bijlage 1. Vraagstelling en onderzoekskader

Vraagstelling

U vraagt om een evaluatie van het Programma Cyberweerbaarheid Watersector BAW met de volgende **deelvragen**:

- Hoe is het programma nu ingericht en wat is desgewenst nodig?
- Welke resultaten zijn tijdens het programma bereikt en welke wil je bereiken?
- Hoe zullen nieuwe wet- en regelgeving en andere ontwikkelingen het programma beïnvloeden?

Dit hebben wij samengevoegd in de volgende **hoofdvraag**:

> In hoeverre hebben de inrichting (programmastructuur en activiteiten) en verrichting (uitvoering) bijgedragen aan de gewenste richting (ambities en doelen) van het Programma Versterken Cyberweerbaarheid in de Watersector en welke veranderingen zijn daarin gewenst voor het vervolg?

Onderzoekskader

Dit onderzoekskader is een nadere uitwerking van de vraagstelling. Het beschrijft de aspecten die we onderzoeken en aanvullende analysevragen ter ondersteuning van het beantwoorden van uw vraagstelling. Daarmee structureert het informatieverzameling en analyse binnen ons onderzoek.

	Onderzoeksaspect	Invulling en resultaten programma	Beoordeling richting/inrichting/verrichting
1.	**Richten**		
	Programma	- Welke ambities en doelen zijn gesteld voor het programma in het programmaplan/jaarplan en andere documenten, zoals programmabrochure, versnellingsafspraken BAW 2020 en bestuurlijke afspraken?	- Sluiten de ambities en doelen nog aan op de behoeften en verwachtingen van de stakeholders/waterpartners? - In hoeverre zouden doelen moeten worden aangescherpt of bijgesteld voor een vervolg van het programma?
	Ontwikkelingen	- Wat wijzigt er in de wet- en regelgeving? Wat is de invloed hiervan op de inrichting/aansturing van het programma? - Welke andere externe factoren zijn van invloed op het programma en op wat voor manier?	- Hoe werken de ontwikkelingen door, in de richting die vanuit het programma is gewenst?
2.	**Inrichten** *Input/throughput*		
	Programma	- Hoe ziet de inrichting en structuur van het programma eruit? - Welke projecten/activiteiten maken onderdeel uit van het jaarplan? - Welke uitgangspunten en kaders zijn gesteld aan het programma? - Welke doelen/gewenste uitkomsten zijn voor de projecten/activiteiten vastgelegd?	- Hoe wordt de inrichting en structuur van het programma beoordeeld? - Hoe wordt teruggekeken op de gestelde uitgangspunten, kaders en doelen? - Sluit dit (nog) aan bij de gewenste richting van het programma? En wat betekent dit voor de toekomstige inrichting/organisatie?
	Governance/bestuurlijk commitment	- Hoe is de governance naar buiten toe ingericht? - Hoe zijn de stakeholders en bestuurders aangehaakt? - Welke financiële dekking was er voor het programma?	- Hoe heeft de governance (binnen en buiten het programma) gefunctioneerd? - In hoeverre zijn stakeholders voldoende aangehaakt en is er sprake van bestuurlijk commitment? - In hoeverre draagt de governance naar buiten toe bij aan het behalen van de doelen? - Is de governance nog passend bij de (toekomstige) opgaven, wensen of eisen? Waarom wel/niet? - Hoe heeft de financiële dekking zich verhouden tot de benodigde financiering?

	Onderzoeksaspect	Invulling en resultaten programma	Beoordeling richting/inrichting/verrichting
3.	**Verrichten** *Output/outcome*		
	Projecten/activiteiten	- Welke resultaten zijn behaald en welke zijn nog voorzien tot eind 2022 en daarna? - Welke resultaten zijn niet behaald?	- Wat zijn succesfactoren voor het behalen van resultaten en wat is er nodig om te slagen? - In hoeverre dragen de resultaten bij aan de ambities/doelen van het programmaplan en aan de digitale veiligheid en weerbaarheid van de waterpartners? - Hebben de resultaten het gewenste effect gehad? - Zijn resultaten zoals beschikbaarheid van kennis en producten ook op langere termijn geborgd? - Welke resultaten zijn op inhoudsniveau gewenst in de jaren 2023 en verder?
4.	**Overig**		
	Aanbevelingen en wet- en regelgeving	- Welke wijzigingen in wet- en regelgeving op het gebied van cyberweerbaarheid zijn te verwachten? - Wat is het effect van deze nieuwe wet- en regelgeving op de waterpartners, het programma en welke aanbevelingen?	- Welke aanbevelingen volgen uit het effect van de nieuwe regelgeving op de waterpartners? - Welke conclusies en aanbevelingen zijn te trekken over voortzetting en continuïteit van het programma op basis van de bevindingen? - Welke governance en inhoud hoort daarbij, met welke inbedding in andere afspraken?

Bijlage 2. Projectenlijst programmaplan (2020)

Nr.	Naam project	Beschrijving project	Startjaar
1	Ketenanalyse	1. Ontwikkeling van een methodiek voor ketenanalyse. 2. Mogelijk: uitvoering analyses. 3. Ingebruikname door sector.	2020
2	Kennishub	Opzetten van hub: kan variëren van een website tot een SCADA competence center. Om kennis, actuele ontwikkelingen, trainingen en technische oplossingen samen te brengen.	2020
3	Oefenfaciliteit	Opzetten van een oefenfaciliteit: in de vorm van toolbox, maar kan ook een oefening zijn, of fysieke oefenfaciliteit.	2021
4	Versterking samenwerking/SOC	Versterken van de samenwerking in de watersector, mogelijk trechteren naar drinkwatersector. In de vorm van een SOC.	2020
5	Methodiek risicoanalyses	Ontwikkeling sectorbrede systematiek voor risicoanalyse: 1. Inventarisatie. 2. Behoeftestelling. 3. Mogelijk implementatie.	2020
6	Crisismanagement-oefening	Oefening in de drinkwatersector; simulatie of serious game (eigen voorstel).	2020
7	Baselines SCADA	Vaststellen baselines en ontwikkeling aanvullende eisen voor SCADA.	2020
8	Risk-appetite	Uitvoeren algemeen risicobeeld van de watersector.	2021
9	Uitvoeren risicoanalyses	Uitvoeren van risicoanalyses naar aanleiding van een methodiek.	2021
10	SCADA-systematiek	Ontwikkelen systematiek voor beoordelen risico's in een SCADA-omgeving	2021
11	Formuleren maatregelen	Formulering van passende maatregelen voor de sector naar aanleiding van uitkomsten vitaliteitsbeoordelingen en ketenanalyse.	2021

Nr.	Naam project	Beschrijving project	Startjaar
12	Vitaliteits-beoordelingen	Maken van gedeeld bestuurlijk beeld van vitaliteit keren en beheren, watertransport en waterzuivering, ook regionaal.	2020
13	Programmakosten	Financiering programmateam bestaat uit 1) inhuur projectcoördinatoren, programma-secretaris 2) facilitaire kosten programma	2020

Bijlage 3. Projectenlijst actueel (2022)

Legenda tabel

Bereikt, wordt naar verwachting bereikt in 2022, staat in 2023 op de planning, nog niet bereikt/planning nog niet hard. De meetdatum van deze tabel is oktober 2022.

Nr.	Project/activiteit	Thema	Toelichting op activiteit en doel	Bereikt
1	Serious game cybercrisis	TT&O	Ontwikkeling seriousgame cybercrisis. Deze game helpt medewerkers hun kennis en handelingsperspectief bij een cybercrisis te vergroten.	
2	Red Team Blue Training	TT&O	Aanbod Red Team Blue Training. Deze RTBT-training leert iedereen die werkt met OT-systemen (Operationele Technologie-systemen) de fundamenten van cybersecurity.	
3	Serious game ketenafhankelijkheden	TT&O	Ontwikkeling seriousgame met meerdere organisaties in de keten. Bij deze game wordt geoefend met incidentscenario's die meerdere organisaties in de keten raken. De nadruk ligt op het verkleinen van de impact van deze ketenincidenten.	
4	Haalbaarheidsstudie Cyber range oefenfaciliteiten	TT&O	Onderzoek met onderzoeksinstituten en stakeholders uit de watersector naar de mogelijkheden voor een cyber range oefenfaciliteit water. In een cyber range omgeving kunnen cybersecurity specialisten offensieve en defensieve vaardigheden oefenen.	
5	Red teaming testmethode	TT&O	Ontwikkeling van een redteaming methode toepasbaar in de watersector. Door red team testen, gebaseerd op realistische dreigingen, krijgen organisaties inzicht in hun sterke en zwakke punten. Ook vergroten ze zo hun weerbaarheid tegen geavanceerde cyberaanvallen.	
6	Handreiking risicoanalyse OT security	KR&M	Handreiking met als doel bestuurders in staat te stellen beter in kaart te hebben welke cybersecurityrisico's voor hun organisatie relevant zijn en waar sturing nodig is.	

Nr.	Project/activiteit	Thema	Toelichting op activiteit en doel	Bereikt
7	Inzicht in dreigingen watersector	KR&M	Op basis van een algemeen strategisch dreigingsbeeld wordt specifiek voor de watersector een dreigingsbeeld opgesteld. Dit wordt vertaald naar een operationeel niveau voor het gerichter nemen van maatregelen.	
8	Handreiking classificeren missiekritieke objecten	KR&M	Handreiking ontwikkeld voor waterschappen met een methode om processen, objecten en systemen te beoordelen. Hiermee kan worden bepaald welke processen, objecten en systemen essentieel zijn voor het continueren van het proces 'keren en beheren waterkwantiteit'.	
9	Actualiseren weerbaarheidsanalyse en actieprogramma 'keren en beheren waterkwantiteit'	KR&M	Het proces keren en beheren waterkwantiteit wordt conform de vereisten vanuit de NCTV opnieuw beoordeeld op vitaliteit. Op basis van de uitkomsten worden maatregelen geïdentificeerd en aanbevolen ter implementatie.	
10	Ontwikkelen methode ketenanalyse	KR&M	Ontwikkelen van een methode voor het uitvoeren van ketenanalyses binnen de watersector. Het doel van de methode is om cybersecurityrisico's voor de keten als geheel in kaart te brengen.	
11	Ketenanalyse hoofd- en regionale watersystemen	KR&M	Samen met RWS en de waterschappen wordt de methodiek voor ketenanalyse toegepast in het hoofdwatersysteem en alle regionale watersystemen. Hiermee worden voor de hele keten onderlinge afhankelijkheden en risico's inzichtelijk en wordt de samenwerking bevorderd.	
12	Adviesdag Ransomware preparedness (RAP)	M&I	Een adviesdag over ransomware preparedness (RAP).	
13	Workshop OT security	M&I	Workshop over basiskennis van OT, nieuwe kennis aan de hand van nieuwe best practices en normen zoals CSIR en IEC62443	
14	Best practices Kwetsbaarheden- en patchmanagement	M&I	Workshop over specifieke eigenschappen patchproces in OT-omgevingen. Resultaten worden ook beschikbaar gesteld in een Whitepaper.	
15	Handreiking industriële automatisering en controle systemen secure HIACSS	M&I	Handreiking over implementatie OT security maatregelen. Draagt bij aan opstap naar uitgebreidere CSIR 3.0.	
16	Handreiking proces coordinated Vulnerability Disclosure (CVD)	M&I	Handreiking over 'Coordinated Vulnerability Disclosure' (CVD) proces, om kwetsbaarheden te melden.	

Nr.	Project/activiteit	Thema	Toelichting op activiteit en doel	Bereikt
17	Verbreding Cyber Security Implementatie Richtlijn voor Waterschappen (CSIR 3.0)	M&I	Ontwikkeling Cybersecurity implementatierichtlijn (CSIR 3.0) door RWS en waterschappen. De CSIR 3.0 is een optioneel kader met een passende set beheersmaatregelen die de vitale infrastructuur met industriële automatisering cyberweerbaar maakt en houdt.	
18	Use cases en app CSIR	M&I	Toepassing CSIR 3.0 in een aantal use cases bij de waterschappen. Ontwikkeling tooling toegankelijkheid maatregelen CSIR. De tooling helpt de asseteigenaar om cybersecurity te borgen in de lifecycle en aan te sluiten op bestaande processen	
19	Implementatie onderzoeksresultaten ketenanalyse	M&I	Op basis van de uitkomsten van ketenanalyses die organisaties uitvoeren, wordt onderzocht welke stappen te zetten om passende maatregelen te implementeren en monitoren. Deze maatregelen kunnen de gesignaleerde cybersecurityrisico's in de keten kleiner maken.	
20	Workshop best practices monitoring en detectie	M&D	Workshop over best practices monitoring en detective. Helpt om organisaties hun monitoring en detectie optimaal in te richten en quick wins te realiseren.	
21	Haalbaarheidsstudie SOC watermanagement	M&D	Haalbaarheidsstudie naar het leveren van een monitoringsdienst vanuit de samenwerking CERT-WM/SOC-RWS aan waterschappen door middel van een proof-of-concept (PoC).	
22	Verkenning samenwerking monitoring en detectie watersector	M&D	Het Programma Versterken Cyberweerbaarheid in de Watersector onderzoekt samen met de watersector of samengewerkt kan worden op het gebied van monitoring en detectie.	
23	Faciliteren en borgen bestuurlijke afspraken	S&E	In de loop van 2022 wordt bezien of, en zo ja in welke hoedanigheid, of verlenging van de samenwerking Bestuursakkoord Water mogelijk en wenselijk is.	
24	ONE conference water en OT track	S&E	Een ONE conference van het NCSC voor het uitwisselen van kennis en expertise.	
25	Uitbouwen CERT-WM functionaliteit	S&E	Actieplan opstellen om robuustheid SOC- en CERT-functie te verbeteren. Dit actieplan sluit aan bij de ambities van het CERT-WM en waarborgt het uitwisselen van informatie en kennisproducten voor de watersector.	

Nr.	Project/activiteit	Thema	Toelichting op activiteit en doel	Bereikt
26	Center of expertise	S&E	In 2022 wordt nader bezien of centrale borging nodig is voor de opgebouwde expertise en samenwerkingsvormen. Uitgangspunt zijn de projecten binnen de vijf thema's en de nieuw te ontwikkelen programmawebsite. Er wordt aansluiting gezocht bij de IenW-brede cybersecurity strategie.	

Bijlage 4. Impact aanstaande wet- en regelgeving

Wet- en regelgeving	Status	Toelichting	Impact Projecten BAW	Bronnen
Europese wet- en regelgeving				
NIS2 Directive en CER Directive ---- Bescherming kritieke infrastructuur en aanbieders van vitale diensten.	Voorstel (In werking in Nederland naar verwachting medio-eind 2024)	De voorstellen voor de Europese richtlijnen NIS2 en CER zijn gericht op het beter beschermen van onze kritieke infrastructuur en vitale diensten. Tezamen zijn beide voorstellen gericht op het verbeteren van de integrale veiligheid van diensten en producten die hieronder vallen. De NIS2 richt zich primair op de digitale veiligheid en de CER richt zich primair op fysieke veiligheid. Indien beide voorstellen worden aangenomen en worden vertaald naar Nederlandse wet- en regelgeving zal dit onder meer de volgende wijzigingen met zich meebrengen: • De scope van organisaties en sectoren die onder deze wet- en regelgeving vallen, zal uitgebreid worden. Voor dit project is het relevant dat in ieder geval het openbaar bestuur en de verwerking van afvalwater in scope zullen vallen. • De verplichting ten aanzien van het rapporteren rondom informatiebeveiliging en incidentmanagement worden versterkt en vergroot. Bovendien zullen er wijzigingen worden ingevoerd die impact hebben op de wijze van melden en rapporteren.	Op basis van een eerste scan van de projecten die onder BAW vallen, zal dit in ieder geval invloed hebben op: • VNAC-Projecten Rijkswaterstaat. • Toezicht en handhaving op de WBNI. • Vitaliteitsbeoordelingen. • Uitbreiding SOC-RWS monitoringsdienst. • Verkenning SOC-Drinkwater. • Methodiek en uitvoering risico-analyses	NIS2 Directive: • Artikel Europarl • Artikel EC CER Directive: • Voorstel • Artikel Zie hiervoor ook de eerste pijler van de Nederlandse Cybersecurity-strategie.

		• Er zullen strengere eisen komen met betrekking tot het nemen van maatregelen in het kader van informatiebeveiliging. Deze strengere maatregelen zullen onder meer betrekking hebben op de volgende onderwerpen: *risicomanagement, supply chain security, encryptie en vulnerability management.* • Het toezicht op de naleving hiervan zal strenger worden en toezichthouders zullen meer instrumenten krijgen om naleving van de maatregelen te verbeteren. Implementatie: momenteel zijn beide richtlijnen nog niet aangenomen binnen de EU. Nadat de richtlijnen zijn aangenomen dienen ze nog vertaald te worden naar Nederlandse wet- en regelgeving. Dit zal onder meer leiden tot wijzigingen in de Wbni, maar mogelijk ook sectorale wet- en regelgeving. De exacte impact is nog niet bekend.	• Ontwikkelen SCADA-norm. • Formuleren maatregelen. • Verplichte diensten en producten van en eisen aan het CERT-WM.	
Cybersecurity Act (relaties met Radio Equipment Directive)	(Deels) in werking	De EU Cybersecurity Verordening versterkt de positie van de ENISA en introduceert een Europees cybersecurity certificeringsstelsel voor ICT-producten, diensten en processen. Op basis van deze verordening worden certificeringsschema's gecreëerd die toezien op specifieke categorieën van producten en diensten, de beveiligingsvereisten die daarop van toepassing zijn, (zoals bijvoorbeeld standaarden of technische specificaties), de wijze waarop de certificering plaatsvindt en de mate van zekerheid die wordt geboden. In Nederland is ter implementatie van deze verordening de Uitvoeringswet cyberbeveiligingsverordening aangenomen. Hierin is onder meer vastgelegd dat het Agentschap Telecom de Nederlandse Nationale Cybersecurity certificeringsautoriteit (NCCA) zal zijn. Momenteel zijn er nog geen certificeringen verplicht op grond van de verordening. Echter op korte termijn is het zeer waarschijnlijk dat dit zal veranderen. Hiervoor zijn momenteel al diverse verkenningen gaande welke onder meer plaatsvinden in het Union Rolling Work Programme for European cybersecurity certification.	Op basis van een eerste scan van de projecten die onder BAW vallen, zal dit in ieder geval invloed hebben op: • VNAC-projecten Rijkswaterstaat. • Haalbaarheidsstudie harmonisatie standaarden voor de cybersecurity van Industrial Control Systems (ICS). • Methodiek en uitvoering risico-analyses.	https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32019

		Wanneer bepaalde certificeringen straks verplicht zullen worden gesteld voor specifieke diensten, producten of processen, zal dit onder meer impact hebben op de wijze waarop binnen de watersector maatregelen worden getroffen en diensten worden beschermd. Zo zou het in de toekomst mogelijk zijn dat bepaalde normen rondom Industriële Controle Systemen (ICS) verplicht worden gesteld. Ook zal er een relatie bestaan met de EU Cyber Resilience Act waarvan een concept gereed was in het najaar van 2022. Deze zal eisen gaan stellen aan producten die op de markt worden gebracht. Producten die worden gebruikt in primaire processen in de watersector zullen daarbij al gauw Class I of Class II producten zijn, welke moeten worden beoordeeld volgens een standaard of door een derde partij. Mogelijk kan het programma hier op termijn ook een rol in vervullen door bijvoorbeeld een onderzoek te doen naar de effecten van de Cyber Resilience Act op de wijze waarop het risicomanagement is ingericht en op het inkoopbeleid.	• Ontwikkelen SCADA-norm. • Formuleren maatregelen.	R0881&from=EN#d1e1099-15-1 Uitvoeringswet cyberbeveiligingsverordening https://www.agentschaptelecom.nl/onderwerpen/cybersecurity-certificering/over-de-csa https://ecer.minbuza.nl/-/europese-cyber-security-act-van-kracht#:~:text=Het%20%20certificatiesysteem%20is%20een%20van,door%20de%20EU%20opgelegd%20kunnen%20worden.&text=Het%20%20certificatiesysteem%20is,EU%20opgelegd%20kunnen%20worden.&text=certi

				ficatiesysteem%20is%20een%20van,door%20de%20EU%20opgelegd
Nederlandse wet- en regelgeving				
Wettelijke verplichting BIO	Plannen	Eén van de plannen binnen de rijksoverheid is om informatieveiligheid binnen de (rijks)overheid een wettelijke basis te bieden. Hiervoor wordt overwogen om een zorgplicht te implementeren, waaraan nadere regels kunnen worden gesteld zoals de BIO. Door het wettelijk verplichten van de BIO is de vrijblijvendheid voorbij. Vanuit de rijksoverheid worden aan medeoverheden vanuit verschillende bronnen informatiebeveiligingseisen gesteld. Door op één plaats een algemene zorgplicht voor informatieveiligheid bij de overheid te regelen, wordt ook een vereenvoudiging van regels binnen de overheid bereikt. Daardoor komt de focus meer te liggen op het feitelijk beveiligen in plaats van administratief beveiligen.	• VNAC-Projecten Rijkswaterstaat. • Toezicht en handhaving op de WBNI. • Uitbreiding SOC-RWS monitoringsdienst. • Verkenning SOC-Drinkwater.	Kamerbrief: BZK Generiek kader voor vitale digitale processen van de overheid (2022-0000478858)
Landelijk dekkend stelsel (LDS)	Plannen	Er zijn plannen voor verdere doorontwikkeling van het Landelijk Dekkend Stelsel.		???

WIJ ZIJN BERENSCHOT, GRONDLEGGER VAN VOORUITGANG

Nederland is continu in ontwikkeling. Maatschappelijk, economisch en organisatorisch verandert er veel. Al meer dan tachtig jaar volgen wij als adviesbureau deze ontwikkelingen op de voet en werken we aan een vooruitstrevende samenleving. De behoefte om iets fundamenteels te betekenen voor mens en maatschappij zit in onze genen. Met onze adviezen en oplossingen hebben we dan ook actief meegebouwd aan het Nederland van vandaag. Altijd op zoek naar duurzame vooruitgang.

Alles wat we doen is onderzocht, onderbouwd en vanuit meerdere invalshoeken bekeken. Zo komen we tot gefundeerde adviezen en slimme oplossingen. Die zijn op het eerste gezicht misschien niet altijd de meest voor de hand liggende. Juist deze eigenzinnigheid maakt ons uniek. Daarbij zijn we niet van symptoombestrijding. En gaan pas naar huis als het is opgelost.

Berenschot Groep B.V.

Van Deventerlaan 31-51, 3528 AG UTRECHT
Postbus 8039, 3503 RA UTRECHT
030 2 916 916
www.berenschot.nl