

Drinkwaterbedrijven, gemeenten, provincies, waterschappen, Rijkswaterstaat en het ministerie van Infrastructuur en Waterstaat werken samen aan:



Programma
**Versterken
Cyberweerbaarheid
in de watersector**
2023 – 2024

Klik op 1 van onderstaande knoppen om verder te gaan.



Introductie

In Nederland zorgen gemeenten, provincies, waterschappen, Rijkswaterstaat en drinkwaterbedrijven voor het leveren van drinkwater, keren en beheren van oppervlaktewater en het transport en het zuiveren van afvalwater. Voor deze maatschappelijke processen gebruiken we geautomatiseerde (procesbesturing) systemen. De digitale dreiging vanuit kwaadwillenden om deze processen te ontwrichten neemt steeds verder toe, concluderen de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD).

Partijen uit de watersector hebben daarom de handen ineengeslagen om de cyberweerbaarheid te versterken en zo aanvallen in de toekomst het hoofd te bieden. In het programma Versterken Cyberweerbaarheid in de Watersector werkt het ministerie van Infrastructuur en Waterstaat samen met partijen in de watersector aan diverse projecten, met name gericht op operationele technologie. Deze projecten ontstaan uit de behoeften die de partijen gezamenlijk hebben. De opgedane kennis komt ten goede aan de gehele watersector.

Verhogen van cyberweerbaarheid

De samenwerking tussen Rijk, gemeenten, waterschappen, provincies en drinkwaterbedrijven is vastgelegd in het Bestuursakkoord Water, en in 2023 opnieuw vastgelegd in bestuurlijke afspraken in het Bestuurlijk Overleg Water. Tegenover de kansen van digitalisering in de watersector zijn er ook uitdagingen op het gebied van cybersecurity. De vijf partijen hebben daarom ook afspraken gemaakt over het verhogen van de cyberweerbaarheid

Visie

Waterveiligheid en digitale veiligheid zijn onlosmakelijk met elkaar verbonden. Nederland moet kunnen vertrouwen op een betrouwbaar en zo veilig mogelijk waterbeheer en (drink)watervoorziening. Hiervoor is het van belang dat het niveau van beveiliging past bij het actuele dreigingsniveau en hierbij behorende cyberrisico's die relevant zijn voor de watersector. Het programma helpt door het initiëren en coördineren van gezamenlijke projecten met als doel om de cyberweerbaarheid in de waterketen te versterken. Deze projecten zijn in lijn met de doelstellingen die zijn vastgelegd in de Nederlandse Cybersecurity Strategie en onderdeel van het beleid om vitale processen continue te versterken. De waterketen staat centraal. Het programma fungeert als de verbindende schakel tussen organisaties in de watersector en vervult een stimulerende rol richting de deelnemende organisaties waarbij de verantwoordelijkheid voor het nemen van de juiste maatregelen bij organisaties zelf blijft. Hiermee draagt het programma bij aan de weerbaarheid van organisaties in de watersector om de gevolgen van cyberdreigingen op te vangen en ketens in de watersector veiliger te maken.

Structuur van het programma





Wil je het volledige overzicht van alle projecten bekijken? Bekijk dan [hier](#) ons jaarplanoverzicht.

Thema's en doelstellingen



Trainen, testen en oefenen

Door te trainen, oefenen en testen krijgen organisaties inzicht in verbeterpunten en kunnen ze zich optimaal voorbereiden op incidenten.



Ketens en risicomanagement

Organisaties helpen met het verkrijgen van inzicht in de dreigingen en (keten-)risico's die voor een organisatie en voor de waterketen als geheel relevant zijn.



Maatregelen en implementatie

Organisaties ondersteunen bij het nemen van de (basis-)maatregelen om de weerbaarheid te versterken.



Monitoring en detectie









































Het bieden van instrumenten waardoor organisaties monitoring en detectie optimaal kunnen inrichten om incidenten zo snel mogelijk op te kunnen merken en zo snel mogelijk te kunnen handelen.








Samenwerking en expertise

De cybersecurityexpertise binnen de watersector verbeteren door het verstevigen van de samenwerking en het borgen van de kennis.

Overzicht projecten

Trainen, testen en oefenen	Ketens en risicomanagement	Maatregelen en implementatie	Monitoring en detectie	Samenwerking en expertise
Bestuurlijke cybercrisis oefening - OT 	Handreiking en workshop 'Grip op aanvalsoppervlak' 	Aandachtspunten implementatie NIS2 	Seminar best practices monitoring en detectie 	Borging resultaten programma 
Curriculum trainingen 	Inzicht in dreigingen watersector (periodiek) 	Stimuleren implementatie 'Responsible Disclosure (RD)' 	Handreiking 'Opvolging cybersecurity meldingen' 	Bestuurlijk commitment vergroten 
Serious game cybercrisis 	Handreiking classificeren missiekritieke objecten 	Webinair en paper beschermen logdata 	Ondersteunen SOC waterschappen 	Gezamenlijke visie en ambitie bepalen 
Red Team / Blue Team training 	Verkennen gedeelde afhankelijkheden toeleveranciers 	Adviesdag Ransomware Preparedness (RAP) 	Monitoring en detectie drinkwatersector 	Versterken programma governance 
Serious game ketenafhankelijkheden 	Methode ketenanalyse 	Best practices kwetsbaarheden- en patchmanagement 	Haalbaarheidsstudie SOC watermanagement 	ONE Conference 2023 
Haalbaarheidsstudie cyberrange oefenfaciliteit 	Ketenanalyse hoofd- en regionaal watersysteem 	Handreiking Basismaatregelen voor cybersecurity van IACS (BIACS) 	Haalbaarheidsstudie scannen op kwetsbaarheden binnen de sector 	ONE Conference 2022 OT-track 
TIBER water 		Inrichten beheer en onderhoud CSIR 		Doorontwikkeling CERT-stelsel watersector 
Red teaming testmethode 		CSIR Tooling 		Uitbouwen CERT-WM functionaliteit 
		Verbreding Cyber Security Implementatie Richtlijn voor waterschappen (CSIR3.0) 		Center of Expertise 
		Ketenregie: uitwerken rollen en verantwoordelijkheden 		
		Implementatie ketenmaatregelen 		

Legenda:

-  Complexiteit instrument | Basis
-  Complexiteit instrument | Gevorderd
-  Complexiteit instrument | Volwassen
-  Nieuw of verder te ontwikkelen
-  Beschikbaar





Contact

De uitvoering van het programma is in handen van het programmateam, gevestigd bij het ministerie van Infrastructuur en Waterstaat.

Meer weten? Neem gerust contact op via cyberweerbaarheidwater@minienw.nl.

Contactpersonen:



Jessica Maes
Programmamanager
jessica.maes@minienw.nl



Eva Maas
Themacoördinator trainen, testen en oefenen
eva.maas@minienw.nl



Florian Lous
Programmasecretaris & -adviseur
florian.lous@minienw.nl



Ministerie van Infrastructuur
en Waterstaat



Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat



 UNIE VAN
WATERSCHAPPEN

