Ministerie van Infrastructuur
en Waterstaat

Nieuwsbrief Q3 2023

Programma
Versterken Cyberweerbaarheid in de watersector

Voor je heb je alweer de derde nieuwsbrief van dit jaar! In de vorige nieuwbrief noemden we ons jaarplan. Het is een belangrijk fundament van het programma. In deze nieuwsbrief lees je over het jaarplan én over een aantal ontwikkelingen in de projecten die we uitvoeren.

Op je gemak alles teruglezen? Je vindt alle artikelen uit deze en komende nieuwsbrieven op versterkencyberweerbaarheid.nl. Houd deze website ook in de gaten voor de nieuwste ontwikkelingen en evenementen.

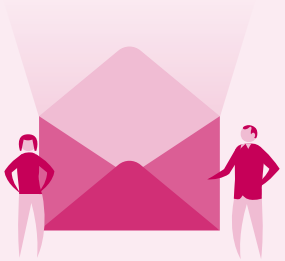
Veel leesplezier!

Interesse om bij te dragen aan de volgende nieuwsbrief?
Laat het ons dan weten en **mail** ons!

Klik op 1 van onderstaande knoppen om verder te gaan.

Voorwoord

Programmanieuws kort



Contact

Voorwoord

Aan de slag met onze ambities – een update

In de vorige nieuwsbrief las je dat we naar aanleiding van de evaluatie aan de slag gingen met het maken van bestuurlijke afspraken en het formuleren van de ambities van het programma. Inmiddels heeft het Bestuurlijk Overleg Water deze afspraken bevestigd en hebben zij ook onze ambities goedgekeurd. Dat we weer hard aan de weg timmeren op basis van deze ambities is wel duidelijk. Dank aan alle lezers die hier een belangrijke bijdrage in leveren.

OT-diner 2023 & ONE Conference
Tussen de oude trams bij De Remise in Den Haag organiseerden we aan de vooravond van de ONE Conference het OT-Diner. Niet alleen vanuit de watersector waren OT-experts aanwezig, maar ook vanuit luchtvaart-, maritieme en de energiesector.

Naast het gezamenlijk diner luisterden we naar presentaties van Dragos en Maersk. We sloten de avond af met een ludieke OT-pubquiz.

Op de ONE introduceerden we samen met het NCSC, de IBD en Rijksinspectie voor Digitale Infrastructuur de IACS-coalitie. Met de kennis in het programma voor de watersector willen we meer samen optrekken om het belang van OT/IACS-kennis te vergroten.

Veel leesplezier!

Jessica Maes, programmamanager

< Vorige pagina

Verder lezen >

Programmanieuws kort

Programmabrochure en jaarplan

Samen zetten we ons in om de cyberweerbaarheid in de Nederlandse watersector te versterken. Daar horen een sterke visie en stevige ambities bij. Met trots presenteren wij daarom de vernieuwde programmabrochure en het vernieuwde jaarplan. Ontdek hoe we een positieve impact willen hebben op de toekomst van het digitale landschap.

Bekijk het jaarplan en de programmabrochure

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	Gezamelijke 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*

< Vorige pagina

Verder lezen >

Lees nu onze visie en ambities

Programma 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.

Ambities
Het programma Versterken Cyberweerbaarheid in de Watersector realiseert haar visie door risico- en vraaggericht te werken. De ambities van het programma zijn als volgt:

- De samenwerking tussen organisaties in de watersector wordt versterkt waardoor organisaties van elkaar kunnen leren en de beperkte capaciteit optimaal wordt benut.
- Organisaties in de watersector worden ondersteund om zicht te hebben op het dreigingslandschap. Het programma organiseert inzicht in strategisch en tactische cyberdreigingen op sectorniveau, en zorgt voor een vertaling naar concreet handelingsperspectief voor organisaties.
- Het zicht op risico's in de primaire procesketen voor de waterketen en toeleverancierskete wordt vergroot. Organisaties worden geholpen om zelf de vertaling te maken naar cybersecurity risico's op organisatieniveau en hier maatregelen op te nemen.
- Het programma maakt inzichtelijk wat de eisen zijn van (nieuwe) wet- en regelgeving. Het programma maakt een vertaling van wettelijke vereisten naar concrete handvatten die organisaties helpen bij de implementatie hiervan.
- Organisaties zijn beter in staat om te reageren op en te herstellen van cyberincidenten en -crises. Daarnaast wordt het leervermogen vergroot. Het programma ondersteunt hierbij door projecten op het gebied van trainen, testen en oefenen.
- Het programma versterkt het bewustzijn bij bestuurders over het belang van cybersecurity.
- Resultaten en ervaringen van het programma worden structureel geborgd en waar mogelijk gedeeld met andere sectoren en organisaties, specifiek op het gebied van Industriële Controle Systemen.

< Vorige pagina

Verder lezen >

De rol van Cyber Ranges en Digital Twins

Het ministerie van Infrastructuur en Waterstaat (IenW) heeft TNO een verkennings-taak gegeven: hoe kunnen twee opkomende technologieën - 'Cyber Ranges' en 'Digital Twins' - bijdragen aan het versterken van de cyberweerbaarheid in de Nederlandse watersector? Dit zijn de belangrijkste resultaten.

Cyber Ranges
Cyber Ranges zijn moderne platforms die dienen als broedplaatsen voor interactieve simulatieomgevingen. Deze platforms creëren een gecontroleerde omgeving waarin je allerlei cyberaanvallen kunt simuleren. Je kunt er verdedigings-mechanismen testen en beveiligingsdreigingen leren detecteren en afweren.
Je kunt Cyber Ranges voor allerlei doeleinden gebruiken, zoals cybersecuritytests, onderzoek, training, beoordeling van cyberweerbaarheid, talentwerving in de cybersecuritysector en nationale en internationale cybersecuritycompetities.

Digital Twins
Digital Twins zijn een boeiende combinatie van fysieke systemen en hun virtuele tegenhangers, vaak in de vorm van een computermodel. Digital Twins zijn oorspronkelijk niet ontworpen voor cybersecurity, maar worden wel gebruikt bij het optimaliseren van kritieke, operationele bedrijfsprocessen. Een Digital Twin maakt een virtuele weergave van fysieke systemen, processen of objecten. Zo kun je prestaties van het werkelijke systeem, proces of object volgen, analyseren en optimaliseren.

Belangrijke vindplaatsen in het rapport
In het rapport 'Een verkenning voor de Nederlandse watersector: Cyber Ranges en Digital Twins' lees je alles over de bevindingen van de verkenning. Zo vind je op pagina 48 gedetailleerde informatie over deze technologieën en aanvullende afbeeldingen op pagina 20.

< Vorige pagina

Verder lezen >

De ketenanalyses zijn van start

Al eerder in de nieuwsbrieven zijn de ketenanalyses aan bod gekomen. TNO voert in opdracht van het ministerie van Infrastructuur en Waterstaat (IenW) een ketenanalyse rond cyberweerbaarheid uit op het gehele hoofd- en regionaal watersysteem. Inmiddels zijn er verschillende presentaties gegeven binnen de waterschappen over deze methodiek en is de planning onder voorbehoud bekendgemaakt.

Waar en wanneer?
Voor de verdeling en planning van de ketenanalyses volgen we de zes regio's die Slim Watermanagement onderscheidt. De functie keren van hoog water als gevolg van stormvloed is een nationale functie en daarom niet aan een regio gebonden. Hiernaast zie je de planning van de analyses.

Welke expertise en hoeveel?
Voor de uitvoering van de ketenanalyse zijn verschillende expertises nodig vanuit de waterschappen en Rijkswaterstaat. Voor elke regio hebben we maximaal zo'n 40 uur per organisatie nodig voor cybersecurityexpertise. Deze tijd zit in het bijwonen van de workshops, het voorbereiden van meetings, het verzamelen van informatie binnen de eigen organisatie en voor het reviewen van de rapportage. De kennis van het watermanagementsysteem die nodig is, komt vanuit de waterschappen en Rijkswaterstaat samen in Slim Watermanagement. Per regio verwachten we een bijdrage van ongeveer 16 uur. Het gaat om een digitale startbijeenkomst, een fysieke bijeenkomst voor de analyse over de keten heen en een review van het resultaat.

< Vorige pagina

Verder lezen >

Toewerken naar structureel inzicht in sectorale dreigingen “keren en beheren” door waterschappen en Rijkswaterstaat

Samen met de waterschappen, Rijkswaterstaat en het Nationaal Cyber Security Centrum (NCSC) hebben we een start gemaakt met een dreigingsbeeld voor ‘Keren en Beheren’. Het Waterschapshuis organiseerde op 29 juni een risicomanagementseminar. De ongeveer 60 deelnemers hebben in verschillende sessies een groot aantal scenario’s uitgewerkt.

Tijdens een vervolgsessie van het risicoseminar georganiseerd door het Waterschapshuis begin december gaan we de scenario’s voorzien van een waarschijnlijkheidsinschatting, samen met de expertise van cybersecuritydreigingsexperts van de Rijksoverheid en experts van de waterschappen en Rijkswaterstaat. Daarna hebben we een mooi product dat we kunnen delen, zodat ook jij weet welke dreigingen nou echt belangrijk zijn voor de watersector!

Het maken van een dreigingsbeeld wordt onderdeel van een proces dat we met elkaar gaan herhalen, zodat we met elkaar op de hoogte zijn van de belangrijkste dreigingen. Drinkwaterbedrijven hebben onlangs ook besloten om een gezamenlijk dreigingsbeeld op te gaan stellen volgens dezelfde methode van het NCSC. Dus daar gaat ook aan gewerkt worden!

< Vorige pagina

Verder lezen >

REMINDER / AGENDA

22 november - Bestuurlijke Cybertafel 2023
Ben jij een bestuurder en werkzaam in de watersector? Of vind jij dat jouw bestuurder ook aanwezig moet zijn? Er zijn nog enkele plaatsen vrij om mee te doen met de bestuurlijke cybertafel. Aanmelden kan via Registreren - Cybertafel

Bestuurlijke Cybertafel 2023 | Activiteit | Versterken cyberweerbaarheid

17 oktober - Red Team - Blue Team Training
De Red Team - Blue Team training is volgeboekt. Je kan je helaas niet meer aanmelden voor deze training.

Red Team - Blue Team Training | Activiteit | Versterken cyberweerbaarheid

< Vorige pagina

Verder lezen >

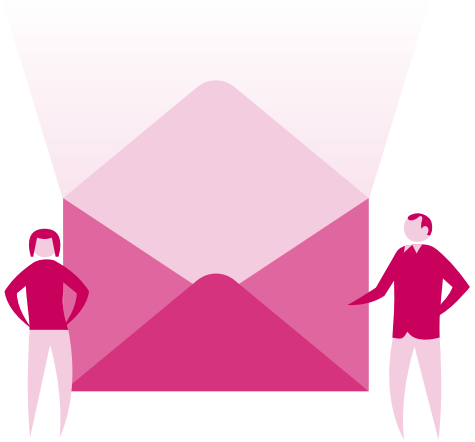
Contact

Heb je een vraag, opmerking of tip?
Mail dan naar cyberweerbaarheidwater@minienw.nl.

Contactpersonen
Jessica Maes, Florian Lous en Eva Maas

Website

Meer informatie over het programma, nuttige documenten en handige links vind je op versterkencyberweerbaarheid.nl.



< Vorige pagina