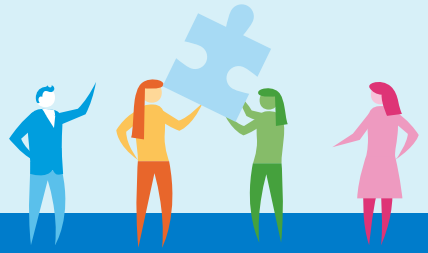
Programma
Versterken Cyberweerbaarheid in de watersector

Ministerie van Infrastructuur en Waterstaat

Nieuwsbrief Q2 2022

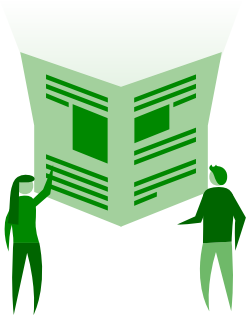
Voor u ligt alweer de tweede nieuwsbrief van 2022 van het programma 'Versterken cyberweerbaarheid in de watersector'. Hiermee brengen wij u op de hoogte van de voortgang van lopende projecten en algemeen nieuws over cybersecurity en de watersector. In deze nieuwsbrief vooral veel kort programmanieuws. In het eerste kwartaal van 2022 is het programma voortvarend aan de slag gaan met bestaande én nieuwe projecten (waarover we u in januari al informeerden). Dus, wilt u meer weten over red teaming, digital twins of patchmanagement, lees dan vooral verder.

Veel leesplezier!



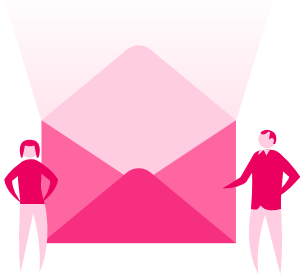
Interesse om bij te dragen aan de volgende nieuwsbrief?
Laat het ons dan weten en **mail** ons!

Klik op 1 van onderstaande knoppen om verder te gaan.



Algemeen nieuws

Programmanieuws kort



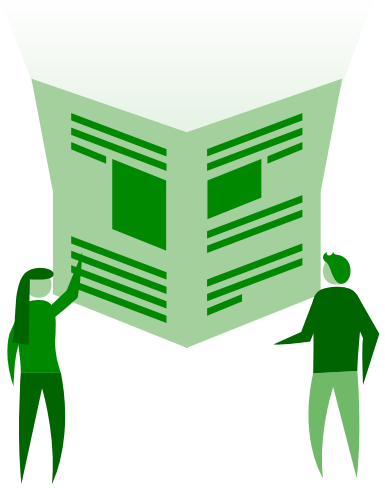
Contact

Algemeen nieuws

Webinar kwetsbaarheden- en patchmanagement voorziet in een behoefte

Donderdag 24 maart organiseerde het programma samen met het Nationaal Cyber Security Centrum (NCSC), Rijkswaterstaat (RWS) en de Inspectie Leefomgeving en Transport (ILT) een webinar over kwetsbaarheden en patchmanagement in het OT-domein. Met zo'n 90 deelnemers was het webinar zeer goed bezocht. Omdat ook tijdens de sessie bleek dat er veel behoefte is aan kennisuitwisseling op dit onderwerp, komt er een vervolg in de vorm van een blog.

Zie hieronder enkele associaties van de deelnemers bij patchmanagement:



< Vorige pagina

Verder lezen >

Programmanieuws kort

Nieuwe collega: Eva Maas

Dag collega's uit de watersector! Bij sommigen wellicht al bekend: ik ga het programma versterken. Jullie zullen mij de komende tijd met name tegenkomen op het thema trainen, testen en oefenen. Ik kijk ernaar uit om samen met jullie en goede stimulans te kunnen geven aan trainen, testen en oefenen binnen de sector als manier om onze gezamenlijke cyberweerbaarheid te verhogen.

In mijn vorige functie heb ik met mijn team in de financiële sector een methode ontwikkeld voor geavanceerde red teamtesten op basis van cyberdreigingen: Threat-Intelligence based Ethical Redteaming (TIBER). Hier heb ik bijgedragen aan de ontwikkeling van de test aanpak, red teamtesten begeleid en met organisaties samengewerkt in het onderling delen en leren van resultaten. Hierbij stond samenwerken en van elkaar leren centraal. Ik hoop ook op die manier met jullie te kunnen samenwerken.

Heb jij ambities voor jouw organisatie op het gebied van trainen, testen en oefenen of wil je graag meedenken over hoe we dit als sector kunnen gaan oppakken? Ik kijk ernaar uit om samen op te trekken! Stuur een mailtje naar ***cyberweerbaarheidwater@minienw.nl*** *of naar* ***eva.maas@minienw.nl****.*

Graag tot snel,
Eva Maas

Denk mee over de ONE conferentie!

In overleg met het NCSC hebben we ruimte gekregen om, waarschijnlijk in het voorprogramma, een aantal sessies te verzorgen op de ONE Conference in oktober met het zwaartepunt op OT security. Daarnaast hebben we gedurende de hele conferentie een ruimte om serious games in de watersector te spelen en demonstreren.

De precieze invulling van deze sessies staat nog niet vast. De longlist van onderwerpen is:

- Hoe kun je de goede maatregelen nemen voor je OT-omgeving op basis van beschikbare raamwerken?
- Risicomanagement voor OT: Waarom is dat zo lastig?
- Kwetsbaarheden- en patchmanagement in OT-omgevingen
- TIBER (threat intelligence based ethical red teaming) voor de watersector
- Samen bouwen aan een OT community
- Toepassingen van digital twins en cyber range

Heb jij meer ideeën of kun je op een andere manier inhoudelijk bijdragen? Graag horen we van je!

< Vorige pagina

Verder lezen >

TIBER watersector: ontwikkeling red teamingaanpak

Om de cyberweerbaarheid van organisaties te versterken, is trainen, testen en oefenen essentieel. Daarom is het als centraal thema opgenomen in het programma. We ontwikkelen hiervoor instrumenten op 3 verschillende niveaus: basis, gevorderd, volwassen.

Voor organisaties in het hoogste volwassenheidsniveau wordt het red teaming testraamwerk Threat Intelligence Based Ethical Redteaming (TIBER) in de watersector toepasbaar gemaakt. Oorspronkelijk was dit ontwikkeld voor de financiële sector. Hiermee wordt aangesloten bij initiatieven om TIBER toepasbaar te maken voor de Rijksoverheid zodat er één TIBER raamwerk voor vitale sectoren en de Rijksoverheid ontstaat. Op dit moment wordt met een geïnteresseerde organisatie uit de watersector geïnventariseerd hoe het project vorm zou kunnen krijgen. In een later stadium hopen wij ook een red teaming aanpak voor organisaties met een ander volwassenheidsniveau te realiseren. De RTBT-trainingen die wij meerdere keren per jaar aanbieden en veel enthousiasme losmaken, zijn een mooie opstap voor het opdoen van kennis in red- en blue teaming.

< Vorige pagina

Quantum

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) bracht onlangs de publicatie uit: '**Bereid je voor op de dreiging van quantum computers**'. Hierin wordt organisaties aangeraden om alvast te gaan werken aan een strategie voor post-quantumcryptografie.

Quantumtechnologie is momenteel nog volop in ontwikkeling. Quantum computing biedt een veel grotere rekenkracht dan traditionele computers. Berekeningen die momenteel enkele weken in beslag nemen, kunnen over ongeveer tien jaar in luttele seconden worden uitgevoerd. Dit maakt het mogelijk om zeer snel complexe berekeningen en simulaties uit te voeren. Quantum biedt dus veel kansen maar er komen ook nieuwe dreigingen uit voort. Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) van de AIVD acht het een reële kans dat quantumcomputers in 2030 al krachtig genoeg zijn om de huidige cryptografische standaarden te breken. De op dit moment meest gebruikte cryptografische 'public key' protocollen zijn dan niet veilig voor een aanval met een quantumcomputer. Momenteel wordt door bepaalde statelijke actoren reeds versleutelde informatie verzameld in afwachting van het moment dat je deze met quantum computing kan ontsleutelen.

Oplossing?
Post-quantumcryptografie is de tak van de cryptografie, die zich bezighoudt met het ontwikkelen van moderne, algoritmische encryptietechnologie. Deze technologie is bestand tegen aanvallen met een quantumcomputer. Er is nog veel onderzoek nodig om nieuwe protocollen te ontwikkelen die niet gebroken kunnen worden door quantumalgoritmes. Het is echter belangrijk om nu al aan de slag te gaan. Dit is het moment om al na te denken over de kroonjuwelen die beschermd moeten worden, welke vormen van cryptografie nu gebruikt worden en welke aanpak dit vraagt. Op dit moment hebben wij nog geen projecten in ons jaarplan opgenomen die hierop voorsorteren, maar indien u hier vanuit uw eigen organisatie meer informatie over wenst dan kunnen wij u wel van meer informatie voorzien. Binnen het ministerie van Infrastructuur en Waterstaat houden diverse collega's zich met dit onderwerp bezig.

Verder lezen >

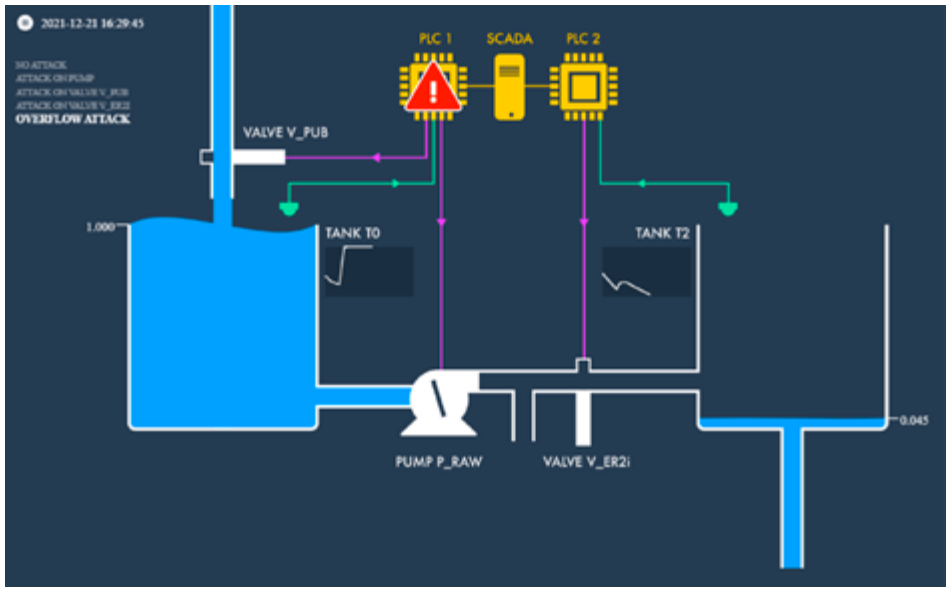
Cyber range en digital twin

Steeds vaker gaan er geluiden op om het oefenen met de eigen OT-systemen van organisaties in de watersector te bevorderen. Digital twin en cyber range faciliteiten bieden mogelijk uitkomst. De afgelopen maanden heeft het programma de eerste stappen gezet om de mogelijke toepassingen van digital twin en cyber range faciliteiten in de watersector in kaart te brengen.

Zo ziet TNO mogelijkheden om de cyberweerbaarheid van de watersector te verhogen door verbeterde cyber attackdetectie in waterdistributienetwerken inclusief de convergerende IT/OT-systemen binnen de sector. Zij willen hierbij inzichtelijk maken hoe aanvallen goed kunnen worden waargenomen. Hierbij is het detecteren van anomalieën (vreemde activiteiten of gedragingen binnen de infrastructuur die een signaal kunnen zijn van een aanval) van groot belang. De onderzoeksvraag is welke detectietechnieken geschikt zijn voor samengestelde IT/OT omgevingen in het algemeen en systemen in de watersector in het bijzonder. Dit met als doel de haalbaarheid en toepasbaarheid van (anomalie)detectie in waterdistributienetwerken en watersysteembeheer te toetsen. Daarbij wordt gebruik gemaakt van een te realiseren prototype voor security monitoring en detectie. Dit prototype kan worden gevalideerd binnen een digital twin en/of operationele context van een waterschap of een drinkwaterbedrijf.

TNO is op zoek naar een geschikte organisatie om dit verder mee te onderzoeken. Interesse in of vragen over dit onderzoek? Deel het met ons via **cyberweerbaarheidwater@minienw.nl**.

Binnenkort brengen we samen met een aantal partijen uit de watersector een bezoek aan TU Delft, waar veel onderzoek wordt gedaan naar de mogelijkheden van cyber range en digital twin- faciliteiten. In hun “control room of the future” kunnen geavanceerde cyberaanvallen op een digital twin van het elektriciteitsnet gesimuleerd worden. Interesse om mee te denken of meer te weten? Laat het ons weten via **cyberweerbaarheidwater@minienw.nl**.



Impressie van TNO simulatie

Adviesdag Ransomware Preparedness (RAP)

Ransomware is op dit moment één van de grootste dreigingen waar organisaties mee te maken kunnen krijgen. Om je als organisatie hier zo goed mogelijk op voor te bereiden, is het belangrijk een aantal basismaatregelen op orde te hebben.

Maar hoe weet je nu of je echt alles hebt gedaan om de kans zo klein mogelijk te maken dat jouw organisatie slachtoffer wordt? Om daar achter te komen willen we een ransomware preparedness (RAP) instrument ontwikkelen. Gedurende een halve of hele dag krijgen organisaties advies van een expert die samen met betrokken medewerkers een aantal basisonderwerpen doorloopt. Doordat de expert aanwezig is op locatie, krijgen organisaties een heel praktisch en bovenal vertrouwelijk beeld, waarmee ze de eigen cyberweerbaarheid concreet kunnen versterken.

Op dit moment bevindt het project zich nog in de ontwikkelfase en is er alle ruimte voor suggesties of het doorgeven van behoeften. Spreekt dit idee jou aan en zou je het graag willen toepassen op de eigen organisatie? Wij zoeken nog pilotorganisaties om bij de ontwikkeling te helpen. Neem vooral contact op via **cyberweerbaarheidwater@minienw.nl**.

Voortgang ketenanalyse

Afgelopen jaar zijn er twee casussen met TNO afgerond voor ketenanalyses in de watersector. Dit waren de ketenprocessen “afvoer van overtollig regenwater” en “inname van oppervlaktewater ten behoeve van de drinkwatervoorziening”. In 2022 zijn we gestart met de derde casus voor de ketenanalyse, het afvalwaterproces. Voor deze casus werken de gemeente Breda en het Waterschap Brabantse Delta samen met TNO aan het in kaart brengen van de ketenrisico’s.

In de tweede bijeenkomst van het projectteam is geanalyseerd welke systemen er gemeenschappelijk gebruikt worden in het gezamenlijke proces. Ook is gesproken over de robuustheid versus de kwetsbaarheid van deze systemen. Specifiek is gesproken over de afhankelijkheid van elkaars informatie; hoe kan je bepalen wat de maximale uitval mag zijn? Hierbij werd onderscheid gemaakt tussen de informatiestromen voor het reguliere proces en de informatie die nodig is als er sprake is van een calamiteit.

Graag wat meer weten of het uitvoeren van ketenanalyses? Neem dan even contact op.

< Vorige pagina

Verder lezen >

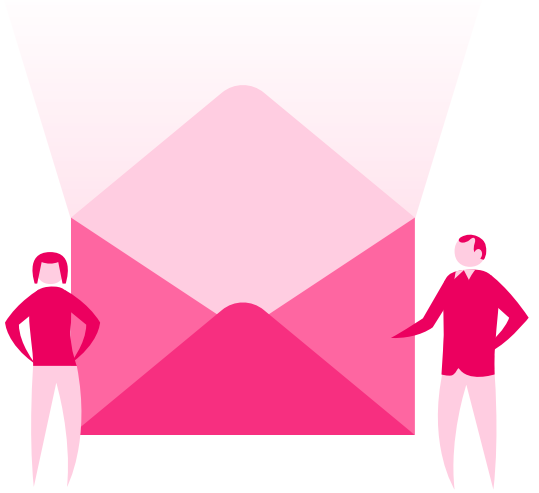
Contact

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

Contactpersonen
Eva Maas , Jessica Maes en Jeroen van den Berg

Website

Meer informatie over het programma, nuttige documenten en handige links kunnen ook geraadpleegd worden op onze webpagina **www.helpdeskwater.nl/pvcw**.



< Vorige pagina