Programma
Versterken Cyberweerbaarheid in de watersector

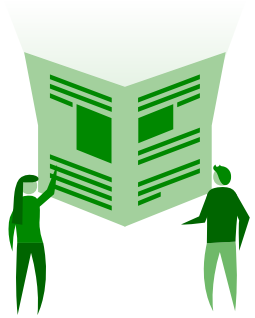
Nieuwsbrief Q1 2021

Voor u ligt de allereerste nieuwsbrief van het programma ‘Versterken cyberweerbaarheid in de watersector’. Hiermee brengen wij u ieder kwartaal op de hoogte van de voortgang van lopende projecten en algemeen nieuws over cybersecurity en de watersector. Daarnaast geven wij ook ruimte aan jullie, onze partners binnen de watersector, om verhalen en nieuwtjes uit de sector met een breed publiek te delen.

In deze editie vertellen we je onder meer over het Bestuursakkoord Water en de voortgang van de gemaakte afspraken, het verscherpte ILT toezicht van Waternet, de versterking van de digitale weerbaarheid van Nederland, serious gaming in de drinkwatersector en Europese ontwikkelingen. Namens het programmateam moedigen wij u aan om deze nieuwsbrief binnen uw netwerk onder de aandacht te brengen.

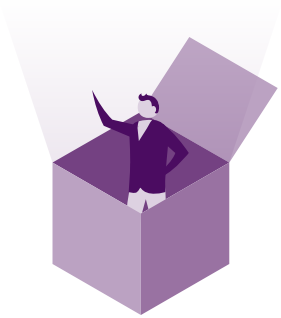
Veel leesplezier!

Versnellingsopties BAW+

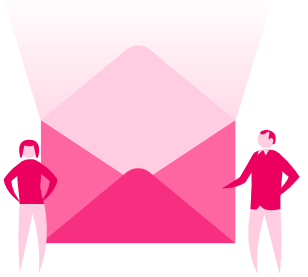


Algemeen nieuws

De watersector aan het woord



Even voorstellen



Contact

Versnellingsopties BAW+

In de Stuurgroep Water van oktober 2020 is afgesproken om de uitvoering van een aantal aanvullende afspraken te intensiveren. Hieronder wordt verstaan de opschaling van deelname aan de projecten en een inhaalslag op de implementatie van de bestaande afspraken.

1. Afspraak: Verdere invoering van het basisniveau informatiebeveiliging en ontwikkeling van aanvullende eisen voor procesautomatisering.

Intensivering: De sectorale standaard die in het kader van het BAW+ voor de watersector (excl. drinkwater) wordt opgesteld - met de CSIR als basis – moet breder beschikbaar gemaakt worden voor andere sectoren/processen.

Status: Deze afspraak wordt in 2 deelprojecten uitgevoerd;

1. CSIR 3.0: onder regie van het Het Waterschapshuis en Rijkswaterstaat werkt een projectteam aan het aanpassen van de Rijkswaterstaat standaard CSIR 2.0 (Cyber Security Implementatie Richtlijn) naar een implementeerbare versie voor de waterschappen.

2. BIACS (Baseline Industriële Automatisering Cyber Security): in afstemming met diverse stakeholders wordt op basis van de Rijkswaterstaat CSIR 2.0 een algemeen kader opgesteld dat bruikbaar is voor meerdere sectoren van het ministerie van Infrastructuur en Waterstaat. Met de ministeries van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Economische Zaken en Klimaat (EZK) en Justitie en Veiligheid (JenV) wordt gekeken naar de bredere toepasbaarheid van dit kader, in navolging van het advies van de Cyber Security Raad (CSR) hierover.

2. Afspraak: Versterking van samenwerking binnen de watersector op het gebied van cybersecurity.

Intensivering: Uitvoering van een verkenning t.b.v. een ‘Proof of Concept’ (PoC) en ontwikkeling van een plan van aanpak. Daarop vooruitlopend worden in een gemeenschappelijk project van Rijkswaterstaat en Het Waterschapshuis twee objecten van de Waterschappen aangesloten en voorbereidingen getroffen voor verdere opschaling voor andere objecten die deel uitmaken van de vitale infrastructuur van Rijkswaterstaat.

Status: Begin april is de werving van een projectleider afgerond en binnenkort zal worden gestart met de uitvoering van het project.

3. Afspraak: Uitvoering van een sectorbrede afhankelijkheids- en kwetsbaarheidsanalyse cybersecurity, die onderling vitale (keten-) afhankelijkheden vaststelt.

Intensivering: Opstellen plan van aanpak voor de tweede fase, waarbij de gedachte uitgaat naar het toepassen van de vastgestelde methodiek voor ketens op het gebied van waterkwaliteit (gericht op drinkwater) en waterveiligheid (gericht op waterkeringen). Afhankelijk van de beschikbare capaciteit wordt toegewerkt naar een brede deelname van experts vanuit de drinkwatersector, provincies, waterschappen, Rijkswaterstaat en gemeenten.

Status: In maart 2021 is gestart met fase 2 van het project waarbij de focus ligt op de keten waterkwaliteit. Hierbij wordt gebruikt gemaakt van de methodiek die n.a.v. fase 1 voorlopig is vastgesteld. Definitieve vaststelling zal gebeuren bij de afronding van fase 2, naar verwachting eind Q2 2021. Ondertussen is het aantal deelnemers aan fase 2 uitgebreid met experts vanuit de gemeenten en de drinkwatersector.

Bestuursakkoord Water

Het Rijk, de Vereniging van Nederlandse Gemeenten (VNG), het Interprovinciaal Overleg (IPO), de Unie van Waterschappen (UvW) en de Vereniging van waterbedrijven in Nederland (Vewin) sloten in 2011 het Bestuursakkoord Water (BAW). Daarin is afgesproken om de doelmatigheid van het waterbeheer te vergroten.

Op 31 oktober 2018 hebben de waterpartners aanvullende afspraken gemaakt op het Bestuursakkoord Water, onder andere over de risico's van digitale dreigingen. Cybercrime, cyberspionage en cybersabotage kunnen systemen en processen verstoren, met grote gevolgen voor de volksgezondheid, veiligheid en economie. Deze digitale bedreigingen vragen van de waterpartners om een gezamenlijke aanpak en inspanning.

Algemeen nieuws

Ministeriële Regeling beveiliging netwerk- en informatiesystemen IenW

Het ministerie van IenW bereidt de ministeriële regeling beveiliging netwerk- en informatiesystemen IenW voor. Deze regeling wordt opgesteld ten behoeve van de beveiliging van netwerk- en informatiesystemen van aanbieders van essentiële diensten (AED's). De regeling is gericht op verhoging van de digitale weerbaarheid binnen de sectoren op het terrein van infrastructuur en waterstaat.

Met het opstellen van deze regeling kan beter worden aangesloten op best practices door het voorschrijven van een risicogestuurd Information Security Management System (ISMS) met bijbehorende maatregelen. De maatregelen gaan uit van de primaire verantwoordelijkheid van AED's zelf, maar geeft de sectorale toezichthouder meer houvast om te sturen op het niveau van de beveiliging en waar nodig ook in te kunnen grijpen. De maatregelen sluiten aan op best practices en/of gangbare normen zoals de ISO27001, ISO27002, IEC 62443 en de Baseline Informatiebeveiliging Overheid.

De regeling heeft tot 29 maart ter inzage gelegen middels een internetconsultatie. Voor meer informatie inclusief bijlages, ga naar: www.internetconsultatie.nl/regeling_beveiliging_netwerk_en_informatiesystemen

Provincies sluiten noodgedwongen landelijke informatiesystemen vanwege kwetsbaarheid

Per 31 maart zijn de websites www.risicokaart.nl en www.zwemwater.nl weer bereikbaar voor het publiek. Beide websites werden in januari offline gehaald nadat beveiligingsrisico's werden geconstateerd. De kaarten kunnen respectievelijk worden geraadpleegd om actuele risico's in de leefomgeving dan wel de hygiëne en veiligheid van buitenzwemplekken in te zien.

Nuttige links:

1. www.noordhollandsdagblad.nl
2. www.bij12.nl/nieuws/risicokaart-nl-en-zwemwater-nl-weer-bereikbaar
3. www.bij12.nl/nieuws/aantal-applicaties-is-beperkt-bereikbaar

ILT plaatst Waternet onder verscherpt toezicht

Stichting Waternet (Waternet) komt onder verscherpt toezicht van de Inspectie Leefomgeving en Transport (ILT). Uit onderzoek van de ILT blijkt dat de drinkwaterorganisatie zowel op bestuurlijk als organisatorisch niveau onvoldoende grip heeft op de eigen cybersecurity. Dit wordt veroorzaakt door tekortkomingen in de uitvoering van de wettelijke zorg- en meldplicht en de besturing van de organisatie. Hierdoor is een verhoogd risico aanwezig op een cyberincident met mogelijke gevolgen voor de kwaliteit en/of de continuïteit van drinkwater. Er zijn geen aanwijzingen dat de kwaliteit en levering van het drinkwater acuut in gevaar zijn.
De ILT ziet de komende tijd toe op de verbetering van de uitvoering van de wettelijke zorg- en meldplicht en de besturing van Waternet.

waternet
waterschap amstel gooi en vecht
gemeente amsterdam

Nuttige links:

1. www.rijksoverheid.nl/documenten/kamerstukken
2. www.ilent.nl/actueel/nieuws

Versterking digitale weerbaarheid in Nederland

Al 2 jaar op rij waarschuwen de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum (NCSC) dat de digitale dreiging een permanent karakter heeft en dat cyberincidenten kunnen leiden tot maatschappij-ontwrichtende schade. Verhoging van de digitale weerbaarheid blijft de belangrijkste maatregel om deze risico's te beheersen en vergt een stevige en gecoördineerde inzet.

Sinds 2018 werkt het kabinet aan de ontwikkeling van een Landelijk Dekkend Stelsel (LDS) van samenwerkingsverbanden om relevante dreigingsinformatie zo snel mogelijk te kunnen delen met betrokken organisaties. Tot voor kort was deze informatievoorziening op basis van de Wet Beveiliging Netwerk- en Informatiesystem (Wbni) beperkt tot vitale aanbieders. Op 2 april heeft het NCSC echter aangekondigd dat Stichting Connect2Trust wordt benoemd tot officiële schakelorganisatie binnen het LDS. Connect2Trust biedt een platform aan waarop deelnemende partijen veilig informatie op het gebied van digitale veiligheid met elkaar en gespecialiseerde cybersecuritypartijen kunnen delen. Daarmee wordt de digitale weerbaarheid van heel Nederland weer een beetje verhoogd.

Op 6 april jongstleden heeft de Cyber Security Raad (CSR) haar adviesrapport 'Integrale aanpak cyberweerbaarheid' gepresenteerd. De boodschap is duidelijk: cyberweerbaarheid moet op het hoogste politieke en ambtelijke niveau regie krijgen en integraal worden aangepakt, mét extra financiële middelen. Het belang van vitale processen wordt daarbij extra benadrukt. In het advies staan 5 speerpunten centraal, te weten:

1. regie op samenwerking en informatiedeling,
2. weerbare, vitale processen,
3. versterking onderzoek en onderwijs,
4. realiseren van cybercrime-handhavingsketen
5. zorgplicht van leveranciers voor veilige producten en diensten voor burgers, bedrijfsleven en overheid.

Nuttige links:

1. www.ncsc.nl/documenten/publicaties
2. www.ncsc.nl/actueel/nieuws/2021/februari
3. www.ncsc.nl/actueel/nieuws/2021/april/2-april
4. www.cybersecurityraad.nl/actueel/nieuws

Red Team Blue Team training voor industrial control systems (ICS)

Samen met het European Network for Cyber Security (ENCS) organiseert het programma Versterken cyberweerbaarheid in de watersector een Red Team – Blue Team-training over de beveiliging van Industrial Control Systems (ICS).
Welke maatregelen kun je als organisatie nemen om een cyberaanval af te wenden of te voorkomen? Deze 3-daagse training helpt OT-professionals om die vraag beter te kunnen beantwoorden aan de hand van zowel theorie als intensieve oefening.
De voertaal van deze training is Engels.

Wanneer?
Maandag 7 t/m woensdag 9 juni 2021
Maandag 4 t/m woensdag 6 oktober 2021

Waar?
Crown Plaza hotel, Den Haag (conform RIVM-richtlijnen)

Meer weten?
Mail naar cyberweerbaarheidwater@minienw.nl

One Conference 2021

Op 28 en 29 september organiseert het NCSC in samenwerking met het Ministerie van EZK en de gemeente Den Haag alweer de 8e editie van de ONE Conference.
De Call for presentations is op 18 april gesloten.

Reserveer **28 en 29 september** dus alvast in je agenda!

One Conference 2021

De watersector aan het woord

Het programmateam ‘Versterken cyberweerbaarheid van de watersector’ heeft een faciliterende rol. Het zijn juist de partijen uit de watersector die de handen ineen hebben geslagen om de cyberweerbaarheid te versterken en aanvallen in de toekomst het hoofd te bieden. Daarom geven wij ook graag het woord aan de vele mensen die hieraan bijdragen. Deze keer Daphne Diephuis, adviseur crisismanagement bij Waterbedrijf Groningen en Kimini Delfos, senior beleidsmedewerker cybersecurity bij het ministerie van IenW.

Oefenen als spel - Serious gaming in de drinkwatersector
Door: Daphne Diephuis

Als je als drinkwatersector de kans krijgt om een serious game te laten ontwikkelen dan denk je niet 2 keer na, maar grijp je die kans met beide handen aan. Als drinkwatersector zijn we gewend te oefenen. Het is de kunst om die oefeningen voor de deelnemers leerzaam, maar ook leuk te laten zijn. Door het in een spelvorm te gieten, met de mogelijkheid het volledig online te spelen, voegen we een nieuw element toe aan het arsenaal van mogelijkheden om medewerkers op alle niveaus te trainen voor crisissituaties. Met dank aan Versterking Nationale Aanpak Cybersecurity-middelen (VNAC) vanuit het ministerie van IenW zijn we volop in de uitwerking van een aantal scenario’s met één gemeenschappelijk thema: cybersecurity. Gezien de actuele ontwikkelingen op het gebied van cybercrime een goede keuze, die de sector gaat helpen zich nog beter te preparen op verstoringen in de drinkwaterlevering.
De eerste game is bijna klaar; serious game-ontwikkelaar Thingks legt er de laatste hand aan. We hopen het spel aanstaande zomer te kunnen spelen met alle bedrijven in de drinkwatersector.

Nieuwsgierig? Bekijk alvast de teaser:

Alisson Teaser V1 - YouTube

ALISSON drinkwater

Europese netwerk- en informatieveiligheid richtlijn (NIB) 2.0

Door: Kimini Delfos

Ook op Europees niveau gebeurt er van alles met betrekking tot cybersecurity. In het eerste kwartaal van 2021 zijn we druk bezig geweest met het doornemen van de wetsartikelen van het concept herziene NIB-richtlijn (Netwerk- en Informatiebeveiliging). Het doel van deze Europese richtlijn is een hoger gemeenschappelijk niveau van cybersecurity in de Europese Unie. Door een flinke uitbreiding van het aantal sectoren is er met name aan de reikwijdte veel veranderd. In tegenstelling tot huidige Nederlandse wetgeving zal ook de sector afvalwater binnen de hernieuwde reikwijdte gaan vallen. Tevens omvat de richtlijn het voorstel dat de AED's (Aanbieders van Essentiele Diensten) worden aangewezen door Europa en niet door de lidstaten zelf.

De impact van deze nieuwe richtlijn is groot. Het is belangrijk om nauwkeurig te analyseren wat het voor onze sectoren betekent en waar wij eventuele belemmeringen zien. We verwelkomen Europese inzet op dit gebied, maar we willen ook dat de inzet zo goed mogelijk werkt en daarvoor is soms maatwerk nodig. De richtlijn wordt op dit moment besproken met de lidstaten. We krijgen de mogelijkheid om eerst vragen te stellen over de artikelen, daarna zal de onderhandeling beginnen. Het ministerie van Infrastructuur en Waterstaat is nauw betrokken bij de interdepartementale overleggen. De herziene NIB-richtlijn zal potentieel veel impact hebben op de sectoren waar IenW verantwoordelijkheid voor draagt. De komende maanden wordt het Nederlandse standpunt verder geformuleerd en beginnen de onderhandelingen met de Europese Commissie. De verwachting is dat de richtlijn in het najaar wordt besproken met het Europees Parlement.

Even voorstellen

Mijn naam is Jeroen van den Berg en sinds het begin van dit jaar ben ik werkzaam als secretaris van het programma ‘Versterken cyberweerbaarheid in de watersector’. Inmiddels heb ik velen van jullie waarschijnlijk al mogen ontmoeten. Graag vertel ik wat meer over mijzelf.

De afgelopen jaren heb ik ervaring opgedaan binnen het domein van nationale veiligheid. In eerste instantie met een focus op het concept ‘hybride dreigingen’ (ook wel statelijke dreigingen genoemd), maar geleidelijk aan zijn mijn interesse en werkzaamheden opgeschoven richting cybersecurity en vitale infrastructuur. Voordat ik aan de slag ging bij het ministerie van IenW heb ik ervaring opgedaan met training en advies over insider risk management.

Ondertussen zit ik alweer 3 maanden in mijn huidige functie en geniet ik van de dynamiek die het werken met partners uit de watersector met zich meebrengt. Voor vragen, opmerkingen of gewoon een virtuele kop koffie, mail naar jeroen.j.vanden.berg@minienw.nl

Contact

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

Contactpersonen:
René Marchal en Jeroen van den Berg

Website

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