Ministerie van Infrastructuur
en Waterstaat

Dagprogramma Ransomware Preparedness scan (RAPs)
Gefaciliteerd door ministerie van IenW (Cyberweerbaarheid in de watersector)

De dreiging van ransomware-aanvallen is in de afgelopen jaren gegroeid en het aantal incidenten stijgt. In augustus 2022 nog werd drinkwaterbedrijf South Staffordshire Water slachtoffer van een ransomware-aanval. Om organisaties te helpen optimaal voorbereid te zijn op een ransomware-aanval biedt het ministerie van Infrastructuur en Waterstaat een ransomware dag aan. Tijdens deze dag komen specialisten van een gerenommeerd cybersecurity bedrijf hun kennis delen en geven ze specifieke en direct uitvoerbare adviezen. Het programma bestaat uit vier delen, waarbij verschillende doelgroepen kunnen aansluiten. Doordat organisaties vooraf een vragenlijst invullen, kunnen de specialisten adviezen toespitsen op de specifieke behoefte van organisaties. Zo versterken ze samen de cyberweerbaarheid van de watersector.

Programma
Versterken Cyberweerbaarheid in de watersector

Voor wie is deze ransomware dag?

Gedurende de verschillende onderdelen van het programma, kijken de cybersecurity-specialisten naar hoe de organisatie ervoor staat op het gebied van cybersecurity en welke maatregelen er nodig zijn om de weerbaarheid te verhogen. Daarom is deze RAP dag onder meer interessant voor OT engineers, assetmanagers, CISO's, ISO's, technisch en functioneel beheerders en security architecten. Sommige onderdelen van het programma zijn daarnaast mogelijk ook interessant voor een bredere doel-groep. Overleg met de specialisten over de invulling voor uw eigen organisatie. Hieronder is per onderdeel aangegeven wat de doelgroep zou kunnen zijn.

Deel 1:
College Ransomware

Het College Ransomware is een interactieve sessie, waarin twee ervaren consultants een realistisch en praktisch beeld presenteren van cybersecurity. De focus ligt hierbij op ransomware. Aanwezigen maken kennis met actuele dreigingen en actoren die relevant zijn voor de wereld van Waterveiligheid. Het college wordt ondersteund door een presentatie op een scherm en de inhoud is toegankelijk voor een brede doelgroep, dus goed te begrijpen. Uiteraard is er ruimte voor interactie.

Er kan gedacht worden aan de volgende onderwerpen:

- Spotting Indicators of Attack (IOA) and Compromise (IOC), specifiek met betrekking tot ransomware-aanvallen.
- Incident/crisis-afhandeling; Wat zijn de redenen voor escalatie en het inroepen van externe hulp, gericht op het handelen van een crisismanagement team (CMT) tijdens een crisis. Onder meer prioritering en communicatie komen aan de orde.

Doelgroep: Het college is breed toegankelijk en in theorie dus voor **alle geïnteresseerde medewerkers.** Maar de bedoeling is vooral dat het **hoger management en bestuurders** uit de watersector deze informatie en lessen meekrijgen.

Deel 2:
Live Hack Demo

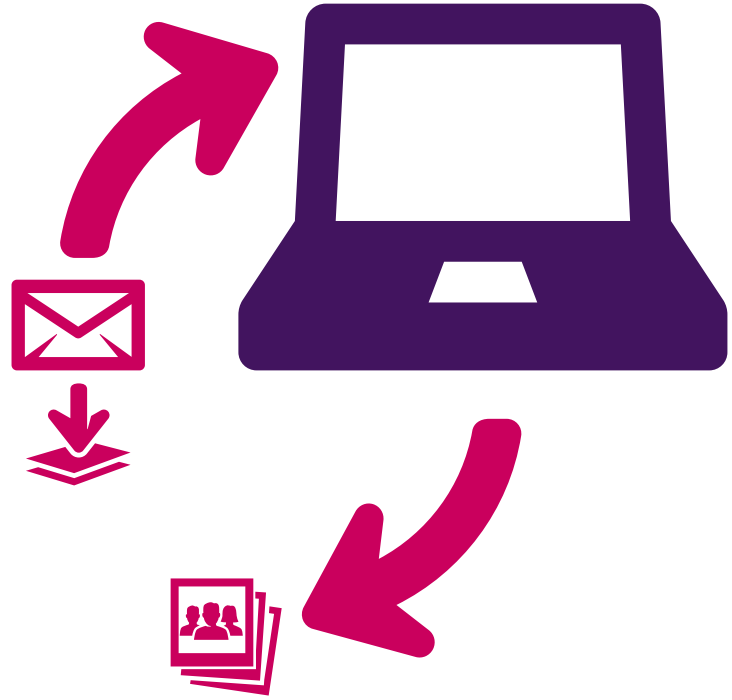
Hoe slaagt een hacker erin om via een e-mailbijlage of -link een werkstation te infecteren met malafide software? We laten het zien in de Live Hack Demo. Eenmaal binnen kan een hacker een systeem voor lange tijd onopgemerkt overnemen en vervolgens documenten, wachtwoorden en andere gevoelige bestanden stelen.

Wij demonstreren onder andere hoe een hacker:
- wachtwoorden binnenhaalt;
- bestanden kan bekijken, downloaden en uploaden;
- screenshots kan maken; en
- keystrokes kan vastleggen.

Met de Live Hack Demo willen we de gevolgen van de hack inzichtelijk maken. Een expert laat zien tot welke informatie hij toegang kan krijgen, op de computer van het slachtoffer. Vanaf het gecompromitteerde werkstation scant de aanvaller het netwerk waar de computer zich in bevindt. Via een openstaande poort treedt de hacker binnen in het station van een gebruiker met hogere rechten binnen het netwerk.

Omdat medewerkers een belangrijke rol spelen bij het voorkomen van geslaagde phishing-aanvallen geeft de expert tips over preventie. Zodra de deelnemers hebben ervaren hoe een hacker te werk gaat, is het tijd om inzicht te geven in hoe andere organisaties zich wapenen tegen ransomware-aanvallen.

Doelgroep: Bestuurders, maar ook breed toegankelijk. Ook inhoudelijke experts kunnen aansluiten.



Deel 3: **Cases**

Hoe wapenen andere organisaties zich tegen ransomware-aanvallen? Daarvan geven we een inkijkje in de 'Cases'. Een aantal succesverhalen zullen de revue passeren. Extra aandacht is er voor cases met een OT-component. We belichten in dit onderdeel met name de defensieve kant aan de hand van één of meerdere casussen. De namen van de betreffende organisaties blijven uiteraard geheim.

Voorbeelden van defensieve maatregelen:
- Het veilig uitvoeren van beheertaken;
- Toegangsbeveiliging, inclusief de implementatie van multifactorauthenticatie op alle internet-facing systemen en -diensten;
- Netwerksegmentatie, waarbij het netwerk logisch is opgedeeld in verschillende segmenten;
- Inzicht in de actuele kwetsbaarheden van systemen en deze proactief opvolgen.

Doelgroep: interessant voor iedereen die betrokken is bij het implementeren van maatregelen.

Deel 4:
Organisatiescan

Tijdens de Organisatiescan – het meest interactieve onderdeel – gaan we de diepte in. We kijken naar hoe de organisatie ervoor staat op het gebied van cybersecurity en welke maatregelen er nodig zijn om de weerbaarheid te verhogen. Het doel van deze sessie is niet kennisdeling, maar aan de slag gaan met de maatregelen.

Op basis van de soort organisatie (grootte, welke kroonjuwelen, volwassenheid, etc.) en de door de organisatie reeds genomen maatregelen (ingevulde vragenlijst vooraf) gaan de consultants het gesprek aan met de deelnemers over de maatregelen die van toegevoegde waarde zijn.

De vragenlijst met maatregelen is gebaseerd op een aantal cybersecurity raamwerken, zoals het NIST Cyber Security Framework (CSF), de CIS Controls v8 en de NEN-ISO/IEC 27001. Er kan gedacht worden aan de volgende maatregelen:

- Het strategisch beleggen en aansturen van cybersecurity;
- In staat zijn om een incident te detecteren aan de hand van end-point detection & response (EDR), netwerkmonitoring en logmonitoring;
- De aanwezigheid van een incident response beleid en plan voor het adequaat reageren op en afhandelen van een cybersecurity incident.

Tijdens dit onderdeel inventariseren we de uitkomsten, de genomen maatregelen en de te nemen maatregelen. **Deze worden niet gedeeld met anderen** buiten de organisatie en zijn alleen bedoeld om de organisatie gerichte aanbevelingen te kunnen geven.

Doelgroep: vooral het kernteam. Geadviseerd wordt om ook hier de verantwoordelijk manager of bestuurder aan te laten sluiten aan het slot, als eigenaar van de risico's.

Meer informatie
Heeft u na het lezen van deze brochure nog vragen of wilt u direct een gratis ransomware dag voor uw organisatie inplannen? Neem dan contact met ons op via **cyberweerbaarheidwater@minienw.nl.**