Ministerie van Infrastructuur en Waterstaat

RAP-dag 2024: Dagprogramma Ransomware Preparedness

De dreiging van ransomware-aanvallen is in de afgelopen jaren steeds groter geworden. En het aantal incidenten stijgt. Wereldwijd zijn er in 2024 al meerdere ransomware-aanvallen op vitale sectoren geweest. Om organisaties te helpen optimaal voorbereid te zijn op zo'n aanval, organiseert het ministerie van Infrastructuur en Waterstaat speciale RAP-dagen die geheel in teken staat van ransomware. Op een RAP-dag komen specialisten van een gerenommeerd cybersecuritybedrijf bij jouw organisatie langs om hun kennis delen en geven ze sectorspecifieke en direct uitvoerbare adviezen. In deze flyer lees je alles over het programma van een RAP-dag en hoe je je kunt aanmelden.

Voor wie is de RAP-dag?

Een RAP-dag is interessant voor bestuurders, CISO's, OT–engineers, assetmanagers, technisch en functioneel beheerders en security architecten. Maar sommige onderdelen van het programma zijn ook interessant voor een bredere doelgroep. Je leest hierna uit welke onderdelen een RAP-dag bestaat en voor welke doelgroep elk onderdeel bedoeld is.

Programma
Versterken Cyberweerbaarheid in de watersector

Programma
Versterken Cyberweerbaarheid in de Luchtvaart- en Maritieme sector

Programma
Versterken Cyberweerbaarheid in de Weg- en Spoorvervoer sectoren

Deel 1: College Ransomware (60 min)

In het college 'Ransomware' leer je over de aard en de implicaties van ransomware. Dit draagt bij aan het verbeteren van de veiligheid en veerkracht van de sector. Je doet mee aan interactieve discussies en beantwoord peilingen, stellingen en verdiepende vragen. En je loopt relevante scenario's en actualiteiten door. Zo krijg je een realistisch en praktisch beeld van cybersecurity en ransomware.

Na dit college weet je hoe ransomware impact kan hebben op jouw organisatie, welke maatregelen je kan nemen om je organisatie te beschermen en wat de best practices zijn bij het reageren op een aanval. Het college wordt ondersteund door een presentatie op een scherm. De inhoud is toegankelijk voor een brede doelgroep en is dus ook goed te begrijpen voor mensen met minder kennis van cybersecurity.

De volgende onderwerpen komen onder andere aan bod:

- Verkenning van ransomware, inclusief een aantal korte cases
- Het detecteren en reageren op Indicators of Attack (IOA) en Indicators of Compromise (IOC)
- Incident- en crisisafhandeling
- Prioritering en communicatie
- Relevante wet- en regelgeving (NIS2/AVG/CRA)

Doelgroep: Het college is breed toegankelijk en in theorie dus voor alle geïnteresseerde medewerkers. Maar het is vooral interessant voor het hoger management en bestuurders uit vitale sectoren, zoals water, maritiem, luchtvaart, weg, automotive en spoor.

Deel 2: Live hack demo (90 min)

Tijdens de 'Live hack demo' krijg je concreet inzicht in hoe ransomware-aanvallen achter de schermen werken. Een ethisch hacker laat ons een onderdeel uit het dagelijkse leven van een hacker zien. Samen met de deelnemers denk je mee met de volgende acties van de hackers én van het zichzelf verdedigende slachtoffer.

De expert laat zien tot welke informatie hij toegang kan krijgen op de computer van het slachtoffer. Maar óók wat je als slachtoffer kan doen om de toegang en schade te beperken. Want je speelt als medewerker een belangrijke rol bij het voorkomen van cyberaanvallen.

Na de 'Live hack demo' weet je hoe een hacker:

- wachtwoorden binnenhaalt;
- bestanden kan bekijken, downloaden en uploaden;
- screenshots kan maken.

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

Deel 3: Cases (60 min)

Cases geven een goed beeld van verschillende succesvolle defensieve maatregelen. Door een aantal relevante cases samen te bespreken, krijg je inspiratie om de huidige staat van maatregelen te controleren en als het nodig is aanvullende maatregelen te implementeren. We geven ook extra aandacht aan cases met een OT-component.

We belichten in dit onderdeel uitgebreid welke defensieve maatregelen er zijn. Aan de hand van concrete voorbeelden, én via een interactieve tool, leer je hoe je deze maatregelen toepast en hoe effectief ze zijn. Vervolgens behandelen we de aanbevelingen die wij graag willen delen met het publiek om de weerbaarheid tegen ransomware binnen de organisatie te verhogen.

Doelgroep: Interessant voor iedereen die betrokken is bij het implementeren van cybersecuritymaatregelen.

Deel 4: Organisatiescan (90 min)

Tijdens de organisatiescan gaan we samen de diepte in en kijken we hoe jouw 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 maatregelen.

Samen met een adviseur kijk je naar het type organisatie waar je voor werkt en de maatregelen die je al genomen hebt. Hiervoor gebruiken jullie onder andere de vragenlijst die je van te voren invult. En je gaat samen in gesprek over de maatregelen die van toegevoegde waarde zijn voor je organisatie.

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. De vragenlijst gaat in op onder andere de volgende onderwerpen:

- 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 een plan voor het adequaat reageren op en afhandelen van een cybersecurity-incident

De uitkomsten van de organisatiescan **delen we niet met anderen** buiten de organisatie. Ze zijn alleen bedoeld om organisaties gerichte aanbevelingen te kunnen geven. Waar mogelijk benchmarken we de organisatie met hun peers, om te kunnen checken hoe weerbaar een organisatie is ten opzichte van vergelijkbare organisaties.

Doelgroep: Inhoudelijk experts en de managers of bestuurders die verantwoordelijk zijn voor het risicomanagement.

Aanmelden

Wil je een RAP-dag voor jouw organisatie? Stuur dan een e-mail naar:

Watersector:
cyberweerbaarheidwater@minienw.nl

De luchtvaart- of maritieme sector:
cyberweerbaarheidluchtvaartmaritiem@minienw.nl

De weg- of spoorvervoersector:
cyberweerbaarheidweg-spoorvervoer@minienw.nl

Goed om te weten:

Vragenlijst: Na je aanmelding krijgt je een vragenlijst. Deze vul je in namens je organisatie.

Advies van specialisten: Op basis van deze vragenlijst kunnen cybersecurityspecialisten adviezen toespitsen op de behoeftes van jouw organisatie. Zij kijken tijdens de RAP-dag hoe je organisatie ervoor staat op het gebied van cybersecurity en welke maatregelen nodig zijn om de weerbaarheid te verbeteren. Deze resultaten en adviezen zijn enkel bestemd voor de organisatie zelf, het ministerie krijgt hier geen inzage in.

Waar en wanneer: Daarna nemen de cyberspecialisten contact met je op om te overleggen waar en wanneer jullie RAP-dag kan plaatsvinden.

Dit is een uitgave van het
Ministerie van Infrastructuur en Waterstaat

juni 2024