



Het Waterschapshuis

Marktconsultatieverslag van Het Waterschapshuis

Ten behoeve van

Test en Oefenscenario's Industriële Automatisering

Versie 1.0

Publicatiedatum: 29 januari 2021

Auteur: K. Zandstra

Ons kenmerk: Z2020-IV-P/H-TenOS-A

Colofon

Titel: Marktconsultatieverslag Test en Oefenscenario's Industriële Automatisering

Auteur(s): K. Zandstra

Contactpersoon: K. Zandstra

Vervangend contactpersoon: S. Wijnhorst

Het Waterschapshuis, 29 januari 2021

Stationsplein 89, 3818 LE Amersfoort

Postbus 2180, 3800 CD Amersfoort

T: 033 460 31 00, F: 033 460 31 01

www.hetwaterschapshuis.nl, inkoop@hetwaterschapshuis.nl

Inhoud

1. Inleiding	2
1.1 Achtergrond marktconsultatie	2
Huidige situatie	2
1.2 Doel marktconsultatie	3
2. Vragen	4
Vraag 1	4
Vraag 2	4
Vraag 3	4
Vraag 4	4
Vraag 5	4
Vraag 6	4
Vraag 7	4
Vraag 8	5
Vraag 9	5
Vraag 10	5
Vraag 11	5
Vraag 12	5
Vraag 13	5
Vraag 14	5
Vraag 15	6
Vraag 16	6
Vraag 17	6
Vraag 18	6
Vraag 19	6
Vraag 20	6
Vraag 21	6
Vraag 22	6

1. Inleiding

Voor u ligt het verslag van de marktconsultatie inzake **Test en Oefenscenario's Industriële Automatisering** zoals door Het Waterschapshuis is gehouden.

Een 11-tal partijen hebben een beantwoording ingediend, waarvan 2 vertrouwelijk en 1 deels vertrouwelijk.

1.1 Achtergrond marktconsultatie

Het Waterschapshuis is een gemeenschappelijke regeling van de Waterschappen (Scr. 2015, 7407 d.d. 13-03-2015). Doel van de regeling is een expertinstituut en service organisatie voor waterschappen in het leven te roepen om voor de deelnemende waterschappen en eventuele derden renderende samenwerking op informatie- en bedrijfsprocessen te realiseren en daarmee de behoeften van algemeen belang van de watersector te behartigen. Het Waterschapshuis (HWH) is de regie-, beheer-, en uitvoeringsorganisatie op het gebied van digitale informatievoorziening van de waterschappen. Het is een dienstverlenende organisatie van en voor de waterschappen die verantwoordelijk is voor de aanschaf en het contractmanagement van (gezamenlijke) informatievoorzieningen en data.

Voor meer informatie zie <https://www.hetwaterschapshuis.nl/>.

Huidige situatie

Per 1 januari 2019 zijn overheden verplicht zich te conformeren aan de Baseline Informatiebeveiliging Overheden (BIO). Iedere overheidsinstelling is zelf verantwoordelijk voor deze implementatie. De BIO is een, op basis van generieke schades en dreigingen voor de overheid standaard basisbeveiligingsniveaus (BBN's), gedefinieerd basisnormenkader met bijbehorende beveiligingseisen. In de BIO staat voor elk basis beveiliging niveau, aan welke controls er moet worden voldaan.

De BIO maatregelen zijn op tactisch en strategisch niveau beschreven. En hiermee toepasbaar binnen het gehele domein van informatie voorziening. Dit betekent dat het maatregelenpakket niet specifiek genoeg is beschreven naar operationeel toepasbare maatregelen voor de industriële automatisering.

- De hier geldende definitie van industriële automatisering, verder te noemen IA, is het geheel van geautomatiseerde besturingen van installaties met behulp van een computer.
- Het industriële domein is het geheel van de automatisering en de hieraan hier aan gekoppelde informatiesystemen, infrastructuur, gegevens en alle hieraan gerelateerde bedrijfsprocessen.

Het lijnmanagement is verantwoordelijk voor de informatieveiligheid. Industriële automatisering (IA) is een domein in het geheel van informatieveiligheid. Inhoudelijke kennis van het IA-domein is bij een relatief kleine groep kennisdragers beschikbaar.

Voldoen aan de BIO voor het IA-domein wordt door het lijnmanagement vaak overgelaten (gedelegeerd) aan de IA-specialisten. De BIO is strategisch en tactisch gegeven. IA is een specialisme dat zich bevindt in het feiten gebied. Deze twee werelden laten zich dan ook niet eenvoudig samenvoegen. Daar IA-teams vaak klein zijn en dus niet voldoende slagkracht hebben is uitvoering geven aan de BIO een hele opgave.

1.2 Doel marktconsultatie

De hoofddoelstelling van de marktconsultatie is om een mogelijk aanbestedingstraject af te stemmen op de visie en ambitie van Het Waterschapshuis binnen de mogelijkheden die er zijn in de markt.

Informatieveiligheid en cyber security zijn onlosmakelijk met elkaar verbonden. Bij vermeldingen over informatieveiligheid wordt hier tevens cyber security bedoeld.

De doelstelling van Test & Oefen scenario's is onder andere een bijdrage leveren aan het verhogen van het bewustzijn op het gebied van informatieveiligheid. Daarnaast een theoretische uitwerking, toegespitst naar industriële automatisering, die implementatie van maatregelen in de operationele industriële automatisering toepasbaar maakt. Om te voldoen aan de BIO basis beveiliging niveau 2. Tevens een praktijk omgeving vormgeven waarmee de mogelijkheid wordt geboden om (theoretische) implementatie resultaten van maatregelen te testen en vaardigheden kunnen worden opgedaan op het gebied van herkennen en handelen bij informatie gerelateerde afwijkingen. Het hoofd bieden aan de weerbaarheid op het gebied van informatieveiligheid verlangt een terug kerende aandacht. Cyber criminelen worden steeds inventiever. Continuïteit in kennisontwikkeling, actueel houden van maatregelen en bijbehorende scenario's zal moeten worden geborgd door afspraken te maken over benodigde middelen. Hieronder vallen financiën, centraal beheer, beschikbaarheid etc.

Voor er overgegaan kan worden aan realisatie is een aanvullend pakket van eisen en voorwaarden nodig. Om dit pakket samen te stellen is ondersteuning gewenst bij het in beeld brengen van aanvullende voorwaarden die een bijdrage leveren voor de vormgeving van test-, en oefen scenario's.

2. Vragen

Vraag 1

Beschrijf uw vormgeving van test en oefen scenario's en waar deze aan zouden moeten voldoen; Hierop werd uiteenlopend geantwoord. Table Top werd vaak genoemd, maar ook klassikale trainingen, serious gaming, e-learning, praktijkruimtes, lookalikes, interactieve simulatie, generieke versus specifieke bewustwordingsscenario's en andere opties werden opgesomd.

Vraag 2

Hoe denkt u ervaringen uit de praktijk te vertalen naar oefen scenario's. Kunt u aangeven hoe u hier invulling aan denkt te geven;

Hierop werd meermaals benadrukt dat beantwoorders het van groot belang vinden dat consultants en waterschappers nauw met elkaar zouden moeten optrekken om succesvol te zijn. Ook het evalueren van de resultaten van de oefenscenario's om deze daarop af te zetten tegen de theorie wordt veelvuldig vermeld. Het 'piloten' van oefeningen komt ook meermaals voorbij, alsmede het afstemmen van oefeningen op het kennis/bewustzijnsniveau van respectievelijke Waterschapsdoelgroepen.

Vraag 3

Kunt u voorbeelden geven hoe een theoretisch test en oefen scenario er uit kan komen te zien; Serious Gaming wordt hierop veelvuldig geantwoord. Ook validatie/verificatie per BIO eis passeert meermaals de revue. Het verzorgen van onderlinge presentaties als oefening wordt ook geopperd, en ook Table Tops van incidenten komen hier weer voorbij.

Vraag 4

Kunt u een beeld van een praktijkruimte schetsen die aansluit bij de industriële automatisering van overheidsinstellingen;

Meermaals wordt PLC/PC/SCADA hierop geantwoord. Ook wordt opgemerkt dat een praktijkruimte generiek zal moeten worden ingericht, gezien de grote diversiteit van apparatuur binnen de Waterschappen. Inrichting van e.e.a. kan in afstemming met leverancier worden uitgevoerd, aldus meerdere beantwoorders. Ook komt Serious Gaming hier weer voorbij.

Vraag 5

Hoe denkt u invulling te geven aan de controle op bruikbaarheid en volledigheid van uitgewerkte test scenario's in relatie tot implementatie van BIO maatregelen; De IEC 62443 standaard wordt hier veelvuldig op aangehaald. Ook de mogelijkheid van geautomatiseerde en ongeautomatiseerde testscenario tools wordt geantwoord.

Vraag 6

Kunt u een procesbeschrijving geven om te komen tot zowel theoretische als praktische test en oefen scenario's;

Het gebruik van een Stappenplan is het meest hierop geantwoord. Ook interviews worden veelvuldig vermeld. Het definiëren van leerdoelen per doelgroep, en het inzetten van klankbordgroepen wordt ook ingezet. CMDB scan tooling, brainstorm sessies en verkennende gesprekken worden ook vermeld.

Vraag 7

Welke mogelijkheden/ideeën heeft u verder om het bewustzijn van informatieveiligheid te vergroten;

E-learning/online gaming is hierop het meest geantwoord. Ook het inzetten van een (fysieke) informatie campagne komt veelvuldig voorbij.

Vraag 8

Kunt u een voorbeeld geven van een door u ingerichte operationele praktijkruimte;

Beantwoorders geven aan dit:

Zelf te kunnen (5);

Extern uit laten voeren (1);

Middels een web-service aan te bieden (1), en;

Geen ervaring hiermee heeft (1)

Vraag 9

Hoe denkt u vorm te kunnen geven aan continuïteit van beheer en onderhoud van een test en oefen omgeving in relatie tot de gebruikersgroep;

Hierop is zeer divers geantwoord. Van het opzetten van een Beheeroverleg / Gebruikersoverleg / SLA / referentieomgeving tot gedelegeerd Product Ownership.

Vraag 10

Kunt u aangeven wat het grootste aandachtspunt, naast die in dit schrijven benoemde punten, is bij het opzetten van test en oefen scenario's;

Cultuur van de organisatie (Waterschappen) wordt hierop het meest geantwoord. Scenario's dienen daarop aan te sluiten. Het inzetten van een generieke dienst voor meerdere deelnemers wordt tegelijkertijd als risico gezien. Ook de noodzaak van het uitdragen van nut en noodzaak van e.e.a. door Management wordt als essentieel gezien.

Vraag 11

Wat ziet u als mogelijkheden om cursisten de laatste ontwikkelingen op het gebied van informatieveiligheid bij te brengen (actueel houden van lesmateriaal)

Het met regelmaat updaten van lesmateriaal wordt hierop het meest geantwoord. Dit loopt uiteen van 'continu' tot 'jaarlijks' updaten. Ook wordt het opzetten van een online community/WIKI hierin als oplossing gezien.

Vraag 12

Wat is uw mening en beeld over onze ambities zoals beschreven in dit document. Missen wij onderdelen?

Diverse beantwoording. Organisatie volwassenheid is essentieel, betrokkenheid/inzet van opdrachtgever(s) is key. Ook, 'het is complexe materie', ga inktvlekkend te werk. Maar ook 'meer ambitie mag'. Antwoorders geven verder aan dat dit van het budget afhangt.

Vraag 13

Welke aanpak en roadmap(s) stelt u voor om te komen tot implementatie van de door u aangedragen oplossing(en) en waarom;

PDCA is hierop meermaals aangehaald. Ook Agile/SCRUM wordt geadviseerd gedurende de implementatie. Een Pilotfase icm een Roadmap wordt tevens als optie beschreven. Klein starten om al lerende de overige deelnemers te implementeren. Ook het aansluiten op het Cyberoefenpakket van de VNG wordt geadviseerd. Het gefaseerd opstellen en implementeren van scenario's behoort tot de mogelijkheden van een beantwoorder. Als laatste wordt de mogelijkheid van het inrichten van een test- en oefenruimte in een bus geopperd.

Vraag 14

Heeft u een beeld van kosten gerelateerd aan onze ambities zoals beschreven in dit document en zo ja, kunt u een inschatting daarvan met HWH delen;

Hierop antwoordde 3 respondenten met 'Nee', niet op dit ogenblik met deze informatie. Een beantwoorder adviseert om geen grote tender uit te zetten i.v.m. het grote innovatieve karakter. Een andere adviseert om 'incrementeel te ontwikkelen'.

Voorts liepen de bedragen uiteen van €40.000,- tot ruim 1.000.000,- op jaarbasis.

Vraag 15

Kunt u aangeven hoe u denkt de centraal, decentraal of outsource voorziening van een cyberlab binnen de diverse waterschappen te kunnen implementeren en beargumenteren hoe u tot deze keuze bent gekomen;

Wederom diverse beantwoording.

- Centraal -3 (1x oefeningen: digitaal/online)
- Centraal in Cloud -2
- Outsource -1
- Nog niet te bepalen -1
- Alles is mogelijk -1

Vraag 16

Hoe denkt u vorm te geven aan continuïteit in beschikbaarheid en kwaliteit van test en oefen scenario's;

Nagenoeg alle beantwoorders antwoorden anders. Middels:

- ISO 9001
- PDCA
- Opdrachtgever eigenaar maken van Test- en Oefenscenario's;
- Trainingen periodiek aanpassen/periodieke updates (2);
- LifeCycle Management;
- Referentieomgeving;
- Gedelegeerd Product Owner;

Vraag 17

Kunt u aangeven hoe u de relatie ziet tussen BIO en NEN-ISO/IEC normen 27001, 27002 en 62443 tot Test & Oefen scenario's;

Het merendeel van de beantwoorders refereert hier aan IEC (ISO) 62443. Ook PDCA in combinatie met de Risk Management cirkel wordt geopperd. Men adviseert tevens een en ander waar nodig aan te vullen met Audits.

Vraag 18

Kunt u aangeven hoe u de samenwerking met het Waterschapshuis denkt vorm te geven;

Middels 'Partnership' is hierop het meest geantwoord. Ook middels Pilots, een kopgroep of een integraal team vanuit opdrachtgever(s).

Vraag 19

Kunt u aangeven hoe u denkt over de vorm van ondersteuning om tot het gewenste resultaat te komen;

Samenwerking en Partnership valt hierop veel te lezen. Onder regie van ('linking pin'-) HWH wordt ook gezien als werkwijze.

Vraag 20

Heeft u ervaring met de CSIR (Cyber Security Implementatie Richtlijn) en kunt u hierop een toelichting geven;

Slechts 1 respondent antwoordt hierop met 'Nee, ik heb hier geen ervaring mee'.

Vraag 21

Beschrijf hoe u de samenwerking ziet tussen de onderliggende waterschappen (of andere organisaties) en het CERT-WM en omschrijf uw rol hierin.

Hierop antwoordt 1 beantwoorder dat hij hier best als 'linking pin' optreedt. Een ander middels SCRUM, met een Product Owner vanuit de opdrachtgever(s). Weer een ander ziet de opdrachtnemer/zich als 'intermediair'.

Vraag 22

Kunt u aangeven welke kennis en ervaring u heeft met de in gebruik zijnde (technische) installaties en IT-infrastructuur van waterschappen.

Hierop antwoorden alle respondenten dat zij, in meer of mindere mate, kennis hebben van deze materie.