

Nadere duiding voorgenomen opdracht van Het Waterschapshuis op het gebied van Security Monitoring en Alarmering

Voorafgaand aan de bijeenkomst van 15 februari willen we de Deelnemers aan de marktconsultatie graag inzicht geven in de voorgenomen opdracht en de beoogde doelstelling ervan.

Doel van de marktconsultatie is om een zo goed mogelijk inzicht te krijgen in de mogelijkheden die de markt kan bieden en in hoeverre de ambities van het Waterschapshuis haalbaar zijn voor de markt.

Aanvullende informatie

We zijn voornemens om Security Operations Center (SOC)-dienstverlening voor alle Waterschappen, het Waterschapshuis en mogelijk andere organisaties binnen de watersector (hierna: Deelnemers) af te nemen van een partij in de markt. Onder de SOC-dienstverlening verstaan wij:

- Monitoring – Het vinden en analyseren van mogelijke cyberbeveiligingskwetsbaarheden, -aanvallen en -incidenten (cf. “Detect” uit het NIST Cybersecurity Framework 2.0)
- Alarmering - Actie ondernemen met betrekking tot een gedetecteerd cyberbeveiligingskwetsbaarheid en -incident (cf. “Respond” uit het NIST Cybersecurity Framework 2.0)
- Beheer en doorontwikkeling van security use cases die voorzien zijn van een detectiemechanisme die de monitoring inhoud geven
- SOC analisten die de meldingen vanuit de monitoring analyseren, verrijken, rapporteren aan de Waterschappen en ons CERT-Water Management (CERT-WM) om in samenwerking de dreiging weg te nemen of het daarmee samenhangende risico te mitigeren tot een aanvaardbaar niveau.

De Waterschappen beschikken over een grote hoeveelheid OT-componenten die in verschillende samenstellingen in een sterk geografisch verspreid landschap hun taak verrichten. Voor de beoogde SOC-dienstverlening is deskundigheid (kennis en ervaring) met dit soort componenten in een vergelijkbare setting (denk aan gemalen of een waterzuiveringen) zeer belangrijk. Kennis van proces automatisering, de wijze waarop de verschillende lagen van de OT-techniek zijn georganiseerd en de bedreigingen die van toepassing zijn op dit soort componenten zijn essentieel om adequaat invulling te geven aan de dienstverlening.

Natuurlijk is het IT-deel van het totale informatieverwerkende en technische landschap ook van belang voor het goed functioneren van een Waterschap, echter het is vooral van belang dat het OT-domein sterk wordt beheerst.

Voor de bewaking van de vitale Waterschapsinfrastructuur en het efficiënt pareren van digitale bedreigingen is er behoefte aan een SOC-dienstverlening die 7 dagen per week, 24 uur per dag bemand is en ons adequaat beschermt tegen digitale dreigingen met deskundige analisten op zowel het proces automatiseringsdeel (PA) als het kantoorautomatiseringsdeel (KA). De SOC-analisten zullen in geval van een bedreiging samenwerken met PA en KA specialisten bij de verschillende Waterschappen. Daarbij zien wij mondelinge communicatie in het Nederlands met onze specialisten als een

noodzakelijke voorwaarde. Immers het controleren van OT-componenten of het oplossen van incidenten zal in het veld moeten gebeuren, denk hierbij aan een waterkering ver buiten de bebouwde kom. Daarbij is het essentieel dat mensen elkaar goed verstaan en begrijpen.

Vanwege het vitale karakter van infrastructuur van de Waterschappen, de Nederlandse en Europese wetgeving, zal de dienstverlening die we zoeken moeten voldoen aan de Nationale en Europees geldende wetten, regels en richtlijnen, op alle vlakken van de dienstverlening. Denk hierbij aan AVG, Wbni, BIO, IEC 62443 en CSIR. Daarnaast vinden we het belangrijk dat de dienstverlener een hoog en betrouwbaar niveau van dienstverlening middels geëigende certificeringen (waarbij vooralsnog wordt gedacht aan ISO9001, ISO27001, ISO27017 en een ISEA3402 Type 2 verklaring, SOC2 verklaring of een ander gelijkwaardig certificaat) aantoont.

Het volwassenheidsniveau op het gebied van informatiebeveiliging en kennis van technologische ontwikkelingen die dit ondersteunen, verschilt per Waterschap. Dit vraagt flexibiliteit en schaalbaarheid van de dienstverlener bij het ondersteunen van een Waterschap. De opdrachtnemer zal dan ook gevraagd worden een implementatieteam ter beschikking te stellen dat Waterschappen kan ondersteunen bij het aansluiten op de SOC-dienst.

Gelet op de snelheid van de ontwikkelingen op dit gebied is het noodzakelijk dat een dienstverlener ook (pro)actief zijn vakinhoudelijke kennis ontwikkelt en daarin tot de voorlopers in het vakgebied behoort en stelselmatig de nieuwste trends en ontwikkelingen in zijn dienstverlening incorporeert.

Inhoud marktconsultatie

Tijdens de marktconsultatie willen we graag de markt bevragen over de volgende onderwerpen:

- Toekomstbestendigheid: om als Waterschappen, het Waterschapshuis en overige Deelnemers op het gebied van informatiebeveiliging toekomstbestendig te zijn, moet de Opdrachtnemer in staat zijn om mee te ontwikkelen met de ontwikkelingen in de markt (zowel organisatorisch, technisch als op basis van dreigingsbeelden). De Opdrachtgever wil absoluut voorkomen dat een statische oplossing wordt geïmplementeerd voor de looptijd van de overeenkomst. Er moet sprake zijn van een partnerschap waarin Opdrachtgever, de Deelnemers en de Opdrachtnemer gezamenlijk de digitale weerbaarheid blijven verhogen en de dienstverlening door ontwikkelen.
- Samenwerking: Voorgaande punt vereist ook een hoge mate van samenwerking. Een goede samenwerking tussen de verschillende partijen kan resulteren in een win-win situatie, waarbij zij profiteren van wederzijds respect, open communicatie, kennis en het delen van gemeenschappelijke doelstellingen. Zo kunnen partijen elkaars verwachtingen, behoeften en uitdagingen beter begrijpen en problemen snel oplossen, het vergroot de flexibiliteit en het aanpassingsvermogen van beide partijen.
- Wijze van instappen: Het Waterschapshuis sluit als Opdrachtgever de Raamovereenkomst met Opdrachtnemer. Het Waterschapshuis wordt ook direct

Deelnemer bij de Raamovereenkomst. Om Deelnemer bij de Raamovereenkomst te worden stuurt elk Waterschap een Verklaring van Deelname aan Opdrachtnemer en het Waterschapshuis. Nadat de Opdrachtnemer in kennis is gesteld van de deelname is de Deelnemer vanaf de in de Verklaring van Deelname genoemde ingangsdatum partij bij de Raamovereenkomst en heeft de Raamovereenkomst rechtstreekse werking tussen Deelnemer en Opdrachtnemer. Opdrachtgever voert namens de Deelnemers de centrale regie met betrekking tot het leveranciers- en contractmanagement. Het is de intentie dat minimaal 22 organisaties de SOC-dienstverlening zullen afnemen. De looptijd van het raamcontract zal minimaal contractlooptijd 4 jaar zijn. Er zal sprake zijn van een gefaseerde aansluiting van de organisatieonderdelen (het eerste jaar 4 organisatiedelen; de 3 jaren erna 6 organisatiedelen per jaar). De

Gevraagd zal worden hoe marktpartijen tegen deze ambities aankijken. Welke kansen en risico's worden onderkend en welke prijsmodellen het beste passen voor dergelijke ambities.