NOTA VAN INLICHTINGEN

behorende bij de marktconsultatie "Incident Response".
Kenmerk: "siw009742"
Datum: 22-03-2023

Inleiding

Deze Nota van Inlichtingen hoort bij de openbare marktconsultatie "Incident Response" met kenmerk "siw009742".
De Nota van Inlichtingen is een aanvulling op het marktconsultatiedocument "Incident Response" versie definitief d.d. 03-03-2023 en alle bijbehorende bijlagen.
Indien er tegenstrijdigheden worden geconstateerd met informatie gegeven in de eerdergenoemde aanbestedingsdocumenten, dan prevaleert de informatie gegeven in de Nota van Inlichtingen.

Ref. nr.	Vraag	Antwoord
1	Snelheid is essentieel bij een goede Cyber Incident Response. In dat kader achten wij het zeer aanbevelenswaard als uw IT-omgeving is uitgerust met EDR (endpoint detection & response). Vinden jullie dit ook? Valt dit binnen jullie definitie van IR of is dit al gerealiseerd?	Sinds 1 december 2022 beschikt de gemeente over een SIEM/SOC dienstverlening, waarbij ook de endpoints zijn betrokken.
2	Hoeveel endpoints heeft uw IT-omgeving?	Circa 500.
3	Is deze opdracht inclusief het detecteren van cyberincidenten? Zo ja, hoe ziet u dat voor zich?	Nee, detectie valt buiten deze opdracht.
4	U noemt onder andere pentesten, inventarisatie en risico analyse als onderdelen van incident response. Hoe ziet u dat? Wij zijn van mening dat dit niet tot incident response behoort maar onderdeel is van een veel breder cybersecurity vraagstuk.	In principe is de Incident Response Dienst inderdaad het onderdeel waarvoor we de marktconsultatie doen. Echter genoemde onderdelen staan natuurlijk niet los van de Incident Response. We zoeken dan ook een partij die ook meerwaarde kan bieden bij het uitvoeren van risico-analyses, advisering beveiligingsmaatregelen. Dit zijn echter wel extra opties die los gezien worden van de Incident Response dienstverlening.
5	Omvat deze opdracht ook preventie in de voorbereiding?	In onze beleving is een goede Incident Response alleen mogelijk als de dienstenaanbieder ook goed op de hoogte is van de systemen, netwerken applicaties bij de klant. De beantwoording van deze vraag is ook onderdeel van de marktconsultatie.
6	U noemt dat de IT diensten van de Gemeente Altena grotendeels zijn uitbesteed. Worden er ook systemen met andere organisaties/ gemeenten gedeeld?	Er worden geen systemen met andere organisaties/gemeenten gedeeld.
7	Is er sprake van strikte scheiding van systemen/ applicaties, ook bij uw IT partner(s)?	Deze vraag is moeilijk te beantwoorden. De leverancier die onze omgeving host zorgt voor segmentatie in het netwerk. Anderszijds is ongeveer 70% een SAAS apllicatie, die bij de leverancier wordt gehost en daardoor automtisch zorgt voor scheiding van systemen.
8	De jaarlijkse kosten voor Incident Response is door u ingeschat op EUR 25.000. Kunt u in grote lijnen specificeren hoe u tot dit bedrag komt?	Dit is puur voor de daadwerkelijke Incident response dienstverlening en is een grove raming op basis van een kort marktonderzoek voorafgaand aan deze marktconsultatie.
9	Bij daadwerkelijke inzet met een CERT (containment, eradicatie en onderzoek) zullen kosten op basis uurtarief aanvullend in rekening worden gebracht. Bent u het daarmee eens?	Deze kosten zullen inderdaad afhakelijk zijn van de schaalgrootte en impact van het incident. Gemeente Altena kan zich erin vinden om hiervoor een uurtarief op te vragen. Wij willen u vragen hiermee rekening te houden in uw beantwoording van vraag 10 en 11 van de marktconsultatie vragen.
10	Beschikt uw organisatie over een cyberverzekering? Zo ja, wenst u deze te continueren?	Ja. De continuering hiervan hangt mede af van het resultaat van deze marktconsultatie en het risico wat resteert.
11	In het marktconsultatiedocument onder 1.2 Gewenste situatie worden een aantal punten benoemd. Wat bedoelt u met “toepasselijke bronnen”? zijn dat systemen, resources of iets anders?	Bronnen waaruit het incident voortkomt.