Verslag marktconsultatie

"Pentest"

Gemeente Bergen op Zoom

Kenmerk:	dCI-000492
Datum:	29 juli 2025
Status:	Definitief

1. Inleiding

De gemeente Bergen op Zoom heeft een marktconsultatie inzake '*Pentest*' georganiseerd. Doel van de marktconsultatie was om de markt met betrekking tot pentesten te verkennen om tot inzichten, suggesties en ideeën te komen voor een actuele en marktconforme aanbesteding.

De gemeente heeft deze marktconsultatie via TenderNed nationaal gepubliceerd om de mondiale markt zoveel mogelijk te bereiken en te betrekken. Vanzelfsprekend zijn de beginselen van transparantie, gelijkheid en non-discriminatie bij deze marktconsultatie in acht genomen. Er heeft een schriftelijke ronde plaatsgevonden in de vorm van een vragenlijst.

De gemeente bedankt alle deelnemers voor hun uitgebreide beantwoording en duidelijke toelichtingen.

Dit eindverslag van de marktconsultatie zal als bijlage bij de aanbestedingsstukken worden gevoegd, wanneer de gemeente besluit om tot een aanbestedingsprocedure over te gaan.

Het verslag is opgebouwd aan de hand van de schriftelijke ronde. De schriftelijke antwoorden zijn puntsgewijs in dit verslag opgenomen. Hierbij zijn de antwoorden (die mogelijk een bedrijfsgevoelig karakter zouden kunnen hebben) geanonimiseerd en op hoofdlijnen opgenomen.

2. Marktconsultatie

Vraag 1

Wat is de naam van uw organisatie? Hoeveel medewerkers zijn er in dienst, en hoeveel daarvan zijn actief als pentester? In welk land is uw organisatie gevestigd?

- Alle deelnemers hebben hun informatie doorgegeven.

Vraag 2

Beschikt u over de volgende certificeringen (indien van toepassing)? ISO 27001 / CREST / OSCP/OSCE/GPEN/CEH/Overig (voor individuele testers)?

- De genoemde certificeringen zijn bevestigd, met uitzondering van CREST.
- Daarnaast zijn ook genoemd: CCV 2.0 keurmerk, CRTP, CPTS, CARTP, OSWP, OSEP, GWAPT, GPEN, CISSP, CRTO, GMOB, GSSP.

Vraag 3

Kunt u een toelichting geven op de diensten die u kunt leveren op het gebied van pentesten?

- Er wordt een overzicht van diensten genoemd zoals o.a. vulnerability assessments, verschillende penetration test op web, mobiel, infrastructuur etc. tot complexe oefeningen zoals adversary simulations en red teaming.
- Afhankelijk van de onderzoeksvraag worden pentesten geleverd op basis van black-, grey- of whitebox perspectief.
- Verschillende testvormen kunnen ook gecombineerd worden om een vollediger beeld te krijgen van de beveiligingspositie.

Vraag 4

Welke suggesties kunt u de gemeente op basis van de beoogde scope en onderzoeksvragen zoals omschreven in hoofdstuk 2 meegeven om de scope nog duidelijker en specifieker te maken, op basis van uw ervaring?

- Mogelijk kan meer toegevoegde waarde worden verkregen wanneer testen risico-gebaseerd worden vormgegeven.
- Geadviseerd wordt per onderdeel (intern, extern, IoT het bereik en de verwachtingen zo concreet mogelijk te formuleren.
- Zorg er ook voor dat onderzoeksvragen uitvoerbaar, toetsbaar en meetbaar zijn.
- Testen of delen van testen kunnen grotendeels ook geautomatiseerd worden uitgevoerd, maar geadviseerd wordt hier een bewuste keuze in te maken, dus de mate van diepgang die gewenst is in de uitvoering van de test.
- Geef in de uitvraag voldoende informatie mee met betrekking tot o.a. IP-adressen, omvang, complexiteit.

Vraag 5

Welke informatie heeft u verder nodig om in een mogelijke aanbestedingsprocedure een inschrijving te kunnen doen?

- De volgende onderwerpen komen in alle beantwoordingen terug:
  - Volledige scope, met o.a. overzicht van systemen, IP-adressen, afhankelijkheden
  - Doelstellingen
  - Beveiligingsregels
  - Tijdlijn en deadlines

Vraag 6

Hoe borgt uw organisatie de veiligheid van pentests in productieomgevingen? Welke standaardmaatregelen worden genomen om verstoringen te voorkomen?

- Bij voorkeur worden testen uitgevoerd in een representatieve acceptatie- of testomgeving.
- Het uitgangspunt is dat de productieomgeving niet wordt verstoord.
- Vooraf vindt een intake met een risicoanalyse plaats.

Vraag 7

Welke ervaring heeft u met het uitvoeren van pentesten binnen een (semi-)overheidsorganisatie?

- Alle deelnemers hebben ruime ervaring binnen de (semi-)publieke sector.

Vraag 8

Welke ervaring heeft uw organisatie met het testen van IoT- of embedded systemen? Indien deze ervaring beperkt is, hoe zou uw organisatie een dergelijke scope benaderen qua tooling, aanpak en methodiek?

- Alle deelnemers hebben ruime ervaring met het testen van IoT- en embedded systemen.

Vraag 9

Ondertekent u standaard een geheimhoudingsverklaring (NDA)?

- Alle deelnemers hebben hier bevestigend op geantwoord, waarbij één deelnemer aangaf dat een dergelijke NDA wel op organisatieniveau wordt ondertekend en niet op medewerkerniveau.

Vraag 10

Hoe gaat uw organisatie om met het testen van SaaS-applicaties die niet in eigen beheer zijn van de gemeente? Wordt hierin samengewerkt met leveranciers of beperkt de test zich tot client-side functionaliteit?

- Het testen van SaaS-applicaties is vrijwel standaard geworden.
- De opdrachtgever is verantwoordelijk voor het afstemmen van de te testen scope met de SaaS-leverancier, inclusief vrijwaringen.
- E.e.a. is wel afhankelijk van de openheid van de SaaS-leverancier, indien de SaaS-leverancier geen medewerking verleent, wordt beperkt tot client-side functionaliteit.
- Geadviseerd wordt om bij Saas-applicaties een TPM/Derdenverklaring op te vragen.

Vraag 11

Wat is uw verwachte doorlooptijd voor de voorbereiding en scoping, uitvoering van de test en rapportage?

- Uiteraard is dit volledig afhankelijk van scope, omvang, complexiteit, aantal en diepte van de onderzoeksvragen, maar in de meeste gevallen is de verwachte doorlooptijd van aanvraag t/m rapportage maximaal 8 à 9 weken.

Vraag 12

Kunt u uw aanpak beschrijven van intake tot rapportage?

- De stappen die worden doorlopen zijn in grote lijnen als volgt:
  - Intake en scoping
  - Voorbereiding en testplanning
  - Uitvoering van de test(en)
  - Rapportage en kwaliteitscontrole
  - Oplevering en toelichting
  - Optioneel: hertest

Vraag 13

Welke methodologieën hanteert u? (Bijv. OWASP, PTES, NIST)?

- Er worden diverse methodologieën genoemd, zoals o.a. Open Web Application Security Project (OWASP), OWASP Application Security Verification Standard (ASVS), OWASP Mobile Application Security Verification Standard (MASVS), OWASP Testing guide, SANS penetration testing methodologie en bijbehorende bronnen, ISACA Information Technology Assurance Framework (ITAF), NIST Technical Guide to Information Security Testing and Assessment (SP 800-115), Open Source Security Testing Methodology Manual (OSSTMM).

Vraag 14

Hoe wordt een pentest uitgevoerd zonder vooraf beschikbare accounts of documentatie (black-box benadering)? Wat is de werkwijze van uw organisatie in dit soort scenario's?

- In een black-box benadering wordt zonder voorkennis een realistische simulatie van een externe aanvaller uitgevoerd, waarbij kwetsbaarheden worden geïdentificeerd.
- De volgende stappen worden daarin op hoofdlijnen doorlopen:
    - Initiële verkenning en informatievergaring
    - Dienst- en kwetsbaarheden detectie
    - Authenticatie omzeilen of accounts verkrijgen
    - Exploitatie van kwetsbaarheden
    - Geen verstoring, wel maximale diepgang
    - Rapportage en aanbevelingen
    - Optioneel: hertest of verdiepende test

Vraag 15

Op welke manier worden detectie- en loggingmechanismen betrokken in de pentestaanpak? Maakt uw organisatie hierbij gebruik van technieken om EDR, antivirus of SIEM-oplossingen te omzeilen?

- Detectie- en loggingmechanismen worden zeker getest, omdat deze een cruciale rol spelen in het vroegtijdig signaleren van aanvallen. Er wordt een aantal stappen doorlopen, zoals analyse van detectie- en logcapaciteiten, evaluatie van het loggingsniveau tijdens de test.

Vraag 16

Hoe ziet de rapportage van uw organisatie eruit? Kunt u voorbeelden geven van hoe technische bevindingen, exploit chains en managementsamenvattingen worden gepresenteerd?

- Over het algemeen komt de inhoud van de rapportage op dezelfde onderdelen neer:
    - Managementsamenvatting
    - Aanpak en methodieken
    - Testverloop
    - Technische bevindingen
    - Praktische aanbevelingen; concrete acties om risico's te mitigeren
- Er zijn voorbeelden van rapportages aangeleverd.

Vraag 17

Kunt u aangeven op basis van de beoogde scope en onderzoeksvragen binnen welke bandbreedte de kosten op jaarbasis zouden liggen voor het uitvoeren van een pentest binnen onze gemeente?

- Uiteraard zijn de kosten op jaarbasis volledig afhankelijk van de scope en behoefte van de gemeente. Er is wel een bandbreedte te benoemen die grofweg uiteenloopt van ca. € 6.000 tot ca. € 50.000 op jaarbasis.

Vraag 18

De gemeente wil uiteraard naast de prijs ook kwalitatieve aspecten laten meewegen in de beoordeling van de offertes. Welke suggesties en/of aandachtspunten heeft u met betrekking tot de beoogde invulling van de kwalitatieve onderdelen van het gunningcriterium? Met andere woorden: op welke aspecten is de door u te leveren dienstverlening onderscheidend?

- Hier wordt een aantal aspecten genoemd, zoals o.a. pentesten met keteninzicht, een flexibele aanpak bij testen van SaaS-applicaties, ondersteuning bij verantwoording en communicatie, transparante rapportage voor meerdere doelgroepen, plan van aanpak.

Vraag 19

Kunt u aangeven of u wel of niet zou inschrijven op basis van de informatie uit deze marktconsultatie?

- Alle deelnemers hebben hier bevestigend op geantwoord, een enkeling benoemt daarbij wel aandachtspunten.

Vraag 20

Kunt u suggesties geven op welke wijze de gemeente de inschrijfkans zou kunnen vergroten?

- Er wordt vooral geadviseerd in de uitvraag een duidelijke heldere scope en doelstellingen te beschrijven.
- Stel een realistisch budget beschikbaar.
- Denk goed na over beperkingen in taal (niet alleen Nederlands, gezien het internationale karakter van deze markt).

Vraag 21

Welke trends en ontwikkelingen ziet u op het gebied van pentesten en hoe speelt u hierop in?

- Er worden verschillende voorbeelden gegeven:
  - AI en hacks op IoT
  - Meer automatisering in de testen
  - Toename van cloud- en hybride-omgevingen
  - Verschuiving van een jaarlijkse pentest naar continuous security testing: Pentesting as a Service (PtaaS)

Vraag 22

Welke tips, informatie of adviezen wilt u de gemeente verder meegeven dat nog niet is behandeld in de bovenstaande vragen, maar naar uw mening wel van belang is voor het opstellen van een goede uitvraag?

- Een tip die wordt gegeven is het classificeren van risico's door leveranciers inclusief aansluiting op de BIO-methodiek.
- Ook wordt geadviseerd zo mogelijk breder te kijken naar cybersecurity en niet alleen op pentesten.

3. Tot slot

- Deelnemende partijen kunnen geen rechten ontlenen aan de informatie die tijdens de marktconsultatie is verstrekt.
- Tijdens de marktconsultatie verstrekte informatie kan afwijken van in de nog op te starten aanbestedingsprocedure te verstrekken informatie.
- Claims over het gebruik van informatie, vertrouwelijkheid of verzoeken om vergoedingen in verband hiermee worden niet gehonoreerd.
- De gemeente is niet gebonden aan de uitkomsten van deze marktconsultatie.
- Er wordt geen vergoeding toegekend aan de deelnemers van deze marktconsultatie.
- De aankondiging van deze marktconsultatie (incl. bijbehorende documenten), deelname of bijdrage aan de marktconsultatie gelden niet als uitnodiging tot inschrijving op de aanbesteding voor de onderhavige opdracht, noch kunnen daaraan rechten worden ontleend.