Bijlage 3

Programma van Eisen

Aanbesteding MDR

Managed Detection and Response

Versie ~~1~~ 2.0

Inhoud

1. Inleiding

De Leidse regio wil een oplossing waarmee 24x7 hoogwaardige, real time monitoring, detectie en analyse van 'digitale bedreigingen' gericht op haar ICT-infrastructuur wordt geleverd. Deze ICT-infrastructuur bestaat onder andere uit:

- Circa 3500 werkplekken (vast en mobiele);
- Servers (web, proxy, applicate, database, etc);
- Print-, scan-, en kopieer apparatuur;
- Wi-Fi voorziening (voor bezoekers en eigen medewerkers);
- Routers en switches;
- Meerdere DMZ zones;
- 3 Firewalls

De infrastructuur van Leiden staat in datacenters van onze Managed Service Provider die ook het technisch beheer hierop uitvoert. De locaties van Leiden zijn verbonden middels glasvezelverbindingen met de datacenters van de Managed Service Provider.

Het internetverkeer vindt plaats aan de kant van Leiden. Hiervoor is een firewall (Palo-Alto) aan de kant van Leiden geplaatst om het internetverkeer te monitoren en te controleren.

De gemeente Leiden heeft meerdere locaties die verbonden zijn via het glasvezelnetwerk SLIB. Sommige locaties worden verbonden via een IPSEC VPN op de Palo-Alto als een glasvezelverbinding niet mogelijk is.

2. Kwetsbaarhedenmanagement

Eis 2.1	Inschrijver voert maandelijks een volledige scan van alle netwerkcomponenten op kwetsbaarheden.
Eis 2.2	Inschrijver voert credentialed/authenticated scans uit.
Eis 2.3	Bij een kwetsbaarheid van een internet facing systeem wordt ~~direct~~ binnen 4 tot 8 uur een advies gegeven welke maatregelen nodig zijn voor het mitigeren of oplossen van de kwetsbaarheid.
Eis 2.4	Inschrijver biedt een dashboard over kwetsbaarheden met uitgebreide rapportage mogelijkheden
Eis 2.5	Kwetsbaarheden dashboard is beveiligd met SSO op Azure AD omgeving van de Gemeente Leiden.
Eis 2.6	Per half jaar een uitgebreide rapportage over de volgende punten: - Welke kwetsbarheden zijn opgelost (of verdwenen) - Welke Kwetsbaarheden zijn bijgekomen - Trends en ontwikkelingen - Aandachtspunten - Dit lijstje is niet limitatief

3. Incident Response Support

Eis 3.1	Inschrijver levert op verzoek van de Gemeente Leiden een expert die 'hoogwaardig advies' kan geven ter zake van het bestrijden van een bedreiging of het minimaliseren van risico's. Deze expert is 24x7 (24 uur per dag, 7 dagen per week) binnen 30 minuten te bereiken.
Eis 3.2	Op verzoek van de Gemeente Leiden neemt de expert van Inschrijver deel aan het crisisteam van de Gemeente Leiden. Deze ondersteuning wordt geleverd via fysieke aanwezigheid dan wel digitale aanwezig van de expert op de crisis locatie van de Gemeente Leiden. De gemeente Leiden bepaalt of dit fysiek dan wel digitaal of een mix hiervan is. Deze deelname kan 24x7 (24 uur per dag, 7 dagen per week) gevraagd worden. Facturatie van bovenstaande is op basis van nacalculatie.
Eis 3.3	Inschrijver geeft tarieven op via het inschrijvingsblad voor deze expert ondersteuning. Dit tarief is inclusief reis- en verblijfkosten.
~~Eis 3.4~~	~~Inschrijver doet het onderhoud op de mogelijk geplaatste netwerk sensoren. Het gaat hier om updates en lifecycle management.~~

4. Monitoring en detectie

Eis 4.1	Inschrijver levert dienstverlening die 24x7 (24 uur per dag, 7 dagen per week) beschikbaar is voor de Leidse regio. Het gaat hier om monitoring en response.
Eis 4.2	~~De dienst monitort alle segmenten van het gehele netwerk en onze cloud systemen (Azure, 365 omgeving)~~ De dienst is technisch in staat om alle segmenten van het gehele netwerk en onze cloud systemen (Azure, 365 omgeving) te monitoren
Eis 4.3	De oplossing van Inschrijver detecteert real-time minimaal de volgende bedreigingen: • Inbraak- en hackpogingen; • Advanced persistent threats (APT, langdurige aanvallen); • Verkeer met bekende risicosites (bijv. malware en phishing sites); • Command&control verkeer (botnets); • Denial-of-service aanvallen op applicatie en netwerk niveau; • Adres en poort scans; • Verdachte afwijkingen ten opzichte van een normale situatie
Eis 4.4	Inschrijver heeft voor de Leidse regio een Nederlandstalig Security Operations Center (SOC) beschikbaar voor de beantwoording van vragen of advies over door het SOC gemelde security incidenten. Rapportages en software mogen in het Engels als de communicatie hier omtrent in het Nederlands plaatsvindt.
Eis 4.5	Het SOC is 24 uur per dag, 7 dagen per week, telefonisch bereikbaar voor de Leidse regio en biedt binnen ~~15~~ 30 minuten contact met de medewerker (of een directe collega) die het security incident aan de Leidse regio heeft gemeld.
Eis 4.6	Een security incident wordt geregistreerd in het ticket systeem van Inschrijver en uitgewisseld met de Leidse regio via het door Inschrijver beschikbaar gestelde dashboard. Dit dashboard dient 24x7 beschikbaar te zijn via een beveiligde verbinding via het internet.

Eis 4.7	Dit dashboard heeft de volgende real-time informatie en functionaliteiten:
	• het uitwisselen, updaten, afmelden en inzage in de voortgang van security incidenten met de Leidse regio;
	• gebruikersbeheer: instelbare rechten;
	• Recente kwetsbaarheden op het netwerk van de Leidse regio
	• Mogelijkheid tot doorklikken naar meer gedetailleerde informatie over een kwetsbaarheid.
	• rapportage:
	  ○ Het aantal actuele security incidenten
	  ○ Inzage in het aantal security incidenten per dag, week, maand en jaar;
	  ○ Het opvragen van verzameld netwerkverkeer in- en uitgaand

~~Eis 4.8~~	~~De monitoring voorziening van Inschrijver analyseert het netwerkverkeer van de Gemeente Leiden op locatie bij de Gemeente Leiden. De ruwe verkeersstromen blijven op locatie bij de Gemeente Leiden. Alerts en/of meldingen vanuit deze monitoring voorziening worden gedeeld met het Security Operations Center van Inschrijver.~~
Eis 4.9	Minimaal de volgende logbronnen in de analyses meenemen:

	- Firewalls logs - DNS logs - Entra ID logs - Microsoft AD logs - Exchange logs - Microsoft 365 omgeving, SharePoint en Onedrive logs - Windows events op Domain Controllers - Microsoft Defender(XDR) - Lijst is niet limitatief
Eis ~~3.4~~ 4.10	Inschrijver doet het onderhoud op de mogelijk geplaatste netwerk sensoren. Het gaat hier om updates en lifecycle management.

5. Rapportages

Eis 5.1	De rapportages dienen minimaal 1 week aangeleverd te zijn alvorens een overleg gepland staat.
Eis 5.2	Maandelijkse rapportage voor operationeel overleg: - Security incidenten - Maandstatistieken en trends - Langdurige verbetering voorstellen
Eis 5.3	Periodiek servicelevel rapportage: - De beschikbaarheid van de dienst - Aantal wijzigingen per maand - Aantal incidenten per maand - Het impactniveau van de incidenten - De response- en oplostijd van de incidenten - Aantal afgehandelde wijzigingen per maand - Aantal wijzigingen binnen SLA - Aantal wijzigingen buiten SLA - Overzicht van de uitgevoerde onderhoudswerkzaamheden
Eis 5.4	Leverancier heeft op ieder ITIL proces een KPI-bouwwerk die maandelijks worden gerapporteerd.
Eis 5.5	Leverancier levert de rapportages pro actief aan naar opdrachtgever het liefst binnen een centraal online systeem.
Eis 5.6	De leverancier geeft real-time inzicht van de service.
Eis 5.7	De inschrijver dient maandelijks een gedetailleerde en gespecificeerde factuur in te dienen. De factuur dient gespecificeerd te zijn per geleverde dienst of product, met een duidelijke omschrijving van de uitgevoerde werkzaamheden en/of geleverde diensten, inclusief de bijbehorende hoeveelheden en tarieven.
Eis 5.8	De inschrijver dient een kostenbeheersplan in te dienen, waarin wordt beschreven hoe de kosten gedurende de looptijd van de overeenkomst worden gemonitord, gecontroleerd en geoptimaliseerd. Dit plan dient binnen drie tot zes maanden na livegang opgeleverd te worden.

6. Assurance en wet-en regelgeving

Eis 6.1	Leverancier gaat een verwerkersovereenkomst aan met Gemeente Leiden op grond van de AVG en op basis van de standaard verwerkingsovereenkomst van de VNG.
Eis 6.2	Leverancier heeft en deelt een geldige ISO27001 certificaat en een VVT die de scope van de te leveren dienst volledig afdekt.
Eis 6.3	Leverancier voldoet aan geldende en toekomstige wet- en regelgeving rondom informatiebeveiliging en privacy (zoals AVG en NIS2). In geval van NIS2 als de regeling definitief gemaakt wordt.

7. Servicemanagement

Helpdesk

Eis 7.1	De helpdesk is telefonisch en online met ticketsysteem.
Eis 7.2	De eerste lijn support is Nederlandstalig
Eis 7.3	De beschikbaarheid van de dienstverlening is 24x7x365 ~~08.30 - 17.00 uur~~
~~Eis 7.4~~	~~De openingstijden van de service-desk zijn uit te breiden naar van 07.30 - 17.30 uur~~
Eis 7.5	Er wordt conform ITIL processen gewerkt. De prioriteitsinschatting wordt in gezamenlijkheid gemaakt, echter na escalatie beslist opdrachtgever ultiem over de toekenning van de urgentie.
Eis 7.6	Opdrachtgever ontvangt een (automatische) bevestiging van ingediende melding binnen 15 min.
Eis 7.7	Opdrachtnemer neemt bij incidenten van P1 en P2 niveau persoonlijk telefonisch contact op binnen ~~15~~ 30 min.
Eis 7.8	Opdrachtnemer hanteert bij incidenten van P1 niveau een ~~oplostijd~~ mitigatie adviestijd maximaal 2 uur (binnen kantooruren)
Eis 7.9	Opdrachtnemer hanteert bij incidenten van P2 niveau een ~~oplostijd~~ mitigatie adviestijd maximaal 4 uur (binnen kantooruren)
Eis 7.10	Opdrachtgever biedt de mogelijkheid een escalatienummer beschikbaar te stellen voor incidenten van P1 niveau buiten kantooruren.
Eis 7.11	De leverancier is verantwoordelijk voor de door opdrachtgever ingediende aanvragen en de afhandeling binnen de leveranciers ~~opdrachtgevers~~ eigen integrale keten.
Eis 7.12	De prioriteitsstelling van incidenten wordt bepaald door de in de SLA opgenomen definities en onderling overleg. De responstijden zijn in de SLA opgenomen. Bij verschil van interpretatie volgt een dispuutsprocedure waarbij het oordeel van de gemeente Leiden leidend is.
Eis 7.13	Een koppeling tussen het ticketsysteem van IDA binnen de gemeente Leiden (Topdesk) en de helpdesk-applicatie van de leverancier is mogelijk. Alle statuscommunicatie verloopt via dit ticketsysteem voor het incident-problem en changemanagement.

Servicemanagement

Eis 7.14	Er vindt in het kader van de contractueel overeengekomen afspraken periodiek overleg plaats tussen leverancier en opdrachtgever. Verslaglegging wordt verzorgd door opdrachtnemer. Indien gewenst (of noodzakelijk) kan de opdrachtgever de frequentie verhogen. Op **strategisch** niveau vindt overleg eenmaal per jaar plaats. Doel van dit gesprek is evaluatie van de prestaties over de afgelopen periode, doornemen van de efficiencyvoorstellen en doelstellingen voor de komende periode. Op **tactisch** niveau vindt overleg minimaal ieder kwartaal plaats tussen de partijen over wijzigingen, evaluatie en bijstelling van de service levels, facturatie, procedures, etc. Op **operationeel** niveau vindt overleg minimaal maandelijks plaats over de uitvoering van de dienstverlening, incidenten, klachten, vragen, etc.
Eis 7.15	In nader overleg wordt een DAP (Dossier Afspraken en Procedures) tussen opdrachtgever en opdrachtnemer opgesteld en gedurende het contract in onderlinge afstemming aangepast waar nodig door de vertegenwoordigers in het operationeel overleg. De DAP is uiterlijk na 6 maanden van de contractondertekening vastgesteld.
Eis 7.16	De leverancier hanteert een roadmap/ontwikkelagenda die gedeeld wordt met opdrachtgever waarin marktontwikkelingen, wettelijke wijzigingen en vernieuwingen in technologie zijn opgenomen binnen het aanbod op basis van bewezen technologie.

Onderhoud en beheer

Eis 7.17	Onderhoud en wijzigingen dienen altijd in overleg met de opdrachtgever plaats te vinden.
Eis 7.18	Bij elke release, service pack, patch wordt een releasenote uitgebracht met alle wijzigingen die de procesgang conform ITIL processen heeft doorlopen. De releasenote bevat een beschrijving van de impact van alle in de release opgenomen wijzigingen. Daarbij is ook iedere functionele verandering voor eindgebruikers beschreven.

Eis 7.19	De leverancier houdt zich aan onderstaande minimale communicatietermijnen: **Regulier onderhoud** Gelijk aan: - Standaard wijziging - Minor wijziging met lage impact - Onderhoud dat al vaker zonder problemen is uitgevoerd. Aankondiging **≥ 5 werkdagen van tevoren** **Groot onderhoud** Gelijk aan: - Minor wijziging met hoge impact - Major wijziging met lage/middel impact Aankondiging **2-4 weken van tevoren** **Zeer groot onderhoud** Gelijk aan: - Major wijziging met hoge impact Aankondiging **≥ 4 weken van tevoren**
Eis 7.20	Met inplannen van onderhoud en wijzigingen die impact hebben op de beschikbaarheid van het netwerk of de applicaties dient in ieder geval rekening gehouden te worden met Nederlandse feestdagen, bijzondere gelegenheden in Leiden, openstellinguren voor burgers en raadvergaderingen en andere bijeenkomsten van gemeenten buiten kantooruren zoals hieronder vermeld. **Openstellingen** Zoeterwoude dinsdag tot 20.00 uur. Leiderdorp woensdagavond tot 20.00 uur, Oegstgeest woensdag tot 20.00 uur, Leiden zaterdagochtend 09.00 - 12.30 uur, **Bijzondere gelegenheden in Leiden** 3de vrijdag april 2de weekend mei, Laatste weekend juni, 2 en 3 oktober, **Raadvergaderingen** Maandagavond gemeente Leiderdorp vanaf 20.00 uur - geen eindtijd. Donderdag gemeente Zoeterwoude vanaf 20.00 uur - geen eindtijd. Donderdag gemeente Oegstgeest vanaf 20.00 uur - geen eindtijd. Donderdag avond gemeente Leiden 20.00 uur - geen eindtijd. (dit wil zeggen dat op dinsdag en woensdag na 20:30 uur en vrijdag middag na 13.00 uur, zaterdag na 13.00uur en zondag iom gemeente Leiden kan worden ingepland).

Aanvullende afspraken

Eis 7.21	Leverancier waarborgt kennisborging binnen haar organisatie. Expertise moet geborgd zijn bij (personele) wijzigingen en overdracht. De leverancier zegt toe dat hij te allen tijde, de beschikking over heeft over de juiste expertise zoals in de dienstverleningsovereenkomst is overeengekomen. Leverancier verplicht zich bij het ontbreken hiervan desnoods op eigen kosten expertise in te huren.
Eis 7.22	~~Informatie over (technische) kwetsbaarheden van informatiesystemen die worden gebruikt, behoort door opdrachtnemer tijdig te worden verkregen en direct gerapporteerd aan opdrachtgever. De evt. blootstelling van de opdrachtgever aan dergelijke kwetsbaarheden dient te worden geëvalueerd en passende maatregelen dienen te worden genomen om het risico te mitigeren.~~ ~~De applicatie wordt minimaal elk jaar (indien gewenst door opdrachtgever en in belang van kwaliteit van de dienstverlening) onderworpen aan een penetratietest door opdrachtnemer. Opdrachtnemer dient de door de opdrachtgever geselecteerde partij toe te staan om een penetratietest uit te voeren.~~ Opdrachtnemer voert jaarlijks pentesten en verschillende compliance audits op het hele platform en dienstverlening uit. Hiervan worden de resultaten en certificeringen gedeeld met de opdrachtgever.

8. SLA en KPI's

Eis 8.1	De leverancier stuurt op voorhand een voorbeeld SLA mee met de aanbieding.
Eis 8.2	De leverancier neemt een ~~bonus~~ malus regeling op in de SLA.
~~Eis 8.3~~	~~Als beschikbaarheid (up-time) van de applicatie dient 99,9% gehaald te worden.~~
Eis 8.4	Gebruik van client software en agents moet lightweight zijn en mag op geen enkele manier de performance van de endpoints nadelig beïnvloeden. De belasting op het systeem mag niet gemiddeld hoger zijn dan 2% op de processor en ~~20~~ 160 MB op het werkgeheugen. Het is mogelijk om van tevoren een nulmeting te laten uitvoeren.