



Belastingdienst

Marktconsultatie

“Incident Response Retainer diensten”

Colofon

Titel : Incident Response Retainer diensten
Kenmerk : TN 613216
Document : Marktconsultatie
Versie : VERSIE 1.0
Datum : 23-09-2026

Afzendgegevens : Inkoop Uitvoeringscentrum (IUC) Belastingdienst
Ministerie van Financiën
J.F. Kennedylaan 8
7314 PS Apeldoorn
Postbus 9050
7300 GM Apeldoorn

Inhoud

Hoofdstuk 1. Algemeen	4
1.1. Leeswijzer	4
1.2. Inleiding	4
1.3. De Belastingdienst	4
1.3.1. Organisatie	5
1.3.2. Ontvlechting	5
1.3.3. Directie Informatievoorziening (IV)	6
1.3.4. Datacenter Services (DCS)	7
1.3.5. DCS als dienstverlener voor de Rijksoverheid	8
1.3.6. Inkoopuitvoeringscentrum (IUC) Belastingdienst	9
Hoofdstuk 2. Context	10
2.1. Inleiding	10
2.2. Doelstelling	10
Hoofdstuk 3. Vragen	11
3.1. Organisatie en ervaring	11
3.2. Retainer-dienstverlening	11
3.3. Incident Response Readiness	12
3.4. Forensisch onderzoek	12
3.5. Ransomware Response	12
3.6. Threat Intelligence	12
3.7. Crisismanagement	12
3.8. Juridische en Compliance Ondersteuning	12
3.9. Technische Respons en Herstel	13
3.10. Cloud en Identiteit	13
3.11. Rapportage, Sturing en Nazorg	13
3.12. Innovatie en Aanvullende Diensten	13
3.13. Maximale toegevoegde waarde m.b.t. investeringen/kosten	13
Hoofdstuk 4. Marktconsultatie procedure	14
4.1. Algemeen	14
4.2. Contact	14
4.3. Marktconsultatiedocument	14
4.4. Planning marktconsultatie	14
4.5. Toelichting en aanvullende vragen	15

4.6. Vormvereisten	15
4.7. Randvoorwaarden deelname aan deze marktconsultatie	15
Bijlage 1. Inzetgebieden IRR Diensten	17

Hoofdstuk 1. Algemeen

1.1. Leeswijzer

In hoofdstuk 1 is algemene informatie over de marktconsultatie te vinden. Hierna worden in hoofdstuk 2 de context en de doelstelling beschreven. In hoofdstuk 3 worden de vragen ten behoeve van deze marktconsultatie gesteld. De procedure voor deze marktconsultatie is te vinden in hoofdstuk 4.

1.2. Inleiding

Een marktconsultatie is een georganiseerde informatie-uitwisseling door middel van vragen en antwoorden met belanghebbenden over de voorgenomen opdracht. Hieruit wordt door de Belastingdienst de haalbaarheid getoetst en de randvoorwaarden vastgesteld. Deze marktconsultatie is een voorbereiding op een mogelijke verwerving van Incident Response Retainer diensten.

De marktconsultatie stelt de Belastingdienst in staat om kennis en ervaring uit de markt halen en eigen ideeën te toetsen, teneinde de kwaliteit van toekomstige opdrachtdocumenten te verbeteren. De Belastingdienst heeft onvoldoende inzicht in het potentieel van de markt op het gebied van Incident Response Retainer diensten. De wens is om de kennis van de markt te benutten om tot een kwalitatieve marktvraag te kunnen komen. Daarom nodigt de Belastingdienst de marktpartijen uit om te reageren. De bijdrage vanuit de markt wordt zeer op prijs gesteld. De marktconsultatie zorgt ervoor dat een toekomstige opdracht goed aansluit op de mogelijkheden die de markt biedt.

Deelname aan de marktconsultatie is geheel vrijwillig en vrijblijvend. Daarnaast heeft het op geen enkele wijze gevolgen voor een eventuele deelname aan de vervolgactiviteiten.

Het doel van de marktconsultatie bestaat uit:

- Het wekken van interesse bij de partijen in de markt;
- Het vaststellen van het potentieel van de partijen in de markt (marktwerking, concurrentie en samenwerking tussen de marktpartijen);
- Het bepalen van de opdrachtstrategie (marktbenadering, inhoudelijke aspecten en randvoorwaarden).

1.3. De Belastingdienst

De Belastingdienst is verantwoordelijk voor de heffing, controle en inning van de rijksbelastingen. Naast fiscaal toezicht voert de Belastingdienst op een aantal niet-fiscale terreinen taken uit.

De Belastingdienst heft en int premies volksverzekeringen, premies werknemersverzekeringen en de inkomensafhankelijke bijdrage Zorgverzekeringswet. Daarnaast is de dienst belast met de opsporing van fiscale en niet-fiscale fraude, mede in opdracht van het ministerie van Justitie en Veiligheid. Verder voert de Belastingdienst in opdracht van het ministerie van Economische Zaken een aantal toezichtstaken uit op het terrein van economische ordening, zoals de controle op de deponeringsplicht van de jaarrekening, en financiële integriteit.

Bij de Belastingdienst werken bijna 27.000 mensen. Een groot deel van onze medewerkers heeft direct contact met burgers en bedrijven. Zij voeren de kerntaken van de Belastingdienst uit. De rest van de medewerkers werkt bij de facilitaire bedrijven, concerndirecties en corporate diensten binnen onze organisatie.

Zie voor meer informatie over de organisatie van de Belastingdienst de internetsites van de Belastingdienst¹ en de rijksoverheid².

¹ www.belastingdienst.nl

² www.rijksoverheid.nl/ministeries/fin

1.3.1. Organisatie

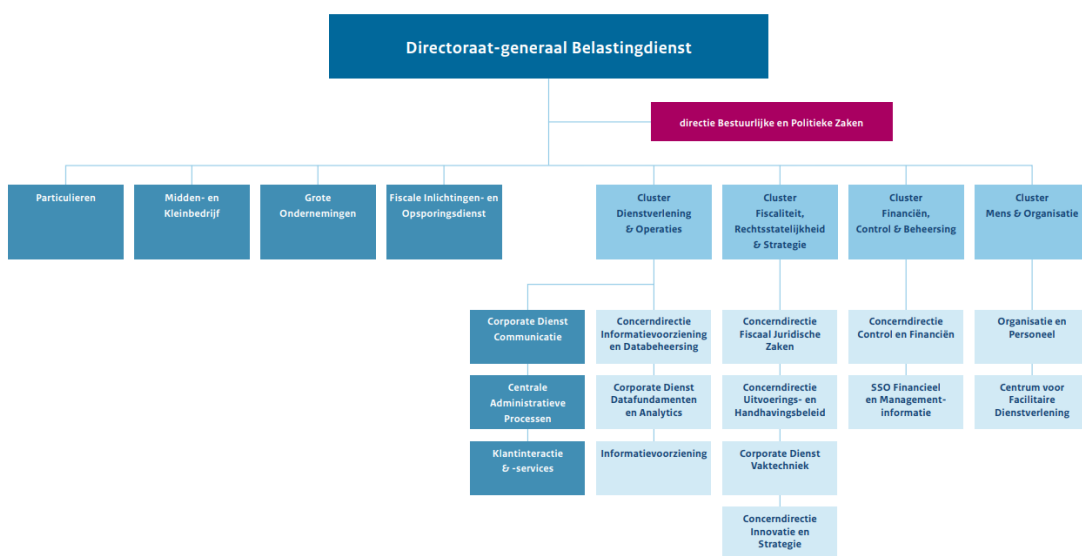
De Belastingdienst is onderdeel van de Rijksoverheid. Onze organisatie is een directoraat-generaal (DG) van het ministerie van Financiën. De Belastingdienst zelf bestaat uit verschillende directies. Deze directies richten zich op een deel van de taken van de Belastingdienst. De directies zijn als volgt georganiseerd:

- De doelgroepdirecties zijn verantwoordelijk voor de uitvoering en de handhaving op burgers en bedrijven. Deze organisatieonderdelen worden aangestuurd door de directeur-generaal van de Belastingdienst. De volgende 4 directies voeren deze taken uit:
 - Particulieren
 - Midden- en Kleinbedrijf
 - Grote Ondernemingen
 - Fiscale Inlichtingen- en Opsporingsdienst (FIOD)
- In cluster Dienstverlening & Operaties (D&O) komen de expertise en taken samen op het gebied van gegevens, integrale productieplanning, IV van de Belastingdienst en (massale) interactie met burgers en bedrijven. De plaatsvervangend directeur-generaal D&O stuurt deze directies aan.
- In cluster Fiscaliteit, Rechtsstatelijkheid en Strategie richten de directies zich op belastingwetgeving en -beleid. Zij worden aangestuurd door de plaatsvervangend directeur-generaal Fiscaliteit, Rechtsstatelijkheid en Strategie.
- De directies met expertise op Financiën, beheersing, Organisatie, Personeel en Facilitair zijn ondergebracht in de clusters Financiën, Control & Beheersing en Mens & Organisatie. Zij worden aangestuurd door algemeen directeurs.

De Belastingdienst is verantwoordelijk voor het:

- heffen, controleren en innen van rijksbelastingen, bijdragen zorgverzekeringswet, premies volksverzekeringen en premies werknemersverzekeringen.
- controleren of de wetgeving op het gebied van economische ordening wordt nageleefd. Bijvoorbeeld de controle op de deponeringsplicht van de jaarrekening en financiële integriteit.
- opsporen en bestrijden van financiële fraude en belastingfraude.

Organogram Belastingdienst



1.3.2. Ontvlechting

Het kabinet besloot in januari 2020 om de organisatieonderdelen Toeslagen en Douane te ontvlechten van de rest van de Belastingdienst. Zo wil de regering goede dienstverlening aan burgers en bedrijven kunnen verzekeren.

Toeslagen en Douane maken daarom geen onderdeel meer uit van de Belastingdienstorganisatie. Dit zijn nu zelfstandige onderdelen van het ministerie van Financiën.

- Het **directoraat-generaal Douane** houdt toezicht op het EU-grensoverschrijdende goederenverkeer, heft en int invoerrechten en belastingen en handhaaft wet- en regelgeving op het gebied van veiligheid, economie, gezondheid en milieu.
- Het **directoraat-generaal Toeslagen** maakt vitale voorzieningen voor iedereen betaalbaar. Dat doet het DG Toeslagen door het uitkeren van toeslagen die voor veel mensen onmisbaar zijn om de kosten te kunnen betalen van de zorgverzekering, de zorg voor kinderen en ruimte om te wonen.

Ook na de ontvlechting zijn Belastingdienst, Douane en Toeslagen met elkaar verbonden en blijven met elkaar samenwerken, onder andere op het gebied van de ICT en informatievoorziening. De Directie Informatievoorziening (IV) van de Belastingdienst ondersteunt de Directoraten Generaal Belastingdienst, Douane en Toeslagen met adequate informatievoorziening en de daarvoor benodigde ICT.

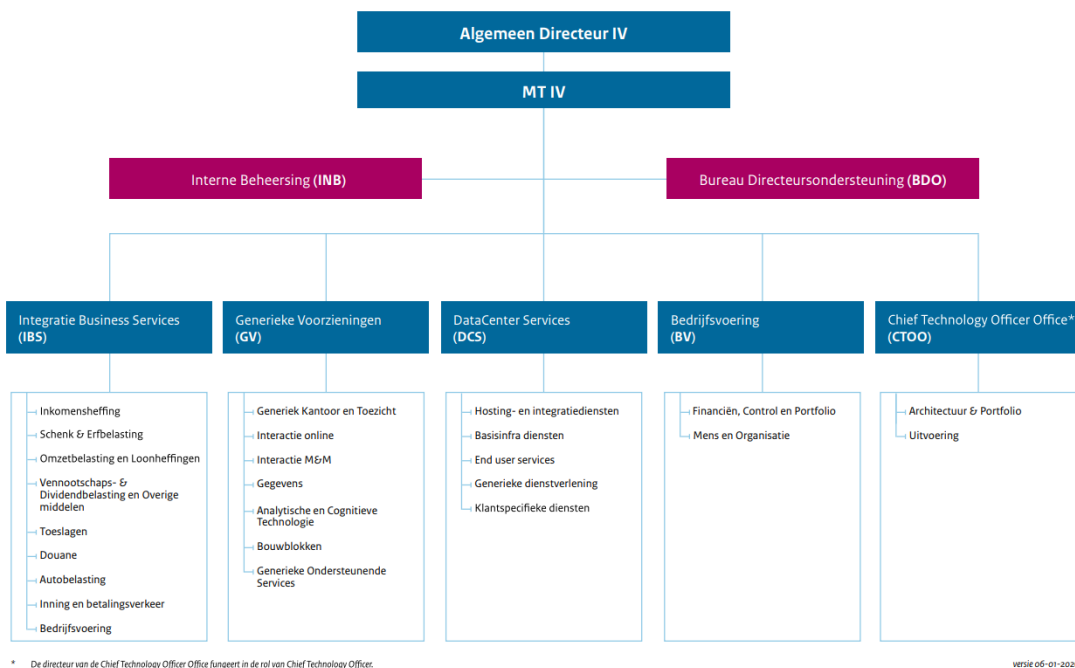
Waar hierna ten aanzien van de onderhavige aanbesteding wordt gesproken over de Belastingdienst, betreft het alle drie genoemde DG's van het ministerie van Financiën.

1.3.3. Directie Informatievoorziening (IV)

IV zorgt voor informatievoorzieningen die bijdragen aan een financieel gezond en veilig Nederland. De organisatie heeft te maken met een ingewikkeld ICT-landschap met veel technologieën voor beheer, onderhoud en vernieuwing. Hierbij is niet alleen behoefte aan modernisering van wat er al is maar ook aan nieuwe producten en diensten die aansluiten bij de huidige maatschappij.

De directie IV is één van de directies binnen het cluster Dienstverlening en Operaties (D&O). De directie ondersteunt de Belastingdienst, Toeslagen en Douane bij het uitvoeren van haar taken door:

- Structureel borgen van de continuïteit van de ICT door middel van voldoende eigen en up-to-date resources, en ICT-expertise.
- Zorgen dat de Belastingdienst, Toeslagen en Douane beschikt over de juiste middelen om het applicatie- en infrastructuurlandschap continu 'fit' te kunnen houden.
- Beleggen van ontwikkeling en exploitatie van IT in één IV, waardoor exploitatie-aspecten vroegtijdig in ontwikkeling worden meegenomen en gedrag in exploitatie direct wordt meegenomen bij de doorontwikkeling van IT.
- Aanbieden van een ICT-infrastructuur die is ingericht op de opslag en het beheer van grote gegevensverzamelingen, en de exploitatie van een hoog volume aan massale transactieprocessen.
- Realiseren van snelheid en adaptiviteit in de ontwikkelmethodiek (agile) en ontwikkelstrategie (automatisering van de. voortbrenging/bouwblokken/standaardisatie). Hierbij worden bewezen marktconforme oplossingen gehanteerd waarbij IV, waar mogelijk, kan acteren als fast follower.
- Inspelen op disruptieve, technologische ontwikkelingen ter ondersteuning van innovatieve businessdoelen van de Belastingdienst, Toeslagen en Douane.
- Mogelijk maken van rechtmatige gegevensverwerking en de Belastingdienst actief te beschermen tegen cyberaanvallen.
- Efficiënter aanbieden van de diensten door hergebruik, gestandaardiseerd werken en het garanderen van applicatie- en infrastructuur-portfoliofitness.
- In het handelen de effecten op de Belastingdienst, Toeslagen en Douane voor ogen houden.



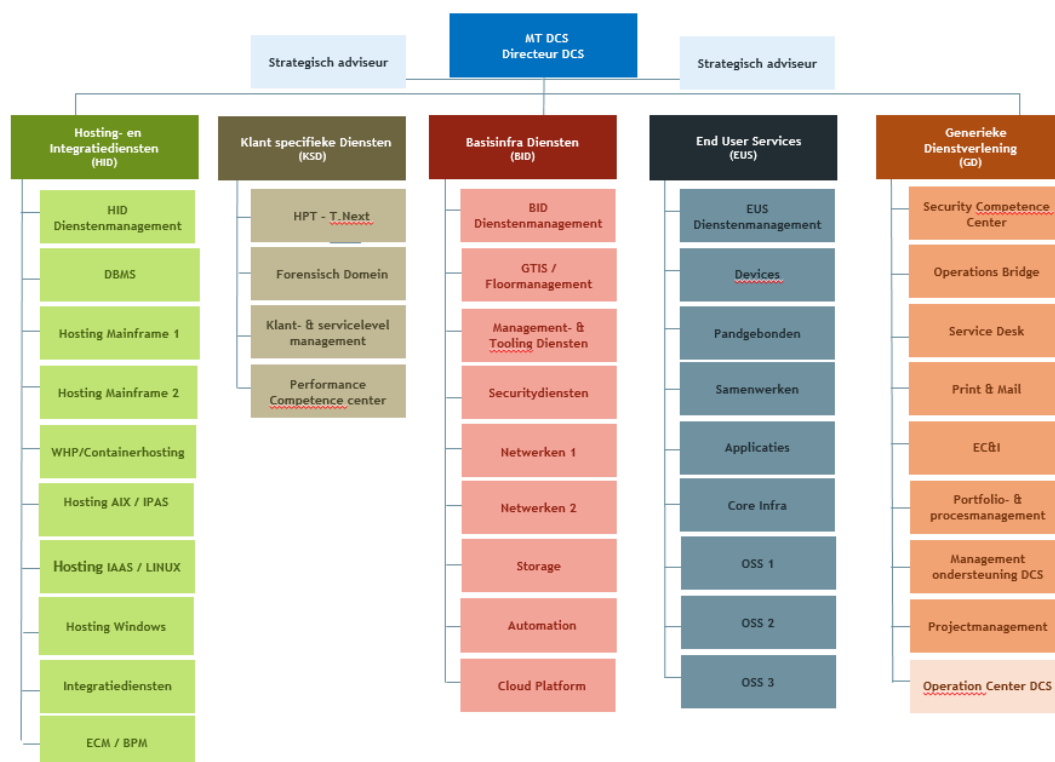
1.3.4. Datacenter Services (DCS)

Datacenter Services (DCS) is een integraal onderdeel van IV dat toeziet op het borgen van de continuïteit, de vernieuwing van de IV-voorzieningen en de doorontwikkeling van de IV-organisatie. DCS levert ICT-dienstverlening op het gebied van infrastructuur, hosting en operatie, waarmee de 24/7-beschikbaarheid van de ICT-systemen van de Belastingdienst én daarmee de continuïteit van de bv Nederland wordt geborgd. DCS levert ook diensten zoals de servicedesk en securitydiensten vanuit het security operating center.

Binnen DCS zijn 5 afdelingen ingericht:

- Hosting- en Integratiediensten is de leverancier van hostingdiensten (inclusief de daaraan onderliggende infrastructuurstaak) en diensten om de platformen met hun daarop draaiende applicaties optimaal met elkaar te integreren. Denk daarbij aan berichtuitwisseling en File Transfer-diensten.
- Basisinfrastructuur-diensten is de leverancier van Datacenter kerndiensten (computervloeren, energie, koeling, netwerken en storage), en management- en securitydiensten om beheer en beveiliging optimaal vorm te geven. Verder kent de afdeling twee diensten die respectievelijk aan de FIOD en IBS Toeslagen worden geleverd.
- End-userservices levert een brede range aan eindgebruikersdiensten, variërend van werkplek tot samenwerking en van telefonie tot video. Een deel van de diensten (waaronder telefonie, video en printen) wordt overheidsbreed geleverd via de rijks producten- en dienstencatalogus (rPDC).
- Generieke Dienstverlening is ingericht om overkoepelende dienstverlening te verrichten. Denk hierbij aan de Servicedesk-activiteiten en het Security Operations Center (SOC) waarvan de activiteiten een breed terrein bestrijken op het gebied van cybersecurity.
- Klant & Organisatie: de afdeling Klant & Organisatie is ingericht om inzicht en overzicht te realiseren over geheel DCS, evenals besturing en verantwoording hierover. Daarnaast onderhoudt de afdeling de formele relatie met andere partijen binnen IV, de Belastingdienst en andere overheden.

Datacenter Services



1.3.5. DCS als dienstverlener voor de Rijksoverheid

De samenwerking binnen de rijksoverheid is belegd bij het directoraat-generaal Overheids Organisatie van het ministerie van Binnenlandse Zaken³.

DCS is een van de rijksbrede dienstverleners. In deze rol faciliteert DCS bijvoorbeeld een van de vier overheidsdatacenters (ODC's) van de rijksoverheid (datacentervoorziening Rijk) en levert DCS als een van de vijf ICT-dienstverleners Pand (IDV-P) de benodigde ICT-diensten in (rijks)overheidsgebouwen⁴.

Concreet betekent dit dat er een structuur gekozen is waarbij meerdere (rijks)overheidspartijen⁵ gebruik kunnen maken van de ICT-diensten van DCS. Aandachtpunten daarin zijn continuïteit en veiligheid als ook modulaire inrichting en flexibiliteit van de ICT-diensten en bijbehorende infrastructuurdiensten, waarvan de te verwerven Incident Response Retainer diensten onderdeel zullen uitmaken.

De te verwerven Incident Response Retainer diensten zullen in eerste instantie worden ingezet voor de Belastingdienst ten behoeve van haar bedrijfsprocessen, maar worden waar nodig ook voor andere organisatieonderdelen van de (rijks)overheid beschikbaar gesteld, die voor hun eigen bedrijfsprocessen, gebruik maken van de ICT-diensten van DCS inclusief de bijbehorende infrastructuurdiensten, zoals de onderhavige hosting en generieke diensten.

Ter indicatie: Tussen de 85 en 90% van de omvang van de ICT-diensten wordt thans afgenomen door de Belastingdienst, tegen 10 tot 15% dat beschikbaar wordt gesteld ten behoeve van andere onderdelen van de (rijks)overheid. Deze verdeling kan na verloop van tijd wijzigen, afhankelijk van besluitvorming binnen de overheid.

³ <https://www.rijksoverheid.nl/onderwerpen/rijksoverheid/bedrijfsvoering-van-het-rijk>

⁴ <https://www.rijksbreddienstverleners.nl/>

⁵ Met opzet wordt gesproken over (rijks)overheid, met haakjes om het woord 'rijks'. Ook overheidsorganisaties die niet tot de rijksoverheid worden gerekend, kunnen in de toekomst ICT-diensten van/via het Belastingdienst ODC gaan afnemen.

1.3.6. Inkoopuitvoeringscentrum (IUC) Belastingdienst

Inkoop Uitvoeringscentrum Belastingdienst (IUC Belastingdienst) is onderdeel van het cluster Financiën, Control en Inkoop (FC&I)⁶ van de Belastingdienst en is het onderdeel van de Belastingdienst dat deze Aanbesteding uitvoert. IUC Belastingdienst verricht inkoopactiviteiten voor de generieke inkoop van de bij zijn ondergebrachte rijks categorieën en daarnaast voor de specifieke inkoop van de Belastingdienst en Domeinen Roerende Zaken. Hij doet dat op een wijze die effectief, doelmatig, transparant en rechtmatig is.

⁶ Het cluster Financiën, Control en Inkoop (FC&I) is die nieuwe naam voor het cluster Financiën, Control en Beheersing (FC&B) binnen de Belastingdienst

Hoofdstuk 2. Context

2.1. Inleiding

De Belastingdienst wil een breed beeld krijgen van de beschikbare dienstverlening en de volwassenheid van leveranciers op het gebied van incident response, digitale forensics, cybercrisismanagement, ransomware-respons, dreigingsinformatie en herstelondersteuning. De marktconsultatie is nadrukkelijk niet uitsluitend gericht op ondersteuning tijdens een incident, maar ook op voorbereiding, weerbaarheidsverhoging, kennisoverdracht en nazorg.

Leveranciers worden gevraagd inzicht te geven in hun capaciteiten, werkwijze, ervaring, beschikbaarheid en eventuele aanvullende diensten die bijdragen aan een effectieve voorbereiding op, respons op en afhandeling van cyberincidenten.

Met deze marktvraag wil de Belastingdienst vaststellen:

- Welke diensten en functionaliteiten door de markt worden aangeboden;
- Welke verschillen bestaan tussen leveranciers op het gebied van expertise, capaciteit en dienstverlening;
- Welke contract- en retainerconstructies gebruikelijk zijn;
- Welke innovatieve of aanvullende mogelijkheden beschikbaar zijn;
- Welke partijen het beste aansluiten bij de toekomstige behoefte van de Belastingdienst op het gebied van cyberincidenten en digitale weerbaarheid.

De in hoofdstuk 3 opgenomen onderwerpen vormen een brede inventarisatie van de mogelijkheden die binnen een incident retainer kunnen worden ondergebracht en dienen als basis voor de verdere uitwerking van de uiteindelijke aanbestedings- of inkoopstrategie.

2.2. Doelstelling

De Belastingdienst is voornemens op termijn Incident Response (IR) Retainer diensten te verwerven. Het doel van deze marktconsultatie is inzicht te verkrijgen in de diensten die toonaangevende leveranciers binnen dit werkveld kunnen bieden evenals de mate van kwaliteit en toegevoegde waarde ervan voor de Belastingdienst als opdrachtgever. Daarbij zijn de volgende aspecten van de complete cybersecurity lifecycle te onderkennen:

- Preventie;
- Readiness & voorbereiding;
- Detectie en identificatie;
- Incident response;
- Crisismanagement;
- Herstel;
- Nazorg en verbetermaatregelen;
- Advies op het gebied van forensics readiness.

Hoofdstuk 3. Vragen

Dit hoofdstuk bevat de vragen die de Belastingdienst heeft ten aanzien van IR Retainer diensten. Het doel van deze consultatie is inzicht te verkrijgen in de mogelijkheden die marktpartijen bieden op het gebied van voorbereiding, respons, crisisbeheersing en herstel bij cybersecurity-incidenten.

De vragen zijn bedoeld als gespreksonderwerpen om inzicht te krijgen in de beschikbare dienstverlening, de volwassenheid van aanbieders en de wijze waarop zij de beste toegevoegde waarde kunnen bieden aan de Belastingdienst bij het voorkomen van c.q. omgaan met cyberincidenten, rekening houdend met de reeds aanwezige kennis en kunde, organisatie, processen en aanwezige oplossingen. De Belastingdienst staat nadrukkelijk open voor aanvullende voorstellen, innovatieve dienstverlening en alternatieve invullingen die bijdragen aan het vergroten van de cyberweerbaarheid.

Waar hieronder wordt gesproken over een incident, wordt een cybersecurity incident bedoeld waarvoor qua aard, omvang en urgentie de IR Retainer dienstverlener wordt ingeschakeld.

3.1. Organisatie en ervaring

Vragen	Organisatie en ervaring
1.	Hoe is uw incident response dienstverlening georganiseerd en welke expertisegebieden zijn daarin vertegenwoordigd?
2.	Welke ervaring heeft u met organisaties die qua omvang, complexiteit of sector vergelijkbaar zijn met de Belastingdienst? Ga ervan uit dat de Belastingdienst retainer diensten wenst te verwerven voor de verschillende inzetgebieden die in algemene zin kunnen worden onderkend, zie hiervoor de bijlage 1 onderaan dit document.
3.	Beschrijf (geanonimiseerd) het verloop van een recente casus waar u uw IR Retainer diensten heeft ingezet. Welke resources heeft u daarvoor ingezet?
4.	Hoe bent u vertegenwoordigd in NL of Europa qua vestigingen/medewerkers?
5.	Wat onderscheidt uw dienstverlening van andere aanbieders in de markt?
6.	Hoe ziet u de samenwerking met het Belastingdienst CSIRT (Computer Security Incident Response Team)? Welke rolverdeling ziet u tussen de Belastingdienst en uw organisatie?
7.	Staat u open om een referentiebezoek met een bestaande klant (lieftst rijksoverheid), vergelijkbaar met de Belastingdienst te organiseren?
8.	Hoe bepaalt u zelf de aard, omvang en urgentie van een incident?
9.	Hoe kunt u ervoor zorgen dat bij gelijktijdige incidenten bij verschillende klanten de dienstverlening aan de Belastingdienst prioriteit krijgt?
10.	Op welke wijze wordt de informatiebeveiliging van de Belastingdienst geborgd tijdens de IR Retainer dienstverlening? Beschikt u bijvoorbeeld, naast andere te geven info, over een recente ISO27001 certificering, of minimaal daarmee vergelijkbaar information security management system (ISMS)?

3.2. Retainer-dienstverlening

Vragen	Retainer dienstverlening
11.	Hoe ziet uw retainer-model eruit en welke diensten kunnen hierbinnen worden afgenomen?
12.	Op welke wijze wordt de beschikbaarheid van door u in te zetten resources (in de vorm van mensen en middelen) tijdens een incident geborgd?
13.	Hoe schaaft u op bij omvangrijke of langdurige incidenten?

14.	Ziet u mogelijkheden om de coördinatie van een cyberincidenten in complexe organisaties, zoals die van de Belastingdienst, over te nemen en hoe ziet dat er dan uit?
-----	--

3.3. Incident Response Readiness

Vragen	Incident Response Readiness
15.	Welke diensten biedt u aan om organisaties voorafgaand aan een incident beter voor te bereiden?
16.	Hoe ondersteunt u organisaties bij het ontwikkelen, testen en verbeteren van incident response plannen en procedures?
17.	Welke soorten oefeningen en simulaties kunt u verzorgen?

3.4. Forensisch onderzoek

Vragen	Forensisch onderzoek
18.	Welke forensische onderzoekscapaciteiten biedt u aan tijdens en na een incident?
19.	Welke expertise heeft u op het gebied van endpoint-, netwerk-, cloud- en identiteitsforensics?
20.	Op welke wijze draagt uw onderzoek bij aan herstel, bewijsvoering en verbetermaatregelen?
21.	Welke bandbreedte heeft u beschikbaar om in korte termijn grote hoeveelheden gegevens naar uw veilige omgeving te kunnen transporteren voor onderzoeksactiviteiten binnen de retainer dienstverlening?

3.5. Ransomware Response

Vragen	Ransomware Response
22.	Welke ondersteuning biedt u bij ransomware-incidenten?
23.	Onder welke omstandigheden ondersteunt u bij onderhandelingen met dreigingsactoren?
24.	Hoe ondersteunt u organisaties bij besluitvorming rondom datadiefstal, afpersing en eventuele publicatie van gegevens?

3.6. Threat Intelligence

Vragen	Threat Intelligence
25.	Welke dreigingsinformatie levert u voorafgaand aan en tijdens een incident?
26.	Hoe vertaalt u dreigingsinformatie naar concrete verbetermaatregelen voor de organisatie?

3.7. Crisismanagement

Vragen	Crisismanagement
27.	Hoe ondersteunt u bestuur, directie en crisismanagementteams tijdens een cyberincident?
28.	Welke expertise levert u op het gebied van besluitvorming, coördinatie en stakeholdermanagement?

3.8. Juridische en Compliance Ondersteuning

Vragen	Juridische en Compliance ondersteuning
29.	Welke ondersteuning biedt u ten aanzien van privacyregelgeving, meldplicht datalekken en andere relevante wet- en regelgeving? Denk daarbij aan de Cbw.
30.	Welke mogelijkheden biedt u voor juridisch houdbare verslaglegging en bewijsvoering?

3.9. Technische Respons en Herstel

Vragen	Technische Respons en Herstel
31.	Hoe ondersteunt u organisaties bij containment, eradication en herstel van een incident?
32.	Welke rol vervult u bij het valideren van herstelmaatregelen en het vaststellen dat een omgeving weer veilig in gebruik kan worden genomen?

3.10. Cloud en Identiteit

Vragen	Cloud en Identiteit
33.	Welke ervaring heeft u met incidenten binnen Microsoft 365, Entra ID, Azure en andere cloudomgevingen?
34.	Hoe ondersteunt u onderzoek en herstel bij identiteitscompromittering en accountmisbruik?

3.11. Rapportage, Sturing en Nazorg

Vragen	Rapportage, Sturing en Nazorg
35.	Welke rapportages levert u tijdens en na afloop van een incident?
36.	Hoe stelt u de Belastingdienst in staat om te sturen op uw prestaties?
37.	Hoe ondersteunt u organisaties bij het uitvoeren van verbetermaatregelen en het versterken van de cyberweerbaarheid na een incident?

3.12. Innovatie en Aanvullende Diensten

Vragen	Innovatie en Aanvullende Diensten
38.	Welke aanvullende diensten of innovatieve mogelijkheden biedt u die volgens u relevant zijn voor een moderne incident retainer? Awareness zou een voorbeeld kunnen zijn.
39.	Welke ontwikkelingen ziet u binnen incident response dienstverlening die organisaties de komende jaren zouden moeten meenemen in hun afweging?

3.13. Maximale toegevoegde waarde m.b.t. investeringen/kosten

Vragen	Crisismanagement
40.	Uiteraard hoopt de Belastingdienst situaties te voorkomen die leiden tot de inzet van een IR Retainer dienstverlener. De te betalen vergoedingen daarvoor kunnen als een verzekering worden gezien voor het minimaliseren van nadelige gevolgen rondom mogelijke toekomstige incidenten. De Belastingdienst wenst niet alleen de premies daarvoor te betalen maar wil daar, in tijden dat er niet op incidenten geacteerd hoeft te worden, toch maximaal toegevoegde waarde voor terug zien. Kunt u aangeven hoe u aan deze wens tegemoet kunt komen, zonder dat dit uw slagkracht en commitment ten tijde van een incident negatief beïnvloedt?
41.	Heeft u naast een periodieke premie andersoortige afrekenmodellen? Kunt u de voor- en nadelen van deze eventuele verschillende afrekenmodellen schetsen?

Hoofdstuk 4. Marktconsultatie procedure

4.1. Algemeen

De Belastingdienst heeft de potentiële leveranciers voor Incident Response Retainer diensten in de markt in beeld gebracht. Deze leveranciers worden uitgenodigd de in hoofdstuk 3 gestelde vragen te beantwoorden en een schets te geven van de te aan te bieden Incident Response Retainer diensten.

Het indienen van schriftelijke reacties kan via de daartoe bestemde module in TenderNed.

4.2. Contact

De Belastingdienst hanteert voor deze formele marktconsultatie heldere regels, daarom dient u alleen met onderstaande contactpersoon(en) over deze marktconsultatie te communiceren. Communiceert u over deze marktconsultatie met andere medewerkers van de of tracht u via andere kanalen om hen te beïnvloeden. Dan kan dat voor reden zijn voor de Belastingdienst om u uit te sluiten van verdere deelname aan deze marktconsultatie.

Contactpersoon	
Naam:	Bart Stoekenbroek
Functie:	Senior Inkoopadviseur ICT
E-mail:	b.stoekenbroek@belastingdienst.nl
Telefoonnummer:	+ 31 6 15 83 27 01

4.3. Marktconsultatiedocument

Op basis van het voorliggende document kunnen marktpartijen een reactie geven op de in deze marktconsultatie gestelde vragen. De Belastingdienst heeft hiertoe in dit document de behoefte omschreven en toegelicht volgens welke procedure deze marktconsultatie verloopt.

Indien u, ondanks de zorg die De Belastingdienst aan dit document heeft besteed, onduidelijkheden of onvolkomenheden aantreft of dat er bij u vragen rijzen, wilt u die dan vóór de ondergenoemde deadline voor het stellen van vragen kenbaar maken. Antwoorden worden vervolgens gepubliceerd in een nota van inlichtingen.

De resultaten van de marktconsultatie kunnen worden verwerkt in aanbestedingsdocumenten en/of openbaar gemaakt, zonder dat deze herleidbaar zijn tot de deelnemers van de marktconsultatie. De Belastingdienst mag vrij over de verstrekte informatie beschikken en deze informatie gebruiken. Wij verzoeken u de vragen schriftelijk te beantwoorden. De door u gegeven informatie zal vertrouwelijk worden behandeld. Mogelijk wordt u benaderd om uw product te presenteren tijdens een bijeenkomst met vertegenwoordigers van de Belastingdienst.

4.4. Planning marktconsultatie

Activiteit	Datum
Publicatie marktconsultatie	23-09-2026
Deadline voor het stellen van vragen	07-10-2026 12:00 uur
Publicatie nota van inlichtingen	14-10-2026
Uiterst moment van insturen beantwoording.	30-10-2026
Optioneel: mondelinge toelichting en aanvullende vragen	Begin tot medio november

4.5. Toelichting en aanvullende vragen

De Belastingdienst zal mogelijkerwijs deelnemers aan deze marktconsultatie uitnodigen voor een vervolg, het zij schriftelijk, hetzij in een aanvullende bijeenkomst, waarin de uitgenodigde deelnemer zijn antwoorden nader kan toelichten en waarbij aanvullende vragen door de Belastingdienst gesteld kunnen worden naar aanleiding van de ontvangen reacties.

4.6. Vormvereisten

Het is uitdrukkelijk niet de bedoeling offertes in te leveren, wij verzoeken u dringend om u te beperken tot de beantwoording van de gestelde vragen in Hoofdstuk 3.

Beantwoording graag kort en krachtig. Uiteraard bent u niet verplicht tot het verstrekken van antwoorden en u bent eveneens vrij bepaalde vragen over te slaan. De bijdrage aan de marktconsultatie/beantwoording van de vragen ontvangen wij bij voorkeur in Word of Excel format. Aanvullende en overige documentatie mag als pdf-bestand worden aangeleverd.

In de begeleidende brief bij de bijdrage aan de marktconsultatie ontvangen wij graag van de contactpersoon aan de kant van de marktpartijen de onderstaande gegevens:

Gegevens	
Naam	
Functie	
Kantooradres	
Telefoonnummer	
E-mailadres	

4.7. Randvoorwaarden deelname aan deze marktconsultatie

Door deelname aan deze marktconsultatie gaat u onvoorwaardelijk akkoord met de alle voorwaarden zoals vermeld in dit marktconsultatiedocument. Hieronder staan de randvoorwaarden limitatief opgesomd:

1. Deelnemen aan de marktconsultatie is voor marktpartijen én de Belastingdienst vrijblijvend;
2. Dit marktconsultatiedocument is uitsluitend bestemd voor marktconsultatie doeleinden;
3. De marktconsultatie is geen onderdeel van de mogelijke aanbesteding maar een consultatieronde;
4. Door de deelnemers aan deze marktconsultatie kunnen geen kosten in rekening worden gebracht aan de Belastingdienst in verband met het uitbrengen van de reactie op deze marktconsultatie en de daarvoor uit te voeren werkzaamheden;
5. Deze marktconsultatie dient uitdrukkelijk niet om een voorselectie te maken van marktpartijen in het kader van een mogelijke toekomstige aanbesteding. Marktpartijen die niet deelnemen aan de marktconsultatie zijn daarmee niet uitgesloten van deelname aan een mogelijk inkooptraject. Evenmin zijn marktpartijen die deelnemen aan de marktconsultatie op enige wijze uitgesloten van, of bevoorrecht in, een eventuele deelname aan een aanbestedings- of inkooptraject;
6. De resultaten van de marktconsultatie worden mogelijk verwerkt in aanbestedingsdocumenten (bijvoorbeeld door tijdens deze marktconsultatie ontvangen informatie te verwerken in het Beschrijvend document), zonder dat deze herleidbaar zijn tot de deelnemers aan de marktconsultatie. Door deel te nemen aan marktconsultatie stemt u hiermee in;
7. Verstrekte informatie in het kader van de marktconsultatie kan afwijken van in de aanbestedingsprocedure te verstrekken informatie;
8. De inbreng van deelnemers aan deze marktconsultatie zal zoveel mogelijk vertrouwelijk behandeld worden, waarbij in ieder geval rekening zal worden gehouden met de gerechtvaardigde belangen van de deelnemers van deze marktconsultatie en de Belastingdienst;

9. De voertaal tijdens deze marktconsultatie is Nederlands, productinformatie mag in het Engels;
10. De Belastingdienst is op geen enkele wijze gebonden aan de uitkomsten van de marktconsultatie;
11. Deelnemers aan de marktconsultatie kunnen geen rechten ontleen aan deelname aan de marktconsultatie of aan enige informatie die tijdens de marktconsultatie wordt verstrekt;
12. Het accepteren of honoreren van eventuele voorwaarden of claims (waaronder voorwaarden of claims t.a.v. Intellectuele Eigendomsrechten zoals auteursrecht) van deelnemers aan deze marktconsultatie over het gebruik van door hen aan de Belastingdienst in het kader van deze marktconsultatie informatie of vertrouwelijkheid en geheimhouding van door de betreffende marktpartij verstrekte informatie is niet mogelijk. Wel zal de Belastingdienst bij het verstrekken, openbaren of verwerken van informatie verkregen van deelnemers tijdens, of voortvloeiend uit, deze marktconsultatie zoveel mogelijk trachten te voorkomen dat deze informatie direct herleidbaar is tot een bepaalde deelnemer van de marktconsultatie.
13. Indien intellectuele eigendomsrechten (waaronder auteursrechten) van een deelnemer of van derden van toepassing zijn dan wordt de Belastingdienst door de betreffende deelnemer aan deze marktconsultatie gevrijwaard van een vordering van deze deelnemer en/of derden op basis van die intellectuele eigendomsrechten (waaronder auteursrechten).
14. De Belastingdienst behoudt zich het uitdrukkelijk het recht voor: De planning van deze marktconsultatie zoals opgenomen in dit document te wijzigen. Daarnaast ook om de marktconsultatie tijdelijk en/of definitief te staken.

Bijlage 1. Inzetgebieden IR Retainer Diensten

Incident Response (IR) retainerdiensten worden tegenwoordig ingezet voor vrijwel alle kritieke ICT-infrastructuurcomponenten binnen moderne datacenters. De focus verschuift daarbij van alleen traditionele servers naar complete hybride infrastructuren, cloudomgevingen en OT-systemen.

1. Servers en besturingssystemen

De meest voorkomende inzet is op:

- Windows Servers
- Linux Servers
- Unix-systemen
- Hypervisor-hosts (VMware ESXi, Hyper-V, Nutanix AHV, KVM)

Typische incidenten:

- ransomware
- privilege escalation
- webshells
- malware
- ongeautoriseerde accounts
- datadiefstal

2. Virtualisatie- en cloudplatformen

Virtualisatie

- VMware vSphere / ESXi
- VMware Cloud Foundation
- Nutanix
- Hyper-V

Cloud

- Microsoft Azure
- AWS
- Google Cloud Platform

Onderzoek richt zich vaak op:

- gecompromitteerde beheeraccounts
- misbruik van service principals
- manipulatie van snapshots
- laterale beweging tussen workloads
- cloud control plane compromittering

3. Netwerkinfrastructuur

IR-retainers worden veel ingezet voor:

- Core switches
- Spine-leaf fabric switches
- Routers
- Firewalls
- Load balancers

- SD-WAN-oplossingen

Voorbeelden:

- Cisco
- Juniper
- Arista
- Fortinet
- Palo Alto Networks
- F5 Networks

Typische incidenten:

- compromittering van beheerinterfaces
- ongeautoriseerde configuratiewijzigingen
- BGP-hijacking
- firewall-omzeiling
- datalekken via netwerkkaparaatuur

4. Identity & Access Management (IAM)

Platformen

- Microsoft Active Directory
- Entra ID (Azure AD)
- Okta
- Ping Identity

Veel voorkomende aanvallen:

- Golden Ticket
- Silver Ticket
- Pass-the-Hash
- Pass-the-Ticket
- MFA-bypass
- Identiteitsfraude

IR-retainers bevatten hiervoor vaak gespecialiseerde AD-forensics.

5. Endpoint- en workloadbeveiliging

Componenten:

- EDR/XDR-platformen
- Endpoint agents
- Workload protection

Voorbeelden:

- Microsoft Defender XDR
- CrowdStrike Falcon
- SentinelOne
- Trellix
- Palo Alto Cortex XDR

6. Container- en Kubernetes-platformen

Platformen

- Kubernetes
- OpenShift
- Rancher
- AKS
- EKS
- GKE

Onderzoek richt zich op:

- gecompromitteerde containers
- supply-chain aanvallen
- kwaadaardige images
- misbruik van service accounts
- ontsnapping uit containers
- Kubernetes control-plane aanvallen

7. Storage-omgevingen

Enterprise storage

- NetApp
- Dell PowerStore
- Dell PowerScale
- Pure Storage
- HPE Alletra

Incidenten:

- ransomware op NAS-omgevingen
- verwijdering van snapshots
- compromittering van storagebeheer

8. Back-up- en herstelplatformen

Producten

- Veeam
- Commvault
- Rubrik
- Cohesity
- NetBackup

Aanvallers proberen vaak eerst back-upomgevingen uit te schakelen voordat encryptie plaatsvindt.

9. Security-infrastructuur

Security tooling

- SIEM
- SOAR
- NDR
- TIP-platformen

Voorbeelden:

- Microsoft Sentinel
- Splunk
- QRadar
- Elastic

- Darktrace

IR-retainers bevatten vaak:

- loganalyse
- threat hunting
- IOC-ontwikkeling
- digitale forensics

10.Databases

- Oracle
- SQL Server
- PostgreSQL
- MySQL
- MongoDB

Incidenten:

- datadiefstal
- privilege escalation
- ransomware
- sabotage van databases

11. HCI-omgevingen (Hyperconverged Infrastructure)

- Nutanix
- VMware VxRail
- HPE SimpliVity

12. Datacenter-OT en facility-systemen

Bij grotere overheids- en enterprise-datacenters zien we ook IR-retainers voor:

- DCIM-systemen
- gebouwbeheersystemen
- koelinstallaties
- UPS-systemen
- noodstroomvoorzieningen
- slimme PDU's

Vanwege NIS2/Cbw vallen dergelijke systemen steeds vaker binnen het incident response bereik.

Wat zit doorgaans in een enterprise IR-retainer?

Voor een groot datacenter omvat de retainer vaak:

- 24x7 incident response
- digitale forensics
- malware-analyse
- ransomware response
- Active Directory forensics
- cloud incident response
- Kubernetes/container forensics
- threat hunting
- tabletop oefeningen
- crisismanagementondersteuning
- juridische ondersteuning bij datalekken

- ondersteuning bij meldingen onder AVG en NIS2
-

Specifiek voor een Rijksdatacenter

Bij een omgeving met duizenden Windows- en Linux-servers, Kubernetes-clusters, cloudworkloads en BIO 2.0/NIS2-verplichtingen worden IR-retainers doorgaans ingericht voor de volgende prioritaire domeinen:

1. Identity (AD / Entra ID)
2. Windows- en Linux-servers
3. VMware- of Nutanix-platform
4. Kubernetes/OpenShift-platform
5. Back-up-omgeving (Veeam, Rubrik, Commvault)
6. Netwerkinfrastructuur (firewalls, routers, switches)
7. Azure/AWS-cloudomgeving
8. SIEM/XDR-platform