Bevindingenoverzicht

Broedkamer en voorlopers

(periode 2012 – feb. 2016)

concept 0.9 (10 augustus 2017)

Inhoud

1. Inleiding

Dit document bevat de bevindingen van het onderzoeksteam bij de uitvoering van het onderzoek naar de Broedkamer en voorlopers, periode 2012 – februari 2016.

Het bevindingenoverzicht wordt gebruikt voor ‘hoor en wederhoor’ met het verantwoordelijk management. Op basis van het afgestemde bevindingenoverzicht wordt het (eind)rapport van dit onderzoek opgesteld.

Bevindingen uit deze onderzoeksperiode (2012 - februari 2016) kunnen achterhaald zijn door ontwikkelingen in 2016 en daarna. Het onderzoek naar ‘Gegevensgebruik D&A’ (periode februari 2016 - maart 2017) geeft hierover nader inzicht.

2. Object van onderzoek

Het object van onderzoek is de Broedkamer en voorlopers, als onderdeel van de afdeling BI&A, in de periode 2012 - februari 2016.

Dit hoofdstuk geeft informatie over ontwikkelingen op het gebied van Business Intelligence (BI), het primaire werkgebied van de Broedkamer en voorlopers en de organisatorische plaats binnen de Belastingdienst. In het organisatorische deel wordt een beeld geschetst van wat er onder de Broedkamer en voorlopers wordt verstaan.
Het gaat niet om bevindingen maar om informatie (uit verklaringen en memo's) die helpt om de inhoud van Hoofdstuk 3 in context te plaatsen.

Historie BI-ontwikkelingen binnen de Belastingdienst

De tekst hieronder is overgenomen uit een memo dat de historie van BI-ontwikkelingen schetst.

1e Fase: Querytalen
In de jaren 90 kwamen de eerste vraagtalen beschikbaar waarmee het mogelijk werd om gegevensverzamelingen te ontsluiten voor rapportages en rudimentaire analyses.
Door de toenmalige afdeling Gegevensmanagement zijn er procedures ontwikkeld waarmee de business (CBI) in staat werd gesteld om gegevens uit databases en bestanden te extraheren en deze ter beschikking te stellen aan afnemers binnen de organisatie.
Vanuit het perspectief dat de business de eigenaar is en over de data mag beschikken, zijn vanuit de IV-voortbrengingsorganisatie geen maatregelen getroffen om logging van de vragen te borgen. Wel boden de moderne relationele databases de mogelijkheid om vast te leggen wie op welk moment een vraag stelde aan de database, wat er gevraagd werd niet.

De organisatieontwikkeling en -besturing zijn ingesteld op de ontwikkeling van één informatiesysteem per belastingwet of aspectdeel van een wet. Zo zijn er separate systemen voor o.m. Omzetbelasting, Loonbelasting, Houderschapsbelasting en Vennootschapsbelasting. Binnen aspectgebieden zijn in een aantal gevallen meerdere informatiesystemen ontstaan die delen van de informatievoorziening verzorgen: Inning kent inmiddels de systemen ETM, COA, INL en ook Douane wordt ondersteund door een veelheid aan systemen.

Aan het einde van de vorige eeuw is in de IT-industrie het begrip datawarehouse geïntroduceerd waarmee een meer geïntegreerde informatievoorziening ten behoeve van managementbeslissingen (Business Intelligence) werd bedoeld.
De Belastingdienst is op enig moment gekanteld van een middelgerichte aanpak naar een klantgerichte aanpak, waarbij de kantoren voor IB, OB, LB en VpB[1] geconcentreerd werden naar Ondernemers en Particulieren eenheden. De behoefte naar een geïntegreerd klantbeeld is toen sterk toegenomen en daar kan een datawarehouse ook in voorzien. De Belastingdienst heeft, gedreven vanuit het IV-aanbod, een Enterprise Datawarehouse ontwikkeld waar via gereguleerde processen, data uit primaire processystemen via daarvoor ontwikkelde ETL[2]- programmatuur werd opgeslagen. De bedoeling is dat vanuit de business subsets aan data worden gedefinieerd in zogenaamde datamarts, die het mogelijk maken om de gegevens vanuit meerdere, deels vooraf bepaalde, views te bekijken en te analyseren.

Query's
De gekozen technische wijze van opslag van data in het EDW[3] maakte de ontwikkeling van datamarts complex en langdurig. En dat heeft er toe geleid dat de reeds bestaande afdeling bij B/CA-CIV[4], later BICC (BI Competence Center) queries ontwikkelde en bleef ontwikkelen om antwoord te geven op verschillende informatievragen voor verschillende doelen:

- Gegevensleveringen aan derden.
  Op basis van afspraken, convenanten en wettelijke verplichtingen dient de organisatie informatie - vaak in de vorm van bestanden- beschikbaar te stellen aan andere (voornamelijk overheids-)partijen.

[1] Inkomsten-, Omzet-, Loon- en Vennootschapsbelasting
[2] Extract Transform Load
[3] Enterprise Data Warehouse
[4] Belastingdienst/ Centrale Administratie - Centrale Informatievoorziening

Deze gegevensleveringen worden op dit moment vaak via EDW verstrekkingen gerealiseerd.

- Informatieverzoeken vanuit de politiek en management van de Belastingdienst.
  Voor het maken van wetsvoorstellen en het beantwoorden van Kamervragen worden door BICC query's ontwikkeld en uitgevoerd.

- Voeding van LOA's.
  Doordat informatiesystemen vanuit tijdgebrek veelal alleen voorzien in de primaire functionaliteit van een systeem, is door de gebruikersorganisatie een veelheid aan zogenaamde Lokaal Ontwikkelde Applicaties (LOA's) gecreëerd waarmee een oplossing wordt geboden voor functionele en technische gebreken in de formele informatiesystemen. Deze LOA's hebben informatie uit de bronsystemen nodig; deze wordt in een groot aantal gevallen via query's betrokken.

Op enig moment (medio 2012/2013) omvatte het aantal medewerkers van het BICC zo'n 60 FTE. Deze medewerkers ontwikkelden query's en voerden ze uit. Vanwege de complexiteit van het betrekken van de data uit het EDW benaderen de meeste query's de bronnen rechtstreeks.

Analytical Workspace Server (AWS)
De gekozen technische wijze van opslag van data in het EDW maakt de ontwikkeling van datamarts complex en langdurig en het snel voorzien in data voor analyses was daarmee niet goed mogelijk.
In een samenwerkingsverband tussen B/CIE en B/CAO is op enig moment het concept van Analytical Workspace Server (AWS) ontwikkeld. Een AWS was een AIX server voorzien van een flinke hoeveelheid diskruimte en het product SAS (een geavanceerde vraagtaal) als vraagtaalinstrument. Iedere doelgroep kreeg zijn eigen AWS, waarmee de toegang tot de data in de AWS beperkt was tot die gebruikersgroep.
Via het BICC kregen de analisten gegevens beschikbaar om in hun AWS te gebruiken voor analyses.

Datawarehouse Appliance
De techniek van de AWS was onvoldoende geschikt voor het gedeeld gebruik van generieke bronnen. Dit heeft geleid tot de verwerving van een Datawarehouse Applicance (DWA) die naast selectieve gedeelde toegang mogelijkheden biedt tot parallelle processing waarmee query's tot een factor honderd of meer kunnen versnellen. In het ontwerp van de DWA infrastructuur is indertijd voorzien in een zogenaamde Channel-Connect verbinding, waarmee vanaf het mainframe data rechtstreeks naar de DWA kon worden verzonden.
Door de beschikbaarheid van betere analytics mogelijkheden is binnen B/CA in die tijd ook de eerste Broedkamer ontstaan, waar met behulp van AWS en DWA analytics processen zijn ontwikkeld.

Inspectie, controle, toezicht

Organisatorisch

2012
In januari 2012 zijn de BI-experts (Business Intelligence), die in PFC-afdelingen in het land werkten, gecentraliseerd in een BI-afdeling in Utrecht.
In 2012, het 'jaar van de Invordering', vond de ontwikkeling van het eerste datafundament 'Incassoketen' onder leiding van de Persoonsgegevens (onderdeel van Semi Massale Processen) plaats. In het najaar van 2012 startte de werving voor de afdeling afdeling/het team BA (Business Analyse). Dit leidde tot: de oprichting van BA ongeveer 1 januari 2013 en werden de eerste medewerkers geworven.

2013
In de loop van 2013 werd de stafafdeling Business Intelligence & Analytics (BI&A) binnen Bedrijfsvoering Belastingen gevormd waarin de medewerkers van BA overgingen. Ook zijn medewerkers van EH&I (Expertisecentrum Handhaving & Intelligence) hierin opgegaan, maar EH&I is ook als zelfstandige afdeling blijven bestaan.
In die tijd is ook begonnen de BI-voorziening binnen Belastingen verder vorm te geven door te bouwen aan gestandaardiseerde gegevenssets waarmee resultaten in de keten, op het hoogste detailniveau en in de tijd zichtbaar werden gemaakt. Een voorbeeld en voorganger hiervan was de Incassoketen. Deze

gegevenssets gaven inzicht in de prestaties en lieten zien waar verbeteringen mogelijk waren, zowel qua efficiency als effectiviteit en zowel op het gebied van procesbeheersing als fraudebestrijding. Door gegevens op deze wijze te genereren moesten de directe effecten van handelen beter meetbaar en zichtbaar worden.

De vraag naar dit soort producten nam steeds meer toe. Om in deze toenemende behoefte te voorzien, werd besloten BI&A ook te zien als een concern brede Broedkamer[5] waarin innovatieve ideeën getoetst en uitgeprobeerd werden om te kunnen beoordelen welke zich leenden voor bredere toepassing. Deze Broedkamer was vormgegeven rond het team business-analisten van bedrijfsvoering.

2014
In februari 2014 is het Programma Broedkamer van start gegaan, om regie op innovaties te realiseren, als een onderdeel van de afdeling BI&A. De Broedkamer was een initiatief waarbij innovatie en het continu verbeteren van de Belastingdienstorganisatie centraal stonden. Dit betekende dat innovaties in de verschillende primaire processen werden geselecteerd en gerealiseerd. Voorbeelden hiervan waren "een slimmere en snellere aanpak van OB fraude of een verbetering in de IH-selectie module".

De Broedkamer bestond uit drie teams
1. Innovatie projectbureau: begeleidt het selecteren (inzicht en overzicht) en implementeren van aangedragen innovaties en werkt hierbij nauw samen met projectleiders en de operatie.
2. Het Analyseteam: is onderdeel van het innovatie projectbureau. Binnen dit team worden data analyses uitgevoerd ten behoeve van innovaties. Het team bouwt voort op de ambitie van 'op feiten gebaseerd sturen' en is opgebouwd vanuit het bestaande fundament van het Belastingen - BI&A team
3. Implementatie support/Implementatie team: levert expertise en tools aan de operatie om de implementatie van innovaties en lokale verbeteringen te realiseren

Middels een Innovatie Board en Programma Board werd per innovatie gezamenlijk met de operatie besloten welke innovaties werden uitgewerkt. Dit gebeurde onder andere op basis van data analyses en keuzes voor de wijze van implementatie. Voor de implementatie van een innovatie werd gedurende een vast te stellen periode intensief samengewerkt met de operatie.

Voor het realiseren van de Broedkamer is ook samengewerkt met externe partijen. Deze partijen hielpen bij de ontwikkeling en implementatie van innovaties.

2016
De afdeling BI&A is per februari 2016 in zijn geheel overgegaan naar de Data en Analitics (D&A)-organisatie.

'Oprichtingsdata'

Januari 2013	***Juni 2013***	***Februari 2014***	***Februari 2016***
Afdeling BA	Afdeling BI&A	Programma Broedkamer (als onderdeel van BI&A)	Afdeling D&A

[5] Een broedkamer biedt een team met een innovatief idee een geschikte plek, in termen van faciliteiten en expertise, om hun ideeën te ontwikkelen en ze te transformeren in een duurzame oplossing.
(bron: memo 060 - Broedkamers 06 11102013, 11-10-2013, Persoonsgegevens

Huisvesting

De Broedkamer en voorlopers zijn op verschillende lokaties in de periode 2012 – februari 2016 gehuisvest.

Persoonsgegevens

'Lokaties'

Datum	Afdeling	Lokatie	Verdieping	Project / Broedkamer
nov. 2012	BA	HG5	4A	
half 2013	BA	GvR500	bovenste	
dec. 2013	BI&A	HG5	4e	
2014	EH&I	HG55	6e	OB-carrousel
	EH&I	HG55	1e	OB-carrousel
1-1-2014	BI&A	HG5	3	
23-2-2016	D&A	HG5	3	

3. Beveiliging Broedkamer en voorlopers

3.1. Inleiding

Dit hoofdstuk beschrijft de aanpak en bevindingen van het deelonderzoek naar beveiliging binnen de Broedkamer en voorlopers, in de periode 2012 tot februari 2016. Dit gerelateerd aan de onderzoeksvraag welke informatiebeveiligingsmaatregelen van kracht waren en hoe deze hebben gewerkt.

3.2. Aanpak onderzoek beveiligingsmaatregelen

Beveiliging is als onderdeel van integraal management en bedrijfsvoering een verantwoordelijkheid van het lijnmanagement op de diverse niveaus van de organisatie. Het beveiligingsbeleid en de beveiligingsnormen van de Belastingdienst zijn vastgelegd in het Handboek Beveiliging Belastingdienst (HBB). Het HBB betreft het basis-beveiligingsniveau; noodzakelijk geachte aanvullende maatregelen dienen te worden bepaald op basis van een risico- en/of kwetsbaarhedenanalyse.

Een vergelijking is uitgevoerd op de verschillende HBB-versies binnen de onderzoeksperiode 2012 - februari 2016. Dit om vast te stellen in hoeverre er wezenlijke wijzigingen, relevant voor het vaststellen van het referentiekader van dit onderzoek, zijn geweest in de loop der jaren. Het gaat hier concreet om de HBB-versies: mei 211, december 2012, december 2013 en december 2014.
We hebben hierbij, binnen de context van dit onderzoek, geen relevante verschillen aangetroffen. Zo zijn bijvoorbeeld al richtlijnen t.a.v. logging en monitoring opgenomen in HBB-versie mei 2011 (o.a. 16.5.2 'Controle op gegevensuitwisseling' en 16.8.3 'Beschikbaarheid logbestanden'.)[6]

Onderzocht is een subset aan maatregelen uit het Handboek Beveiliging Belastingdienst (HBB), versie 2011 (geldend in 2012), te weten een aantal maatregelen die gerelateerd zijn aan gegevensgebruik t.b.v. data-analyse. De subset uit het HBB is opgenomen bijlage 3.

3.3. Bevindingen

3.3.1. Algemeen

Beveiligingsbeleid Belastingdienst
Net als voor alle andere bedrijfsonderdelen binnen de Belastingdienst, geldt het HBB als beveiligingsbeleid voor de Broedkamer en voorlopers.

Dataprotectie
In 2015 is het document '20150506 Nota Data Governance binnen BI&A' door het toenmalig managementteam van BI&A vastgesteld als beleid voor aanvullende beschermingsmaatregelen. Het is door de afdeling D&A (vanaf februari 2016) gehanteerd als de uitwerking van de dataprotectie.

Risicoanalyse Broedkamer en voorlopers
Op 7 december 2015 is een bedreigingen- en kwetsbaarhedenanalyse uitgevoerd door BI&A. De uitkomsten van deze analyse zijn door de afdeling D&A[7] in 2016 opgepakt en vallen daarmee buiten scope van het onderzoek naar de Broedkamer en voorlopers.

In de onderzoeksperiode zijn bij de Broedkamer en voorlopers verder geen vastleggingen van risicoanalyses aangetroffen. In gesprekken is aangegeven dat 'de risicoanalyse met betrekking tot

Inspectie, controle, toezicht

[7] Oprichtingsdatum: 01-02-2016

de levering van productiedata in hoofden zat en niet op papier'.

3.3.2. Bevindingen beveiligingsmaatregelen

Deze paragraaf gaat nader in op een aantal maatregelen, zoals opgenomen in het HBB. Uit het HBB is een subset gemaakt van maatregelen die gerelateerd zijn aan gegevensgebruik t.b.v. data-analytics. (zie bijlage 3).

Inspectie, controle, toezicht

3.3.2.1. Betrokkenheid management bij beveiliging

Door het voormalig management wordt aangegeven dat vanaf het begin van BI&A (juni 2013) het besef er was dat er extra maatregelen genomen moesten worden, gezien het specifieke karakter van de afdeling en de omgang met grote hoeveelheden (privacygevoelige) data. Vanuit BI&A is aan CIO-office hierbij om hulp gevraagd en door een juridisch adviseur (op het gebied van privacy) is onderzoek verricht. (Dit was i.h.k.v. een afstudeeronderzoek van de betrokken adviseur.)
Op basis van het onderzoeksrapport[8] is een 'privacy en security project' gestart met daarbij vooral de focus gericht op privacy. O.a. wordt gestart met het uitvoeren van PIA's (eind 2014 voor het eerst uitgevoerd). Het onverantwoord omgaan met gegevens werd als hoogste risico gezien. Dat was voornamelijk gebaseerd op basis van de Wet bescherming persoonsgegevens (Wbp) en de geheim-houdingsplicht van de Awr. Datalekken van eigen medewerkers werd als een verwaarloosbaar risico gezien vanwege het verplichte afgeven van een VOG, eed/gelofte en GHV, USB-ontheffingen die werden ingetrokken, een aangeboden awareness programma, etc. De afdeling Kwaliteitszorg was bij het inrichten van beveiliging betrokken. Medewerkers 'beschermen' tegen informatie die ze niet mochten zien was het doel. Datalekken werd hierbij niet als groot risico gezien

Er komt later in de onderzoeksperiode meer aandacht voor privacy en security. Voorbeelden hiervan zijn het bewustwordingsprogramma (2015) en de aandacht voor dataprotectie (nota Data Governance binnen BI&A uit 2015).

In de onderzoeksperiode is een aantal rapporten/ adviezen uitgebracht op het gebied van (informatie) beveiliging/ privacy (rapport Persoonsgegevens rapport Liquid Hub[10], onderzoek naar datastromen en datamanagement door Persoonsgegevens (zie ook H.4 'Signalen en opvolging'). In interviews is aangegeven dat hiermee niets zichtbaars is gedaan.

3.3.2.2. Toegangsbeleid

De huisvesting van de medewerkers van de Broedkamer en voorlopers heeft altijd plaatsgevonden in Rijksgebouwen (Herman Gorterstraat 5 en 55, Graadt van Roggenweg 500). Fysieke toegang is gekoppeld aan een toegangspas (Rijkspas of bezoekerspas). De hoofdingang van deze gebouwen hebben tourniquets met een kaartlezer.
Aangegeven wordt dat er geen sprake is geweest van verbijzonderde toegangsbeveiliging; de etages/ kamers waren niet afzonderlijk beveiligd m.b.v. een toegangspas met specifieke autorisaties. Eenmaal toegang tot het gebouw, betekende toegang tot de afdeling.
Op de Graadt van Roggeweg waren de data-analisten de enige gebruikers van de bovenste etage; 'vreemden' werden hier snel gesignaleerd, omdat dit grotendeels een open ruimte was.

Lokaties van de onderzochte 'stand-alone omgevingen':
- PoC Accenture: server in Rekencentrum; medewerkers in Utrecht (onbekend)

[8] Juridishe aspecten van datamining en profiling door de Belastingdienst, 10 oktober 2014
[9] 'Review of Investeringsagenda De Belastingdienst', 20 mei 2015
[10] 'Belastingdienst BIA Observaties & Aanbevelingen', 26 maart 2015
[11] 'Investigating Data Streams', december 2015

- OB-Carrousel Fraude: server(s) in Utrecht (HG5) en werkplekken in Utrecht (HG55)
- OB-Negatief: server bij IBM en medewerkers onbekend

3.3.2.3. Beleid voor informatie-uitwisseling

Aangegeven wordt dat 'vanaf dag 1 het beleid is geweest dat data altijd op één plek blijft'. De 'leidende principes' zijn geformuleerd en gecommuniceerd in de vorm van de 10 geboden (eerste versie van juli 2014). Hierin is ten aanzien van informatie-uitwisseling o.a. aangegeven:
- 'Laat de data centraal staan op Teradata en/of de AWS. Distribueer data zo weinig mogelijk.'
- 'Maak gebruik van de uitwisselingsmap [...] voor het uitwisselen van data. Verwijder de gegevens direct uit de uitwisselingsmappen. Gebruik geen clouddiensten.'
- 'Stel persoons- en bedrijfsgegevens wanneer je deze buiten D&A gebruikt alleen beschikbaar aan de daarvoor geautoriseerde medewerker. In alle overige rapportages, analyses en presentaties die buiten D&A worden gebruikt zijn de persoons- en bedrijfsgegevens geanonimiseerd.'

Zie ook bijlage 6: 'De 10 geboden van informatiebeveiliging.'

3.3.2.4. Beleid voor draagbare computers en communicatievoorzieningen

Zie ook 'Beleid voor telewerken/ thuiswerken' (Zie: 3.3.2.5).

Onderzoek laptopgebruik inhuurmedewerkers (Accenture).
Dit onderwerp is gedurende het onderzoek opgekomen op basis van signalen dat er eigen werkplekken door medewerkers van Accenture werden gebruikt. De bevindingen zijn:
- In 2013 en 2014 werd in projecten informatie nodig voor het betreffende project gedeeld via USB en mail. Dit betrof alle soorten informatie binnen de projectgroep. Dit was met toestemming van het management, hierbij werd aangegeven dat externen als internen ingezet moesten worden. Gebrek aan DWB werkplekken maakte dat dit de enige manier was om informatie met leden van de projectgroep te delen.
- Aangegeven wordt dat er eind 2014 een richtlijn is gegeven dat er geen vertrouwelijke informatie naar externe accounts gestuurd mag worden, hierop worden echter meerdere uitzonderingen toegestaan.
- De afspraken over het vernietigen van gegevens waren per project verschillend maar bij alle projecten zijn hier contractueel afspraken over gemaakt.
- Gebruik eigen werkplekken was tegen de afspraken die met Accenture zijn gemaakt (raamovereenkomst).
- Na december 2016 was het gebruik van eigen werkplekken door externe medewerkers niet meer toegestaan (december 2016 ligt buiten scope audit).
- Gebruik van eigen werkplekken op het netwerk van de Belastingdienst is niet (meer) via logging vast te stellen.
- Technisch was het niet uitgesloten dat medewerkers van Accenture met behulp van hun 'eigen' werkplekken en permissies data hebben gekopieerd naar een Belastingdienst vreemde omgeving (lees hun eigen werkplekken). Er zijn geen vastleggingen meer beschikbaar die hierover zekerheid geven.
- De SAS logging op de AWS laten geen vreemde machinenamen zien.

Inspectie, controle, toezicht

3.3.2.5. Beleid voor telewerken/ thuiswerken

Opzet is dat inhuurmedewerkers altijd werken op een werkplek van de Belastingdienst.
Vanaf het moment dat met de DWB wordt gewerkt (2014) geldt het uitgangspunt dat inhuur-medewerkers die met data werken de DWB niet mogen meenemen. Voor medewerkers die (vanuit Utrecht) in Apeldoorn moeten werken, wordt daarvoor een ontheffing verleend. Deze regelgeving was al langer van kracht, maar is op 02-12-2016 vastgelegd in een memo (20161202 Gebruik

Externe Laptops v1.0).

Thuiswerken is toegestaan, maar alleen voor belastingdienstmedewerkers. Inhuurmedewerkers werken op kantoor en met een DWB-werkplek Thuiswerken is voor inhuurmedewerkers niet toegestaan; deze regel geldt vanaf januari 2013.
Uit Interview: Inhuurmedewerkers hadden in voorkomende gevallen hun eigen laptop bij zich. In de beginperiode was het moeilijk om hen duidelijk te maken dat ze echt alleen op de DWB-werkplek mochten werken. 'Dat heeft wat tijd gekost'.

3.3.2.6. 'Clear desk'- en 'clear screen'-beleid

Is onderdeel van beleid Belastingdienst en awarenesstrainingen en de '10 geboden van informatiebeveiliging':
- 'Vergrendel je scherm wanneer je de werkplek verlaat.'
- 'Laat vertrouwelijke documenten niet slingeren. Gooi ze in de afgesloten papierbak wanneer ze niet meer nodig zijn. Houd je aan de Cleandesk policy.'

We hebben geen vastleggingen van uitgevoerde controles (door de CFD) in de onderzoeksperiode.

3.3.2.7. Beleid voor geheimhouding

Inhuurmedewerkers tekenen een geheimhoudingsverklaring (GHV) en krijgen alleen toegang tot data na het tekenen hiervan en het volgen van een awareness-sessie.
Met Accenture is een 'wederkerige geheimhoudingsverklaring' opgesteld (2012); niet alle Accenture-medewerkers hebben hierdoor een GHV bij de Belastingdienst getekend. (De wederkerige geheimhoudingsverklaring gold alleen voor inhuur onder prestatiecontract. Individuele inhuurmedewerkers, dus ook van Accenture, die worden ingehuurd onder een broker-overeenkomst dienen wel een GHV in te leveren.)

3.3.2.8. Beleid voor algemeen beveiligingsgedrag personeel

Zie 'Bewustzijn, opleiding en training t.a.v. beveiliging' (3.3.2.11).

3.3.2.9. Beleid voor aanvaardbaar gebruik van bedrijfsmiddelen

Zie 'Bewustzijn, opleiding en training t.a.v. beveiliging' (3.3.2.11).

3.3.2.10. Screenen

I.h.k.v. dit onderzoek is 'screening' geïnterpreteerd als het waarborgen dat er 'betrouwbare' medewerkers in dienst worden genomen.

De HR-afdeling heeft een lijst samengesteld van medewerkers die bij de afdeling BI&A en/of D&A hebben gewerkt. Op dit overzicht is de aanwezigheid aangegeven van een geheimhoudingsverklaring (GHV), VOG en kopie-ID in het personeelsdossier.

Inhuurmedewerkers
Uit de beoordeling van de aangeleverde lijst van 169 personen blijkt dat er niet voor iedereen een VOG (Verklaring Omtrent Gedrag) of kopie-Identiteitsbewijs (ID) aanwezig is. Soms is de oorzaak bekend omdat de documenten bij een ander onderdeel van de Belastingdienst liggen of al vernietigd zijn. De geheimhoudingsverklaring is eveneens niet altijd aanwezig. In een aantal gevallen is de oorzaak dat er een zogenaamde wederkerige geheimhoudingsverklaring met de partij waarvan medewerkers worden ingehuurd wordt, is afgesloten.

Inspectie, controle, toezicht

Vast personeel
Uit de beoordeling van de lijst met 157 personen blijkt dat niet voor iedereen de VOG, kopie-ID en geheimhoudingsverklaring/Eed/Belofte aanwezig is. In enkele gevallen is de oorzaak dat de personeelsdossiers niet meer te benaderen zijn of de persoon uit dienst is.

Inspectie, controle, toezicht

3.3.2.11. Bewustzijn, opleiding en training t.a.v. beveiliging

Met het vaststellen van de nota 'Data Governance binnen BI&A' van 6 mei 2015 werd het bewustwordingsprogramma verplicht gesteld voor alle medewerkers van BI&A en dit is doorgezet in D&A. De kick-off van het bewustwordingsprogramma werd gestart op 15 juni 2015 op de diverse teamoverleggen. De eerste plenaire sessie was op 26 augustus 2015.
Het bewustwordingsprogramma bestaat o.a. uit een plenaire klassikale training en de online cursus iBewustzijn Overheid.
(bron: e-mail P-gv. *08-05-2017)*

Awareness
In 2015 hebben er meerdere plenaire cursussen plaatsgevonden:
26 augustus: 54 deelnemers
15 september: 9 deelnemers
29 september: 11 deelnemers
23 november: 6 deelnemers
16 december: 5 deelnemers

In 2016 hebben er meerdere plenaire cursussen plaatsgevonden:
14 januari: 2 deelnemers
25 januari: 24 deelnemers
29 juni: 2 deelnemers*
21 december: 10 deelnemers*
** buiten scope van de onderzoeksperiode, maar opgenomen voor de volledigheid 2016*

iBewustzijn
Uit de beoordeling van de aangeleverde gegevens blijkt dat niet iedereen de benodigde certificaten van de iBewustzijn cursus heeft behaald.

Door een aantal mensen is de cursus nog niet gevolgd of niet voltooid. Verder is in het verleden regelmatig vrijstelling voor de iBewustzcijn cursus gegeven aan externen, die relatief te kort of weinig aanwezig waren en geen toegang hadden tot de data.

Inspectie, controle, toezicht

3.3.2.12. Naleving gedragsregels voor beveiliging

Zie 'Afhandelen en evalueren beveiligingsmeldingen' (3.3.2.15).

3.3.2.13. Kritische en risicovolle functies

Er zijn binnen BI&A (en later D&A) geen kritische en risicovolle functies onderkend. Er is wel gesproken om de medewerkers die op fraude-projecten werken, aan te merken als risicovol en extra te laten screenen. Maar om dat te kunnen doen moeten zij als vertrouwensfuncties geregistreerd worden (wat goedgekeurd moet worden door de minister) en dat was voor Belastingen-Bedrijfsvoering een brug te ver.

'Wel zijn medewerkers die op een Grote Ondernemingen-project werkzaam waren, aangemerkt voor de insiderregeling. Maar voordat de landelijk vertrouwenspersoon integriteit en ongewenste omgangsvormen en compliance officer dit kon effectueren, was het project afgelopen.'

Inspectie, controle, toezicht

3.3.2.14. Beëindiging dienstverband en functiewisseling

Bij beëindigen dienstverband wordt in IMS binnen 7 werkdagen de autorisatie automatisch (koppeling met SAP-HR) stopgezet. Dit geldt zowel voor inhuur als vaste medewerkers. Dit geldt voor alle medewerkers waarvan in SAP-HR de aanstelling afloopt.
IMS blokkeert in dit geval automatisch de toegang tot de DWB-werkplek, dus feitelijk is de 'voordeur' dicht. Ook SAP- en mainframe-autorisaties worden automatisch verwijderd. Voor sommige doelsystemen vindt er nog een automatische workflow plaats om de verwijderactie te doen. Als deze handmatige workflow niet of niet tijdig wordt uitgevoerd, dan is het technisch mogelijk dat een account blijft bestaan.
De AWS autorisaties worden via een handmatig proces gezet. De opdracht wordt door een lokale toepassingsbeheerder via AAA ingediend. De trigger voor een toepassingsbeheerder om een AAA (aanvragen, afhandelen van autorisaties) opdracht in te dienen is een notificatie uit IMS nadat er een roltoewijzing heeft plaatsgevonden.
Bij functiewisseling vindt geen automatische schoning van autorisaties plaats. Dit is een verantwoordelijkheid van de 'latende' manager en indien deze dat heeft nagelaten, dan kan de nieuwe manager ook de autorisaties uit de vorige functie verwijderen.

3.3.2.15. Afhandelen en evalueren beveiligingsmeldingen

Er wordt door BI&A een incidentlogboek bijgehouden vanaf december 2014. Er werd toen het eerste serieuze incident gesignaleerd en vanaf dat moment is het log bijgehouden.
Het log doet verslag van de afhandeling van de meldingen en de getroffen oplossing/ maatregelen.

Zie voor inhoudelijke meldingen 4.4. 'Signalen over gegevens buiten de Belastingdienst en oneigenlijk gegevensgebruik'.

3.3.2.16. Autorisaties

Algemeen

Broedkamer: autorisaties worden op basis van rollen toebedeeld. In het verleden waren er meer mogelijkheden voor iedereen vanwege algemene autorisaties. Pas later zijn er op de SAS-servers zones ingesteld. Op basis van bepaalde rollen, die gekoppeld zijn aan een medewerker, is alleen die data toegankelijk voor een medewerker waarvoor hij geautoriseerd is.
(bron: interview Persoonsgegevens

Bij de Broedkamer waren 10 personen die profielen in IMS konden aanmaken en toekennen. Rolscheiding heeft hier ontbroken.
(bron: interview Persoonsgegevens

In de begintijd werden autorisaties door middel van het AAA-tool verwerkt. Later kwam er een autorisatiematrix voor AWS'en. Per AWS is een differentiatie gemaakt wie in welke AWS mag. Zo

is er bijvoorbeeld een dedicated AWS voor de IH-productieverwerkingen.
(bron: interview Persoonsgegevens

Vanaf 2014 wordt er gewerkt met standaard autorisatie-profielen. Daarvoor bestonden er ook profielen, maar sinds 2014 is er een autorisatie-template om aanvragen te kunnen doen. Dit template wordt doorgezet naar IMB of IV-accent.
(bron: interview Persoonsgegevens

De AWS autorisaties worden via een handmatig proces gezet door het 'BLA team' van B/CAP. De opdracht wordt door een lokale toepassingsbeheerder via AAA ingediend. De trigger voor een toepassingsbeheerder om een AAA opdracht in te dienen, is een notificatie uit IMS nadat er een roltoewijzing heeft plaatsgevonden.

Toegang tot de data binnen de AWS'en kon niet worden gedifferentieerd. Na de invoering van de Teradata-machine zijn er meer mogelijkheden gekomen tot het compartimenteren van data. (zie ook H.2 Object van onderzoek en H.5.3.1. Risicoanalyse analytische werkomgevingen).

USB-ontheffingen

Naar USB-gebruik is onderzoek gedaan. Het is namelijk een mogelijkheid om gegevens met een USB (stick of (externe) schijf) buiten de Belastingdienstomgeving te brengen vanaf de Belastingdienst werkplek als de betrokkene toegang heeft tot bestanden of bestandsuitwisseling. Zoals bijvoorbeeld de AWS mogelijkheid om gegevens naar de werkplek te downloaden (zie ook H6.2). De bevindingen zijn:

- In de periode 2012 tot de schoningsactie die eind 2015 is uitgevoerd, waren USB ontheffingen voor interne BI&A medewerkers ruimschoots aanwezig. Het grootste gedeelte van USB-ontheffingen kwam met de persoon mee uit een vorige functie.
- Er wordt op de werkplek (C:schijf) gelogd welke user een USB heeft gebruikt. Wat het gebruik heeft ingehouden, wordt niet vastgelegd. Zoals bijvoorbeeld: welke bestanden worden er uitgewisseld.
- Er zijn in de onderzoeksperiode werkplekken in gebruik geweest waarbij versleutelen naar USB devices niet werd afgedwongen. Dit betreft de XP werkplekken, de voorganger van de huidige Belastingdienst werkplek (DWB). Overigens is ontsleutelen van de gegevens door de gebruiker van de huidige Belastingdienst werkplek (DWB) mogelijk.

Er is door D&A lijstwerk opgeleverd waaruit is af te leiden wie er wel/niet USB ontheffing hadden *(bronnen zijn IMS en AAA)*.

Jaar	type	Org	groep	versie	Ja	Nee	Onbekend	Aantal
2012*	-	-	-	-	-	-	-	-
2013	overzicht	D&A	medew	v2	35	19	7	61
2014	overzicht	D&A	intern	v2	35	27	1	63
2014	overzicht	D&A	inhuur		0	29	0	29

* De afdelingen BI&A en D&A bestonden toen nog niet.

Eind 2015 is er een schoningsactie op USB-ontheffingen in gang gezet. Bij aanvang is op 19 november 2015 geconstateerd dat 47 personen binnen BI&A USB-rechten hebben.

BI-medewerkers hadden uit hoofde van hun regionale PFC functie USB-ontheffing en hebben deze ontheffing meegenomen naar BI&A en later D&A. BI-medewerkers hebben vanaf eind 2014 rechten gekregen om via de AWS te kunnen gaan werken. Die rechten gaf deze medewerkers extra toegang tot gegevens op Belastingplichtige niveau dan die waarover ze vanuit hun oude rol al beschikten.
(bron: e-mail Persoonsgegevens

Eind 2015 hadden 18 medewerkers (BA & Data & Infra) van de 47 personen toegang tot de AWS én een USB-ontheffing. Na het intrekken van de rechten eind 2015 hebben 4 medewerkers van het toenmalige team Data & Infra, uit hoofde van hun rol (reserve) Data Guardian een USB-ontheffing én toegang tot de AWS.

3.3.2.17. Controleren van systeemgebruik

De SAS Enterprise Guide[12] activiteiten worden gelogd, maar daar vindt geen controle (lees: monitoring) op plaats.
(bron: interview Persoonsgegevens

Zie ook: Risico-analyse (5.2.4) Logging en monitoring.

3.3.2.18. Leveren van gegevens buiten overeengekomen productiedoeleinden

Tot aan 2015 (SNA-oplossing) is het zeer aannemelijk dat gegevens van belastingplichtigen zijn gekopieerd naar omgevingen die niet door de IV-organisatie in beheer waren en dat externen de mogelijkheid hebben gehad vertrouwelijke gegevens te raadplegen en te kopiëren naar eigen media (die niet onder beheer van de Belastingdienst waren).
(bron: interview Persoonsgegevens

In de periode, waarin met stand-alone oplossingen is gewerkt, kon data alleen geladen worden middels portable devices (zoals externe schijven en USB-sticks)..
(bron: interview Persoonsgegevens

3.3.2.19. Toegangsdiensten

Zie: Toegangsbeleid (3.3.2.2).

3.3.2.20. Overeenkomsten inhuur derden

Contractueel is vastgelegd dat medewerkers van Accenture geen geheimhoudingsverklaringen (GHV's) hoefden aan te leveren. Er is hiertoe een wederkerige geheimhoudingsverklaring (2012) vastgesteld tussen de Belastingdienst Persoonsgegevens en Accenture.
De wederkerige geheimhoudingsverklaring gold alleen voor inhuur onder prestatiecontract. Individuele inhuurmedewerkers, dus ook van Accenture, die worden ingehuurd onder een broker-overeenkomst dienen wel een GHV in te leveren.

In een begeleidende brief bij de wederkerige geheimhoudingsovereenkomst staat e.e.a. opgenomen hoe Accenture de vertrouwelijkheid van gegevens waarborgt.

3.3.2.21. (Controle-technische) functiescheidingen en zonering technische infrastructuur

Zie: Risico-analyse (5)

3.3.2.22. Inrichting verbijzonderde ruimten

Zie: Toegangsbeleid (3.3.2.2)

[12] Grafical User Interface voor SAS-toepassingen

4. Signalen en opvolging

4.1. Inleiding

Dit hoofdstuk geeft de bevindingen van het deelonderzoek naar de onderzoeksvraag wat is gedaan met signalen (aan de Broedkamer en voorlopers), in relatie tot geconstateerde risico's en/of feiten omtrent daadwerkelijk oneigenlijk gegevensgebruik of het buiten de Belastingdienst brengen van gegevens.

Van deze signalen is onderzocht in hoeverre opvolging heeft plaatsgevonden d.m.v. (formele) besluitvorming. Hiertoe is geïnventariseerd of de signalen zijn opgenomen op de agenda en/of in de notulen van de relevante besluitvormende organen.

Daarnaast is onderzoek gedaan naar de afhandeling van gemelde incidenten en of deze incidenten hebben geleid tot oneigenlijk gebruik van gegevens / het naar buiten brengen van gegevens buiten de Belastingdienst.

4.2. Signalen algemeen

Onderstaande tabel geeft een overzicht van signalen en hun opvolging:

Signaal		Zichtbare opvolging	Onderzochte besluitvormende organen
Onderzoeks- en adviesrapporten*	Persoonsgegevens Mei 2015, september 2015) - LiquidHub 2015 - Inrichting Infra en beveiliging t.b.v. de pilot OB Fraude, maart 2014 *(niet aangetroffen)*	Nee	- MT BD - RvB - PIPP - Miniconferentie COO
Incidenten/ integriteits-schendingen	- Zelfanalyses HBB - Rapportages Informatiebeveiliging	Nee	- MT BD - RvB - PIPP - Miniconferentie COO
	- Incidenten logboek BI&A	Ja	- Intern BI&A
Overige signalen	- Aanschaf (buiten CIE om) van zware stand alone machine t.b.v. BI in juni 2012. Deze machine bevatte vertrouwelijke gegevens. *(mailbericht dir. B/CIE d.d.26-08-2012)* - Onveilige ontwikkelservice op de inmpsu01 (SAS 9.3) in september 2013. Gesignaleerd in memo B/CIE waarnaar in een verslag is verwezen. *(memo niet aangetroffen)* Ook gesignaleerd in mailbericht van 19-12-2013 - Productie werkzaamheden op niet productierijpe AWS omgeving voor de periode april 2013 tot medio 2015. *(mailbericht)* - Memo Aanvullende bevindingen data warehousing *(1 oktober 2014)*	Nee	- MT BD - RvB - PIPP - Miniconferentie COO - CFO overleggen 2012- 2016

* Toelichting rapporten: zie bijlage 4

Zoals uit bovenstaand overzicht blijkt hebben wij geen (formele) besluitvorming aangetroffen inzake beveiliging en gegevensgebruik. Gemelde incidenten zijn wél opgevolgd. (Zie hoofdstuk 4.4).

4.3. Besluitvorming en vastlegging

Gedurende het onderzoek is gebleken dat naast bovengenoemde besluitvormende organen besturing van de Broedkamer tevens heeft plaatsgevonden vanuit een aantal andere organen:

'De besturing van de Broedkamer is belegd bij een Programboard, gestart rond maart 2014. De Programboard nam alle besluiten over faseovergangen, projecten etc. Vanaf het moment dat de investeringsagenda ging lopen is de programboard besturing omgezet in een besturing door het PIPP.' *(Bron: gespreksverslag interview* Persoonsgegevens

Onderzocht is in hoeverre van de bijeenkomsten van deze organen verslaglegging heeft plaatsgevonden.

Overlegorgaan	Vastlegging geconsta-teerd	Toelichting;
Programboard Broedkamer IH en OB	Nee	**Vergaderdata:** (Bron mail Persoonsgegevens 9 mei 2017) - 10 juli 2014, PB Broedkamer OB (niet doorgegaan) - 16 oktober 2014, PB Broedkamer IH (wel doorgegaan) - 13 november 2014, PB Broedkamer OB (wel doorgegaan) - 14 januari 2015, PB Broedkamer IH (wel doorgegaan) - 3 juni 2015, PB Broedkamer IH (wel doorgegaan) Periodiek werden (door Accenture) documenten (o.a. slidedecks) opgeleverd aan Programboards (en later PIPP). Deze documenten werden nooit verstrekt aan de leden, niet vooraf, niet achteraf. Slidedecks werden gepresenteerd tijdens het overleg. Door Accenture werd een soort van verslag / samenvatting opgesteld. Voor zover bekend zijn deze verslagen / samenvattingen nooit vastgesteld. *(Bron: mail Persoonsgegevens 12 juni 2017).*
Innovation Board	Nee	-

Zoals uit bovenstaand overzicht blijkt heeft verslaglegging van Program Boards en Innovation Board niet of slechts beperkt plaatsgevonden. (Formele) opvolging van signalen ten aanzien van beveiliging en gegevensgebruik vanuit deze organen hebben wij hierdoor niet vast kunnen stellen.

Inspectie, controle, toezicht

Samengevat:
Er is een aantal signalen geweest, gerelateerd aan beveiliging en het (oneigenlijk) gebruik van data; daarvan is echter in geen van de gevallen (formele) opvolging geconstateerd in één van de besluitvormende organen.

Opvolging van gesignaleerde incidenten heeft wél plaatsgevonden (zie hoofdstuk 4.4).

4.4. Signalen uit incidenten logboek BI&A

Het incidenten logboek van BI&A (zie ook 3.3.2.15. 'Afhandelen en evalueren beveiligings-meldingen') bevat vijf meldingen over de periode december 2014 - februari 2016:
- 11-12-2014: Data lekmelding
- 10-09-2015: Ongewenste toegang tot onderliggende data SAS VA
- 03-11-2015: FI-nummers van Externen
- 17-11-2015: Bestanden kunnen naar de cloud
- 25-11-2015: (Pseudo) VIP's zijn zichtbaar in DM/DI (Dynamisch Monitoren en Debiteuren Inzicht)

- Data lekmelding:
  Er vindt een grote kopieslag van data uit een Datalab van Teradata plaats onder het userid van een medewerker.
  Oorzaak is dat er automatisch (en ten onrechte) alle data uit een Teradata Datalab wordt gekopieerd.
  Als maatregel wordt de kopieslag centraal gestopt. Schade wordt als 'nihil' ingeschat.

- Ongewenste toegang tot onderliggende data SAS VA
  Via SAS-tooling is het mogelijk om connectie te maken met de SAS VA server. Vervolgens kan alle onderliggende data geraadpleegd worden.

- FI-nummers van Externen
  Voor een uitsluitingslijst zijn de FI-nummers (fiscale nummers) van externen nodig. De FI-nummers van externen staan niet in SAP-HR. Mogen de FI-nummers uit andere bestanden gehaald worden? Dit is niet toegestaan. De FI-nummers in primaire systemen zijn verzameld met als doel de fiscale taak van de Belastingdienst en niet het gebruik voor het interne proces. Advies wordt gegeven om de lijst van VOG's (Verkaring Omtrent Gedrag) te bekijken. Die zijn wel verzameld voor gebruik in het interne proces.

- Bestanden kunnen naar de cloud
  Test-bestand met gefingeerde cijfers via iPad in cloud geplaatst. Casus is ingebracht bij het Tactisch Beveiligingsoverleg (TBO).

- (Pseudo) VIP's zijn zichtbaar in DM/DI
  Geen omschrijving bij vermeld.
  Als oplossing is aangegeven dat de vips niet meer zichtbaar zijn in de dataset.

Samengevat:
Het incidenten logboek bevat geen gevallen waarin daadwerkelijk is vastgesteld dat gegevens buiten de Belastingdienst zijn gebracht en/of oneigenlijk zijn gebruikt.
Incidenten zijn allen afgehandeld door de afdeling BI&A.

5. Risicoanalyse Onderzoeksteam

5.1. Inleiding

Om nader onderzoek te kunnen doen naar het buiten de Belastingdienst brengen van gegevens [13] en oneigenlijk gegevensgebruik, is door het onderzoeksteam een risico-analyse uitgevoerd naar de (on)mogelijkheden hiertoe.
Dit hoofdstuk geeft de uitkomst van deze analyse in een algemeen deel (geldend voor de gehele Belastingdienst) en een specifiek deel (geldend voor de Broedkamer en voorlopers).
In de paragrafen wordt eerst de in de analyse onderkende situatie beschreven, in een kader wordt dan de bevinding gegeven. Deze bevindingen zijn vooruitlopend op het loggingsonderzoek gedaan, deze zijn niet door de latere uitkomsten van het loggingsonderzoek weerlegd.

5.2. Risicoanalyse algemeen Belastingdienst

Deze paragraaf beschrijft de risico's die samenhangen met de omgeving van programma Broedkamer en voorlopers.

5.2.1. Beperkingen van het onderzoek

In een onderzoek naar pogingen om gegevens ten onrechte buiten de Belastingdienstomgeving te brengen kan onderscheid gemaakt worden in geslaagde en niet geslaagde pogingen. In dit onderzoek is gericht gezocht naar geslaagde en niet geslaagde pogingen.

Het is belangrijk te vermelden dat het mogelijk is om gegevens ten onrechte bij de Belastingdienstomgeving te brengen zonder traceerbaarheid in logging. Denk hierbij aan foto's en filmopnames van bijvoorbeeld beeldschermen.

Het is onmogelijk om met zekerheid aan te tonen dat er geen pogingen, al dan niet succesvol, gericht op het naar buiten brengen van gevoelige gegevens van de Belastingdienst hebben plaatsgevonden in de onderzoeksperiode.
Dit is een onderzoeksrisico bij dit onderzoek.

5.2.2. Beveiligingsbeleid

De Belastingdienst gaat uit van vertrouwen in haar medewerkers waar dat kan en past vele maatregelen toe die het bedrijfsbelang en het belang van de medewerker beschermen (organisatorisch, contractueel, functiescheiding, zonering (fysiek), scheiden van omgevingen (logisch), autorisaties, logging etc.). Het Handboek Beveiliging Belastingdienst (HBB) [14] beschrijft dat er een onweerlegbare vastlegging van gebeurtenissen noodzakelijk is om achteraf controle te kunnen uitoefenen en/of foutsituaties te kunnen uitzoeken. Ook beschrijft het HBB dat het vastleggen tevens noodzakelijk is als bewijsmiddel voor private of strafrechtelijke vordering. Voor welke concrete situaties dit toepasselijk zou moeten zijn is echter niet beschreven. In het HBB wordt voor de analyse en specificatie van eisen te stellen aan informatiesystemen wel als voorbeeld het lekken van data genoemd.
De Belastingdienst vertrouwt in het beveiligingsbeleid op de eed/gelofte en de VOG.

Het beveiligingsbeleid van de Belastingdienst geeft een concrete richtlijn voor monitoring.

[13] Gegevens van belastingplichtigen, belastingschuldigen en toeslaggerechtigden.
[14] We hebben een 'verschillen-analyse' uitgevoerd op de HBB-versies vanaf 2011 tot 2016; hieruit komen geen essentiële verschillen, gerelateerd aan het object van onderzoek, naar voren.

Inspectie, controle, toezicht

5.2.3. Scenario's onterecht buiten de Belastingdienst brengen van gegevens[15]

Onderdeel van het werk van de Belastingdienst is het (doelgebonden) delen van informatie met vertrouwde partijen (o.a. intermediairs). Het buiten de Belastingdienst brengen van gegevens met andere partijen of andere doeleinden, wordt gezien als het lekken van data.

Voor dit onderzoek is in de expertsessie geïnventariseerd welke scenario's voor het lekken van data er zijn. Dat blijken er veel te zijn als er rekening wordt gehouden met het kennisniveau van hoog geclassificeerde IT-professionals en de eigenschappen van de gebruikte IT-voorzieningen. Zo zijn er scenario's mogelijk waarbij met behulp van de standaard werkplek van de Belastingdienst (DWB, en eerder de XP-werkplek) en toegang tot het internet er gegevens buiten de Belastingdienst kunnen worden gebracht. Initieel is toegang tot risicovolle internetdiensten, zoals webmail en filesharingdiensten, waarmee massaal gegevens op het internet kunnen worden uitgewisseld geblokkeerd. Dit wordt black-listing genoemd. Echter het onderhoud van deze blacklist loopt altijd iets achter op het moment van beschikbaar zijn van op dit punt kritische internetdiensten. Er zijn derhalve diensten die ter beschikking hebben gestaan en daarom mogelijk gebruikt kunnen zijn door medewerkers van de Belastingdienst waarmee het uitwisselen van data heeft kunnen plaatsvinden. Ook zijn er scenario's denkbaar waarbij via het reguliere e-mailverkeer van de Belastingdienst gevoelige gegevens naar externe e-mailadressen verstuurd kan worden. Logging van metagegevens over alle uitgaande e-mailverkeer is beschikbaar, maar wordt niet structureel geanalyseerd of gemonitord.

5.2.4. Logging en monitoring

Infrastructuur en services die daarop beschikbaar worden gesteld, kennen in alle aangetroffen situaties een eigen logging, waarin niet alle gebeurtenissen zijn opgenomen en waarvoor een bewaartermijn op basis van analyse en specificatie van beveiligingsvereisten is bepaald. Vrijwel alle scenario's om gericht gevoelige gegevens naar buiten de Belastingdienst te brengen vereisen meerdere stappen, veelal gaat het daarbij minimaal om de stappen:

- Onttrekken van data aan een bronsysteem;
- Toepassen van een transport mogelijkheid.

Als beide activiteiten:

- Separaat gelogd worden;
- Separaat betrekking kunnen hebben op toegestane reguliere werkzaamheden;

geeft correlatie van bijbehorende logging nog steeds géén indicatie voor een poging tot het lekken van data, omdat het hier reguliere werkzaamheden kan betreffen. Er is dus aanvullende informatie noodzakelijk om een poging tot het gericht lekken van data te kunnen onderkennen.

Monitoring op lekken van gegevens naar buiten de Belastingdienst (actief toezicht) is niet ingericht. Als er een concrete aanleiding is waarbij uit een casus duidelijk is waarnaar gezocht moet worden (zoals wie, wat, wanneer, etc.) is het mogelijk om achteraf onderzoek te doen (reactief toezicht). Als logging niet meer beschikbaar is ontbreekt vanzelfsprekend die onderzoeksmogelijkheid. In dit onderzoek aangetroffen vormen van logging kennen verschillende bewaartermijnen.

De toegepaste logging en monitoring is niet ingericht op het detecteren van pogingen om data buiten de Belastingdienst te brengen. *Risico hiervan is dat ongemerkt gevoelige gegevens buiten de Belastingdienst worden gebracht.*

[15] Met gegevens wordt bedoeld gevens van/over belastingplichtigen, belastingschuldigen en toeslaggerechtigden.

5.3. Risicoanalyse Broedkamer en voorlopers

De risicoanalyse voor de Broedkamers en voorlopers is opgebouwd, en in de volgende paragrafen uitgewerkt, op basis van de volgende indeling:

- De analytische werkomgeving (cliënt-side)
- Gegevenstransport
- Stand-alone oplossingen (server-side)

Beheersing van servers geplaatst binnen een rekencentrum van de Belastingdienst wordt in deze analyse niet meegenomen, omdat deze centraal beheerd en fysiek afgeschermd zijn.

5.3.1. Risicoanalyse analytische werkomgevingen (AWS+, AWS en kantoorautomatisering)

Inspectie, controle, toezicht

5.3.2. Risicoanalyse gegevenstransport

Vanaf april 2014 is er een technische voorziening om gegevens rechtstreeks beschikbaar te stellen in de analytische werkomgeving. Dit impliceert dat in alle situaties hieraan voorafgaand de vraag aan de orde is op welke wijze gegevens voor analyse zijn aangeleverd en geladen in de analytische werkomgeving. Dit zal veelal datatransport m.b.v. een verplaatsbaar medium zijn geweest.

Bij het transport van gegevens doen zich risico's als verlies en onopgemerkt dupliceren voor.

5.3.3. Risicoanalyse standalone oplossingen

Standalone oplossingen (geplaatst buiten een rekencentrum) brengen aanzienlijke risico's met zich mee. Weging van deze risico's hangt sterk af van de gebruikte gegevens (bijvoorbeeld of er van vooraf geanonimiseerde/gepseudonimiseerde gegevens gebruik is gemaakt). Aspecten die het risico bepalen zijn:

- gevoeligheid van de gegevens en de vorm waarin deze beschikbaar zijn gesteld;
- aansluitingen, zoals aanwezige verbindingen (denk aan netwerk, internet etc.);
- de fysieke beveiliging en de bijbehorende autorisaties;
- de beheer- en gebruiksautorisaties;
- afvoer en vernietiging van gebruikte gegevensdragers;
- uitgevoerd toezicht en aanwezigheid van een audit trail.

Standalone oplossingen buiten een rekencentrum brengen aanzienlijke risico's op onopgemerkt buiten de Belastingdienst brengen van gegevens met zich mee en oneigenlijk gegevensgebruik omdat het stelsel van maatregelen zoals die in een gecontroleerde omgeving wordt gehandhaafd ongemerkt doorbroken kan worden, bijvoorbeeld omdat toezicht op de naleving van het stelsel van maatregelen ontbreekt.

6. Loggingonderzoek

6.1. Inleiding

Dit hoofdstuk beschrijft de aanpak en bevindingen van het deelonderzoek naar het mogelijk naar buiten de Belastingdienst brengen van gevoelige gegevens door medewerkers van programma Broedkamer en voorlopers vanaf 2012 tot en met januari 2016.

6.2. Aanpak loggingonderzoek

Met experts binnen de IV-keten van de Belastingdienst is onderzocht welke scenario's van het ten onrechte buiten de Belastingdienst brengen van gegevens en/of misbruik er zijn en of en hoe deze acties via logdata traceerbaar zijn. Tijdens expertsessies werd duidelijk dat er zeer veel scenario's mogelijk zijn tot en met, zo goed als, onzichtbare hacking toe. Deze laatste variant is niet meegenomen als scenario. De uitkomst waren scenario's om dit onderzoek in te richten op basis van twee type data: applicatieve logging, vooral gericht op SAS en Teradata, en een infrastructurele logging onderzoek, vooral gericht op Splunk, Irongate en Blue Zone.
NB. Een handeling van een medewerker kan leiden tot een spoor van registraties die gelogd worden binnen verschillende applicaties en infrastructurele componenten.

Binnen de Belastingdienst zijn diverse loggings beschikbaar waar activiteiten van medewerkers in worden geregistreerd. Voor de onderzoeksperiode 2012 – februari 2016 levert de bewaartermijn van logdata echter beperkingen op. Niet alle logging over deze periode is beschikbaar en zeker gesteld. Over de jaren 2012, 2013 en (grotendeels) 2014 is geen logdata aanwezig. De SAS-logging gaat terug tot november 2014 en e-mails zijn beschikbaar vanaf oktober 2015 (bewaartermijn van 18 maanden) tot einde van de onderzoeksperiode (februari 2016).

De beschikbare loggegevens over de analyse omgeving die onderzocht wordt is door het SOC (Security Operations Centre) beschikbaar gesteld. Het SOC is een onderdeel van de Belastingdienst dat onder B/CIE valt en is daarmee onafhankelijk van de broedkamer en voorlopers. Door het SOC is het volgende uitgevoerd.
- Het beschikbaar stellen van een onderzoeksomgeving.
- Het laden van de loggings in de onderzoeksomgeving (een kwestie van dagen). Deze onderzoeksomgeving kent een adequate beveiliging.
- Hulp bieden bij het zoeken naar de juiste tooling ten behoeve van het onderzoek.

De juistheid en volledigheid van de logging is gewaarborgd via de Persoonsgegevens (houder van een kopie van loggegevens) die middels een kluisprocedure én een formele vrijgave van de HDD met een back-up van de logging. Het laden van de loggegevens is gedaan onder toezicht van een auditor.

We hebben selecties gemaakt op de logging. Deze selecties hadden veelal een nog dusdanige omvang dat kritische deelwaarnemingen nodig waren. Deze zijn genomen op basis van vooraf bepaalde 'kenmerken' (bijvoorbeeld afwijkingen in de tekst, omvang van het datatransport, e.d.) en professional judgement van de onderzoekers.

Bovenstaande aanpak betekent dat niet alle, als 'verdacht aangemerkte' logdata is onderzocht. Doelstelling van dit onderzoek was immers niet het vaststellen van de volledigheid, maar vaststellen of gegevens daadwerkelijk buiten de Belastingdienst zijn gebracht en/of oneigenlijk zijn gebruikt.

Logging onderzoek type 1: Applicatie logging
Gestart is met opvragen van alle applicatie logging van de AWS+'en die bij BI&A/ Broedkamer en voorlopers in gebruik zijn en waren en waarin gebruikersactiviteiten zijn opgenomen. Deze logging is door IV-accent via Persoonsgegevens B/CIE aan het onderzoeksteam beschikbaar gesteld en ten behoeve van het onderzoek geplaatst op een separate en beveiligde onderzoekomgeving.

Vervolgens zijn op functioneel niveau scenario's gedefinieerd die:

- logischerwijs niet passen bij de werkzaamheden van BI&A/ Broedkamer en voorlopers en/of
- duiden op het rechtstreeks verzenden van gegevens naar buiten de Belastingdienst via e-mail of filetransfer en/of
- duiden op het opslaan van gegevens op netwerkschijven of de c:-schijf van de werkplek van de Belastingdienst (DWB).

Deze functionele scenario's zijn vervolgens vertaald naar instructies in de SAS-code. De logdata is hierop geanalyseerd met query's. De uitkomsten uit deze logging zijn vervolgens gebruikt om acties uit de infrastructurele loggings, waaronder de firewall en mailserver, te zoeken en te duiden.

Logging onderzoek type 2: Infrastructurele logging

Met behulp van experts van B/CIE en IV-accent zijn scenario's geïnventariseerd waarmee gegevens vanaf de AWS+ 'en, DWB en of devices van derden, buiten de Belastingdienst zouden kunnen worden gebracht.

De beschikbare logging van de firewall en mailserver maar ook de logging van netwerk-componenten en de AIX servers, is geanalyseerd op mogelijk activiteiten die duiden op het naar buiten brengen van gevoelige gegevens door gebruikers die werkzaam zijn bij BI&A/ Broedkamer en voorlopers.

Daarnaast zijn er drie 'projecten' onderkend waarbij de risico-inschatting hoog is zodat deze nader onderzoek rechtvaardigen. De hoge risico-inschatting van deze projecten zit in het feit dat deze omgevingen zijn genoemd als standalone omgevingen[16] , waarbij externe leveranciers betrokken zijn geweest. In dit type omgevingen bestaat een verhoogd risico op onopgemerkt buiten de Belastingdienst brengen en oneigenlijk gebruik van gegevens (zie paragraaf 5.3.3.). Het betreft de projecten:

- POC Accenture 2012 (6.3.5)
- Labtest Fraude OB-Carrousel 2013 (6.3.6)
- Labtest OB-Negatief 2014 (6.3.7)

Tijdens het onderzoek bleken, naast de hierboven genoemde onderwerpen, er nog twee onderwerpen risicovol te zijn vanuit het oogpunt van het buiten de Belastingdienst brengen van en/of oneigenlijk gebruik van gegevens:
- USB-gebruik in het algemeen (zie 3.3.2.16) en
- laptopgebruik door medewerkers van een inhuurorganisatie (3.3.2.4).

6.3. Bevindingen

In deze paragraaf staan alle bevindingen uit de werkprogramma's. In de rapportage worden de voor de onderzoeksvragen relevante bevindingen overgenomen.

6.3.1. Algemene bevindingen

Een algemene bevinding, welke direct het gevolg is van de gehouden expertsessies, betreft een beperking van de uitkomst. Het loggingonderzoek kan nooit 100% garanties geven over het al dan niet optreden van situaties waarin sprake is van het buiten de omgeving van de Belastingdienst brengen van gegevens en misbruik. Hier zijn twee oorzaken voor aan te wijzen:

- Niet alles wordt gelogd, er worden keuzes gemaakt wat wel en wat niet te loggen. Bedenk hierbij dat nu dagelijks 1 terabyte aan logging informatie wordt gegenereerd.
- Er zijn hacking varianten te bedenken die logging omzeilen. Echter het uitgangspunt voor dit onderzoek is het profiel van de reguliere medewerker en inhuurmedewerker en niet de interne hacker.

[16] Een omgeving die los staat van de infrastructuur van de Belastingdienst

6.3.2. Applicatief gerichte logging

Op basis van de SAS logging is vastgesteld dat:
- Er specifiek naar gegevens van Vips is gezocht (oneigenlijk gebruik).
- Databestanden en programmatuur worden regelmatig naar de C:\schijf van werkplekken gelezen en geschreven. Dit is niet de goede manier om gegevens uit te wisselen. Maar het gebeurt dus. Vooral het bestaan van een SAS-analyse (programmacode en data) op de C:\ schijf is opmerkelijk want dat houdt tevens een risico op de beschikbaarheid in.
- Er e-mailberichten vanuit de code worden gestuurd naar externe e-mailadressen. Via deelwaarneming is vastgesteld dat het in de onderzochte gevallen gaat om e-mailberichten met daarin statusmeldingen van SAS-processen op de AWS. De e-maillogging uit Ironport bevestigd dit beeld.
- Er wordt gezocht op individuele bankrekeningnummers. Een relatie met betrokken BI&A gebruikers is echter na onderzoek niet vastgesteld.
- Er userid- en wachtwoordcombinaties van collega's worden gebruikt om op een Teradata-omgeving aan te loggen. Risico is dat hiermee onbevoegd gegevens kunnen worden ingezien. Hiervan hebben we overigens geen voorbeeld gevonden.
- Userid en wachtwoord combinaties zichtbaar zijn in de logging.
- Er gebruik wordt gemaakt van een single signon macro waarvan om beveiliging technische redenen is afgesproken deze niet (meer) te gebruiken.

Inspectie, controle, toezicht

6.3.3. Infrastructureel gerichte logging

Hieronder worden de bevindingen uit het logging onderzoek type 2 naar infrastructuur gerichte logging opgesomd:
- Niet voor de volledige periode is logging gevonden.
  Proxylogging is aanwezig vanaf: 12-11-2015 tot de D&A onderzoeksperiode maart 2016 en e-maillogging is aanwezig voor de periode: 16-11-2015 tot aan de D&A onderzoeksperiode tot maart 2016.
- Geen verdacht transport aangetroffen bij medewerkers met een gouden internet abonnement.
- 24 e-mails van de 13110 zijn als verdacht bestempeld met mogelijke fiscale inhoud welke naar buiten worden gebracht. 17 e-mails zijn verwijderd omdat de betrokken medewerkers niet meer bij de Belastingdienst werkzaam zijn. Overeenkomstig de voorgeschreven procedure wordt al het e-mail verkeer van een vertrekkende medewerker gewist. Vier gebruikers hebben de verdachte e-mail zelf verwijderd. Slechts 3 e-mails zijn aangetroffen. Onderstaand een beschrijving van de 3 e-mails.

  (1) Een e-mail betreft het herzenden van 5000 regels 'sample' data met informatie geleverd door McKinsey, deze informatie is oorspronkelijk afkomstig van Graydon (leverancier van kredietwaardigheid info). Met het herzenden vanuit de Belastingdienst gaat de e-mail terug naar de bron McKinsey. Wel is dit een andere collega binnen McKinsey. Hier worden dus geen fiscale gegevens naar buiten gebracht ook niet als verrijkte info op de kredietwaardigheidsinformatie. Wel bestaat er een indicatie dat op een later moment de KvK nummers als een verrijkingsslag op deze data alsnog zijn verstrekt.

  (2) Resultaten van een pilot wordt naar 2 medewerkers van Accenture door een Belasting-dienstmedewerker gedeeld. Het gaat om aangifte data van 1101 unieke (1119 regels) bedrijven met data verdeeld over in 31 kolommen. Voor de vulling van de kolommen moet gedacht worden aan FINR (geen persoonsgegevens), aangifte omzetbelastinggegevens, geschatte aangifte en omzetgegevens. Hier wordt data van Bedrijven naar buiten gebracht.
  NB. In dit geval worden er gegevens buiten de Belastingdienst gebracht.