

Ministerie van Financiën

Rapport van bevindingen onderzoek informatiebeveiliging programma Broedkamer en voorlopers

Versie 1.0

Datum 21 september 2017
Status Definitief

Colofon

Titel	Rapport van bevindingen onderzoek informatiebeveiliging programma Broedkamer en voorlopers
Auteur(s)	
Auditteam	
Bijlagen	
Inlichtingen	

Inhoud

1	**Inleiding**	**7**
1.1	Aanleiding	7
1.2	Context	7
2	**Samenvatting**	**8**
3	**Doelstelling en verantwoording**	**10**
3.1	Doelstelling	10
3.2	Verrichte werkzaamheden	10
3.3	Beperkingen onderzoek	11
3.4	Verspreidingskring rapportage	12
4	**Bevindingen**	**13**
4.1	Inrichting programma Broedkamer en voorlopers	13
4.2	Onderzoek naar de beveiliging bij het programma Broedkamer en voorlopers in de periode 2012 – februari 2016	13
4.2.1	De Belastingdienst heeft het beveiligingsbeleid en de verantwoordelijkheden vastgelegd	13
4.2.2	Het beveiligingsbeleid van de Belastingdienst geeft een richtlijn voor monitoring, maar er is geen monitoring op het opmerken van datatransport door medewerkers van het programma Broedkamer of voorlopers	14
4.2.3	Beveiligingsbeleid en -maatregelen programma Broedkamer en voorlopers: er is sprake van beveiligingsbewustzijn; bedreigingen- en kwetsbaarhedenanalyse aan het einde van de onderzoeksperiode uitgevoerd	14
4.2.3.1	Maatregelen organisatorische beveiliging: maatregelen gericht op gedrag van de medewerkers later in onderzoeksperiode ingericht en niet volledig geëffectueerd	14
4.2.3.2	Maatregelen fysieke beveiliging: er werd voor het programma Broedkamer en voorlopers geen verbijzonderde toegangsbeveiliging toegepast	15
4.2.3.3	Maatregelen logische beveiliging: logische scheiding niet mogelijk vanuit de beschikbare ICT service	15
4.3	Signalen over risico's en de opvolging daarvan ten aanzien van oneigenlijk gebruik of het naar buiten de Belastingdienst brengen van gegevens, zijn niet in beschikbare verslagen van besluitvormende organen aangetroffen	16
4.4	Risico inventarisatie onderzoeksteam	16
4.4.1	De analytische werkruimte biedt mogelijkheden om data over te brengen naar de werkplek en rechtstreeks naar buiten de Belastingdienst	16
4.4.2	De werkplek biedt mogelijkheden om data naar buiten de Belastingdienst te brengen	16
4.4.3	Toegepaste projectmatige IT oplossingen bieden mogelijkheden voor het buiten de Belastingdienst brengen van gegevens en oneigenlijk gegevensgebruik	17
4.5	Onderzoek om vast te stellen of getracht is gegevens buiten de Belastingdienst te brengen of oneigenlijk te gebruiken	17
4.5.1	Er zijn gegevens buiten de Belastingdienst gebracht	17
4.5.2	Er is datatransport zichtbaar zonder dat de inhoud vastgesteld kan worden	18
4.5.3	Er zijn drie gegevensopvragingen die betrekking hebben op individuele belastingplichtigen	18
4.5.4	Toegepaste projectmatige IT oplossingen hebben risico's opgeleverd op oneigenlijk gebruik van gegevens en buiten de Belastingdienst brengen van gegevens	18

4.5.5 Er is gebruik gemaakt van USB-ontheffingen en daarmee was er sprake van een risico op het buiten de Belastingdienst brengen van gegevens en oneigenlijk gegevensgebruik 19
4.5.6 Externe medewerkers werkten met gegevens op niet-Belastingdienstwerkplekken; dit betekent dat er gegevens buiten de Belastingdienst zijn gebracht 19

5 Ondertekening 20

1 Inleiding

1.1 Aanleiding

In het Kamerdebat d.d. 9 februari 2017 zijn vragen gesteld naar aanleiding van een tv uitzending van 1 februari 2017. In deze uitzending is gesteld dat bij het koppelen van gegevens voor fraudebestrijding door de Belastingdienst belangrijke beveiligingsrisico's aan het licht zijn gekomen. De Staatssecretaris van Financiën heeft naar aanleiding van het Kamerdebat meerdere onderzoeken toegezegd. Dit onderzoek naar de informatiebeveiliging bij het programma Broedkamer en voorlopers is één van de in gang gezette beveiligingsonderzoeken.

1.2 Context

Het onderzoek naar de informatiebeveiliging bij het programma Broedkamer en voorlopers is in opdracht van de DG Belastingdienst uitgevoerd door de Belastingdienst, onder direct gezag van de hoofddirecteur Informatievoorziening. De Directeur Bedrijfsvoering IV is de opdrachtnemer. Het onderzoek is uitgevoerd door auditors van de IV-organisatie van de Belastingdienst. De uitvoerders hebben geen rol/bemoeienis gehad met het programma Broedkamer en voorlopers.

De objectiviteit en degelijkheid van het onderzoek is geborgd door een onderzoek door de Auditdienst Rijk (ADR) van de aanpak, de uitvoering, de bevindingen en de rapportage van het onderzoek. Dit is conform de toezegging in de brief aan de Kamer van 14 februari 2017.

2 Samenvatting

Inleiding
De Staatssecretaris van Financiën heeft naar aanleiding van het Kamerdebat op 9 februari 2017 toegezegd onderzoek te zullen doen naar de informatiebeveiliging bij het programma Broedkamers en voorlopers. Het onderzoek heeft zich gericht op de periode 1 januari 2012 tot 1 februari 2016.

Beperkingen onderzoek
Het onderzoek richt zich grotendeels op niet meer bestaande situaties van jaren geleden waarover de onderzoeksinformatie beperkt is. Zo werden projectmatige IT oplossingen gebruikt die nu niet meer bestaan en zijn over een klein deel van de onderzoeksperiode nog loggegevens beschikbaar.

Beveiligingsmaatregelen programma Broedkamers en voorlopers
Binnen de Belastingdienst is beveiliging, als onderdeel van integraal management en bedrijfsvoering, een verantwoordelijkheid van het lijnmanagement op de diverse niveaus van de organisatie met als Rijksbrede uitgangspunt het vertrouwen in de medewerker.
Het beveiligingsbeleid van de Belastingdienst geeft een richtlijn voor monitoring. Er wordt echter geen monitoring uitgevoerd op het detecteren van pogingen, door medewerkers van het programma Broedkamer en voorlopers, om data buiten de Belastingdienst te brengen.

Het programma Broedkamer en voorlopers volgt het principe, dat in het beveiligingsbeleid van de Belastingdienst wordt gehanteerd, dat beveiliging werkt vanuit het eigen beveiligingsbewustzijn van de medewerker. Een risico- en/of kwetsbaarhedenanalyse is een belangrijke pijler in het beveiligingsbeleid. Een dergelijke analyse is eind 2015 uitgevoerd.

Signalen en opvolging
Ten aanzien van de signalen in relatie tot geconstateerde risico's en/of feiten, die tijdens het onderzoek zijn gevonden, hebben we in de onderzochte verslagen van besluitvormende organen geen besluit(en) aangetroffen.

Buiten de Belastingdienst brengen van gegevens en oneigenlijk gegevensgebruik
De door het programma Broedkamer en voorlopers gehanteerde analyseomgeving, Belastingdienstwerkplekken, IT middelen en toegepaste (projectmatige) IT oplossingen bieden mogelijkheden om gegevens buiten de Belastingdienst te brengen.
Externe medewerkers werkten met gegevens op niet-Belastingdienstwerkplekken; dit betekent dat gegevens buiten de Belastingdienst zijn gebracht. Er is echter geen informatie beschikbaar over omvang en inhoud van dit gegevensgebruik.

In het onderzoek, aan de hand van kritische deelwaarnemingen op basis van de beschikbare loggegevens over een beperkte periode, hebben wij één geval aangetroffen waarbij gegevens via e-mail buiten de Belastingdienst zijn gebracht[1]. In de bijlage van de e-mail zijn gegevens uit het omzetbelastingsysteem opgenomen van ongeveer 1.100 bedrijven. Dit bestand bevat geen bedrijfsnamen.

[1] Dit type bevinding is vergelijkbaar met die in het 'Rapport van bevindingen onderzoek gegevensgebruik D&A'.

Daarnaast zijn er drie gegevensopvragingen die betrekking hebben op individuele belastingplichtigen.

3 Doelstelling en verantwoording

3.1 Doelstelling

De Staatssecretaris van Financiën heeft in zijn brief van 14 februari 2017 een nadere beschrijving gegeven van de onderzoeken die in zijn eerdere brief van 8 februari 2017 over de uitzending van Zembla waren aangekondigd[2].

Het doel van het onderzoek naar de informatiebeveiliging bij het programma Broedkamer en voorlopers is als volgt omschreven:
'dit onderzoek richt zich op het programma Broedkamer en de voorlopers[3] daarvan en beslaat de periode van 2012 tot februari 2016. Het doel van dit onderzoek is drieledig:
a. aan de hand van in elk geval beschikbare of reconstrueerbare loggegevens over gebruik van systemen, applicaties en data vaststellen of in genoemde periode gegevens van belastingplichtigen, belastingschuldigen of toeslaggerechtigden[4] buiten de Belastingdienst zijn gebracht dan wel oneigenlijk[5] zijn gebruikt;
b. in kaart brengen welke informatiebeveiligingsmaatregelen in de genoemde periode van kracht waren en hoe deze hebben gewerkt en op basis daarvan vaststellen welke risico's hebben bestaan en
c. in relatie tot geconstateerde risico's en/of feiten omtrent daadwerkelijk oneigenlijk gegevensgebruik of het buiten de Belastingdienst brengen van gegevens, signalen inventariseren en bekijken wat daarmee is gedaan.'

De opbouw van het rapport gaat van generiek naar specifiek. Achtereenvolgens wordt ingegaan op doelstelling b (zie paragraaf 4.2), c (zie paragraaf 4.3) en a (zie paragraaf 4.4 en 4.5).

3.2 Verrichte werkzaamheden

Deze opdracht is uitgevoerd overeenkomstig NOREA Richtlijn 4401, "Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie." In dit rapport wordt geen zekerheid verschaft, omdat er geen assurance opdracht is uitgevoerd. Indien andere (aanvullende) werkzaamheden of een assurance opdracht zouden zijn uitgevoerd, zouden wellicht andere onderwerpen zijn geconstateerd en gerapporteerd.

Dit rapport bevat feitelijke bevindingen van het onderzoeksteam over de genoemde periode van 1 januari 2012 tot 1 februari 2016. Er wordt geen samenvattend oordeel of conclusie gegeven over de mate van voldoen aan de van toepassing zijnde beveiligingsnormen, zoals onderdelen van het Handboek Beveiliging Belastingdienst (HBB). Bevindingen met een vertrouwelijk karakter zijn niet in detail opgenomen.

[2] Kamerstukken II 2016/17, 31 066, nrs. 340 en 344.
[3] Het 'programma Broedkamer en voorlopers' wordt beschreven in paragraaf 4.1.
[4] In dit rapport wordt onder gegevens verstaan: gegevens van belastingplichtigen, belastingschuldigen of toeslaggerechtigden.
[5] Oneigenlijk gegevensgebruik: gegevensopvragingen die niet aannemelijk lijken bij de functie van het programma Broedkamer en voorlopers.

Het onderzoeksteam heeft de te verrichten werkzaamheden samen met de opdrachtnemer, de directeur Bedrijfsvoering IV, afgestemd met de gedelegeerd/operationeel opdrachtgever, de hoofddirecteur IV. Over de wijze van uitvoering van de opdracht is frequent overleg geweest.

Voor het in kaart brengen welke informatiebeveiligingsmaatregelen in de genoemde periode van kracht waren, is het Handboek Beveiliging Belastingdienst (HBB) gebruikt.
Het onderzoek van wat er is gedaan met risico's en/of feiten omtrent oneigenlijk gegevensgebruik of het buiten de Belastingdienst brengen van gegevens, is uitgevoerd met behulp van beschikbare verslagen van besluitvormende organen ten aanzien van het programma Broedkamer en voorlopers.
Vanuit de infrastructuur en applicaties is op basis van een risicoanalyse geïnventariseerd welke scenario's voor het naar buiten brengen en oneigenlijk gebruik van gegevens mogelijk waren. Er is nagegaan op welke wijze het naar buiten brengen en oneigenlijk gebruik van gegevens via beschikbare logging traceerbaar zou kunnen zijn. Door middel van tooling zijn uit de beschikbare logging handelingen geselecteerd die mogelijk duiden op het naar buiten brengen van gegevens en/of oneigenlijk gegevensgebruik. Hierop zijn kritische deel-waarnemingen gedaan.
De risicoanalyse heeft ook geleid tot onderzoek naar drie projectmatige IT oplossingen en gebruikte IT middelen.

3.3 Beperkingen onderzoek

De aard van de materie/de onderzoeksobjecten brengt inherente beperkingen met zich mee. Het is namelijk niet mogelijk om alle al dan niet geslaagde pogingen om gegevens buiten de Belastingdienst te brengen vast te stellen. Dit is bijvoorbeeld te wijten aan situaties die niet te loggen zijn. Bij het laatste kan gedacht worden aan het meenemen van printjes met gegevens en fotografische vastleggingen van gegevens.

Een andere beperking heeft te maken met het feit dat het onderzoek zich richt op situaties van veelal jaren geleden. In die tijd werden projectmatige IT oplossingen gebruikt die nu niet meer feitelijk te onderzoeken zijn, omdat deze niet meer bestaan.
Omdat er ook niet altijd gegevens of documentatie beschikbaar is, zijn verklaringen van functionarissen in voorkomende gevallen niet te verifiëren.

De bewaartermijn van gegevens, die nodig zijn om vast te stellen wat er is getransporteerd, is soms beperkt. Om vast te stellen wat er is gebeurd dienen loggegevens te worden gecombineerd met gegevens uit andere bronnen. Om bijvoorbeeld te kunnen achterhalen wat de inhoud van een e-mail is, inclusief eventuele bijlagen, dient gebruik te worden gemaakt van (back-ups van) het e-mailsysteem. Dit is alleen mogelijk als de e-mailbox inclusief de betreffende e-mail hierin nog beschikbaar is. Dit betekent dat verwijderde e-mails niet meer te achterhalen zijn.
Over de onderzoeksperiode bleek de logging van de data-analyse omgeving vanaf februari 2014 en de logging over verstuurde e-mails en internet gebruik vanaf medio november 2015 beschikbaar te zijn. Dat betekent dat over het naar buiten brengen van gegevens via de werkplek voor minder dan drie maanden loggegevens van de onderzoeksperiode beschikbaar is.

3.4 Verspreidingskring rapportage

De directeur Bedrijfsvoering IV verstrekt deze rapportage aan de opdrachtgever, de DG Belastingdienst, en de gedelegeerd/operationeel opdrachtgever, de hoofddirecteur IV.

4 Bevindingen

4.1 Inrichting programma Broedkamer en voorlopers

Vanaf 2012 werden binnen het dienstonderdeel Belastingen omgevingen voor data-analyse ingericht om in projectverband analysemodellen voor toezicht en invordering te ontwikkelen. In 2013 is het Business Analyse (BA) team opgericht. In de loop van 2013 zijn de Business Intelligence (BI) medewerker(s) daaraan toegevoegd wat resulteerde in de vorming van het BI&A team[6]. Het programma Broedkamer is in 2014 gestart binnen het team BI&A. Vanuit het programma Broedkamer vond regie plaats op data-analyse projecten en werd ondersteuning verleend aan projecten om, door middel van data-analyse, innovatieve ideeën te implementeren binnen Belastingen. Er werden bijvoorbeeld analysemodellen ontwikkeld om niet compliant gedrag te detecteren en te (laten) behandelen.
Voor de realisatie van modellen en innovaties met behulp van gegevensverzamelingen is door het programma Broedkamer en opvolgers door medewerkers van de Belastingdienst samengewerkt met medewerkers van externe partijen.
Het team BI&A is in februari 2016 opgegaan in het dienstonderdeel Data & Analytics.

Om modellen en innovaties te maken, is gebruik gemaakt van data uit bronsystemen van de Belastingdienst en beschikbare analyseomgevingen, bijvoorbeeld een Analytical Workspace Server (AWS (2012) en AWS+ (2013)).

Er werden in samenwerking met leveranciers projectmatige IT oplossingen gecreëerd in aanvulling op het bestaande aanbod van de Belastingdienst.

4.2 Onderzoek naar de beveiliging bij het programma Broedkamer en voorlopers in de periode 2012 – februari 2016

4.2.1 De Belastingdienst heeft het beveiligingsbeleid en de verantwoordelijkheden vastgelegd

Binnen de Belastingdienst is beveiliging, als onderdeel van integraal management en bedrijfsvoering, een verantwoordelijkheid van het lijnmanagement op de diverse niveaus van de organisatie met als Rijksbrede uitgangspunt het vertrouwen in de medewerker. Het beveiligingsbeleid en de beveiligingsnormen van de Belasting-dienst zijn vastgelegd in het Handboek Beveiliging Belastingdienst (HBB).

Het HBB beschrijft het basis-beveiligingsniveau; uitwerkingen van het HBB en noodzakelijk geachte aanvullende maatregelen worden binnen de dienstonderdelen bepaald op basis van een risico- en/of kwetsbaarhedenanalyse.

[6] Business Intelligence & Analytics

4.2.2 Het beveiligingsbeleid van de Belastingdienst geeft een richtlijn voor monitoring, maar er is geen monitoring op het opmerken van datatransport door medewerkers van het programma Broedkamer of voorlopers

In het HBB is een richtlijn voor het monitoren van activiteiten opgenomen.

Er is geen monitoring op het detecteren van pogingen, door medewerkers van het programma Broedkamer en voorlopers, om data buiten de Belastingdienst te brengen.

4.2.3 Beveiligingsbeleid en -maatregelen programma Broedkamer en voorlopers: er is sprake van beveiligingsbewustzijn; bedreigingen- en kwetsbaarhedenanalyse aan het einde van de onderzoeksperiode uitgevoerd

Wij hebben over de beginperiode van het programma Broedkamer en voorlopers geen vastleggingen aangetroffen van beveiligingsbeleid en –maatregelen waaruit blijkt dat beveiligingsrisico's, gepaard gaande met de inzet van specifieke werkomgevingen, werden onderkend en gemitigeerd.
Met leveranciers zijn afspraken gemaakt over informatiebeveiliging. De verantwoordelijkheid voor het toezicht op de afspraken is niet vastgelegd.

Uit interviews maken we op dat er vanaf het begin van de afdeling BI&A het besef was dat extra beveiligingsmaatregelen genomen moesten worden. De argumenten hiervoor waren het specifieke karakter van de afdeling en de omgang met grote hoeveelheden (privacygevoelige) data.
In juli 2014 zijn leidende principes vastgesteld, 'de 10 geboden van informatiebeveiliging'. De 10 geboden werden door middel van posters in de werkruimten bekendgemaakt aan de medewerkers. Hierin wordt onder andere ingegaan op het zorgvuldig gebruik van gegevens.
In 2015 is binnen BI&A beleid vastgesteld voor aanvullende beveiligingsmaatregelen van gegevens. Hierna is gestart met een bewustwordingsprogramma (Awareness (2015) en iBewustzijn (2016)).
Eind 2015 is er een bedreigingen- en kwetsbaarhedenanalyse uitgevoerd. Een dergelijke analyse is een belangrijke pijler in het HBB op basis waarvan transparant en proactief managen van beveiligingsrisico's wordt verwacht.

4.2.3.1 Maatregelen organisatorische beveiliging: maatregelen gericht op gedrag van de medewerkers later in onderzoeksperiode ingericht en niet volledig geëffectueerd

Geheimhouding/screenen
Bij aanvang van de inhuurperiode moesten externe medewerkers een geheimhoudingsverklaring (GHV) ondertekenen en de Belastingdienstmedewerkers moesten bovendien de eed/belofte afleggen. Daarnaast werd een Verklaring Omtrent Gedrag (VOG) en een kopie-Identiteitsbewijs gevraagd.
Wij hebben niet alle hiervoor genoemde documenten aangetroffen. Voor wat betreft de ontbrekende GHV's wordt dit (deels) verklaard door de toepassing van een wederkerige geheimhoudingsverklaring die met de betreffende leverancier is afgesproken.

Bewustwordingsprogramma
In mei 2015 werd een bewustwordingsprogramma verplicht gesteld voor alle medewerkers van BI&A (Belastingdienstmedewerkers en externe medewerkers). Dit programma bestond uit plenaire trainingen Privacy en Security en een cursus iBewustzijn Overheid. Van een groot deel van de medewerkers hebben wij de benodigde certificaten per begin februari 2016 niet aangetroffen.

4.2.3.2 Maatregelen fysieke beveiliging: er werd voor het programma Broedkamer en voorlopers geen verbijzonderde toegangsbeveiliging toegepast

De huisvesting van de medewerkers van het programma Broedkamer en voorlopers heeft plaatsgevonden in Rijksgebouwen. Er werd gebruik gemaakt van de standaard-dienstverlening voor toegangsbeveiliging van Belastingdienstgebouwen, verleend door het Centrum voor Facilitaire Dienstverlening (CFD) van de Belastingdienst. De hoofdingang en personeelsingang van de gebouwen waarin het programma Broedkamer en voorlopers gehuisvest waren, waren voorzien van tourniquets met kaartlezers. Ook waren de afzonderlijke etages voorzien van kaartlezers.

Tot begin 2014 werd alleen toegang verkregen tot een etage/afdeling bij een verleende autorisatie. In 2014 werden de toegangsrechten van de Rijkspas voor alle medewerkers uitgebreid. Dat betekent dat medewerkers van de Belastingdienst die niet bij het programma Broedkamer en voorlopers werkzaam waren de betreffende etages vanaf dat moment konden betreden.

4.2.3.3 Maatregelen logische beveiliging: logische scheiding niet mogelijk vanuit de beschikbare ICT service

De data-analyseomgeving biedt geen scheiding van omgevingen
De AWS (en later AWS+) kent geen logische scheiding van test-, pilot en productieomgevingen. Dit betekent dat wijzigingen gevolgen kunnen hebben voor de beschikbaarheid en betrouwbaarheid van informatieproducten ten behoeve van informatiegestuurde handhaving en/of inning.

De data-analyseomgeving biedt geen projectgebonden autorisatiestructuur
Inzet van de AWS/AWS+ voor meerdere projecten en autorisaties voor meerdere AWS'en, brengt een risico op oneigenlijk gebruik van gegevens met zich mee.
De AWS/AWS+ kent in de loop van de onderzoeksperiode een op rollen gebaseerde autorisatiestructuur (in het begin waren er algemene autorisaties op de SAS[7] servers), echter binnen één AWS/AWS+ zijn deze rollen generiek en dus niet te differentiëren naar projecten. Bij het programma Broedkamer en voorlopers worden meerdere projecten binnen één AWS/AWS+ uitgevoerd. De projectmedewerkers kunnen daardoor toegang hebben tot alle data die op de desbetreffende AWS/AWS+ zijn opgeslagen. Projectmedewerkers hebben ook toegang tot meerdere AWS'en. Als een medewerker bijvoorbeeld alleen betrokken is bij OB[8]-projecten dan kunnen gegevens uit andere bronsystemen die op de AWS van dit project staan niet voor deze medewerker worden afgeschermd.

[7] Merknaam van marktconforme statistische software die onderdeel uitmaakt van een AWS/AWS+.
[8] Omzetbelasting.

4.3 Signalen over risico's en de opvolging daarvan ten aanzien van oneigenlijk gebruik of het naar buiten de Belastingdienst brengen van gegevens, zijn niet in beschikbare verslagen van besluitvormende organen aangetroffen

In relatie tot geconstateerde risico's en/of feiten omtrent daadwerkelijk oneigenlijk gegevensgebruik of het buiten de Belastingdienst brengen van gegevens, is door ons een inventarisatie uitgevoerd van signalen en is vervolgens nagegaan wat daarmee is gedaan.
Wij hebben in de onderzochte periode ten aanzien van de geïnventariseerde signalen, in de beschikbare notulen en/of verslagen van bijeenkomsten van besluitvormende organen geen besluitvorming aangetroffen.
Van enkele besluitvormende organen zijn overigens geen (vastgestelde) verslagen gevonden.

Er zijn twee onderzoeken/adviesopdrachten ten aanzien van de organisatie-inrichting en (beveiliging van) datagebruik (Oliver Wyman 2015 en LiquidHub 2015[9]). Er is geen formele besluitvorming aangetroffen ten aanzien van de implementatie van maatregelen naar aanleiding van gesignaleerde risico's in deze rapporten.

Van beveiligingsincidenten wordt door de afdeling BI&A, overeenkomstig het HBB, een logboek bijgehouden. Het logboek bevat geen gevallen van oneigenlijk gebruik of het buiten de Belastingdienst brengen van gegevens.

4.4 Risico inventarisatie onderzoeksteam

Het onderzoeksteam heeft na de analyse van het systeemlandschap en het beveiligingsbeleid de specifieke risico's in beeld gebracht bij de toegang en het gebruik van gegevens.

4.4.1 De analytische werkruimte biedt mogelijkheden om data over te brengen naar de werkplek en rechtstreeks naar buiten de Belastingdienst

De software, gebruikt in de AWS+ en diens voorgangers, maakt het mogelijk om gegevens waarmee gewerkt wordt op te slaan op de werkplek, maar óók deze te mailen rechtstreeks vanuit deze analyseomgevingen (zonder tussenkomst van de werkplek met de daarop geïnstalleerde e-mail functionaliteit).
Dit brengt een risico met zich mee op het naar buiten brengen van gegevens.

4.4.2 De werkplek biedt mogelijkheden om data naar buiten de Belastingdienst te brengen

In het ontwerp van de Belastingdienstwerkplek is een balans gezocht tussen beveiligingsmaatregelen en de eigen verantwoordelijkheid en het bewustzijn van de gebruiker.

[9] 'Review of Investeringsagenda De Belastingdienst', 20 mei 2015 (Oliver Wyman); 'Belastingdienst BIA Observaties & Aanbevelingen', 26 maart 2015 (LiquidHub); 'Investigating Data Streams', december 2015 (Oliver Wyman).

De gebruikte werkplek is beveiligd, maar de hierop aangeboden functionaliteit biedt mogelijkheden om data buiten de Belastingdienst te brengen. Zoals bijvoorbeeld de mogelijkheid om e-mail met bijlagen te versturen. Daarnaast is middels ontheffingen gebruik van USB devices (USB-sticks en USB-schijven) mogelijk. Op het gebruik van USB devices wordt in paragraaf 4.5.5 ingegaan.
Externe medewerkers maakten gebruik van niet-Belastingdienst werkplekken waarvan het ontwerp onbekend is. Op het gebruik van niet-Belastingdienst werkplekken wordt in paragraaf 4.5.6 ingegaan.
Het gebruik van de (niet-)Belastingdienst werkplekken brengt een risico met zich mee op oneigenlijk gebruik en het naar buiten brengen van gegevens.

4.4.3 Toegepaste projectmatige IT oplossingen bieden mogelijkheden voor het buiten de Belastingdienst brengen van gegevens en oneigenlijk gegevensgebruik

Er werd gewerkt met projectmatige IT oplossingen, waarbij door leveranciers ingerichte analyseomgevingen werden ingezet, waarvan het beheer ook (gedeeltelijk) buiten de gecontroleerde omgeving van de Belastingdienst plaatsvond. Dergelijke projectmatige IT oplossingen brengen risico's op onopgemerkt buiten de Belastingdienst brengen van gegevens en oneigenlijk gegevensgebruik met zich mee, 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. Het beschikbaar stellen van gegevens vanuit de primaire systemen aan deze analyseomgevingen levert een verhoogd risico op. Op het gebruik van projectmatige IT oplossingen wordt in paragraaf 4.5.4 ingegaan.

4.5 Onderzoek om vast te stellen of getracht is gegevens buiten de Belastingdienst te brengen of oneigenlijk te gebruiken

Deze paragraaf behandelt de uitkomsten van het onderzoek naar het buiten de Belastingdienst brengen van gegevens en oneigenlijk gebruik van gegevens.

4.5.1 Er zijn gegevens buiten de Belastingdienst gebracht

Ons onderzoek van loggegevens door middel van een kritische deelwaarneming heeft aangetoond dat gegevens buiten, de beveiligde omgeving, van de Belastingdienst zijn gebracht[10].

Een Belastingdienstmedewerker stuurt via e-mail de resultaten van een analyse naar twee externe e-mailadressen van een leverancier. In de bijlage zijn gegevens uit het omzetbelastingsysteem opgenomen van ongeveer 1.100 bedrijven. Dit bestand bevat geen bedrijfsnamen.

[10] Het type bevindingen in de paragrafen 4.5.1 en 4.5.2 is vergelijkbaar met die in het 'Rapport van bevindingen onderzoek gegevensgebruik D&A'

4.5.2 Er is datatransport zichtbaar zonder dat de inhoud vastgesteld kan worden

Er zijn in het onderzoek van loggegevens door middel van een kritische deelwaarneming 21 e-mails aangetroffen die ons opvallen door naamgeving van de bijlage en/of de 'onderwerpregel' maar niet meer te achterhalen zijn[11]. In vier gevallen heeft een gebruiker zelf de e-mail verwijderd. In 17 gevallen is de e-mail verwijderd omdat de medewerker niet meer bij de Belastingdienst werkzaam is.

4.5.3 Er zijn drie gegevensopvragingen die betrekking hebben op individuele belastingplichtigen

Het onderzoek middels een kritische deelwaarneming heeft geleid tot drie gegevensopvragingen die betrekking hebben op individuele belastingplichtigen.

- In oktober 2014 en april 2015 hebben twee medewerkers opvragingen gedaan op basis van individuele bankrekeningnummers.[12]
- In augustus 2015 is door een medewerker een opvraging gedaan op basis van de indicatie VIP.[13] [14]

4.5.4 Toegepaste projectmatige IT oplossingen hebben risico's opgeleverd op oneigenlijk gebruik van gegevens en buiten de Belastingdienst brengen van gegevens

In deze paragraaf komen projectmatige IT oplossingen aan de orde. Er zijn leveranciers ingezet die specifieke IT oplossingen hebben gebruikt voor projecten van het programma Broedkamer en voorlopers.

Casus IT oplossing beheerd door externen
Voor een project is door externen bij de Belastingdienst, in een afgeschermde ruimte, een specifieke IT oplossing gerealiseerd. Hierop zijn gegevens vanuit de Belastingdienstomgeving geplaatst. Het beheer van de IT oplossing werd door externen uitgevoerd, waarbij betreffende medewerkers toegang hebben gehad tot deze gegevens. Wij hebben geen documentatie aangetroffen van de wijze waarop de Belastingdienst toezicht op het beheer, gebruik en verwijderen van gegevens door deze externen heeft uitgevoerd. Het ontbreekt aan nadere informatie om daadwerkelijk oneigenlijk gebruik en het buiten de Belastingdienst brengen van gegevens vast te kunnen stellen.

Casus IT oplossing beheerd door Belastingdienst
Eén project is gerealiseerd op een AWS met een gedoogstatus binnen het rekencentrum van de Belastingdienst, waarvoor het standaard beveiligingsbeleid niet volledig werd uitgevoerd.
Het ontbreekt aan nadere informatie om daadwerkelijk oneigenlijk gebruik en het buiten de Belastingdienst brengen van gegevens vast te kunnen stellen.

[11] Het type bevindingen in de paragrafen 4.5.1 en 4.5.2 is vergelijkbaar met die in het 'Rapport van bevindingen onderzoek gegevensgebruik D&A'.
[12] Dit hoeft niet te betekenen dat er sprake is van 'misbruik'. Binnen de context van de opdracht is dit niet onderzocht.
[13] Belastingplichtigen die een hoge openbare functie vervullen of die om één of andere reden in publicitaire zin een kwetsbare positie bekleden.
[14] De waarnemend directeur van het organisatieonderdeel D&A heeft verklaard dat deze opvraging van gegevens over VIP's werkgerelateerd is geweest. De opvraging kwam voort uit een onderzoek waar VIP-gegevens bij betrokken waren en een testcasus is gemaakt. Het onderzoeksteam is hierover geïnformeerd. Binnen de context van de opdracht kan het onderzoeksteam niet beoordelen of het gebruik werkgerelateerd is.

Casus IT oplossing buiten Belastingdienst
Voor een project zijn geanonimiseerde gegevens via een externe schijf beschikbaar gesteld aan een leverancier. Er zijn afspraken gemaakt met de leverancier dat deze het beheer, de beveiliging en vernietiging van de gegevens verzorgt. Vastleggingen waaruit blijkt dat de gegevens daadwerkelijk geanonimiseerd zijn en de maatregelen volledig en juist hebben gewerkt hebben wij niet aangetroffen. Er ontbreekt informatie om daadwerkelijk oneigenlijk gebruik van gegevens vast te kunnen stellen.

4.5.5 Er is gebruik gemaakt van USB-ontheffingen en daarmee was er sprake van een risico op het buiten de Belastingdienst brengen van gegevens en oneigenlijk gegevensgebruik

Een USB-ontheffing stelt de gebruiker in staat om gebruik van USB-devices (USB-sticks en USB-schijven) te maken en hierop gegevens van de Belastingdienst te plaatsen. Het versleutelen van gegevens op USB-devices werd niet afgedwongen.

Over de gehele periode zijn er USB-ontheffingen geweest. In november 2015 waren er 47 USB-ontheffingen verleend aan medewerkers van de afdeling BI&A. Hiervan hadden 18 medewerkers toegang tot een AWS. De USB-ontheffing kwam over het algemeen mee uit een voorgaande functie. Overigens is de USB-ontheffing niet aan externe medewerkers uitgegeven.
Het aantal USB-ontheffingen is eind 2015 teruggebracht tot vier medewerkers.

Van USB-devices, wordt het gebruik gelogd, maar de inhoud van het dataverkeer niet. Daarom is niet vast te stellen of er gegevens met behulp van USB-devices buiten de Belastingdienst zijn gebracht.

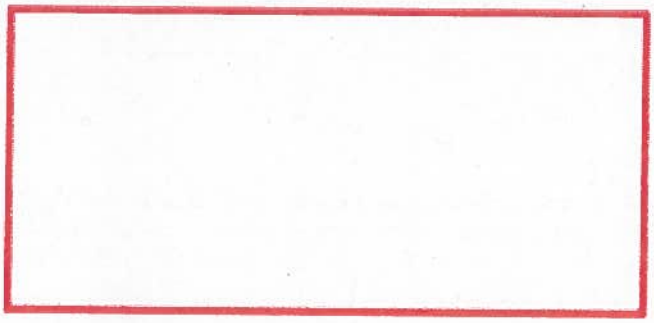
4.5.6 Externe medewerkers werkten met gegevens op niet-Belastingdienstwerkplekken; dit betekent dat er gegevens buiten de Belastingdienst zijn gebracht

Externe medewerkers maakten gebruik van niet-Belastingdienstwerkplekken wegens een tekort aan Belastingdienstwerkplekken.
Belastingdienstmedewerkers hebben aangegeven dat in voorkomende gevallen hierop gegevens zijn geplaatst via USB-devices en e-mail. Dit betekent dat in deze gevallen gegevens buiten de Belastingdienst zijn gebracht. Er is echter geen informatie beschikbaar over omvang en inhoud van dit gegevensgebruik.

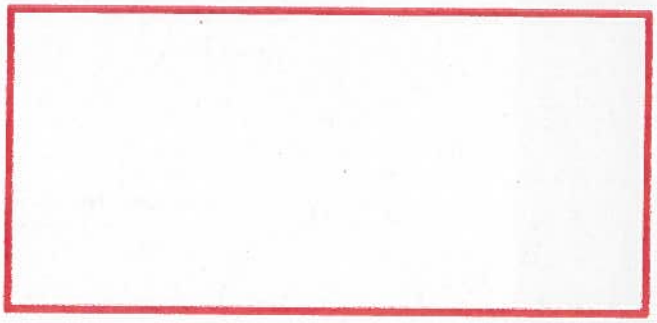
Het is ook mogelijk geweest om met een niet-Belastingdienstwerkplek verbinding met het Belastingdienstnetwerk te maken en met de juiste AWS+ gebruikersnaam-wachtwoord combinatie in te loggen op een AWS+. Deze toegang had gebruikt kunnen worden om gegevens op een niet-Belastingdienstwerkplek te plaatsen.
Er ontbreekt in deze situatie informatie om oneigenlijk gebruik en buiten de Belastingdienst brengen van gegevens daadwerkelijk vast te kunnen stellen.

5 Ondertekening

Ondergetekende verklaart dat dit onderzoek overeenkomstig de daarbij gestelde zorgvuldigheidseisen is uitgevoerd.



21 september 2017



21 september 2017