Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

288

Vragen van het lid **Omtzigt** (CDA) aan de Staatssecretaris van Financiën over *informatiebeveiliging* (ingezonden 18 oktober 2017).

Antwoord van Staatssecretaris **Wiebes** (Financiën) (ontvangen 25 oktober 2017).

Vraag 1
Herinnert u zich dat u op 8 februari 2017 het volgende aan de Kamer schreef: «Naar aanleiding van de signalen over mogelijke onregelmatigheden bij de aanbesteding van de ondersteuning van het programma Broedkamer, heb ik een extern forensisch onderzoek in gang gezet naar deze aanbestedingsprocedure. Bij het uitzetten van de opdracht wordt er op gelet dat de uitvoerende partij onafhankelijk is ten opzichte van alle deelnemers aan de aanbesteding en niet eerder op enigerlei wijze betrokken is geweest.
In het onderzoek zal onder meer aandacht worden besteed aan de rechtmatigheid en ordelijkheid van de aanbestedingsprocedure zelf, aan mogelijke voorkennis over de opdracht bij de leverancier waaraan de opdracht is gegund en mogelijke banden tussen medewerkers van de Belastingdienst en van de gekozen leverancier. Het onderzoek wordt verricht in opdracht van de directeur-generaal Belastingdienst en ondersteund door een begeleidingscommissie. Mocht uit dit onderzoek blijken dat sprake is van een vermoeden van een strafbaar feit, dan zal daarvan aangifte worden gedaan. De onderzoeker wordt verzocht zijn rapport half mei op te leveren»?[1]

Antwoord 1
Ja.

Vraag 2
Wie voert het extern forensisch onderzoek uit? Welke uiterste leveringstermijn is bij de opdrachtverlening gegeven?

Antwoord 2
Het onderzoek wordt uitgevoerd door advocatenkantoor NautaDutilh. In het contract is geen opleverdatum opgenomen, omdat vooraf moeilijk een schatting kon worden gemaakt van de omvang van de met de opdracht gemoeide werkzaamheden. In eerst instantie is aan de onderzoekers

[1] Kamerstuk 31 066, nr. 340

ah-tk-20172018-288
ISSN 0921 - 7398
's-Gravenhage 2017

gevraagd het rapport medio mei op te leveren. Ik heb uw Kamer in april en juni geïnformeerd over het feit dat het onderzoek langer duurt dan voorzien en over de redenen voor de uitloop.[2]

Vraag 3
Heeft u een tussentijdse rapportage ontvangen? Zo ja, kunt u die aan de Kamer doen toekomen?

Antwoord 3
Ik heb geen tussentijdse rapportages ontvangen, omdat dat niet past in het onafhankelijke en forensische karakter van het onderzoek. Periodiek heeft overleg plaatsgevonden tussen NautaDutilh en de begeleidingscommissie over de voortgang van het onderzoeksproces.

Vraag 4
Kunt u de brieven, mails en rapporten die zijn uitgewisseld tussen de onderzoekers en de begeleidingscommissie en anderen bij de rijksoverheid aan de Kamer doen toekomen?

Antwoord 4
Het onafhankelijke onderzoek bevindt zich in een afrondende fase. De onderzoekers leggen de bevindingen vast in een rapportage en geven een verantwoording over het onderzoek, waarin ook zal worden ingegaan op de medewerking van het ministerie en de looptijd van het onderzoek. Zodra ik het rapport heb ontvangen zal ik uw Kamer informeren en het rapport toesturen.

Vraag 5 en 6
Heeft u aangifte gedaan naar aanleiding van tussentijdse signalen? Zo ja, wanneer en tegen wie?
Heeft u naar aanleiding van het onderzoek andere actie ondernomen? Zo ja, welke actie?

Antwoord 5 en 6
Tijdens van het onderzoek naar de aanbestedingsprocedure voor de Broedkamer heb ik geen signalen ontvangen. Of het nodig is om aangifte te doen of andere acties te ondernemen kan daarom ook pas na afronding van het onderzoek worden bepaald.
In mijn brief van 8 februari 2017[3] heb ik aangegeven dat bezien zou worden hoe de checks en balances in het inkoopproces versterkt zouden kunnen worden. Dat heeft geleid tot een aantal maatregelen:
- Er wordt scherper toegezien op mogelijke belangenverstrengeling bij inhuur.
- Er wordt strikt de hand gehouden aan het principe «inhuur stuurt geen inhuur aan».
- Mogelijk kritische dossiers worden altijd door eigen personeel uitgevoerd.
- Inzien door externen van informatie in inkooptrajecten geschiedt alleen op een locatie van de Belastingdienst.

Vraag 7
Kunt u aangeven wat u vindt van het feit dat in de voorlopers van de Broedkamer:
a. belastinggegevens van alle Nederlanders beschikbaar waren;
b. meer dan 40 mensen data met een USB stick konden downloaden en dat de loggegevens daarvan kennelijk niet zijn teruggevonden en onderzocht;
c. alle medewerkers van de Belastingdienst toegang hadden tot de ruimte met die computers;
d. medewerkers gegevens naar buiten konden mailen;
e. in de verslagen geen opvolging aan beveiligingstekortkomingen is gevonden?

---

[2] Kamerstuk31 066, nr. 355, bijlage, blz. 28) en nr. 371 (blz. 35).
[3] Kamerstuk 31 066, nr. 340.

Antwoord 7
Dat belastinggegevens van zeer veel belastingplichtigen beschikbaar waren bij de Broedkamer (waaronder begrepen de voorlopers daarvan) is een direct gevolg van het karakter van dit programma. Het in samenhang analyseren van deze gegevens was de basis voor uit te voeren toezicht op naleving van de belastingwetgeving.
Er waren bij de Broedkamer 18 medewerkers met een USB-ontheffing die ook gebruik maakten van de analyseomgeving AWS, waarin ook persoonsgegevens stonden. Dit waren alleen interne medewerkers. De USB-ontheffingen zijn inmiddels in de hele Belastingdienst ingetrokken en er geldt een zeer stringent beleid voor het verstrekken van nieuwe ontheffingen. Bij de afdeling D&A zijn sinds intrekking in februari 2017 geen ontheffingen meer verleend. Van USB-sticks werd wel gelogd dat zij gebruikt werden, maar niet de inhoud van het dataverkeer.
De servers waarop zich de gegevens bevonden stonden in beveiligde ruimtes die niet voor alle belastingdienstmedewerkers toegankelijk waren. Toegang tot de kantoorruimtes van het programma Broedkamer was voor belastingdienstmedewerkers mogelijk met een Rijkspas.
Dat medewerkers gegevens naar buiten konden mailen vanuit de analyseomgeving was niet conform de beveiligingsvoorschriften van de Belastingdienst. Deze mogelijkheden zijn dan ook afgesloten.
Dat geen besluitvorming is aangetroffen over opvolging van signalen over risico's voor oneigenlijk gebruik of het buiten de Belastingdienst brengen van gegevens past bij de indruk dat bij de Broedkamer sprake was van een werkwijze waarin het resultaat centraal stond en ten koste ging van zorgvuldige omgang met gegevens. Het management heeft hier onvoldoende op gestuurd en ook de technische maatregelen bleken uiteindelijk onvoldoende. Het toont aan dat er niet voldoende aandacht was voor de wijze waarop wordt omgegaan met gegevens. De IT-beveiligingsmuren om de Belastingdienst zijn hoog en stevig, maar daarbinnen moeten het besef van en de concrete maatregelen voor veilig omgaan met gegevens beter. Daarvoor zijn al verschillende maatregelen getroffen, zoals ik in de brieven van 30 juni en 2 oktober 2017 heb aangegeven.[4]

Vraag 8
Kunt u de «bedreigingen- en kwetsbaarhedenanalyse» die is uitgevoerd over de databeveiling bij de voorlopers van de Broedkamer in 2015 aan de Kamer doen toekomen?[5]

Antwoord 8
Het document waar u naar vraagt betreft een intern memo dat is gewisseld tussen ambtenaren. Ik acht het onwenselijk als communicatie tussen ambtenaren onderling onderdeel van het publieke debat wordt. Hiervoor verwijs ik ook naar de kabinetslijn in het kader van artikel 68 van de Grondwet omtrent het verstrekken van inlichtingen staat beschreven in de Kamerbrief van 25 april 2016 van de Minister van BZK[6]. Ik kan u wel in geobjectiveerde vorm kort de strekking van het memo geven. Het memo beoogt alleen een theoretische classificatie te geven van denkbare situaties die de continuïteit en veiligheid van de werkzaamheden van de Broedkamer kunnen bedreigen.
De theoretische classificaties zijn in het memo als volgt beschreven:
Bedreiging: een situatie die een nadelige invloed kan hebben op het betrouwbaar functioneren van (een deel van) de bedrijfsvoering.
Kwetsbaarheid: hoe gevoelig ben je voor de bedreiging, in relatie tot de preventieve maatregelen die je getroffen hebt.
Hoofdsoorten bedreigingen:
- Personeel: bedreigingen die de veiligheid van bezoekers en medewerkers in gevaar kunnen brengen;
- Reputatie: bedreigingen die de reputatie kunnen schaden;
- Continuïteit: bedreigingen die de continuïteit van de processen kunnen verstoren.

---

[4] Kamerstuk 31 066, nrs. 367 en 379.
[5] Bijlage 2 bij Kamerstuk 31 066, nr. 379, paragraaf 4.2.3
[6] Kamerstuk 16, 28 362, nr. 8.

Kans (zonder preventieve maatregelen):
Zeer laag: Kans van optreden gemiddeld eens per 1.000 jaar
Laag: Kans van optreden gemiddeld eens per 100 jaar
Midden: Kans van optreden gemiddeld eens per 10 jaar
Hoog: Kans van optreden gemiddeld eens per 5 jaar
Zeer hoog: Kans van optreden gemiddeld eens per jaar
Kwetsbaarheid niveau (met preventieve maatregelen):
Laag: Kans dat ernstige schade geleden wordt is minder dan 25%
Midden: Kans dat ernstige schade geleden wordt ligt tussen 25% en 50%
Hoog: Kans dat ernstige schade geleden wordt is groter dan 50%
Het memo bevat niet de uitkomst van een analyse van de feitelijke bedreigingen en kwetsbaarheden van de Broedkamer. Ter illustratie is een overzicht van denkbare situaties bijgevoegd.

Vraag 9
Kunt u het rapport «investigating data streams» van Oliver Wyman uit 2015 aan de Kamer doen toekomen? Kunt u een reactie geven op de bevindingen daarin en de opvolging die daaraan is gegeven?

Antwoord 9
De onderzoekers concluderen dat de aanbevelingen in de onderzochte periode niet zijn opgevolgd in formele besluiten. Dat is de periode daarna, in juni 2016, wel gebeurd. In lijn met de hoofdaanbevelingen in het rapport heeft de toenmalige Raad van Bestuur van de Belastingdienst in juni 2016 besloten een Datamanagement Forum in te richten bij de Belastingdienst, met als opdracht om integraal datamanagement vorm te geven. Eind 2016 is dit van start gegaan. Binnen de structuur van het Forum worden operationele en beleidsmatige kwesties rond gebruik van gegevens behandeld. De eerste resultaten daarvan zijn de ontwikkeling van een beleidsvisie op het omgaan met gegevens en het oplossen van een aantal concrete operationele kwesties rond gebruik van gegevens.
De activiteiten die in het kader van het Datamanagement Forum worden verricht, krijgen een plaats in de nieuwe structuur van de Belastingdienst. Datamanagement (waarvan informatiebeveiliging onderdeel uitmaakt) wordt in alle lagen van de Belastingdienst doorgevoerd: in strategie, uitvoering en control.
Gelet op de aard van dit rapport en de mogelijke risico's van brede verspreiding, stuur ik het gehele rapport nu ter vertrouwelijke inzage aan de Kamer[7]. Ik streef ernaar u voorafgaand aan het Algemeen Overleg op woensdag 25 oktober een openbare[8] versie te sturen waarin de vertrouwelijke passages onzichtbaar gemaakt zijn.

Vraag 10 en 13
Kunt u een appreciatie geven bij elk van de bevindingen van «het Rapport van bevindingen onderzoek informatiebeveiliging programma Broedkamer en voorlopers»?
Kunt u een appreciatie geven van elk van de bevindingen in het «Rapport van bevindingen onderzoek gegevensgebruik D&A»?

Antwoord 10 en 13
De appreciatie van de bevindingen uit de twee onderzoeken heb ik gegeven in de brief van 2 oktober 2017.

Vraag 11 en 15
Van welke datalekken die zijn geconstateerd, is aangifte gedaan bij de autoriteitspersoonsgegevens? Kunt u per geconstateerde datalek bij de Broedkamer en haar voorgangers sinds 2012 aangeven wanneer die geconstateerd is, wanneer er aangifte is gedaan of waarom er geen aangifte is gedaan?
Van welke datalekken die zijn geconstateerd is aangifte gedaan bij de Autoriteit Persoonsgegevens? Kunt u per geconstateerd datalek bij de

[7] Ter vertrouwelijke inzage gelegd, alleen voor de leden, bij het Centraal Informatiepunt Tweede Kamer
[8] Aanhangsel Handelingen, vergaderjaar 2017–2018, nr. 290

Broedkamer en haar voorgangers sinds 2012 aangeven wanneer die geconstateerd is, wanneer er aangifte is gedaan of waarom er geen aangifte is gedaan?

Antwoord 11 en 15
Over de periode van de Broedkamer is één geval geconstateerd waarin gegevens via e-mail buiten de Belastingdienst zijn gebracht. Dit geval is niet gemeld bij de Autoriteit Persoonsgegevens, omdat hierbij geen sprake was van persoonsgegevens maar van gegevens van bedrijven, zonder vermelding van de bedrijfsnaam.
Ik neem aan dat in vraag 15 wordt gedoeld op de periode van de afdeling D&A. Op 2 februari 2017 is bij de Autoriteit Persoonsgegevens melding gemaakt van een vermoedelijk datalek op grond van de mededeling van het programma Zembla dat het beschikte over een USB-stick met een groot aantal documenten. Op 29 juni 2017 is bij de Autoriteit Persoonsgegevens melding gemaakt van 11 incidenten die mogelijk als datalek te kwalificeren waren. Deze melding is gedaan op grond van tussentijdse bevindingen in het onderzoek naar gegevensgebruik bij D&A.

Vraag 12 en 14
Welke maatregelen zijn er genomen tegen de medewerkers van de Belastingdienst die via bankrekeningnummers gegevens van belastingplichtigen en gegevens van VIP's hebben opgevraagd?[9]
Hoe vaak hebben medewerkers gezocht naar de gegevens van individuele belastingplichtigen? Welke acties zijn ondernomen tegen deze medewerkers?

Antwoord 12 en 14
In de onderzoeksrapporten wordt een aantal gevallen genoemd waar mogelijk sprake was van niet-functionele gegevensopvragingen. Deze zijn vervolgens nader onderzocht. Bij deze nadere analyse zijn geen indicaties gevonden dat de persoonsgegevens niet functioneel zijn gebruikt. Er zijn om die reden geen maatregelen getroffen tegen de desbetreffende medewerkers.

Vraag 16
Kunt u een overzicht geven van de signalen die klokkenluiders gegeven hebben over de beveiliging van de gegevens bij de Broedkamer en haar voorlopers en wat er met deze signalen gebeurd is?

Antwoord 16
In het onderzoek naar gegevensgebruik bij de Broedkamer en voorlopers hebben de onderzoekers signalen over risico's en feiten ten aanzien van het daadwerkelijk oneigenlijk gegevensgebruik of het buiten de Belastingdienst brengen van gegevens geïnventariseerd. Zij hebben zich gericht op drie typen bronnen. Het eerste type betrof memo's en mailberichten. Hierin werden vier signalen aangetroffen over vermeend onveilige hardware en vermeende aanschaf van hardware buiten de gebruikelijke inkoopprocedure. Het tweede type betrof twee rapporten van Oliver Wyman en Liquid Hub waarin adviezen en randvoorwaarden voor inrichting van de Broedkamer waren opgenomen; deze adviezen gingen ook over de beveiliging. Er is in de periode waarover het onderzoek zich uitstrekt geen formele besluitvorming aangetroffen over maatregelen naar aanleiding van de signalen uit deze twee typenbronnen. Over het rapport van Oliver Wyman heeft buiten de onderzoeksperiode wel besluitvorming plaatsgevonden (zie het antwoord op vraag[10].
Het derde type betrof het logboek van beveiligingsincidenten. Bij analyse van dit logboek zijn door de onderzoekers geen incidenten aangetroffen die het buiten de Belastingdienst brengen van gegevens betroffen.
Overigens is nooit met zekerheid te zeggen dat een dergelijk overzicht volledig is, omdat men uiteraard geen kennis kan hebben van wat men niet gezien heeft.

[9] Bijlage 2 bij Kamerstuk 31 066, nr. 379, paragraaf 4.5.3
[10] bijlage 2 bij Kamerstuk 31 066, nr. 379, paragraaf 4.5.3

Vraag 17
Waarom verklaarde u in de Kamer dat er actief gemonitord is, terwijl uit de onderzoeken blijkt dat er in het geheel geen monitoring heeft plaatsgevonden?

Antwoord 17
Zoals ik in mijn brief van 2 oktober 2017 heb aangegeven, heeft wel monitoring plaatsgevonden, maar deze was dominant gericht op de continuïteit in de bedrijfsvoering en op monitoring van kwaadaardige invloeden van buiten naar binnen. Monitoring van e-mailverkeer op het buiten de Belastingdienst brengen van persoonsgegevens vond niet systematisch plaats.

Vraag 18
Kunt u deze vragen een voor een beantwoorden en voor dinsdag 24 oktober 2017 te 11 uur aan de Kamer doen toekomen?

Antwoord 18
Dit is helaas niet gelukt.

Nr.	Bedreiging	Toelichting
1	**Geen aanlevering van data**	**Of geen juiste, tijdige of volledige aanlevering**
2	Menselijke fouten	Bij aanlevering Bij verwerking door D&A Onopzettelijk en opzettelijk
3	Single points of knowledge (SPOK's)	
4	**Beschikbaarheid infra (verbindingen)**	**Internet eruit Apeldoorn eruit Software niet beschikbaar**
5	**SNO's sluiten niet aan bij actuele situatie**	**De processen bij D&A worden niet gezien als primaire processen, terwijl er inmiddels producten van D&A een essentieel onderdeel van het primaire proces zijn**
6	De bijdrage van D&A aan het primaire proces is niet voldoende inzichtelijk	
7	**Wijzigingen in transactiesystemen komen niet door Nieuwe systemen komen niet door (D&A zit niet aan de ontwerptafel)**	**Wijzigingen of nieuwbouw in het primaire proces kan invloed hebben op de producten van D&A.**
8	Niet alles wordt goed vastgelegd in procesplaten	
9	Grote uitval van personeel	
10	**Data lekkage**	**Onopzettelijk en opzettelijk Buitenstaander of medewerker (intern en extern)**
11	Geen hardware beschikbaar	Bv na een ontruiming waarbij je je laptop niet meer kunt meenemen en het pand langere tijd niet beschikbaar is
12	Uitval van gebouw	
13	Prioritering bij crisis	Dit heeft weer een relatie met nummer 5 en 6
14	Geen deelname aan damagetafels	Dit heeft weer een relatie met nummer 5, 6 en 13
15	Rationalisatie	Met als doel om de bronsystemen te rationaliseren. Dit kan betekenen dat de brondata in hoge mate gewijzigd gaat worden en wij dus onze datafundamenten moeten herzien.
16	Ontbreken van aandacht voor producten van D&A in de MTHV's	
17	Onbekendheid van D&A bij o.a. IM	
18	**Privacy (intern en extern)**	**De rechtmatigheid van het gebruik van gegevens geen betrokkenheid van vaktechniek**