Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

31 066 Belastingdienst

Nr. 1271 **BRIEF VAN DE STAATSSECRETARIS VAN FINANCIËN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 juli 2023

In oktober 2022 meldt de NRC dat het doen van onderzoek naar mogelijke corruptie binnen de Belastingdienst bemoeilijkt wordt vanwege technische beperkingen[1]. Het zou niet te achterhalen zijn of medewerkers vertrouwelijke (persoons)gegevens buiten het doel van hun werkzaamheden hebben geraadpleegd en hebben gedeeld met het criminele milieu. Tijdens de regeling van werkzaamheden van 11 oktober jl. heeft het lid Azarkan (DENK) verzocht om een brief over monitoring en logging bij de Belastingdienst (Handelingen II 2022/23, nr. 10, item 16).

Uit voorgedane gevallen van corruptie blijkt dat Nederland niet immuun is voor corruptie. Eveneens is uit recentelijke strafrechtelijke onderzoeken gebleken dat corrupte ambtenaren in een aantal gevallen te linken zijn aan de georganiseerde criminaliteit[2]. Casussen zoals bij de Belastingdienst hebben laten zien dat het herkennen van corruptiesignalen bij overheidsorganisaties moet worden ontwikkeld, vergroot en geborgd.

De georganiseerde criminaliteit gedijt niet zonder corruptie. De overheid beschikt over veel kwetsbare en gevoelige gegevens en is daarmee ongewild een potentiële facilitator van de misdaad. Iedere overheidsorganisatie moet zich bewust zijn van hun aantrekkelijkheid voor criminelen en daar maatregelen tegen nemen. Ieder departement en iedere organisatie is zelf verantwoordelijk voor het nemen van voldoende preventieve maatregelen om corruptie tegen te gaan. Indien er gekozen wordt om gegevens van een groep mensen met een kwetsbaar beroep af te schermen, zal dit al bij de bronregistratie gedaan moeten worden. Het gaat om beroepen waar gewerkt wordt met fiscale- en persoonsgegevens die burgers in gevaar kunnen brengen als deze in handen komen van criminelen. Door rijksbreed met afgeschermde gegevens te werken, is het voor criminele informatiemakelaars minder makkelijk gegevens te kopen om bijvoorbeeld Belastingdienstmedewerkers om te kopen en af te persen

[1] Gegevens van Belastingdienst zijn goudmijn voor criminelen (NRC, oktober 2022)
[2] Gegevens van Belastingdienst zijn goudmijn voor criminelen (NRC, oktober 2022)

kst-31066-1271
ISSN 0921 - 7371
's-Gravenhage 2023

omdat minder mensen toegang hebben tot deze gegevens. Met een hoge prioriteit onderzoekt het Ministerie van Justitie en Veiligheid samen met het Ministerie van Binnenlandse Zaken mogelijkheden om (bron)gegevens nog beter af te schermen.

Met deze brief informeer ik, mede namens de Minister van Justitie en Veiligheid, uw Kamer over de verbeter- en beheersmaatregelen van de Belastingdienst in het kader van weerbaarheid van medewerkers tegen ondermijnende criminaliteit.

Programma weerbaarheid Belastingdienst

Ik neem als Staatssecretaris Fiscaliteit en Belastingdienst de signalen rondom corruptie en ondermijnende criminaliteit bij de Belastingdienst zeer serieus. Mede naar aanleiding van gevallen van (mogelijke) corruptie en ondermijning binnen de Belastingdienst is de Belastingdienst in november jl. gestart met het programma *«Weerbaarheid tegen ondermijnende criminaliteit»*. Het doel van het programma is om de Belastingdienst(medewerkers) weerbaarder te maken tegen corruptie, ondermijnende criminaliteit en infiltratie. Dit programma bouwt voort op bestaande acties bij de Belastingdienst om medewerkers bewust te maken van de risico's van ondermijning. Binnen het programma zijn themagewijs, onder andere in samenwerking met het Ministerie van Justitie en Veiligheid, (verbeter)acties geïdentificeerd. Deze gestarte en in een aantal gevallen afgeronde acties licht ik hieronder per thema toe.

Thema 1 «Bewustwording ondermijningsrisico's»

Dit thema heeft als doel om Belastingdienstmedewerkers bewust te maken van de risico's die bestaan bij het werken met kwetsbare gegevens. Dit wordt gedaan door, naast de bestaande opleidingen, drie nieuwe opleidingen aan te bieden en via een bewustwordingscampagne met het Centraal Meldpunt Agressie (CMA) van het Ministerie van Financiën. Vanaf het derde kwartaal 2023 wordt voor alle medewerkers de training weerbaarheid beschikbaar. Voor bepaalde functiegroepen binnen de Belastingdienst, die met gevoelige gegevens werken, is deze training verplicht om te volgen. In deze training wordt geleerd hoe je ondermijning kan herkennen en hoe je er mee om moet gaan. Vanaf het derde kwartaal van 2023 kan ook de onlinetraining «wanneer je benaderd wordt» gevolgd worden. En managers worden opgeleid hoe zij op de werkvloer het gesprek met medewerkers over ondermijningrisico's aan kunnen gaan. Het eerstvolgende level van de online security awareness game, dat sinds 2022 verplicht is voor alle Belastingdienstmedewerkers, is «diamant» waar specifiek aandacht is voor ondermijning(srisico's).

In samenwerking met het Centraal Meldpunt Agressie (CMA) is in het eerste kwartaal van dit jaar een bewustzijnscampagne voor Belastingdienstmedewerkers gestart om agressie te melden en is een standaard protocol ontwikkeld voor meldingen over ondermijning met daarbij een voorziening om 24-uurs opvolging van deze meldingen mogelijk te maken. Naast deze voorziening heeft de Belastingdienst een uitgebreid meld- en advieslandschap (o.a. vertrouwenspersonen, (externe) meldpunten) die medewerkers en leidinggevenden begeleiden en ondersteunen bij het melden van integriteitskwesties en/of het bespreken van dilemma's.

Thema 2 «Toegang tot Belastingdienst-werkomgeving en (IT)-voorzieningen»

Dit thema heeft als doel om de kantoren en systemen van de Belastingdienst zo moeilijk mogelijk toegankelijk te maken voor onbevoegden en medewerkers de middelen te bieden om dit te voorkomen. Vanaf het tweede kwartaal van dit jaar is de bewustzijnscampagne op fysieke beveiliging in uitvoering wat aandacht vraagt voor het bestaande fysieke veiligheidsbeleid. Onderdeel hiervan is onder andere de campagne «zichtbaar dragen Rijkspas», net als de inzet van hologram machines die veiligheidsmaatregelen uitleggen. Daarnaast wordt de fysieke beveiliging regelmatig getest via penetratietesten. De bevindingen hieruit hebben aanleiding gegeven om een aanvullend verbeterprogramma in te zetten. Dit verbeterprogramma betreft zowel bewustzijns- als fysieke maatregelen.

De Belastingdienst houdt toezicht en handhaaft de belastingwetten en streeft ernaar om dit dienstverlenend te doen. Om plaatsonafhankelijk te kunnen werken binnen de Belastingdienst zijn autorisaties in het verleden ruim toegewezen aan medewerkers om daarmee de dienstverlening te borgen. Vanwege het veranderde dreigingsbeeld, is het niet meer wenselijk om autorisaties ruim toe te kennen. Om te zorgen dat medewerkers alleen toegang hebben tot de gegevens die zij daadwerkelijk nodig hebben, zijn overbodige autorisaties ingetrokken. Ook zijn de richtlijnen van het autorisatiebeheer herijkt. Periodiek wordt getoetst of het beheer juist toegepast is. De verouderde informatiesystemen van de Belastingdienst zijn niet altijd ingericht conform de huidige standaarden voor deze systemen. Daarom is in een deel van de verouderde informatiesystemen additionele log- en monitorsoftware ingebouwd.

Thema 3 «Weten met wie je werkt»

Dit thema heeft als doel om Belastingdienstmedewerkers erop te kunnen laten vertrouwen dat zij in een veilige (zonder dat sprake is van criminele invloeden) omgeving werken. Onderzocht wordt of versterking van screeningsmogelijkheden en het uitbreiden van vertrouwensfuncties waar gewerkt wordt met gevoelige informatie kan bijdragen aan het verwezenlijken van deze doelstelling. Bij elke vorm van versterking van de screening is vereist dat per functie gemotiveerd wordt waarom de maatregel gerechtvaardigd en proportioneel is in relatie tot de te ondervangen kwetsbaarheid.

Het Ministerie van Financiën heeft een project voor het aanwijzen van kwetsbare functies gestart. Kwetsbare functies zijn functies waar gewerkt wordt met fiscale- en persoonsgegevens die andere burgers in gevaar kunnen brengen als deze in handen komen van criminelen. Dit kunnen functies zijn die kwetsbaar zijn voor o.a. ondermijning, waarbij het kan gaan om zowel bedreiging als verleiding. Er is met behulp van TNO een tool in ontwikkeling op wetenschappelijke basis om deze functies te toetsen op kwetsbaarheid. Op basis hiervan worden preventieve maatregelen getroffen.

Screeningsmogelijkheden

Het versterken van de screeningsmogelijkheden bij kwetsbare functies kan bijvoorbeeld via een Verklaring Omtrent Gedrag Politiegegevens (VOG P). Een VOG P is een VOG, waarbij naast justitiële documentatie (strafblad) ook altijd politiegegevens worden geraadpleegd. En waarbij deze politiegegevens op zichzelf doorslaggevend kunnen zijn voor de weigering van de VOG. Ook als de aanvrager geen strafblad heeft. Het is

voor de Belastingdienst nu nog niet mogelijk om voor een aangewezen groep (functies) een VOG P op te laten vragen. Het opvragen van een VOG P kan alleen voor de door de Minister voor Rechtsbescherming aangewezen werkgevers en functies in de «Regeling aanwijzing functies VOG Politiegegevens». Volgens de in de Wet veiligheidsonderzoek verankerde «sluitstukgedachte» is versterking van de screening aan de orde na implementatie van alle in redelijkheid te nemen beveiligingsmaatregelen.

Onderzoek KPMG

De Belastingdienst heeft, na een minicompetitie, KPMG opdracht gegeven om de (mogelijke) kwetsbaarheden omtrent corruptie en ongewenste invloeden van derden te actualiseren en om te toetsen hoe de bedrijfs- en werkprocessen van de Belastingdienst beter beschermd kunnen worden tegen deze kwetsbaarheden. Daarnaast wordt via dit onderzoek ook het risico- en dreigingsbeeld van ondermijning binnen de Belastingdienst geactualiseerd en een vervolgaanpak voorgesteld. Het onderzoek wordt uitgevoerd naar voorbeeld van Douane om de beheersing van de corruptierisico's te vergroten[3]. Ik verwacht de resultaten van dit onderzoek in november 2023 en zal uw Kamer daarover informeren.

Thema 4 «Leren van anderen en versterken van het netwerk in weerbaarheid tegen ondermijning»

Dit thema heeft als doel om te leren van overheidsorganisaties die met dezelfde risico's te maken hebben en daar beheersmaatregelen op hebben ontwikkeld. Naast de al bestaande overleggen op het gebied van cyber security en digitale weerbaarheid met onder andere het Nationaal Cyber Security Centrum en het Chief Information Office beraad is ook regulier overleg met de Rijksrecherche.

Recente casussen onderstrepen de noodzaak om ons nadrukkelijk bewust te zijn van corruptie en integriteitsrisico's binnen overheidsorganen. De Minister van Justitie en Veiligheid, verantwoordelijke voor de strafrechtelijke aanpak van corruptie, en de Minister van Binnenlandse Zaken en Koninkrijksrelaties, verantwoordelijke voor het rijksbrede integriteitsbeleid hebben dit onderwerp daarom, conform de toezegging tijdens de begrotingsbehandeling van het Ministerie van Justitie en Veiligheid van 17 november 2022,[4] geagendeerd bij de Ministeriële Commissie Aanpak Ondermijning.

Over de voortgang en uitkomsten wordt uw Kamer in de ondermijningsbrief die halfjaarlijks wordt opgesteld door het Ministerie van Justitie en Veiligheid geïnformeerd.

De Staatssecretaris van Financiën,
M.L.A. van Rij

[3] Kamerstuk 31 934, nr. 55
[4] Handelingen II 2022/23, nr. 24, items 6 en 11.