Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

26 643 Informatie- en communicatietechnologie (ICT)

17 050 Misbruik en oneigenlijk gebruik op het gebied van belastingen, sociale zekerheid en subsidies

Nr. 309 **BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE**

Den Haag, 3 maart 2014

Naar aanleiding van berichten in pers (De Telegraaf digitaal d.d. 21 en 23 januari 2014) over toegenomen internetfraude en fraude met behulp van ID-bewijzen verzocht uw Kamer om schriftelijke informatie. Naar aanleiding daarvan bericht ik u mede namens de Staatssecretaris van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties het volgende.

In mijn brief van 20 december 2013 (Kamerstuk 17 050, nr. 450) wordt Rijksbrede aanpak van fraude uiteengezet. Deze aanpak hangt samen met de integrale Kabinetsvisie op de aanpak van identiteitsfraude, met als motto «slim voorkomen, vlot herstellen», waarover de Minister van Binnenlandse Zaken en Koninkrijksrelaties u bij brief van eveneens 20 december 2013 heeft geïnformeerd (Kamerstuk 26 643, nr. 301). Waar eerstgenoemde brief zich vooral richt op de aanpak van fraude met publieke middelen (de zogenaamde verticale fraude), gaat de brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties vooral in op de aanpak van identiteitsfraude als modus operandi bij veel verschillende vormen van illegale en criminele activiteiten die zich onder meer uiten in fraude met publieke middelen. Gezien de samenhang tussen identiteitsfraude als werkwijze en internetfraude behandel ik beide onderwerpen in deze brief.

Voor de uitvoering van de in beide brieven van 20 december 2013 aangegeven maatregelen werken de betrokken Ministeries samen in een rijksbrede anti-fraudestrategie. Beide brieven mogen duidelijk maken dat fraude, in welke vorm dan ook, serieuze aandacht heeft van het Kabinet.

Rijksbrede anti-fraudestrategie

De recente ervaringen met fraude met diverse regelingen op het gebied van individuele inkomensoverdrachten en subsidies, gecombineerd met het inzicht dat een sluitende aanpak ervan alleen in gezamenlijkheid kan worden gerealiseerd, heeft geleid tot de ontwikkeling van een rijksbrede

kst-26643-309
ISSN 0921 - 7371
's-Gravenhage 2014

anti-fraudestrategie. Door middel van risico-analyses is op de belangrijkste beleidsdomeinen van de Rijksoverheid in beeld gebracht welke aanvullende maatregelen nodig zijn. De focus van de in mijn brief van 20 december 2013 gepresenteerde Rijksbrede aanpak ligt op fraude met publieke middelen. Tegelijkertijd versterkt een groot aantal van de maatregelen tegen deze categorie van fraude ook de aanpak van fraude tegen burgers en bedrijfsleven (de zogenaamde horizontale fraude). De aanpak richt zich immers voor een belangrijk deel op het wegnemen van het instrumentarium van fraudeurs en het weren van beroepsfraudeurs. Deze categorie criminelen maakt geen onderscheid tussen publieke of private gelden. Ik beperk mijn aandacht dan ook niet tot fraude met publieke middelen, maar besteed – zoals ik in mijn brief van 20 december heb aangegeven – ook aandacht aan horizontale fraude. In dit verband kan ik u melden dat voor 2014 tussen het Openbaar Ministerie en de politie per eenheid kwantitatieve afspraken zijn gemaakt voor de aanpak van horizontale fraude. Landelijk worden ten minste 1.500 zaken aangepakt. In het kader van deze brief is het relevant te melden dat binnen die kwantitatieve afspraken, fraude tegen financiële instellingen en internet gerelateerde fraude nadrukkelijk aandacht hebben. Voor de periode 2015–2018 worden nieuwe afspraken gemaakt.

Identiteitsfraude

In zijn brief van 20 december 2013 heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties reeds aangegeven, dat zowel de overheid als private partijen permanent samenwerken aan verbeteringen van hun identiteitsinfrastructuren en het beheer en gebruik ervan. Tegenover hen staan fraudeurs, die met steeds geraffineerdere methoden kwetsbare plekken in de identiteitsinfrastructuren vinden. Aan beide zijden worden steeds nieuwe methoden en technieken ontwikkeld en toegepast; bedreiging en beveiliging zijn in een permanente wedloop met elkaar verwikkeld. Identiteitsfraudeurs en de «facilitators» die hen bedienen zijn doorgaans goed geïnformeerd, innovatief en technisch competent. Ze opereren als criminele organisaties over landsgrenzen heen, waarbij zij het verrassingselement aan hun zijde hebben: de keuze waar, hoe en wanneer ze toeslaan. Als de preventie of opsporing op één plek wordt versterkt, wijzigen ze makkelijk van aanvalsstrategie.
Gelukkig komt identiteitsfraude steeds beter in beeld, nemen veel organisaties en sectoren maatregelen en is er een ontwikkeling gaande richting meer samenwerking. Zo nemen banken maatregelen tegen skimming en phishing om te voorkomen dat derden onrechtmatig gebruik maken van de identificerende persoonsgegevens van hun cliënten. Uiteraard zal ook de cliënt alert moeten blijven op mogelijk misbruik van zijn gegevens. Preventie en weerbaarheid tegen misbruik zijn in de eerste plaats een verantwoordelijkheid van consumenten en bedrijven zelf. Volgens berichtgeving in de pers (De Telegraaf digitaal d.d. 23 januari 2014) heeft de politie mensen die aangifte hebben gedaan van fraude en nog geen vervangend ID-bewijs hebben het advies gegeven om een tweede, vervangend identiteitsbewijs mee te nemen. De politie heeft dit advies bedoeld voor mensen die naar het buitenland reizen en hun identiteitsbewijs kwijt raken waardoor zij zich niet meer kunnen legitimeren. Burgers die te maken hebben met diefstal en verlies van hun identiteitsbewijs, al dan niet gepaard gaande met misbruik van hun identiteit door derden, zijn niet ontslagen van de wettelijke plicht zich op vordering van een bevoegde autoriteit te kunnen identificeren. Een paspoort, ID-kaart en rijbewijs voldoen in het algemeen aan de eisen om zich rechtsgeldig te kunnen identificeren, al is in verschillende bijzondere wetten opgenomen dat identificatie niet met een rijbewijs mag plaatsvinden.

Het tonen van een van deze drie documenten hoeft voor de meeste burgers in het algemeen geen probleem zijn. Ingeval aangifte is gedaan van diefstal zal bij controle kunnen worden volstaan met het tonen van het bewijs van aangifte.

De politie heeft een Handreiking Identiteitsfraude opgesteld om de politiefunctionaris te helpen bij het benutten van het huidige wettelijk instrumentarium bij het opnemen van de aangifte van misbruik van identificerende persoonsgegevens. Het onderliggende delict is meestal te kwalificeren als valsheid in geschrifte, oplichting en diefstal van gegevens. Momenteel is bij de Eerste Kamer een wetsvoorstel in behandeling dat tot doel heeft de mogelijkheden tot repressieve bestrijding van fraude met identificerende persoonsgegevens, biometrische gegevens en identiteitsbewijzen te verruimen (Kamerstuk 33 352, A). Misbruik van identificerende persoonsgegevens wordt bijvoorbeeld strafbaar gesteld als strafbaar feit. Overtreding van deze nieuwe bepaling wordt in het wetsvoorstel bedreigd met een gevangenisstraf van maximaal 5 jaar. De handreiking ID-fraude van de politie zal hierop worden aangepast en onder de aandacht van de uitvoerende functionarissen worden gebracht.

Op initiatief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties worden er voortdurend maatregelen genomen die de mogelijkheden tot frauderen met identificerende persoonsgegevens tegengaan. Daarmee wordt invulling gegeven aan (technische) veiligheidskenmerken die deels internationaal zijn voorgeschreven.

Daarnaast worden voorzieningen getroffen die burgers de mogelijkheid geven om hun identiteitsdocumenten, pasjes en digitale identiteiten onmiddellijk te blokkeren en instanties op te roepen tot verhoogde alertheid op hun gegevens. Ook moet online verifieerbaar zijn welke identiteitsdocumenten geldig en welke ongeldig zijn. Met deze instrumenten kunnen burgers zelf een bijdrage leveren om identiteitsfraude te voorkomen. CheckID en StopID zijn de instrumenten die momenteel worden ontwikkeld om deze doelstellingen te realiseren.

CheckID wordt een website waarop bedrijven, overheden en particulieren in binnen- en buitenland kunnen controleren of een Nederlands paspoort of identiteitskaart nog in omloop mogen zijn. Een document dat als gestolen of vermist is geregistreerd, levert bij bevraging een «hit» op. Op die manier kan op eenvoudige wijze worden voorkomen dat fraudeurs met gestolen of vermiste documenten transacties sluiten. Op die manier wordt een bijdrage geleverd aan het voorkomen van fraude met identificerende persoonsgegevens.

StopID wordt ook een online voorziening. Hiermee kunnen houders van Nederlandse paspoorten en identiteitskaarten bij verlies, diefstal of (vermoedens van) misbruik hun document direct blokkeren. Het nummer van het vermiste document wordt dan geregistreerd in nationale en internationale registers. Ook is dan via CheckID te raadplegen dat het document niet meer geldig is.

Het Centraal Meldpunt Identiteitsfraude (CMI) is bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties ingesteld om burgers de mogelijkheid te bieden om gevallen van fraude met identificerende persoonsgegevens te melden. Waar mogelijk staat het CMI hen met raad en daad ter zijde en treedt het CMI in overleg met de betrokken organisaties.

Daarnaast wordt door opsporingsfunctionarissen gebruik gemaakt van het Expertise Centrum Identiteitsfraude en Documenten van de Koninklijke

Marechaussee (ECID), dat verantwoordelijk is voor de inhoud van de internationale database Edison TD, waarin de echtheidskenmerken staan van meer dan 4.000 reis- en verblijfsdocumenten uit 200 landen. Het ECID maakt ook gebruik van False and Authentic Documents Online (FADO). FADO is een door de EU ontwikkeld elektronisch naslagwerk m.b.t. de reisdocumenten van de EU.

De aanpak van identiteitsfraude is een van de gemeenschappelijke projecten en programma's die in het kader van de rijksbrede aanpak van fraude worden uitgevoerd. De Minister van Binnenlandse Zaken en koninkrijksrelaties werkt de Kabinetsvisie de komende tijd uit in een projectplan Aanpak Identiteitsfraude. De activiteiten hiervan maken deel uit van de kabinetsbrede uitvoeringsagenda aanpak fraude.

Internetfraude

Naar aanleiding van de door uw Kamer gevraagde reactie op het bericht in de pers (noot: De Telegraaf digitaal d.d. 21 januari 2014) dat internetfraude toeneemt merk ik het volgende op.
Het vrije verkeer op het internet biedt vele mogelijkheden om zonder direct fysiek persoonlijk contact relaties aan te gaan, contracten te sluiten en betalingen te verrichten. Daar zijn zowel voor- als nadelen aan verbonden. Het is in de eerste plaats de verantwoordelijkheid van degene die – soms ongevraagd – wordt benaderd via het internet om zich ervan te vergewissen met wie hij of zij te doen heeft en bij twijfel het contact te verbreken.

Ik interpreteer het begrip internetfraude als fraude die wordt gepleegd met behulp van het dataverkeer via het internet. Het internet wordt als middel gebruikt voor bijvoorbeeld voorschotfraude, datingfraude en acquisitiefraude (dit zijn enkele vormen van zogenaamde horizontale fraude). In die gevallen wordt het slachtoffer met een persoonlijke benadering via het internet onder valse voorwendselen overgehaald om een contract te sluiten of een bedrag al dan niet als voorschot over te maken op een bankrekeningnummer van – naar later blijkt – soms fictieve personen, zonder dat daar een prestatie tegenover staat. De emotionele schade is in gevallen van fraude minstens zo groot als de financiële schade. In veel gevallen heeft het slachtoffer civielrechtelijke mogelijkheden om de schade te verhalen. Minderdraagkrachtigen kunnen daartoe het Juridisch Loket benaderen en indien zij daarvoor in aanmerking komen op grond van de Wet op de rechtsbijstand gebruik maken van een toegevoegd advocaat.

Daarnaast kan het slachtoffer aangifte doen als er sprake is van een misdrijf, zoals oplichting en diefstal. In juli 2013 heb ik uw Kamer geïnformeerd over de verbeterde werkwijze van de politie ten aanzien van het opnemen van aangiften. Dat laat onverlet, dat als geen sprake is van een strafbaar feit het doen van aangifte geen zin heeft.
In mijn brief van 20 december 2013 heb ik aangegeven dat in het Inrichtingsplan van de Nationale Politie een totale capaciteit voor financieel-economische criminaliteit is voorzien van 1.156 fte.
Ter bevordering van de kennis bij de politie is in 2012 in mijn opdracht de bundel «Alledaags politiewerk in en gedigitaliseerde wereld» tot stand komen als handreiking voor de behandeling van delicten met een digitale component. Deze bundel bevat onder meer een uitgebreid uiteenzetting over de verschillende vormen van criminaliteit met een financieel oogmerk, waarbij gebruik wordt gemaakt van het internet. Speciale aandacht wordt gegeven aan het opnemen van aangiften. Het landelijk Meldpunt Internet Oplichting (dat is te bereiken via www.mijnpolitie.nl) is het mogelijk aangifte te doen, aangifte in te zien en te controleren of er

meldingen over een verkoper zijn gedaan. Tevens bevat de website tips voor veilig handelen.

Daarnaast kunnen slachtoffers terecht bij de Fraudehelpdesk, die zich richt op intensieve samenwerking met bedrijfsleven en strafrechtelijke en bestuursrechtelijke handhavers, met als doel (potentiële) slachtoffers zo goed mogelijk te informeren en te verwijzen. Deze benadering van slachtoffers draagt bij aan een grotere aangiftebereid. De website van de Fraudehelpdesk is inmiddels een miljoen keer bezocht. Ongeveer 70.000 meldingen van oplichting zijn geregistreerd. Ik verwacht dat de Fraudehelpdesk hiermee bijdraagt aan een vergroting van het bewustzijn bij burgers en bedrijven van de risico's op fraude.

Slachtoffers van fraude kunnen, zoals alle slachtoffers van criminaliteit, bij Slachtofferhulp Nederland terecht voor juridische, praktische en psychosociale ondersteuning. De slachtoffers die Slachtofferhulp Nederland ondersteunt zijn zowel slachtoffers van babbeltrucs, van pinpasfraude, identiteitsfraude als van beleggingsfraude en piramidespelen. Slachtoffers kunnen in psychische problemen komen door de financiële situatie waarin ze zijn beland. Maar ook het vertrouwen van slachtoffers kan ingrijpend zijn geschaad. En met name mensen die slachtoffer zijn geworden aan de deur of in huis kunnen hierdoor gevoelens van onveiligheid ontwikkelen. Een deel van deze slachtoffers zijn kwetsbare mensen: door hun leeftijd, hun beperkte verstandelijke vermogens of hun beperkte sociale netwerk.

Op 10 februari is een wetsvoorstel (noot: wetsvoorstel implementatie richtlijn 2013/40/EU over aanvallen op informatiesystemen) in consultatie gegeven, dat moet leiden tot strafbaarstelling van het vernielen, computersystemen ontoegankelijk maken door aan wachtwoorden te sleutelen of computers bestoken met spam. Criminelen kunnen hiervoor straks een gevangenisstraf van maximaal twee jaar tegemoet zien. Nu is dat nog één jaar. Wanneer zij deze delicten plegen met behulp van een zogeheten «botnet» wordt de maximumstraf drie jaar. Brengt een computerdelict ernstige schade toe of richt het zich tegen een vitale infrastructuur – bijvoorbeeld een overheidsnetwerk of energiecentrale – dan wordt de maximale gevangenisstraf vijf jaar. Het wetsvoorstel sluit aan bij een eerder wetsvoorstel dat de opsporing en vervolging van cybercrime verbetert en versterkt.

Preventie

Wat de Minister van Binnenlandse Zaken en Koninkrijksrelaties in zijn brief van 20 december 2013 schrijft over een gezamenlijke verantwoordelijkheid van burgers, bedrijfsleven en overheid om identiteitsfraude te voorkomen, geldt in gelijke mate voor fraude die met gebruikmaking van het internet wordt gepleegd. In beide gevallen zullen burgers en bedrijven zich samen met de overheid moeten wapenen tegen malafide personen die zich door middel van het internet en / of misbruik van identiteitsgegevens schuldig maken aan strafbaar handelen. Preventie is daarbij onontbeerlijk. Dat gebeurt onder meer door met advertenties en televisiespots bij burgers en bedrijven het bewustzijn te bevorderen van de risico's op het internet.

Uitvoering van de in beide genoemde brieven opgenomen maatregelen is prioriteit van het kabinet.

De Minister van Veiligheid en Justitie,
I.W. Opstelten