



> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer
Postbus 20018
2500 EA DEN HAAG

Concept versie 20131120

**Directoraat-generaal
Bestuur en
Koninkrijksrelaties**
Directie Burgerschap en
Informatiebeleid

Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl

Contactpersoon

Kenmerk

Uw kenmerk

Datum 18 november 2013
Betreft Kabinetsvisie aanpak identiteitsfraude -
'Slim voorkomen, vlot herstellen'

Op 10 april 2013 had ik overleg met de vaste commissie voor Binnenlandse Zaken over de toekomstbestendigheid van de identiteitsinfrastructuur. De deelnemers aan dat overleg deelden het besef dat identiteitsfraude een serieus en groeiend probleem is. Er was steun voor de gepresenteerde maatregelen. Tegelijkertijd bestond het beeld dat de aanpak wat gefragmenteerd was. Met deze brief wil ik namens het kabinet een integrale visie op de aanpak van identiteitsfraude delen met uw Kamer. Na een analyse van het probleem vindt u een visie op de aanpak van identiteitsfraude zoals het kabinet beoogt. Deze visie hangt samen met de Rijksbrede aanpak van fraude, waarover u door de minister van V&J wordt geïnformeerd. Het kabinet biedt u deze visie op de aanpak van identiteitsfraude samen aan met de eerste monitor 'Identiteit in Cijfers'. Doel is om die monitor jaarlijks op te stellen, om een altijd actueel en met de jaren steeds scherper inzicht te hebben in ontwikkelingen op het gebied van identiteit en identiteitsfraude.

Vooraf: definities identiteit en identiteitsfraude

Er bestaan veel definities van identiteitsfraude – nationaal en internationaal¹. Dat maakt het lastig om de problemen gerelateerd aan identiteitsfraude en de aanpak ervan eenduidig in kaart te brengen. Het kabinet geeft in deze visie een brede uitleg aan het begrip identiteit:

Een *identiteit* is een verzameling eigenschappen waarmee een individu zich onderscheidt van anderen. Die verzameling kan in diverse situaties anders van samenstelling zijn, met natuurlijke (of biometrische) eigenschappen (zoals geslacht, lengte, gewicht, stem en de structuur van gelaat, ogen, oren, handen, huid en DNA), eigenschappen die het 'verhaal' van iemand vertellen (zoals naam, geboortedatum, familie, opleiding, werk en hobby's, maar ook voorkeur voor winkels en muziek, online surfgedrag en politieke kleur) en eigenschappen met een administratieve waarde (zoals BSN, adres en bankrekeningnummer).

In 2007 introduceerde het WODC een definitie van identiteitsfraude² waaronder alle vormen van criminaliteit vallen waarbij iemand met kwade bedoelingen

¹ De diverse landen, VN en OECD hanteren verschillende definities.

² Deze definitie is afkomstig uit het onderzoek 'Identiteitsfraude, een afbakening; een internationale begripsvergelijking en analyse van nationale strafbepalingen' dat de Universiteit Utrecht in 2007 in opdracht van het WODC heeft gehouden (www.wodc.nl/onderzoeksdatabase/identiteitsfraude.aspx?cp=44&cs=6796).

bewust de schijn oproept van een identiteit die niet bij hem hoort, daarbij gebruik makend van de identiteit van een bestaande of gefingeerde persoon. Het kabinet sluit in deze visie aan bij die definitie:

Identiteitsfraude is het opzettelijk (en) (wederrechtelijk of zonder toestemming) verkrijgen, toe-eigenen, bezitten of creëren van valse identificatiemiddelen en het daarmee begaan van een wederrechtelijke gedraging of: met de intentie om daarmee een wederrechtelijke gedraging te begaan.

Het begrip identificatiemiddelen moet hier breed worden uitgelegd: ook bijvoorbeeld het verhaal waarmee een fraudeur zich voordoe als verkoper van een bedrijf geldt als identificatiemiddel, of een kostuum dat de indruk moet wekken dat iemand een bepaalde functie bekleedt, of een e-mailaccount of een website onder de naam van iemand anders.

Datum

18 november 2013

Kenmerk

Maatschappelijke urgentie: structurele schade

Identiteit is goud waard. Wie zich op betrouwbare wijze kan identificeren, heeft toegang tot een snel groeiend aanbod van diensten en producten wereldwijd en weet zich gezeurd van de rechten die verbonden zijn aan een woonstaat en nationaliteit. De centrale vraag is: "Ben jij wie je zegt wie je bent? Dan kunnen we zaken doen." De meeste mensen gaan hier eerlijk mee om. Maar de stijgende waarde van identiteitsgegevens en het groeiende aantal mogelijkheden om identiteitsgegevens te bemachtigen trekt wereldwijd fraudeurs aan.

Identiteitsfraude is *modus operandi* bij veel verschillende vormen van illegale en criminele activiteiten, zoals illegale grenspassage, illegale arbeid, mensensmokkel³, drugshandel, terrorisme, witwassen van geld en vele typen fraude. Identiteitsfraude maakt daders ongrijpbaar of laat verkeerde mensen opdraaien voor een sanctie. Ze brengt de overheid financiële schade toe: voorzieningen worden verleend aan mensen die daar geen recht op hebben. Ook bij fraude tussen burgers onderling of tussen burgers en bedrijfsleven speelt identiteitsfraude een grote rol: uit het recente Nationaal Dreigingsbeeld blijkt dat in 80% van alle fraudegevallen gericht tegen burgers, bedrijfsleven en financiële instellingen sprake is van enige vorm van misbruik van identiteiten. Bijna 2 miljoen Nederlanders zijn tussen 2007 en 2012 slachtoffer geweest van enige vorm van identiteitsfraude⁴. Zij hebben naar schatting 2,8 miljard euro schade geleden⁵. Ook de emotionele impact op slachtoffers kan ingrijpend zijn, net als de reputatieschade die zij ondervinden.

Identiteitsfraude berokkent de samenleving structurele schade en zal dat bij verdere toename nog sterker gaan doen. Ze ondermijnt het vertrouwen in de financiële instellingen, tast de betaalbaarheid van voorzieningen aan en kan leiden tot een vermindering van het maatschappelijke draagvlak voor sociale voorzieningen en tot aantasting van het rechtsgevoel. Ingrijpende incidenten in de digitale dienstverlening kunnen wantrouwen losmaken tegenover de digitale economie en de digitale overheid. En de relatie tussen een persoonlijk profiel en geautomatiseerde handelingen van apps, robots en op termijn zelfs elektronische implantaten brengt uiteenlopende gezondheids- en veiligheidsrisico's met zich

³ Uit de Criminaliteitsbeeldanalyse Mensensmokkel 2012 bleek dat misbruik van identiteits- en verblijfsdocumenten de meest voorkomende *modus operandi* is van mensensmokkelaars.

⁴ Bron: PWC 2013. Recenter onderzoek van het CBS bevestigt dit beeld: in 2012 waren bijna 370.000 mensen slachtoffer van fraude bij aan- of verkopen via internet. Dat komt neer op drie procent van de Nederlandse bevolking van 15 jaar en ouder.

⁵ Bron: Update onderzoek 'Omvang van identiteitsfraude en maatschappelijke schade in Nederland', PWC, juni 2013

mee. Een betrouwbare en sterk beveiligde identiteit wordt in de toekomst een kwestie van levensbelang.

Datum
18 november 2013

Kenmerk

Voor het voorkomen van identiteitsfraude en het herstellen van de schade ervan zijn betrouwbare identiteitsinfrastructuren nodig die het mensen mogelijk maken om hun identiteit (of aspecten daarvan) voor anderen op een verifieerbare wijze kenbaar te maken, om de door anderen geclaimde identiteit (of relevante aspecten daarvan) te verifiëren en om in het geval van misbruik vast te stellen wie erachter zit, waar en wanneer misbruik heeft plaatsgevonden, hoe de gevolgen van misbruik kunnen worden hersteld en hoe verdere gevolgen kunnen worden voorkomen.

Dergelijke identiteitsinfrastructuren worden ontwikkeld door diverse private en publieke partijen, zoals bijvoorbeeld banken die hun klanten voorzien van een rekeningnummer, bankpas en identifier en een veilige omgeving voor online bankieren, of ziekenhuizen die medische en administratieve gegevens van hun patiënten veilig bewaren en patiënten een pas met foto meegeven voor identificatie. Kenmerkend voor Nederland is dat veel van deze infrastructuren zijn gebaseerd op de identiteitsinfrastructuur die door de overheid wordt onderhouden, met als kernelementen de Gemeentelijke Basisadministratie (GBA), het Burgerservicenummer (BSN), paspoort, ID-kaart, rijbewijs en DigID en voor buitenlanders die naar Nederland komen de Basisvoorziening voor Vreemdelingen (BVV) en een verblijfsdocument.

Zowel de overheid als private partijen werken permanent aan verbeteringen van hun identiteitsinfrastructuren en het beheer en gebruik ervan, vanuit de soms niet eenvoudig te verenigen perspectieven van betrouwbaarheid, privacy, gebruikersgemak en efficiëntie. 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 verweven. Fraudeurs hebben het verrassingsmoment aan hun zijde: de keuze waar, hoe en wanneer ze toeslaan. Overheid, bedrijfsleven en burgers staan daar het sterkst tegenover wanneer ze goed samen optrekken in een integrale aanpak van identiteitsfraude.

Analyse: steeds kwetsbaarder voor identiteitsfraude

Particulieren, overheden en bedrijfsleven worden steeds kwetsbaarder voor identiteitsfraude. Belangrijkste oorzaken:

1. *Het aantal kwetsbare plekken waar fraudeurs kunnen toeslaan neemt toe.*
2. *Daders kennen geen grenzen en gebruiken steeds geraffineerdere methoden.*
3. *Het potentieel voor voorkomen en herstellen wordt onvoldoende ontsloten.*

1. *Het aantal kwetsbare plekken waar fraudeurs kunnen toeslaan neemt toe.*
In Nederland bestaat een algemeen gebrek aan alertheid voor identiteitsfraude. Het zit niet in de Nederlandse omgangsvormen om de identiteit van een ander te wantrouwen. Niet aan de deur, niet aan de telefoon, niet in de winkel of aan de balie. Een zorgvuldige controle van een identiteitsbewijs wordt al gauw als onvriendelijk ervaren. Ook in situaties waar een bepaalde mate van professionele waakzaamheid functioneel kan zijn. Dat levert veel plekken op waar fraudeurs kunnen toeslaan.

Dat gebrek aan alertheid maakt niet alleen burgers kwetsbaar voor

identiteitsfraude, maar ook bedrijven en overheidsinstanties. Meer dan een miljoen mensen hebben professioneel te maken met het vaststellen, registreren en verifiëren van persoonsgegevens (bij gemeenten, IND, politie, Koninklijke Marechaussee, banken, uitzendbureaus, verzekeringsorganisaties, ziekenhuizen, kamer van koophandel, notarissen, horeca, beveiligingsbedrijven, et cetera). Behalve alertheid zijn ook kennis en vaardigheden in veel sectoren onvoldoende aanwezig. En waar kennis aanwezig is, is zij vaak moeilijk te borgen door de mobiliteit van medewerkers. Het gaat hier om kennis van documenten en echtheidskenmerken, van 'look-alike fraude' (het gebruik van een document door iemand die lijkt op de rechtmatige documenthouder) en van de verschillende (veranderende) fraudevormen. Daarnaast ontbreken op veel plaatsen vaak de nodige technische hulpmiddelen en de steun van een gespecialiseerd backoffice. Ook staat identiteitsverificatie onder druk van eisen aan dienstverlening (snelheid, klantvriendelijkheid).

Datum
18 november 2013
Kenmerk

Het aantal plekken waar fraudeurs kunnen toeslaan neemt vooral toe door het toegenomen internetgebruik. Miljoenen Nederlanders zijn steeds actiever aanwezig in de online wereld. Openheid is de norm. "Ik deel, dus ik leef." Dat leidt tot een toename van mogelijkheden voor fraudeurs om identiteitsgegevens te vergaren en te misbruiken. Via Google en Facebook kunnen nauwkeurige profielen opgesteld worden waar fraudeurs mee aan de haal kunnen gaan.

Ook de overheid en private partijen zijn steeds actiever in de digitale wereld. "Digitaal waar mogelijk, persoonlijk waar nodig", in de benadering van de Manifestgroep⁶. Digitale dienstverlening prikkelt tot slimmer en zuiniger werken en biedt uitstekende kansen voor economische groei. Het kabinet zet dan ook in op vergaande digitalisering van de dienstverlening van de overheid in 2017 en heeft met de EU een ambitieuze digitale agenda. Maar digitalisering van de dienstverlening creëert ook nieuwe openingen voor fraudeurs.

2. Daders kennen geen grenzen en gebruiken steeds geraffineerdere methoden. Identiteitsfraudeurs en de 'facilitators' die hen bedienen zijn doorgaans goed geïnformeerd, innovatief en technisch competent. Ze opereren als criminele organisaties over landsgrenzen heen. En als de preventie of opsporing op één plek wordt versterkt, duiken ze ergens anders weer op.

Het zoeken naar nieuwe kwetsbare plekken is te zien in de verschuiving van methoden die identiteitsfraudeurs gebruiken. Het vervalsen van reisdocumenten, bijvoorbeeld, is steeds moeilijker geworden. In 1981 werd door de Raad van de Europese Unie een resolutie vastgesteld die betrekking heeft op de beveiliging van paspoorten en andere reisdocumenten tegen vervalsingen. Deze resolutie wordt periodiek aangepast. In 2000 is deze resolutie ingrijpend aangevuld en zijn daarin ook minimumveiligheidsnormen opgenomen. Als gevolg van de steeds hogere drempel voor vervalsing van identiteitsdocumenten uit EU-landen duiken nu fraudeurs op die zich richten op de manier waarop documenten worden verstrekt en op look-alike fraude. Jaarlijks worden een kwart miljoen Nederlandse reisdocumenten en rijbewijzen als verloren of gestolen opgegeven. Dat is een groot potentieel voor look-alike fraude alleen al met Nederlandse documenten.

⁶ De Manifestgroep (MFG) is een informeel samenwerkingsverband van AgentschapNL, Belastingdienst, Centraal Administratiekantoor (CAK), Centraal Bureau voor de Statistiek (CBS), Centraal Justitieel Incassobureau (CJIB), Centrum Indicatiestelling Zorg (CIZ), College van Zorgverzekeringen (CVZ), Dienst Regelingen, Dienst Uitvoering Onderwijs (DUO), Immigratie- en Naturalisatiedienst (IND), Kadaster, Kamers van Koophandel (KVK), RDW, Sociale Verzekeringsbank (SVB) en Uitvoering Werknemersverzekeringen (UWV).

Daarnaast is een verschuiving te zien naar het onder andermans of gefingeerde naam aanvragen van identiteitsdocumenten, bijvoorbeeld door fraude met geboorte- of huwelijksakten: die zijn nauwelijks beveiligd tegen namaak en vervalsing. Er bestaan internationaal ook geen standaards voor. In veel landen worden geboortes bovendien niet geregistreerd, waardoor de deur voor identiteitsfraude – onder andere gerelateerd aan kinderhandel – open staat.

Datum
18 november 2013
Kenmerk

Een veelgebruikte vorm van identiteitsfraude is misbruik van kopieën van identiteitsbewijzen⁷. Via een kopie komen fraudeurs in het bezit van naam, geboortedatum en BSN: op veel plaatsen genoeg om financiële transacties aan te gaan. De methoden om aan persoonsgegevens te komen, zijn gewiekst en brutaal, variërend van vissen in brievenbussen, tot het insceneren van een sollicitatiegesprek ('vacatureripping') of van de verhuur van een huis.

Er is vooral een steile groeicurve te zien in identiteitsfraude gefaciliteerd door het internet. In 2012 was ongeveer 40 procent van de ondernemers slachtoffer van cybercrime⁸. Ook particulieren worden bestookt met phishing mails, malware/spyware en hyperlinks naar kopieën van vertrouwde websites (pharming). Met de identiteitsgegevens van een ander, of met valse gegevens, kunnen fraudeurs op afstand zaken doen bij publieke en private instellingen. Daarnaast zijn op online marktplaatsen veel fraudeurs actief onder valse identiteiten. Internetfraude is zeer aantrekkelijk voor criminelen: het is een low-risk crime (misdad wordt niet in persoon gepleegd, maar via computers), de doelgroep is reusachtig, de pakkans is laag (alleen zichtbaar voor specialisten), fraudeurs kunnen vrij van grenzen opereren en online diensten en toepassingen komen steeds met nieuwe versies, die nieuwe kwetsbaarheden hebben, waarover de kennis zich snel verspreidt.

3. Het potentieel voor voorkomen en herstellen wordt onvoldoende ontsloten. Veel organisaties en sectoren nemen maatregelen tegen identiteitsfraude. Vaak betreft het publieksvoorlichting; de Consumentenbond, internetproviders, banken en een grote groep partners van 'Alert Online' bijvoorbeeld geven burgers en bedrijven tips voor veilig online gedrag. In veel sectoren wordt personeel getraind op het herkennen van identiteitsfraude. Soms worden grootscheeps nieuwe technieken en systemen geïntroduceerd, zoals de overstap met het pinnen 'van strip naar chip' in 2005. En soms levert een slimme truc veel winst op, zoals het standaard blokkeren van bankpassen in landen waar skimmen nog mogelijk is, of het overmaken van 1 cent voor identificatie via de bankrekening bij het afsluiten van een nieuwe telefoonabonnement.

In diverse sectoren wordt gemonitord op risicopatronen. Webwinkels bijvoorbeeld worden gealarmeerd door opmerkelijk surfgedrag. Creditcardmaatschappijen bellen hun klanten bij een vermoeden van misbruik. Ook bestaan binnen een aantal sectoren registers waarin signalen over incidenten worden gedeeld, zoals het Incidentenwaarschuwingssysteem van financiële instellingen en het Fraude en Informatiesysteem Systeem Holland (FISH) van verzekeraars.

Ook in het publieke domein wordt de aanpak van identiteitsfraude met diverse maatregelen verbeterd. Het Centraal Meld- en informatiepunt voor Identiteitsfraude en -fouten (CMI), de Fraudehelpdesk en het Landelijk Meldpunt

⁷ Identiteitsfraude met kopieën van identiteitsbewijzen is geanalyseerd in het Bestuurlijk Dossier Identiteitsfraude, OM Parket Noord-Nederland, 2013.

⁸ <http://www.politie.nl/onderwerpen/cybercrime.html#feiten-en-cijfers>

Internetoplichting geven voorlichting en helpen slachtoffers bij het doen van aangifte en het oplossen van hun zaak. Binnen de Belastingdienst is de hulp aan slachtoffers van identiteitsfraude sinds anderhalf jaar beter georganiseerd en dankzij een landelijke registratie is het mogelijk patronen te herkennen en daders sneller op te sporen. Het wijzigen van bankrekeningnummers bij de Belastingdienst is veiliger geworden door voorbevestigingen en wordt nog veiliger met de komst van het nieuwe proces "wijzigen bankrekeningnummers" (april 2014). De minister van SZW heeft een pilot aangekondigd met de ID12 pas in de champignonsector, die naar Zweeds voorbeeld inzicht moet verschaffen in wie op welke werkplek werkt en daarmee het toezicht versterkt en zwart werken bemoeilijkt. En er worden voorbereidingen getroffen voor een eID-stelsel: een publiek-privaat stelsel waarbinnen burgers, consumenten en ondernemers zowel publieke als private authenticatiemiddelen gebruiken, waarmee ze veilig online zaken kunnen doen met de overheid en het bedrijfsleven⁹.

Datum
18 november 2013
Kenmerk

Veel verbeteringen in de publieke sector hebben te maken met een verbeterde samenwerking tussen verschillende instanties. Het programma Identiteit op Orde heeft met dat doel experts van veel verschillende organisaties bij elkaar gebracht en brengt een kennisplatform van wetenschappers voort. De verschillende overheidsdiensten als de Koninklijke Marechaussee, politie, IND, OM en RDW weten elkaar steeds beter te vinden op het gebied van identiteit en identiteitsfraude, onder andere in regionale samenwerkingsverbanden. Ook landelijke expertisecentra als het Expertisecentrum voor Identiteitsfraude en Documenten (ECID), Expertisecentrum Rijbewijzen, Bureau Documenten, het Nederlands Forensisch Instituut (NFI) en het Expertisecentrum Vreemdelingen en Mensenhandel (ECVM) kijken breder dan het eigen domein. Vanwege het belang van de GBA als noodzakelijk informatiesysteem voor veel overheidstaken is eind 2011 de kwaliteitsagenda GBA gestart om met name de adresgegevens op een zo hoog mogelijk niveau te brengen¹⁰. Er wordt gebouwd aan de Basisregistratie Persoonsgegevens (BRP), die de actualiteit en kwaliteit van gegevens moet verbeteren en die mogelijkheden moet bieden voor het leggen van verbanden tussen in de GBA geregistreerde personen door enkelvoudige opslag van gerelateerde persoonsgegevens. Er zijn afspraken over koppeling van gegevens van de SVB, het UWV en de Belastingdienst aan de GBA. Gemeenten signaleren afwijkende vestigingspatronen die ook van belang zouden kunnen zijn voor andere gemeenten. Met het programma Identiteitsmanagement en Immigratie (IDMI) is fors geïnvesteerd in de vreemdelingenketen: aangezien identiteit daar van wezenlijk belang is voor het krijgen van een verblijfsvergunning, is in de vreemdelingenketen bij uitstek bijzondere aandacht voor identiteitsfraude, door Koninklijke Marechaussee, IND, Vreemdelingenpolitie en Dienst Terugkeer en Vertrek (DTV). Ook in de strafrechtketen krijgt identiteit bijzondere aandacht: verdachten hebben belang bij identiteitsfraude voor het ontlopen van straf of minder straf doordat relevante antecedenten onder water verdwijnen. Om deze reden is de WIVVG (Informatie voor Verdachten en/ of Veroordeelden) ingevoerd. Deze wet maakt gebruik van biometrische kenmerken mogelijk bij verdachten van

⁹ PM verwijzing naar brief aan Kamer over eID stelsel; momenteel in voorbereiding

¹⁰ Deze kwaliteitsagenda heeft als doel om de gemeenten als bijhouders van de GBA en de gebruikers van de gegevens optimaal te ondersteunen bij hun taakuitvoering. Over de vele maatregelen en de stand van zaken heeft BZK bij brieven van 5 juli 2012 en 23 mei 2013 de Tweede Kamer geïnformeerd (Kamerstukken 27 859, nrs. 57, 58, 60 en 65). In de brieven en het debat rond fraude met toeslagen (Kamerstuk 17 050, nr 435) is aangekondigd om de kwaliteitsagenda versterkt in te zetten: de risicoprofielen die zijn ontwikkeld door de gemeenten in relatie tot het inschrijven van personen worden actief gedeeld met alle gemeenten, voorts komt er meer samenwerking in de keten van afnemers van de GBA en is sprake van intensivering van de deskundigheidsbevordering van GBA-ambtenaren.

misdrijven waarvoor voorlopige hechtenis is toegestaan. De kern is dat de politie (of een andere opsporingsdienst) identificeert en ketenpartners de identiteit in het vervolg (vervolg, berechting en executie van straf) steeds kunnen verifiëren, zodat er zekerheid is over de juiste identiteit van verdachten en veroordeelden.

Datum
18 november 2013
Kenmerk

Met al deze maatregelen worden veel van de geschetste problemen al aangepakt. Maar het is niet voldoende tegenover de geraffineerde werkwijzen van fraudeurs en de veelheid aan kwetsbare plekken waar zij kunnen toeslaan. Het ontbreekt aan een integrale, informatie gestuurde aanpak waarin partners in publieke en private sector de krachten samenballen¹¹. Grote organisaties en zware ketens zijn nooit zo efficiënt en effectief in hun verdediging als de kleine, creatieve, wendbare dadergroepen die hen bestoken en makkelijk van aanvalsstrategie kunnen veranderen. Dat maakt dat de pakkans te laag is en de handhaving onvoldoende. Het antwoord zal niet komen van klassieke bolwerken, maar van moderne netwerken die snel reageren en slim anticiperen op identiteitsfraude.

Bij het ontwikkelen van deze visie met fraudedeskundigen uit publieke en private sector werd breed erkend dat identiteitsfraude een gemeenschappelijk probleem is. De motivatie om dat probleem samen aan te pakken is groot. Dat biedt een goede kans om het potentieel van mensen en maatregelen beter te benutten.

Visie: slim voorkomen, vlot herstellen

We mogen niet verwachten dat identiteitsfraude ooit is uit te bannen. Het is net als met gezondheid. Mensen zijn door de eeuwen heen altijd en overal wel bestookt door ziektekiemen – oude bekenden of nieuwe. We ontwikkelen daar generatie op generatie een steeds sterkere weerstand tegen. Maar vroeg of laat wordt iedereen wel eens getroffen. Het is dan belangrijk om er op tijd bij te zijn en de juiste behandeling toe te passen. Zo is het ook met identiteitsfraude. Er zijn altijd wel criminelen op zoek naar kwetsbare plekken in het systeem – met oude en nieuwe methoden. De meeste mensen en organisaties ontwikkelen er een gezonde weerstand tegen door voorzichtig om te gaan met gegevens en door steeds betere technieken en methoden te benutten. Maar iedereen kan wel eens slachtoffer worden van identiteitsfraude. Dan is het zaak om de fraude zo snel mogelijk te detecteren en adequaat te behandelen.

Het kabinet heeft een toekomst voor ogen waarin alerte en goed geïnformeerde burgers en organisaties zich uitstekend weten te weren tegen pogingen tot identiteitsfraude. Identiteitsfraudeurs stuiten op een hecht web van actuele kennis en slimme technologische toepassingen. En als ergens een identiteitsfraudeur toeslaat, dan wordt dit vroeg ontdekt en met vereende krachten vlot verholpen.

Burgers, overheid en bedrijfsleven hebben een gezamenlijke verantwoordelijkheid voor het voorkomen en herstellen van identiteitsfraude. Burgers moeten er zelf voor zorgen dat ze een gezonde weerstand hebben tegen pogingen tot identiteitsfraude, door voldoende waakzaam te zijn en door de beschikbare middelen – zoals beveiligingssoftware – op de juiste manier te gebruiken. Zij zijn ook de eersten die in actie moeten komen als ze slachtoffer zijn van identiteitsfraude, of een poging daartoe.

Datzelfde geldt voor organisaties, in publieke en private sector: zij zijn zelf

¹¹ Europol pleit in haar Threat Assessment Internet Facilitate Organised Crime iOCTA, File nr: 2530-264 (pag 8) uit 2011 nadrukkelijk voor publiek en private samenwerking.

verantwoordelijk voor een gezonde weerstand tegen identiteitsfraude. Van organisaties mag daarnaast worden verwacht dat ze hun klanten zo goed mogelijk beschermen tegen identiteitsfraude, door zorgvuldig om te gaan met het verwerven, beveiligen en gebruiken van persoonsgegevens, door verzoeken om correctie en verwijdering van gegevens adequaat te behandelen en door klanten actief te voorzien van de benodigde informatie en middelen om identiteitsfraude te voorkomen.

Datum
18 november 2013
Kenmerk

De rol van de overheid bij het voorkomen en herstellen van identiteitsfraude: zij zorgt online en offline voor een robuuste identiteitsinfrastructuur met betrouwbare ijkpunten: contactmomenten tussen burgers en overheid waarin goed opgeleide professionals met hulp van geavanceerde apparatuur een identiteit met de grootst mogelijke zekerheid vaststellen, registreren en verifiëren. De overheid borgt een aantal elementaire identificerende gegevens voor alle Nederlanders en iedereen die in Nederland verblijft. De overheid stelt heldere richtlijnen vast voor de veiligheid en betrouwbaarheid van particuliere identiteitsinfrastructuren en identificatiemiddelen en voor de begeleiding van slachtoffers van identiteitsfraude en -fouten. De overheid werkt samen met het bedrijfsleven en maatschappelijke organisaties aan een integrale aanpak van identiteitsfraudeurs. En de overheid monitort voortdurend de ontwikkelingen in de wereld van identiteitsfraude en verkent de grenzen van de bestrijding van deze groeiende tak van misdaad, samen met experts in publieke en private sector in binnen- en buitenland.

De visie in vijf beleidslijnen: aanpak van identiteitsfraude

Een effectieve aanpak van identiteitsfraude vraagt om een gecoördineerde inspanning van overheid, bedrijfsleven, maatschappelijke organisaties en burgers. De impact van initiatieven in diverse sectoren en ketens wordt groter door afstemming in een landelijk netwerk en aansluiting op internationale ontwikkelingen. In de eerste plaats gaat het om het beter en breder benutten van bestaande kennis, technieken en methoden. In de tweede plaats gaat het om het beter op elkaar afstemmen van nieuwe maatregelen die door diverse partijen in publieke en private sector getroffen worden. In de derde plaats gaat het om het afspreken van een gezamenlijke richting voor ontwikkelingen op de lange termijn. Het kabinet onderscheidt daarbij vijf samenhangende beleidslijnen:

1. Gezonde weerstand

Voorkomen is beter dan genezen. De preventie van identiteitsfraude moet permanent evolueren met nieuwe vormen van bedreiging. Kennis en alertheid zijn sleutelfactoren, gedragen door bewustwordingscampagnes en fraude-alerts. Bundeling van initiatieven uit publieke en private sector moet de algehele preventie versterken, doordat kennis en informatie een bredere doelgroep bereiken en doordat geldende regels en beschikbare middelen langs verschillende wegen onder de aandacht worden gebracht.

De menselijke factor zal op termijn echter niet voldoende blijken tegenover de steeds ingrijpendere impact van identiteitsfraude. Er zullen zeker veel mensen zijn die zich met de meest actuele kennis en middelen goed weten te weren tegen identiteitsfraudeurs, maar er zullen ook altijd mensen zijn die daar niet of beperkt toe in staat zijn. Daarom wil het kabinet de weerstand tegen identiteitsfraude op termijn zo goed mogelijk 'hard' organiseren: zo hoog mogelijke fysieke barrières opwerpen tegen identiteitsfraude.

Dat begint bij het minimaliseren van het gebruik van identificerende gegevens en

bij het veilig bewaren ervan. Op beide punten gaan het borgen van privacy en het voorkomen van identiteitsfraude hand in hand. Overheid en bedrijfsleven zijn gebonden aan het principe van dataminimalisatie¹². Dat principe geeft aan dat persoonsgegevens slechts mogen worden verwerkt als daartoe een noodzaak bestaat. Het principe is leidend bij het registreren en bewaren van gegevens in systemen. Bij de rijksdienst bijvoorbeeld wordt met het toetsmodel privacy impact assessment beoordeeld of systemen zo worden gebouwd dat er zo min mogelijk persoonsgegevens in worden opgeslagen en bewaard. De campagne 'laat je niet zomaar kopiëren' was een invulling van het dataminimalisatieprincipe voor kopietjes van identiteitsbewijzen; de ID-cover van de NVVB (Nederlandse Vereniging voor Burgerzaken) is daar een slim en praktisch hulpstuk bij. Verplaatsen van het BSN naar de achterkant van het paspoort en de identiteitskaart is een praktische stap in diezelfde richting. Met digitalisering van de dienstverlening van overheid en bedrijfsleven en een eID-stelsel zijn kopietjes van identiteitsbewijzen en papieren correspondentie in de toekomst minder nodig, waardoor criminelen minder kans maken om aan identiteitsgegevens te komen door kopietjes te bemachtigen of in brievenbussen te vissen. Voor wat betreft het veilig bewaren van gegevens is op termijn winst te boeken met het compartimenteren van identiteiten¹³ en het enkelvoudig en waar nodig versleuteld opslaan van gegevens: hackers hebben minder kansen naarmate identiteitsgegevens op minder plaatsen zijn opgeslagen. Dat is technisch mogelijk door niet dezelfde gegevens in veel verschillende systemen te bewaren, maar slechts op één goed beveiligde plek, met voor verschillende partijen een beveiligde toegang tot per situatie verschillende deelverzamelingen van die gegevens. De BRP zet met de enkelvoudige opslag van gerelateerde persoonsgegevens een belangrijke stap in die richting.

Datum
18 november 2013
Kenmerk

Tegelijkertijd moet er rekening mee worden gehouden dat er altijd wel gegevens in handen komen van kwaadwillenden en dat niet is na te gaan hoeveel gegevens er al in het criminele circuit bekend zijn. Hackers voorspellen dat alle gegevens die in databases zijn opgeslagen op een dag gehackt kunnen worden – zij het op afstand, zij het door handlangers aan de bron. En het is een feit dat de virtuele wereld niet aan geheugenverlies lijdt: eenmaal verstrekte gegevens verspreiden zich snel en laten zich moeilijk vernietigen. Daarom wil het kabinet richting een situatie waarin de combinatie van naam, adres, Burgerservicenummer en andere persoonsgegevens nergens nog voldoende is voor het plegen van identiteitsfraude. Dat kan door in de toekomst bij controles altijd te vragen om een persoonlijke 'sleutel' die fraudeurs moeilijk kunnen bemachtigen

Een dergelijke persoonlijke sleutel zal moeten bestaan uit slimme en voor de situatie voldoende betrouwbare toepassingen van de drie-eenheid '*wie je bent, wat je weet en wat je hebt*'. Het hoogste betrouwbaarheidsniveau – online en offline – bestaat uit een combinatie van een pas met een chip en een smart device (*wat je hebt*; bijvoorbeeld DigID-kaart in combinatie met smart phone), tweestapsverificatie (*wat je weet*; bijvoorbeeld met een dubbel wachtwoord, pincode, sms of een persoonlijke vraag-antwoordcombinatie) en biometrische

¹² De Wbp legt het principe van dataminimalisatie neer. Persoonsgegevens mogen slechts worden verwerkt als daarvoor een noodzaak bestaat (art 8). Art. 11, lid 1 bepaalt daarnaast dat persoonsgegevens slechts mogen worden verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn (relevantie-eis). Verder is van belang dat verwerking van gevoelige persoonsgegevens in principe verboden is (art. 16-23 Wbp), en slechts onder strikte(re) voorwaarden is toegestaan.

¹³ Het principe van compartimenten van identiteiten is vergelijkbaar met het compartimenteren van olietankers: als er midscheeps een gat ontstaat, stroomt niet meteen de hele tanker leeg.

kenmerken (*wie je bent*; bijvoorbeeld stem- of gelaatsherkenning). Veel landen verkennen nieuwe technieken en concepten. Datzelfde geldt voor innovatieve trendsetters als Apple, Google en Facebook. Het kabinet wil met goed oor voor het maatschappelijke debat over dit thema onderzoeken hoe nieuwe technologie in uiteenlopende situaties optimaal ingezet kan worden voor het voorkomen van identiteitsfraude, het beschermen van privacy, het bevorderen van economische bewegingsvrijheid, het gebruiken van mobiele platforms en het vergroten van de mogelijkheden voor burgers om zelf gegevens te kunnen beheren en delen.

Datum
18 november 2013
Kenmerk

2. Betrouwbare controles

Een goede en efficiënte dienstverlening in publieke en private sector is slechts mogelijk dankzij betrouwbare identiteitsgegevens. Dat betekent voor veel instanties zoveel als een paradigmawijziging – zeker in een context van vergaande digitalisering van de dienstverlening: door de identiteit van burgers op de juiste momenten zorgvuldig te controleren, leveren organisaties grote winst op voor heel het maatschappelijk en economisch verkeer, doordat die controles ruimte scheppen voor efficiënte dienstverlening en burgers beschermen tegen identiteitsfraude. Zorgvuldige controles bedienen de burgers.

Dat vraagt om een investering in de 'ijkpunten' van de Nederlandse identiteitsinfrastructuur: face-to-face contacten tussen burgers en overheid waarbij goed opgeleide professionals met hulp van geavanceerde apparatuur een identiteit met de grootst mogelijke zekerheid vaststellen, registreren en verifiëren. Een belangrijk initiatief in die richting is het programma 'Naar betrouwbare persoonsgegevens' van de NVVB, dat zich richt op de ontwikkeling van kennis en vaardigheden van ambtenaren burgerzaken.

Ook een regionale concentratie van kennis en apparatuur, met ondersteuning van landelijke expertisecentra, kan de ijkpunten van de identiteitsinfrastructuur naar een hoger betrouwbaarheidsniveau tillen. In Oost-Nederland is positief gereageerd op een voorstel van de burgemeesters van Enschede, Apeldoorn en Zwolle om samen te werken aan de inschrijving in de GBA.

Het kabinet wil onderzoeken op welke slimme manieren extra controles kunnen worden toegepast bij het verstrekken van overheidsmiddelen en onder welke omstandigheden de overheid bepaalde identiteitsmiddelen kan intrekken. Om fraudeurs niet in de kaart te spelen is het van belang ook aandacht te besteden aan minder voorspelbare identiteitscontroles.

Op termijn moeten partijen met actuele kennis over identificerende gegevens een betere plek krijgen in het beheer en de validatie van gegevens die voor veel partijen van belang zijn. Dat geldt zowel voor identiteitsvaststelling bij geboorte en immigratie, als voor identiteitsverificatie bij emigratie en overlijden, als voor correctie van gegevens wanneer registraties onjuist blijken. Het gaat hier om het beter benutten van specifieke kennis en kunde van onder andere gemeenten, politie, Koninklijke Marechaussee, IND, buitenlandse posten, Belastingdienst, zorginstellingen en financiële dienstverleners.

3. Vroege diagnose

Een vroege diagnose van gevallen van identiteitsfraude is van groot belang om snelle behandeling mogelijk te maken en om verspreiding te voorkomen. Opgave voor de betrokkenen van de diverse disciplines is om als netwerk te opereren en

om integrale defensiestrategieën en gerichte trainings- en communicatieprogramma's te ontwikkelen en implementeren. Dat moet op een manier gebeuren die beantwoordt aan de creativiteit en wendbaarheid van criminele organisaties en hun internationale speelveld.

Datum
18 november 2013
Kenmerk

Er zijn al diverse initiatieven tot interdisciplinaire samenwerking, zoals bij het Centrum voor Informatiebeveiliging en Privacy (CIP) onder regie van het UWV, de infobox Crimineel en Onverklaarbaar Vermogen (iCOV), de te vormen expertisegroep fraudebestrijding onder regie van de Belastingdienst en de samenwerking tussen de Nationale Politie en de Koninklijke Marechaussee in de oprichting van vreemdelingenpolitieloketten en ID-desks. Dat zijn grote stappen die de 'intelligence' versterken vanwaaruit identiteitsfraude en andere vormen van fraude kunnen worden bestreden. De Ministeriële Commissie Fraude is in het leven geroepen voor een integrale aanpak van fraude waar het misbruik van overheidsmiddelen betreft.

De crux voor een vroege diagnose is het goed registreren van identiteitsfraude, het stapelen van casussen, het herkennen van patronen en het doorrechercheren op onregelmatigheden in het gedrag van groepen of individuen. Voorwaarde daarvoor is dat gegevens of indicatoren voor mogelijke fraude die de overheid of andere organisaties beschikbaar hebben met de juiste partijen worden gedeeld, met waarborgen voor privacy en voor rechtsbeginselen als het non-discriminatiebeginsel, gelijkheidsbeginsel en verbod op willekeur en met waarborgen tegen 'false positives' (de onterechte veronderstelling dat iemand fraudeert). De aanpak hiervan staat beschreven in de Rijksbrede antifraudestrategie die de minister van V&J u zal toezenden.

4. Adequate behandeling

Voor slachtoffers is het van belang dat zij zich erkend voelen in hun probleem, dat zij beschermd worden tegen hernieuwd slachtofferschap en dat zij ondersteuning krijgen bij aangifte en bij schadeloosstelling en herstel. Van de eerste aangifte van identiteitsfraude bij de politie tot het geheel oplossen van de zaak wil het kabinet dat de slachtoffers centraal staan.

Belangrijkste is dat de schade zich niet verder verspreidt. Dat is mogelijk door het direct ontwaarden van gestolen (of verloren) identificatiemiddelen: slachtoffers moeten hun identiteitsdocumenten, pasjes en digitale identiteiten onmiddellijk kunnen blokkeren en instanties kunnen oproepen tot verhoogde alertheid op hun gegevens. Ook moet online verifieerbaar zijn welke identiteitsdocumenten geldig en welke ongeldig zijn. Repressie haakt hier in op preventie.

Iedere instantie in publieke en private sector heeft zelf de verantwoordelijkheid om slachtoffers van fraude (en fouten) te helpen door foutieve of gecorrumpeerde gegevens te verwijderen of te corrigeren. Wanneer het probleem zich verspreidt over meerdere administraties, moet herstel vanuit het netwerk komen. Dat vraagt om maatwerk: de beste methode is dat afgevaardigden van betrokken instanties samen aan tafel zitten om een probleem op te lossen. Voor schrijnende gevallen is er hulp van het Centraal Meld- en Informatiepunt Identiteitsfraude en -fouten (CMI) en de Fraudehelpdesk. Het kabinet zet in op een geïntensiveerde samenwerking tussen het CMI, Fraudehelpdesk en andere organisaties die er zijn om slachtoffers te helpen.

Voor de publieke sector geldt dat ruim 600 organisaties gebruik maken van de

Gemeentelijke Basisadministratie (GBA). Cruciaal voor een adequate behandeling van identiteitsfraude is dan ook dat burgers op tijd signaleren wanneer er iets loos is met hun gegevens in de GBA en dat fouten vlot hersteld worden. Het kabinet roept burgers op om er zelf voor te zorgen dat hun gegevens in de GBA kloppen, wat in 2013 is onderstreept met de campagne 'Voorkom gedoe, kijk het na'.

Datum
18 november 2013
Kenmerk

Op de lange termijn moet het spreiden van de gevolgen van fraude en fouten voorkomen worden door de eerder genoemde enkelvoudige opslag van gegevens.

5. Effectieve repressie

Bij de bestrijding van identiteitsfraude zijn het opwerpen van barrières en een verhoogde alertheid van private en publieke partijen in het handelsverkeer van doorslaggevend belang. Een effectieve en gerichte aanpak van fraudeurs vraagt om een verbinding tussen het strafrecht en andere vormen van handhaving, toezicht en nalevingsbevordering. Op die manier is er sprake van meer afgestemde en integrale handhaving waarin het strafrecht tijdig en situationeel wordt ingezet. De minister van V&J gaat hier in zijn antifraudebrief nader op in.

Bij een effectieve repressie van identiteitsfraude mag niet vergeten worden dat misbruik van identiteiten overwegend een faciliterende handeling is om een delict te plegen. Identiteitsfraude is geen doel op zich, maar een middel, wat ook uit de gehanteerde definitie voortvloeit. De aanpak van identiteitsfraude staat dan ook niet op zichzelf, maar maakt deel uit van de aanpak van criminaliteitsfenomenen waarbij identiteitsfraude modus operandi is.

Fraude met identiteitsdocumenten is strafbaar volgens artikel 231 van het Wetboek van Strafrecht¹⁴. Fraude met identificerende persoonsgegevens (het aannemen van een valse naam of een valse hoedanigheid) vormt onderdeel van meer algemene delictsom beschrijvingen als oplichting (artikel 326 Sr), flessentrekkerij (artikel 326a Sr) en bedreiging (artikel 284 e.v. Sr)¹⁵. Voorts kent het Wetboek van Strafrecht specifieke strafbaarstellingen voor de aanpak van misdrijven waartoe fraude met identificerende persoonsgegevens vaak de opstap vormt. Bij die misdrijven gaat het bijvoorbeeld om mensensmokkel, witwassen, bank- of uitkeringsfraude, terrorisme of drugs- en wapengerelateerde misdrijven.

Strenge repressiemaatregelen moeten in combinatie met stevige preventiemaatregelen een afschrikkende werking vormen: bij potentiële fraudeurs moet het verhaal rondgaan dat identiteitsfraude in Nederland een onbegonnen zaak is.

¹⁴ Wetboek van Strafrecht, Artikel 231: "1. Hij die een reisdocument valselyk opmaakt of vervalst, of een zodanig stuk op grond van valse gegevens doet verstrekken dan wel een aan hem of een ander verstrekt reisdocument ter beschikking stelt van een derde, met het oogmerk het door deze te doen gebruiken als ware het aan hem verstrekt, wordt gestraft met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie. 2. Met dezelfde straf wordt gestraft hij die in het bezit is van een reisdocument waarvan hij weet of redelijkerwijs moet vermoeden, dat het vals of vervalst is, dan wel opzettelijk gebruik maakt van een niet op zijn naam gesteld reisdocument."

¹⁵ Voetnoot: wetsvoorstel wijziging van het Wetboek van Strafrecht en de Wegenverkeerswet 1994 in verband met de verbetering van de aanpak van fraude met identiteitsbewijzen en wijziging van het Wetboek van Strafvordering, de Beginselenwet justitiële jeugdinrichtingen en de Wet DNA-onderzoek bij veroordeelden in verband met de verbetering van de regeling van de identiteitsvaststelling van verdachten en veroordeelden (33352). Dit wetsvoorstel voorziet erin dat meer fraudeleuze gedragingen met identiteitsbewijzen strafbaar worden gesteld. Voorts wordt hiermee misbruik van identificerende persoonsgegevens afzonderlijk strafbaar gesteld en meer op één lijn gesteld met misbruik van reisdocumenten en identiteitsbewijzen waarvoor artikel 231 van het Wetboek van Strafrecht wel een aparte strafbaarstelling kent.

Internationale aanpak

Een integrale aanpak van identiteitsfraude op Europees niveau is nog veel complexer dan een aanpak met Nederlandse partners: de lidstaten hebben alle hun eigen historie van vaststellen, registreren en verifiëren van persoonsgegevens en daaruit zijn heel verschillende wetten, regels, systemen en middelen voortgevloeid. Het spreekt voor zich dat de aanpak op mondiaal niveau nog complexer is.

Datum

18 november 2013

Kenmerk

Toch is een grensoverschrijdende aanpak cruciaal voor preventie en bestrijding van identiteitsfraude. Zoals eerder aangegeven in deze brief: de georganiseerde misdaad kent geen grenzen. Hoe sterk ook de nationale aanpak, via kwetsbare plekken in andere landen blijven de gevolgen van identiteitsfraude Nederland bereiken. Daarnaast zijn internationaal opererende dadergroepen niet te bereiken met een nationale aanpak. Het grensoverschrijdende karakter van identiteitsfraude – in het bijzonder in de digitale wereld – levert grote uitdagingen op voor Europese en internationale samenwerking. Het kabinet pleit daarom voor intensiveren van de samenwerking op EU-niveau voor het voorkomen en bestrijden van identiteitsfraude.

Uitvoeringsagenda aanpak identiteitsfraude

De visie die u in deze brief is voorgelegd zal worden uitgewerkt in een uitvoeringsagenda Aanpak Identiteitsfraude. Die agenda zal recht doen aan de vele initiatieven die al worden genomen in de aanpak van identiteitsfraude. Het gaat dan zeker om de initiatieven waarbij deskundigen van verschillende disciplines en sectoren elkaar opzoeken om samen te leren en samen zaken aan te pakken – regionaal, nationaal en internationaal. Het zijn dergelijke fijnmazige verbeteringen die het netwerk van fraudebestrijders het flexibele karakter geven dat nodig is om fraudeurs te slim af te zijn. Wanneer vanuit de visie nieuwe maatregelen voortvloeien waarvoor nog geen middelen zijn voorzien in de begroting(en), worden business cases opgesteld. De business cases worden getoetst voordat besloten wordt of de maatregelen worden getroffen.

Voor de zomer van 2014 zal het kabinet u een voorstel voor deze uitvoeringsagenda sturen. Het kabinet hecht eraan hierbij het belang van het verbreden van de visie en het uitwerken van een uitvoeringsagenda in publiek-private samenwerking te benadrukken, net als de hoofdrol die burgers zelf vervullen bij de aanpak van identiteitsfraude.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,

dr. R.H.A. Plasterk