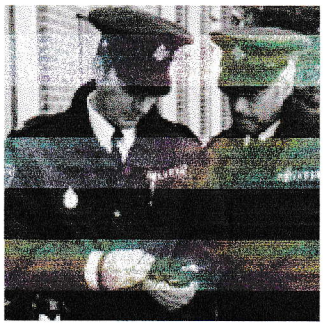
Punt 2.1.9.

Politie overtreedt wet bij opvragen telecomdata



Gepubliceerd: Donderdag 28 april 2011
Auteur: Andreas Udo de Haes

De politie en Nationale Recherche overtreden stelselmatig de wet bij het opvragen van klantgegevens van telecombedrijven. Van de 22 onderzochte bevragingen waren er maar liefst 14 onwettig.

Dat concludeert privacytoezichthouder College bescherming persoonsgegevens (CBP). Op alle vlakken gooien de opsporingsdiensten met de pet naar de wettelijke regels voor het opvragen van NAW-gegevens van telecomklanten.

Het CBP heeft onderzoek gedaan bij het CIOT, het Korps Haaglanden en de Nationale Recherche en het beeld is ontluisterend.

Opsporingsdiensten hebben totale lak aan de plichten en beperkingen die de wetgever heeft gesteld voor wie, wanneer en hoe privacygevoelige klantgegevens mag opvragen bij telecomproviders.

Onwettig en onbevoegd

Dit gebeurt officieel via de CIOT-database, het Centraal Informatiepunt Onderzoek Telecommunicatie is toegankelijk voor een select aantal politieambtenaren die uit deze databank naw-gegevens, mailadressen en ip-adressen kunnen opvragen. de CIOT wordt circa 3 miljoen keer per jaar geraadpleegd.

Duidelijke procedures voor het verlenen en intrekken van deze toegang (autorisatie) ontbreken. Daardoor zijn feitelijk alle autorisaties die zijn verleend in strijd met de wet, concludeert het CBP.

Ook kunnen veel agenten die sowieso niet bevoegd zijn de database in. Bij het Korps Haaglanden kunnen 25 agenten in het CIOT rondneuzen, terwijl er maar 6 bevoegd zijn.

Slecht beveiligd

Daarnaast doet de politie regelmatig direct een verzoek aan een telecomaanbieder voor klantgegevens, om het CIOT heen. In dergelijke gevallen blijkt geen sprake is van een adequate beveiliging bij het versturen van de data.

Ten slotte heeft het CBP 22 concrete bevragingen onderzocht. Bij het korps Haaglanden zijn vijf van de elf en bij de Nationale Recherche negen van de elf onderzochte bevragingen in strijd met de wet.

Deadline voor korpsen

Vorig jaar kwam bij een audit can het CIOT al een aantal misstanden boven water, maar het CBP legt nu stelselmatig misbruik van bevoegdheden bloot.

Onlangs zag minister Opstelten van Veiligheid en Justitie de bui al hangen en gaf opsporingsdiensten twee maanden de tijd om de procedures op orde te brengen.

Deze maatregelen werden aangekondigd vóórdat dit CBP-rapport uitkwam. Maar Opstelten was op de hoogte van de voorlopige conclusies van het CBP en heeft de maatregelen daar al op afgesteld, meldt het ministerie desgevraagd.

Per 1 mei moeten alle korpsen en de Nationale Recherche de zaken op orde hebben, anders worden ze afgesloten van de CIOT-database. Ze kunnen dan overigens nog wel bevragingen doen via andere korpsen die de procedures wel netjes volgen.

Relevante whitepaper: Data-opslag in de cloud
Download
BIJ DIT ARTIKEL ADVERTEREN?

COLLEGE BESCHERMING PERSOONSGEGEVENS

Politiekorpsen overtreden wet bij opvragen telecomgegevens via CIOT

Onderzoek CBP naar gegevensuitwisseling tussen opsporingsdiensten en telecommunicatieaanbieders

Persbericht, 28 april 2011

De gegevensuitwisseling tussen de opsporingsdiensten en telecommunicatieaanbieders via het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) vindt niet plaats overeenkomstig de toepasselijke wet- en regelgeving met de daarin opgenomen waarborgen tegen misbruik van de bestanden. Dat concludeert het College bescherming persoonsgegevens (CBP) na onderzoek bij het CIOT, het regionaal politiekorps Haaglanden en de Dienst Nationale Recherche (DNR) van het Korps Landelijke Politiediensten (KLPD). Burgers moeten erop kunnen vertrouwen dat zorgvuldig met hun telecomgegevens wordt omgegaan en dat alleen bevoegde personen gebruik maken van de bestanden bij het CIOT. Het CBP heeft onder meer geconstateerd dat formele procedures voor het toekennen en intrekken van autorisaties voor toegang tot het CIOT-informatiesysteem (CIS) bij de korpsen Haaglanden en DNR ontbreken en dat niet alle autorisaties aan de opsporingsambtenaren en de medewerkers van het CIOT rechtsgeldig zijn verleend. Daarnaast is de beveiliging van de telecomgegevens bij rechtstreekse opvragingen door opsporingsdiensten bij de telecommunicatieaanbieders – dus zonder tussenkomst van het CIOT – onderzocht. Het CBP concludeert dat er in dergelijke gevallen geen sprake is van een adequate beveiliging. Het gaat hier om gevoelige gegevens waarvoor zware beveiligingseisen gelden om verlies of onrechtmatige verwerking van de gegevens door onbevoegden te voorkomen. Tot slot is ook de rechtmatigheid van een aantal specifieke bevragingen onderzocht. Het CBP concludeert dat bij het korps Haaglanden vijf van de elf en bij de DNR negen van de elf onderzochte bevragingen in strijd met de wet zijn.

Lees hier het rapport van definitieve bevindingen CIOT (241 KB)

Lees hier het rapport van definitieve bevindingen politiekorps Haaglanden (288 KB)

Lees hier het rapport van definitieve bevindingen DNR (316 KB)

Het CBP heeft onder meer geconstateerd dat bij de korpsen Haaglanden en DNR formele procedures voor het toekennen en intrekken van autorisaties voor toegang tot het CIS ontbreken. De formele procedures zijn van belang om te waarborgen dat alleen bevoegde gebruikers toegang hebben tot het systeem en dat onbevoegde toegang wordt voorkomen.

Ook heeft het CBP geconcludeerd dat de autorisaties voor toegang tot het CIS aan zowel de medewerkers van het CIOT die beheerstaken uitvoeren op het CIS als aan de opsporingsambtenaren niet rechtsgeldig zijn verleend. Rechtsgeldige autorisaties vormen een waarborg tegen toegang door willekeurige personen tot in dit geval zeer gevoelige gegevens.

Uit het onderzoek is ook gebleken dat de rechtstreekse bevragingen door de onderzochte opsporingsdiensten aan de telecommunicatieaanbieders – buiten het CIOT om – via een openbare telefoonlijn zonder aanvullende beveiligingsmaatregelen worden verzonden. Het CBP concludeert dat er geen sprake is van een passend beveiligingsniveau. De combinatie van bijvoorbeeld identificerende gegevens met gegevens van een misdrijf levert zeer gevoelige gegevens op. Hiervoor moeten extra beveiligingsmaatregelen worden getroffen om de vertrouwelijkheid en de integriteit van de gegevens te waarborgen. Het CBP concludeert dat er sprake is van strijd met de wet omdat er geen extra beveiligingsmaatregelen zijn genomen om deze gevoelige gegevens te beveiligen.

Tot slot is ook de rechtmatigheid van een aantal specifieke bevragingen onderzocht. Het CBP concludeert dat bij het korps Haaglanden vijf van de elf en bij de DNR negen van de elf onderzochte bevragingen in strijd met de wet zijn, in die zin dat de korpsen de betreffende bevragingen van het CIS niet konden verantwoorden.

BINNENLAND

Reiziger is ov-chip spuugzat

door door Harry van Gelder

Reizigers en vervoerbedrijven zijn woedend op chipkaartbeheerder Trans Link Systems (TLS) na nieuw trammelant met de ov-chipkaart. „Ik ben het geklungel van TLS meer dan zat! Onze reizigers lijden hieronder. Wij gaan de schade bij TLS claimen", zegt directeur Anne Hettinga van streekvervoerder Arriva.

Foto: ANP

Tienduizenden reizigers van bus, trein, tram of metro kregen gisteren te maken met een landelijke storing van het ov-chipkaartsysteem. Tegoeden en abonnementen die via internet waren aangeschaft, konden bij de oplaadpalen niet op de chipkaart worden gezet, waardoor mensen niet konden reizen.

Een woordvoerder van reizigersorganisatie Maatschappij Voor Beter Openbaar Vervoer vindt het ongelooflijk dat reizigers moeten boeten voor fouten bij de chipkaartbeheerder. „TLS maakt een fout en de reiziger kan het weer zelf uit gaan zoeken."

Lees verder in De Telegraaf van vandaag.

Maandag 20 februari 2012. Het laatste nieuws het eerst op NU.nl

Ministers erkennen ernst KPN-hack

Laatste update: 20 februari 2012 17:25

AMSTERDAM - De hackers die inbraken bij KPN hebben inderdaad toegang geha het internetverkeer en konden bovendien de routering van dit verkeer beïnvloede

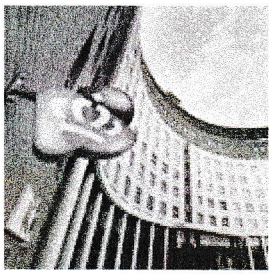


Foto: ANP

Dat erkennen de ministers Ivo Opstelten (Veiligheid en Justitie Maxime Verhagen (Economische Zaken, Landbouw en Innova

Zij stuurden over de hack bij KPN een brief naar de Tweede K die opgepikt is door Tweakers.net. In de brief schrijven de min dat de hackers toegang hebben gekregen tot de DNS-systeme KPN.

"De hackers hebben gebruikersrechten gehad op een van de routers. Daarmee had tijd routering van het internetverkeer van de consumentenklanten van KPN beïnvloed kunn worden", aldus Opstelten en Verhagen in de brief.

De ministers erkennen dat er geen bewijs is gevonden dat het internetverkeer ook beïn onderschept is. Dat stelden de hackers zelf ook al.

KPN maakte gebruik van sterk verouderde software die inmiddels geüpdatet is. Boven heeft KPN een aantal veiligheidsmaatregelen versneld uitgevoerd.

Toegang

In eerste instantie beweerde KPN dat alleen toegang tot persoonsgegevens verschaft v Door de toegang tot diepere servers konden de hackers internetverkeer in theorie onderscheppen en bijvoorbeeld omleiden.

In de brief benadrukken de ministers het belang van goede beveiliging in het algemeen zich steeds verder digitaliserende maatschappij is het van cruciaal belang dat elke orga uiterst zorgvuldig omgaat met klant- en of persoonsgegevens. Het betreft hier in veel g een eigen verantwoordelijkheid van deze organisaties."

Wel wijzen Opstelten en Verhagen op wet- en regelgeving en toezicht vanuit de overhe

Eerdere berichten

Vandaag

- Ministers erkennen ernst KPN-hack
- 'Scholieren achter Griekse cyberaanval'
- Mogelijk ook Pirate Bay-blokkade in Engeland
- 'Grotere databundels bij T-Mobile'
- Weer internetproblemen voorafgaand aan verkiezingen Iran
- Hi biedt 'onbeperkt' mobiel internet
- 'Samsung gaat films streamen op tablets en smartphones'
- Samsung zet lcd-tak opzij
- 'Winkels benutten internet onvoldoende'

Politiek wil debat over ict-veiligheid bij overheid na DigiNotar-hack

Door **Wilbert de Vries**, woensdag 7 september 2011 08:24, views: 11.840

Een meerderheid van de Tweede Kamer wil een debat met minister Donner van Binnenlandse Zaken over de DigiNotar-hack. Het is volgens de Kamerleden niet voor het eerst dat een ict-project bij de overheid faalt. De regie zou zoek zijn.

De Kamerfractie van de SP laat weten ontevreden te zijn over de antwoorden die Donner dinsdag gaf tijdens het wekelijkse vragenuurtje in de Kamer. Volgens SP-Kamerlid Sharon Gesthuizen is er inmiddels 'kamerbrede steun voor een uitgebreid debat over het debacle bij DigiNotar'. Dit debat wordt waarschijnlijk volgende week gehouden.

Tijdens het vragenuurtje stelde de minister onder meer dat het internet nooit 100 procent veilig kan zijn en dat Nederland niet het enige land is met dit probleem. Volgens Gesthuizen bagatelliseert Donner het achterliggende probleem. "De overheid en ict zijn tot nog toe een ongelukkige combinatie", aldus de politica. "Dat de burgers en bedrijven van Nederland inmiddels wekenlang ten prooi hebben kunnen vallen van kwaadwillenden reken ik hem heel erg zwaar aan."

Gesthuizen stelt dat internetters ervan op aan moeten kunnen dat de overheid alles doet om de veiligheid op het internet te waarborgen. "De burgers van Nederland hebben recht op de allerhoogste garantie van veiligheid wanneer zij door de overheid verplicht een overheidswebsite gebruiken. Dat vertrouwen is beschadigd en de minister heeft dat nog niet hersteld."

De overheid besloot vrijdag de banden met DigiNotar door te snijden, omdat niet gegarandeerd kon worden dat de PKIoverheid-certificaten van DigiNotar nog veilig waren. Misbruik van de overheidscertificaten is niet aangetoond. Hetzelfde blijkt te gelden voor een aantal andere certificaat-autoriteiten, waaronder het Ministerie van Justitie, de Nederlandse Orde van Advocaten, TenneT, Renault-Nissan en de TU Delft; ook de veiligheid van certificaten van die autoriteiten kan niet worden gegarandeerd, omdat DigiNotar ze verzorgde.

Eerder al hadden ook de browsermakers aangegeven de DigiNotar-certificaten op de zwarte lijst te zetten. Zo blokkeerde Chrome 247 DigiNotar-certificaten en kondigden ook Mozilla en Microsoft aan de certificaten van DigiNotar niet langer te vertrouwen. Microsoft heeft op verzoek van de overheid besloten de update die de DigiNotar-certificaten in de ban moet doen, in Nederland nog niet automatisch uit te rollen.

Dit moet bedrijven en overheden wat tijd geven om de omstreden certificaten te vervangen, zo zei Donner eerder deze week tijdens een persconferentie. DigiNotar heeft in Nederland zo'n 58.000 ssl-certificaten uitgegeven en als deze van de ene op de andere dag ongeldig worden verklaard, leidt dit volgens de minister tot 'maatschappelijke schade'. "We denken dat de overheid nog drie tot vier dagen nodig heeft om de certificaten te vervangen", zei Donner maandag. "Voor de certificaten op machines voor contacten tussen machines onderling is langer nodig." Wanneer de hele overstap op nieuwe certificaten voor deze machine-to-machine-certificaten is afgerond, kon Donner niet precies aangeven.

Wel gaf de minister aan dat de tijd hiervoor beperkt is door de updatedruk vanuit Microsoft. Die druk is dinsdagavond iets opgevoerd, toen het softwarebedrijf de bewuste update vrijgaf. Internetters en systeembeheerders die niet willen wachten tot de automatische update uitkomt, kunnen deze nu al downloaden en installeren.

DigiNotar kwam een week geleden in het nieuws, toen bleek dat hackers systemen van het bedrijf hadden gebruikt om valse certificaten te genereren. Hoewel DigiNotar de hack 19 juli ontdekte, trok het bedrijf niet aan de bel. Uit het onderzoek van Fox-IT blijkt dat het aan adequate beveiliging bij DigiNotar ontbrak en dat de eerste sporen van de aanvallers al dateren van 17 juni. De laatste valse certificaten werden aangemaakt op 22 juli, drie dagen na de ontdekking.

Vrijdag 16 maart 2012. Het laatste nieuws het eerst op NU.nl

'Ministers moeten uitleg veiligheid overheidsites geven'

Laatste update: 2 september 2011 11:06

AMSTERDAM – Drie PVV-Kamerleden hebben aan vier ministers vragen gesteld over de valse certificaten die na een hack bij Diginotar zijn uitgegeven. Overheidswebsite zijn daardoor potentieel onveilig.

Foto: Chris Heijmans

De Kamerleden Elissen, Hernandez en Kortenoeven eisen opheldering van de ministers van Veiligheid en Justitie, Buitenlandse Zaken, Binnenlandse Zaken en Koninkrijksrelaties en die van Defensie.

Ten eerste wil de PVV weten of de 'blunder' gevolgen heeft voor het gebruik van DigiD.

Certificaten

De website van DigiD gebruikt certificaten van het bedrijf Diginotar, dat één van de partijen is die certificaten voor websites uitgeeft. Door deze certificaten worden pagina's als veilig aangemerkt.

Na een hack vanuit de Iraanse overheid waren deze certificaten vals en kon er bijvoorbeeld bij Gmail meegekeken worden. Dit was mogelijk omdat gebruikers via het valse certificaat naar een andere website werden doorgestuurd die er hetzelfde uitzag als Gmail, maar niet beveiligd was.

Privacy Nederland

De Nederlandse overheid maakt ook gebruik van de certificaten van Diginotar. De AIVD houdt de situatie in de gaten. De PVV-Kamerleden vragen aan de ministers of er nadere inspectie nodig is om de privacy van Nederlandse burgers te waarborgen.

"Gaat de blunder bij Diginotar gevolgen hebben voor de elektronische dienstverlening van de overheid? Gaan burgers hier hinder van ondervinden?", aldus de PVV. Ook is de partij benieuwd naar de gevolgen voor de samenwerking tussen Diginotar en de overheid nu bedrijven als Google, Microsoft en Mozilla in hun browsers waarschuwen voor de certificaten.

Cyberwarfare

De PVV wil dat de ministers gaan onderzoeken of Iran inderdaad achter de hack van Diginotar zit. "Is hier sprake van cybercrime of cyberwarfare", is te lezen in de brief.

GroenLinks stelde eerder deze week al Kamervragen met dezelfde strekking. Ook D66 is niet te spreken over de onstane situatie.

Tekst en uitleg

Sharon Gesthuizen van de Socialistisch Partij heeft geen rust om op de beantwoording van schriftelijke vragen te wachten. Zij benadrukt tegenover NU.nl dat er veel vragen leven, waarop zo snel mogelijk antwoord moet komen. Daarom vindt ze ook dat de ministers tijdens het vragenuurtje in de kamer al tekst en uitleg moeten geven.

Zo moet duidelijk worden welke informatie in verkeerde handen is gevallen, waarom de AIVD met de zaak aan de slag is gegaan, wat er precies gebeurd is en wat mensen moeten doen. Daarnaast hoopt ze er vandaag of dit weekend door de overheid meer tekst en uitleg wordt gegeven.

Eerdere berichten

Vandaag
- Miljoenenboete voor Samsung en LG om misleiden consumenten
- Geen schikking tussen Opta en KPN
- KLPD waarschuwt voor schadelijke nepmail
- PayPal maakt betaaloplossing voor smartphones
- Google weer onder vuur om privacy

Gisteren
- NU.nl adviseert controle na cyberaanval
- FBI faalt bij kraken ontgrendelpatroon Android
- Korte tijd malware verspreid via NU.nl
- Google voert grote wijziging in zoekmachine door
- 'Ziggo ziet af van eigen telecomnetwerk'
- 'Providers verdacht van Europese afspraken'
- Cyberaanval op BBC mogelijk afkomstig van Iraanse overheid
- 'Apple ondervraagd in onderzoek naar machtsmisbruik Google'

Eerder
- Providers eisen andere rechter in zaak Pirate Bay
- Atlas van Stolk digitaliseert beeldcollectie

Vrijdag 16 maart 2012. Het laatste nieuws het eerst op NU.nl

'Diginotar negeerde misbruik en was slecht beveiligd'

Laatste update: 6 september 2011 13:03

DEN HAAG – Het Beverwijkse bedrijf Diginotar wist al op 28 juli dat mensen in Iran daadwerkelijk werden misleid. Ook blijkt de beveiliging op cruciale punten afwezig te zijn geweest, waardoor misbruik kinderlijk eenvoudig was.

Foto: ANP

Dat blijkt uit het onderzoek dat is gehouden door Fox IT naar aanleiding van de hacks bij Diginotar, een dochter van beveiligingsbedrijf Vasco Data Security.

Een overheidsbron heeft NU.nl en Webwereld dit onderzoek laten inzien.

De Nederlandse instantie die gaat over ICT-veiligheid bij de overheid hoorde pas vorige week maandag van Duitse collega's van problemen met certificaten van Diginotar.

Een Iraniër had dit gemeld op een forum van Google. DigiNotar zelf wist in juni al van een digitale inbraak bij het bedrijf en stelde een maand later onderzoek in. Maandag deed het bedrijf pas aangifte van de digitale inbraak.

Uit het onderzoek blijkt nu dat op 28 juli al duidelijk was dat er daadwerkelijk ook misbruik van nepcertificaten werd gemaakt en dat dit verkeer ook grotendeels uit Iran kwam.

Van het misbruik is door de onderzoekers een animatie gemaakt.

Regels

Het beeld dat Fox IT schetst is ontluisterend voor een bedrijf dat beveiligingscertificaten verkoopt. Zo blijkt tegen de regels in, de technische omgeving voor het aanmaken van deze digitale identiteitsbewijs gewoon vanaf de werkplek benaderbaar te zijn geweest.

Daarbij was het systeem ingericht dat iemand die op de werkplek bij Windows was aangemeld ook bij de beveiligde omgeving kon komen.

Daarbij hebben de onderzoekers ook bewijzen aangetroffen dat de omgeving van overheidscertificaten met het netwerk van het bedrijf verbonden was. Dat zou helemaal niet mogen, omdat deze systemen in een afgesloten kluis staan. Het zou technisch onmogelijk moeten zijn hier via een netwerk bij te kunnen komen.

Onveilig

Maar ook met de beveiliging blijkt van alles mis te zijn. Zo ontbrak het aan anti-virusbescherming voor het Windows besturingssysteem.

Ook detectiemogelijkheden om de inbraak te ontdekken blijken niet te hebben gefunctioneerd. Verder blijkt het opslaan van bewerkingen in een logboek onvoldoende te zijn geregeld.

Verder heeft het bedrijf ook in de administratie steken laten vallen. Zo stellen de onderzoekers vast dat er overheidscertificaten zijn aangemaakt, waarbij niet meer te achterhalen is hoe dat heeft kunnen gebeuren. Juist die vastlegging is cruciaal voor de rol van een digitale notaris.

Daarnaast blijken ook andere beveiligingspraktijken slecht te zijn. Wachtwoorden van systeembeheerders waren zo slecht gekozen dat deze geautomatiseerd zijn gekraakt. Dat maakt niet alleen de inbraak mogelijk, maar door de toegang tot het certificaatsysteem konden de Iraniërs ook meteen kwaadaardige handelingen uitvoeren.

Sleutels

Oud-Diginotar-medewerker Remko de Graaf meldt in RTL Nieuws dat het bedrijf tegen de regels in kopieën van sleutels bewaarde in een losse database.

Als dat verhaal klopt dan hebben medewerkers of hackers ook de mogelijkheid gehad om misbruik van verbindingen te maken of ten onrechte digitale handtekeningen te zetten.

Gemakzucht

De oorzaak zou niet kwaadaardig zijn, maar juist met gemakzucht te maken hebben. Door de opslag van sleutels is het eenvoudig om op een later moment een eventuele fout te herstellen.

Dezelfde sfeer ademt het rapport uit: een bedrijf waar medewerkers vooral technische obstakels maximaal uit de weg ruimen om simpel te werken.

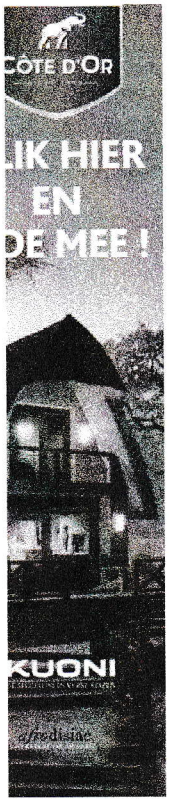
De onderzoekers gaan niet zover om de overheid van Iran te beschuldigen. Wel stellen ze dat de aanval is gericht op het afluisteren van het Iraanse volk.

Lees alles over de hack bij Diginotar

Eerdere berichten

Vandaag

Vrijdag 16 maart 2012. Het laatste nieuws het eerst op NU.nl



Diginotar deed geen aangifte hack

Laatste update: 6 september 2011 12:47

AMSTERDAM – Het bedrijf Diginotar heeft niet alleen de Iraanse kraak van het bedrijf voor betrokkenen geheim gehouden ook is geen aangifte gedaan. Als er nu onderzoek loopt dan is dat pro-actief handelen van het Openbaar Ministerie.

Dat ontdekte NU.nl op basis van onderzoek.

Al op 19 juli was bij het bedrijf Diginotar bekend dat er was ingebroken en dat hackers valselijk certificaten hadden aangemaakt. Ook is duidelijk dat vermoedelijk de Iraanse overheid achter de kraak heeft gezeten.

Strafrechtelijk onderzoek

"Er is bij ons geen aangifte gedaan over de inbraak bij Diginotar", meldt Wim de Bruin, voorlichter bij het Landelijk Parket aan NU.nl. Hij erkent dat dit niet betekent dat er vervolgens geen strafrechtelijk onderzoek is gestart.

Het Openbaar Ministerie kan ook op eigen gezag een onderzoek starten. "Daarover kan ik geen mededelingen doen, want dan hebben we het over lopende opsporing." Overigens kan een strafrechtelijkonderzoek zich ook tegen het bedrijf Diginotar keren, omdat de onderneming de betrokken partijen niet heeft geïnformeerd en geen aangifte heeft gedaan.

Inmiddels is bekend dat er wel een strafrechtelijk onderzoek is gestart. Dit is gedaan op verzoek van Diginotar. Maandag zal Diginotar formeel aangifte doen.

Mogelijk strafbaar

Twee advocaten stellen tegenover NU.nl op voorwaarde van anonimiteit dat het nalaten van handelen strafbaar kan zijn. Het gaat er dan om dat het algemeen bekend is dat dissidenten in Iran gevaar lopen. Mocht iemand om het leven komen en kan dat aan de nalatigheid worden toegeschreven dan is er sprake van dood door schuld.

Nadat Diginotar gehackt werd, konden valse certificaten worden uitgegeven waardoor ogenschijnlijk veilige websites, niet beveiligd waren. De Iraanse overheid kon meelezen en gegevens kopiëren.

Maatregelen nemen

"Ik vind absoluut dat de nalatigheid onderzocht moet worden. Dat zou interessante jurisprudentie opleveren hoe we met dit soort zaken moeten omgaan", zeg SP-kamerlid Sharon Gesthuizen tegen NU.nl.

Ze wijst erop dat je kunt vermoeden dat mensen gevaarlopen, omdat bij andere incidenten in China dissidenten zijn opgespoord met uit communicatie verkregen gegevens.

Verantwoordelijkheid

"Mensenrechten zijn fundamenteel en bedrijven hebben daar een verantwoordelijkheid in te nemen", stelt ook Europarlementariër Marietje Schaake van D66. "Ik vind dat ze minimaal dat ze kenbaar hadden moeten maken dat de kraak speelde. Zo hadden mensen maatregelen kunnen nemen om zichzelf te beschermen."

Vasco Data Security, het moederbedrijf van Diginotar, reageerde niet op diverse verzoeken om commentaar.

Eerdere berichten

Vandaag

- 'Handelen overheid snel en adequaat in DigiNotar-crisis'

Eerder

- Onderzoek Diginotar richt zich op overheid
- 'Doden gevallen in Iran door Diginotarhack'
- Onderzoek naar overheids-ICT na Diginotarhack
- 'Computerinbraken verplicht melden'
- Debat over DigiNotar pas volgende week
- Kamer debatteert over Diginotar
- SP wil 'crash team' voor internetproblemen
- Moederbedrijf DigiNotar lijdt miljoenenschade
- 'Kans op schadevergoeding DigiNotar nihil'
- Chronologie DigiNotar
- Diginotar failliet verklaard
- Hackers zijn beveiligingsproblemen beu
- Voor veilig ICT hele dag 'op kabels kijken'
- OPTA zet Diginotar buitenspel
- Windowsupdate bij gemeenten verloopt soepel
- Internet Explorer blokkeert sites met Diginotarcertificaten
- Overheid onderzoekt certificatenstelsel
- Helft NU-lezers vreest privacyschending na Diginotarhack
- Gemeenten geadviseerd Windows niet automatisch te updaten

Zaterdag 3 september 2011. Het laatste nieuws het eerst op NU.nl

SP wil parlementair onderzoek ICT-beveiliging

Laatste update: 3 september 2011 17:33

DEN HAAG – Na alle problemen met overheidscertificaten is de maat voor de SP vol. Er moet een parlementair onderzoek naar digitale veiligheid komen.

Foto: ANP

Daarvoor pleit het SP-kamerlid Sharon Gesthuizen. Directe aanleiding zijn de problemen voor de overheid die zijn ontstaan na het hacken van certificaten bij het bedrijf DigiNotar.

Hierdoor is de veilige toegang van websites bij de overheid niet langer te garanderen en moeten versneld nieuwe certificaten worden uitgegeven.

"We zagen het ministerie woensdag nog beweren dat er niets aan de hand was, terwijl de klus door de inbrekers al lang en breed geklaard was. Helaas is er de afgelopen jaren aan de lopende band sprake van incidenten als het om ICT veiligheid gaat", vertelt Gesthuizen tegenover NU.nl.

Ook wees ze op eerdere beveiligingsproblemen rond DigiD en de OV-chipkaart. Dit laat volgens de SP zien dat de zaken te vaak niet op orde zijn en dat essentiële informatie over veiligheidsissues niet boven tafel komt voordat cruciale beslissingen worden genomen. Gesthuizen zal minister Donner komende week ter verantwoording roepen.

Bewustzijn

"Er werden zaken gedaan met een bedrijf dat duidelijk niet in staat was de veiligheid te borgen. Dat is zeer kwalijk - het heeft bij het ministerie absoluut aan controle en bewustzijn geschort", stelt ze dan ook.

Maandag bleek dat de Iraanse overheid het verkeer naar Google tapt, zodat communicatie zoals bijvoorbeeld Gmail niet langer veilig is. Dit was mogelijk doordat een computer in Iran door het bedrijf DigiNotar als echte Google-computer is aangemerkt voor verkeer dat uit Iran kwam. Ook certificaten van Yahoo, Skype en enkele softwareleveranciers blijken te zijn vervalst.

Het bedrijf ontdekte de problemen al op 19 juli, maar heeft de problemen onder de pet gehouden en weigert commentaar.

Eerst debat

D66 zegt in een reactie de gedachte van de SP te steunen. "Internetveiligheid staat duidelijk op de tocht", stelt kamerlid Kees Verhoeven tegenover NU.nl. Daarbij wijst hij ook naar de vele privacyproblemen die de laatste tijd bij allerhande systemen spelen.

Toch wil hij eerst liever een debat op hoofdlijnen voeren. Als dat onvoldoende bevredigend is staat hij open voor een parlementair onderzoek. Daarbij kan niet worden volstaan met de huidige inspanningen.

Eerdere berichten

Vandaag

- SP wil parlementair onderzoek ICT-beveiliging
- Politie slaags met extreem rechts in Londen
- Sandor Kepiro overleden
- Berlusconi niet uit politiek
- Zoektocht naar drenkeling Oude Maas
- Tripoli krijgt veiligheidsraad
- Ouders aangehouden om cocaïne in luier

Rechtbank Den Haag, sector civiel recht
29 november 2010; 10.00 uur
rolnr. 2010/1807

Staat der Nederlanden/Stichting Privacy First e.a.

Pleitnota mrs. C.M. Bitter en G.J.S. ter Kuile

1 Inleiding

1.1 De invoering van vingerafdrukken in de Nederlandse reisdocumenten per 28 juni 2009 was per die datum verplicht op grond van de Europese paspoortverordening. In EU-verband wordt de implementatie van de verordening gezien als "een belangrijke stap [gezet] in de richting van het gebruik van nieuwe elementen waarmee paspoorten en reisdocumenten beter kunnen worden beveiligd en een betrouwbaarder verband kan worden gelegd tussen de houder en zijn reisdocument, dat daardoor beter beschermd is tegen frauduleus gebruik" (overweging 2 van wijzigingsverordening 444/2009). In de nog voor deze zitting door eisers ingebrachte producties, waaronder het rapport Happy Landings, worden bezwaren tegen het gebruik van vingerafdrukken in reisdocumenten aangevoerd (De WRR vermeldt op de website dat de inhoud en de ingenomen standpunten voor rekening zijn van de auteur.). Die bezwaren kunnen geen rol spelen in de procedure. Nederland heeft ten aanzien van de opname van vingerafdrukken in de reisdocumenten geen keus, maar is verplicht de Europese verordening na te leven. Dat is een gegeven in deze procedure.
Hoe vingerafdrukken in de reisdocumenten moeten worden opgeslagen in de chip van de reisdocumenten is uitgewerkt in twee beschikkingen van de Europese Commissie met specificaties waaraan moet zijn voldaan. In deze procedure gaat het er evenmin om of daaraan in de Nederlandse reisdocumenten is voldaan. Dat is het geval.

1.2 Verder benadrukt de Staat nog eens dat de onderwerpen die in deze procedure aan de orde kunnen komen ook in zoverre beperkt zijn dat de nationale uitvoeringsregelgeving grotendeels nog niet is ontworpen en vastgesteld. Die

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Actueel

7 nieuwsberichten gevonden

- **Nieuwe tarieven voor 2012: tarief paspoort en NIK daalt. Tarief jeugd-NIK stijgt. [/nederlands/Actueel/Nieuwe_tarieven_voor_2012_tarief_paspoort_en_NIK_daalt_Tarief_jeugd_I**
  nieuwsbericht | 01-11-2011

- **Nieuw model Nederlandse reisdocumenten [/nederlands/Actueel/Nieuw_model_Nederlandse_reisdocumenten]**
  nieuwsbericht | 07-10-2011

- **Geldigheid van de Nederlandse identiteitskaart buiten de landen van de Europese Unie. [/nederlands/Actueel/Geldigheid_van_de_Nederlandse_identiteitskaart_buiten_de_landen_van_**
  nieuwsbericht | 13-07-2011
  In de media is het bericht verschenen dat de Nederlandse identiteitskaart (binnenkort) geen officieel reisdocument meer is en er daarom alleen nog maar binnen de landen van de Europese Unie mee kan worden gereisd. Naar aanleiding van dit bericht wordt aan het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de vraag gesteld of het nu nog wel mogelijk is met een Nederlandse identiteitskaart te reizen naar landen die geen lid zijn van de Europese Unie. Het antwoord daarop is ja!

- **Opslag vingerafdrukken voor nu stopgezet [/nederlands/Actueel/Opslag_vingerafdrukken_voor_nu_stopgezet]**
  nieuwsbericht | 28-04-2011
  De huidige opslag van de vingerafdrukken in de decentrale reisdocumentenadministraties wordt voor nu gestopt. Minister Donner van Binnenlandse Zaken en Koninkrijksrelaties is tot de conclusie gekomen dat gebruik van de vingerafdrukken voor verificatie en identiteitsvaststelling niet mogelijk is zonder een te hoog percentage gevallen waarin een 'misser' wordt aangegeven.

- **Reist u binnenkort naar de VS? [/nederlands/Actueel/Reist_u_binnenkort_naar_de_VS]**
  nieuwsbericht | 08-01-2010
  Met een geldig Nederlands paspoort kan gewoon zonder visum naar de Verenigde Staten worden gereisd. Dit geldt ook voor paspoorten die zijn uitgegeven voor 28 augustus 2006. Deze paspoorten bevatten geen chip.

- **Afschaffing bijschrijving kinderen in reisdocument [/nederlands/Actueel/Afschaffing_bijschrijving_kinderen_in_reisdocument]**
  nieuwsbericht | 08-01-2010
  Bijschrijvingen van kinderen in het paspoort van ouder(s) blijven geldig tot 26 juni 2012. Daarna moeten kinderen een eigen reisdocument hebben. Dit is het gevolg van een wijziging van de Europese verordening die voorschrijft waaraan reisdocumenten moeten voldoen.

- **Invoering vingerafdrukken [/nederlands/Actueel/Invoering_vingerafdrukken]**
  nieuwsbericht | 26-06-2009
  De Nederlandse reisdocumenten moeten op grond van Europese regelgeving vanaf 28 juni 2009 vingerafdrukken in de chip bevatten. Dit vloeit voort uit de verordening (EG) nr. 444/2009 van het

Europees Parlement en de Raad van 28 mei 2009 tot wijziging van Verordening (EG) nr. 2252/2004 van de Raad betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten.

Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2010–2011

25 764 Reisdocumenten

Nr. 47

VERSLAG VAN EEN ALGEMEEN OVERLEG

Vastgesteld 19 mei 2011

De vaste commissie voor Binnenlandse Zaken[1] en de vaste commissie voor Europese Zaken[2] hebben op 27 april 2011 overleg gevoerd met minister Donner van Binnenlandse Zaken en Koninkrijksrelaties over:

- **de brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties d.d. 14 februari 2011 over de implementatie van de EU-verordening betreffende de normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten (25 764, nr. 45);**
- **de brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties d.d. 18 maart 2010 betreffende vingerafdrukken in Nederlandse reisdocumenten (25 764, nr. 42);**
- **de brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties d.d. 27 april 2011 betreffende reisdocumenten (t.b.v. AO 27 april 2011) (25 764, nr. 64).**

Van het overleg brengt de commissie bijgaand woordelijk geredigeerd verslag uit.

De voorzitter van de vaste commissie voor Binnenlandse Zaken,
Dijksma

De voorzitter van de vaste commissie voor Europese Zaken,
Verburg

De griffier van de vaste commissie voor Binnenlandse Zaken,
Van der Leeden

[1] Samenstelling:
Leden: Dijksma (PvdA), voorzitter, Van Beek (VVD), Van der Staaij (SGP), Koopmans (CDA), Van Bochove (CDA), Aptroot (VVD), ondervoorzitter, Smilde (CDA), Paulus Jansen (SP), Ortega-Martijn (ChristenUnie), Brinkman (PVV), Van Raak (SP), Thieme (PvdD), Dibi (GroenLinks), Heijnen (PvdA), Elissen (PVV), Monasch (PvdA), Schouw (D66), Marcouch (PvdA), De Boer (VVD), Hennis-Plasschaert (VVD), Lucassen (PVV), Verhoeven (D66) en Grashoff (GroenLinks).
Plv. leden: Van Dam (PvdA), Van der Burg (VVD), Dijkgraaf (SGP), Sterk (CDA), Bruins Slot (CDA), Van der Steur (VVD), Knops (CDA), Jasper van Dijk (SP), Rouvoet (ChristenUnie), Van Klaveren (PVV), Rik Janssen (SP), Ouwehand (PvdD), Van Gent (GroenLinks), Kuiken (PvdA), Fritsma (PVV), Vermeij (PvdA), Pechtold (D66), Wolbert (PvdA), Van Nieuwenhuizen (VVD), Taverne (VVD), Bontes (PVV), Hachchi (D66) en Voortman (GroenLinks).

[2] Samenstelling:
Leden: Van Bommel (SP), ondervoorzitter, Van der Staaij (SGP), Albayrak (PvdA), Verburg (CDA), voorzitter, Ormel (CDA), Ferrier (CDA), Nicolaï (VVD), Eijsink (PvdA), Van Dam (PvdA), De Roon (PVV), Jansen (SP), Ten Broeke (VVD), Ouwehand (PvdD), Wiegman-van Meppelen Scheppink (ChristenUnie), Bontes (PVV), Groot (PvdA), Braakhuis (GroenLinks), Nieuwenhuizen (VVD), Schouw (D66), El Fassed (GroenLinks), Hachchi (D66) en Dijkhoff (VVD).
Plv. leden: Irrgang (SP), Dijkgraaf (SGP), Jacobi (PvdA), Haverkamp (CDA), Bruins Slot (CDA), Omtzigt (CDA), Azmani (VVD), Samsom (PvdA), Timmermans (PvdA), Elissen (PVV), Hennis-Plasschaert (VVD), Thieme (PvdD), Voordewind (ChristenUnie), Driessen (PVV), Dikkers (PvdA), Dezentjé Hamming-Bluemink (VVD), Van Veldhoven (D66), Van Tongeren (GroenLinks), Pechtold (D66), Huizing (VVD) en Kortenoeven (PVV).

kst-25764-47
ISSN 0921 - 7371
's-Gravenhage 2011

uitgangspositie gewenst om op die wijze verder gaan. Graag een reactie van de minister op dit punt.
Ik heb benadrukt dat de VVD een discussie over de toekomst nooit uit de weg gaat. Wij zijn heel blij met de plannen van de minister om de nationale identiteitskaart uit de Ppw te halen. Dat zou echt goed nieuws zijn, omdat mensen daarmee hun keuzevrijheid terugkrijgen. De vraag is wanneer we dit gaan doen, hoe we dit gaan doen en hoeveel tijd er voor nodig is. Het teruggeven van de keuzevrijheid als het gaat om intra-EU-reizen is belangrijk, zeker op een gevoelig dossier als dit.
Nu we hebben erkend dat het gebruik van biometrie op zijn zachtst gezegd een complexe zaak is, is mijn vraag of het een idee is om in Nederland een biometrie-coördinator in het leven te roepen, net zoals het VK en Duitsland hebben gedaan. Dit is iemand die zich door de lagen en zuilen van de overheid kan bewegen met een goed netwerk en kennis van zaken op het gebied van biometrie, identiteitsfraude en identiteitsmanagement. Met het oog op de EU-dimensie moet dit iemand zijn die over Europese kennis, ervaring en contacten beschikt.
Het beeld dat tijdens de hoorzitting van afgelopen week werd geschetst over het agentschap BPR kan de toets van het betamelijke niet doorstaan. Ik zeg dit voorzichtig. Duidelijk werd dat tijdens het besluitvormingsproces knelpunten te simplistisch zijn voorgesteld danwel zijn verzwegen, terwijl een alomvattend beeld van de stand van zaken uiteraard van cruciaal belang is voor een goed verloop van het besluitvormingsproces. Onafhankelijke adviezen zouden door het agentschap zijn beschouwd als een verstoring van de werkzaamheden. Daar ben ik van geschrokken. Dat kan en mag nooit de bedoeling zijn. Ik wil de minister vragen om op korte termijn volledige openheid van zaken te geven als het gaat om de onafhankelijke informatievoorziening richting de Tweede Kamer.
Naar aanleiding van twee voorbeelden heb ik nog een andersoortige vraag. Een man, niet getrouwd maar wel tweeëntwintig jaar samen met dezelfde vrouw, heeft drie kinderen. Die kinderen dragen om welke reden ook de achternaam van zijn vrouw. Nu werd de vader laatst aangehouden op het vliegveld omdat men hem verdacht van kindersmokkel of in ieder geval het verschil in achternaam niet geheel vertrouwde. De gemeente kon wel een soort verklaring afgeven, maar vader is niet zeker van de juridische status daarvan in het buitenland. Hij vraagt zich af in hoeveel talen zo'n verklaring dan moet worden opgesteld. Het tweede voorbeeld betreft een vrouw die sinds zes jaar is gescheiden van haar man. Haar dochter heeft zijn achternaam en een eigen paspoort. Elke keer dat ze door de douane gaan wordt moeder verhoord. Onaangenaam. Nu heeft moeder geprobeerd dit te voorkomen door steeds een internationale geboorteakte mee te nemen. De vraag is waarom het niet mogelijk is om op het paspoort van het kind de namen van beide ouders te vermelden. Het is een vraag met een heel ander karakter, maar niet minder belangrijk. Graag hoor ik van de minister wat de mogelijkheden zijn.

De heer **Heijnen** (PvdA): Voorzitter. Het is een heuglijke dag. Minister Donner trekt de stekker uit de opslag van de vingerafdrukken, zowel bij gemeente als Rijk. Ik kan deze brief niet anders lezen. Gelet op de discussie met betrekking tot de voorwaarden waarop het ooit tot opslag zou kunnen komen en gelet op hetgeen in de achterliggende tijd is gebeurd, acht ik het niet mogelijk dat wij hier ooit nog zullen praten over een voorstel om die biometrische gegevens op te slaan. Dat brengt mij tot de vraag wanneer wij de aanpassingen van de Ppw van deze minister kunnen verwachten. Het is ook een feestdag, omdat burgers die principiële bezwaren hebben tegen het afgeven van hun vingerafdrukken in de nabije toekomst over een ID-kaart kunnen beschikken. Ze kunnen zich daarmee identificeren waar nodig, ook voor het reizen binnen de EU. Mijn vraag aan de minister is wanneer dit in werking treedt. Kan hij het traject schetsen?

gestemd. Tot onze vreugde is de discussie over de veiligheid van de achterliggende techniek steeds breder op gang gekomen. De biometrie bleek niet veilig en makkelijk te manipuleren. Meer gemeenten kwamen daarachter en hielden er mee op, de gegevens op te slaan. De gemeente Roermond constateerde een foutmarge van 21%. Ook partijen die destijds deze techniek verdedigden komen erop terug. Zij zijn geschrokken. Dat siert hen. Vraag is wel of de Tweede Kamer destijds bij de besluitvorming voldoende geïnformeerd is geweest om de technische risico's van de biometrietechniek in te schatten. Wat was de rol van het agentschap BPR daarbij? Ook ik sluit me aan bij het pleidooi voor een onafhankelijk onderzoek daarnaar door een geschikte instantie, wellicht TNO.
Nu maakt ook de minister een pas op de plaats. Hij zegt voor een bepaalde periode geen decentrale opslag te willen. Waarom kiest hij voor deze tijdelijkheid, als bij de huidige stand van de techniek alle deskundigen zeggen dat het niet veilig kan? Je hebt niets aan de met deze techniek opgeslagen gegevens, dus moet je er definitief mee ophouden. Opslag wordt pas weer bespreekbaar zodra proportionaliteit, noodzakelijkheid en technische betrouwbaarheid vast zijn komen te staan. Wij zijn er geen voorstander van. Wat gaat er gebeuren met de verouderde databases? Wij zeggen dat ze moeten worden vernietigd. Je hebt er niets aan; ze zijn nutteloos en incompleet. Graag een reactie van de minister hierop. Volgens mij kan hij het simpel doen door een aanpassing van de Paspoortuitvoeringsregeling.
Waarom blijft de minister, ondanks het besluit voor de decentrale opslag, vasthouden aan het nut van het uitgangspunt van centrale opslag? Zijn uitgangspunt dat centrale opslag onvermijdelijk is als je wilt overstappen op een systeem dat reisdocumenten bij iedere willekeurige gemeente kunnen worden aangevraagd, deel ik niet. Nu kun je via een ambassade een paspoort aanvragen ongeacht je oorspronkelijke woonplaats in Nederland. Je moet de telefoon en de fax gebruiken, maar het kan al. De uitspraak van de minister gaat dus niet op. Graag een reactie van de minister op dit punt.
Het is goed om de ID-kaart uit de Ppw te halen. Betekent dit dat je een ID-kaart kunt aanvragen zonder opname van je vingerafdruk erin? Zo ja, met ingang van wanneer is dat het geval? Wij vinden dit een goede ontwikkeling.
De Europese verordening die tot opslag van vingerafdrukken in het paspoort verplicht, leidt bij meer EU-landen tot problemen. Wij zijn gecharmeerd van de Duitse methode. Zij beperken het alleen tot opslag in de chip in het paspoort, op vrijwillige basis. Kennelijk laat de verordening dat toe. Eigenlijk zijn we nog meer gecharmeerd van de Engelse methode. Bij hen is de verordening niet van toepassing. Kan dat misschien voor ons ook gelden? Opslag is voor betrouwbare identificatie en uit respect voor privacy in Engeland kennelijk niet nodig, dus hier ook niet.

Minister **Donner**: Voorzitter. De afgelopen maanden heb ik mij gebogen over de problematiek die hier aan de orde is. Ik heb dat eerder aan de Kamer gemeld in antwoord op vragen daarover. Gelet op de verschillende signalen en onderzoeken moet inderdaad worden bezien wat de verdere lijn moet zijn in de brede toepassing van de wetgeving zoals die is aanvaard, in het bijzonder het gebruik van vingerafdrukken dat daarin is opgenomen. Overigens wordt het opnemen van de vingerafdrukken niet geregeld in de Ppw, maar in de Europese verordening. Dit mag volgens Europees recht niet in de Ppw worden geregeld.
Ik heb de Kamer zodra zij daar om heeft gevraagd ingelicht, ook over het feit dat ik door verschillende signalen de tijd wilde nemen voor onderzoek. Ik heb in de tussentijd laten inventariseren hoe andere lidstaten van de Europese Unie met de materie omgaan. Die resultaten heb ik de Kamer op 14 februari toegestuurd. Daarnaast heb ik me georiënteerd op de verschillende publicaties, onderzoeken en argumenten die werden

Ministerie van Veiligheid en Justitie

Handreiking politie
Identiteitsfraude

Handreiking Identiteitsfraude

Identiteitsfraude is een verschijnsel dat in omvang lijkt toe te nemen. Om fraude met gebruik van een andere of een valse identiteit te voorkomen en te bestrijden is het van groot belang dat politie en Justitie de instrumenten inzetten die er zijn. Die bestaande instrumenten zijn grotendeels toereikend en waar dat nog niet het geval is zal aanvulling van wetgeving worden bevorderd. Op basis van de geldende wetgeving is in samenwerking met de politie en Koninklijke marechaussee (Kmar) deze handreiking voor gebruik in de praktijk opgesteld.

Doelstelling van de handreiking

Deze handreiking heeft ten doel de politiefunctionaris te helpen bij het benutten van de bestaande wettelijke instrumenten bij het opnemen van de aangifte om identiteitsfraude te bestrijden. De handreiking dient voor de meest voorkomende aangiften van strafbare feiten bijvoorbeeld valsheid in geschrifte, oplichting en diefstal van gegevens etc. Maar om zo compleet mogelijk te zijn wordt hierna het hele arsenaal aan delicten genoemd. Voor de ingewikkelde aangiften/ casussen, bijvoorbeeld op het terrein van computervredebreuk, wordt geadviseerd een deskundige op het gebied van identiteitsfraude in te schakelen.

Identiteitsfraude

Een standaarddefinitie van identiteitsfraude is er (nog) niet. Er zijn er verschillende definities van het begrip in omloop. In deze handreiking wordt gebruikt gemaakt van een definitie die in een onderzoeksrapport van het WODC [1] wordt gebruikt:

"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".[2]

[1] Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) is een onderdeel van het Nederlands Ministerie van Justitie en is gevestigd in Den Haag. De kerntaken van het WODC zijn de productie en verspreiding van wetenschappelijke kennis over onderbouwing en effecten van beleid en over relevante maatschappelijke processen op het brede terrein van Justitie en Vreemdelingenzaken en Integratie.

[2] U.R.M.Th. de Vries, Tigchelaar, H, van der Linden, M, Hol, A.M., 'Identiteitsfraude: een afbakening, een internationale begripsvergelijking en analyse van nationale strafbepalingen', Den Haag, 2007 p 228

te vormen om de aangifte op te nemen. Artikel 161 van het Wetboek van Strafvordering bepaalt bovendien dat de politie een verplichting heeft om aangifte op te nemen van enig strafbaar feit (een ieder die kennis draagt van een begaan strafbaar feit, is bevoegd daarvan aangifte of klacht te doen). Uiteraard moet er daarvoor wel een vermoeden zijn van identiteitsfraude.

Of identiteitsfraude plaats heeft door een vals of vervalst identiteitsdocument of doordat iemand zich verschuilt achter de identiteit van een ander of niet bestaande persoon maakt geen verschil: in alle gevallen begint de fraude met een mismatch tussen de persoon en zijn/haar ware identiteitsgegevens. Er is sprake van een onrechtmatige persoonsverwisseling, die op de volgende wijze kan gebeuren[4]:

- **Overname van identiteitsgegevens:** het overnemen van iemands identiteitgegevens en hier vervolgens misbruik van maken, zonder toestemming van de persoon. De fraudeur weet andermans identiteitsgegevens frauduleus te bemachtigen en lift vervolgens onrechtmatig op deze identiteit mee.
- **Identiteitsdelegatie:** medegebruik maken van iemands identiteit, met toestemming van die persoon. Als je een andere persoon inschakelt voor het afleggen van je schoolexamen, maak je je schuldig aan identiteitsdelegatie.
- **Identiteitsruil:** gebruik maken van de identiteit van een ander met toestemming van elkaar. Er is sprake van identiteitsruil als persoon A de gevangenisstraf van crimineel B uitzit onder de naam van crimineel B. Crimineel B maakt gebruik van identiteit van persoon A als niet eerder of niet ter zake veroordeelde persoon oftewel "vrije vogel" in de maatschappij.
- **Identiteitscreatie:** het creëren van fictieve identiteit, al dan niet met gedeeltelijke identiteitsgegevens van bestaande personen.

Bovengenoemde opzettelijke identiteitsveranderingen gebeuren door middel van valse of vervalste documenten. De fraudeur heeft het volgende arsenaal tot zijn beschikking: vervalste documenten, valse documenten, valselijk verkregen documenten en lookalikefraude. Een vervalst document is een origineel document waarin de fraudeur veranderingen heeft aangebracht. Een vervalst document wordt veelal door een ander gebruikt dan de rechtmatige houder van het document. Het valse document is helemaal vals. Een origineel document dat op valse gronden is gekregen, is een valselijk verkregen document. Het is de fraudeur gelukt door middel van manipulatie van een vals/vervalst brondocument of met behulp van een corrupte ambtenaar een nieuw, origineel document te bemachtigen. Bij lookalikefraude blijft het originele document intact en doet de fraudeur zich voor de houder van het document. Hij/zij vertoont enige uiterlijke gelijkenis met de foto in het document dat hij/zij misbruikt. Bij identiteitsdelegatie en identiteitsruil hoeft geen sprake te zijn van een vals/vervalst document. Wel kan er sprake zijn van een vals identificatiemiddel zoals vermeld in de definitie van identiteitsfraude.

Casus ter illustratie van het probleem

Om het fenomeen identiteitfraude beter te begrijpen ter illustratie het verhaal van Niels, een slachtoffer van identiteitsfraude. In juni 2006

[4] Rapportage "Ben je wie je zegt dat je bent?" Gemeente Amsterdam, Dienst Persoons- en Geo-informatie, Amsterdam 2009

BB
BINNENLANDS BESTUUR

POLITIE SCANT VINGERAFDRUK OP STRAAT

Sjors van Beek 19 jul 2011 9 reacties

De politie kan sinds kort vingerafdrukken afnemen op straat en die meteen online controleren. Zo'n 125 politie-agenten bij diverse regiokorpsen lopen inmiddels rond met speciale afleesapparatuur. Een eerste proef loopt tot begin 2012, dan wordt bekeken of de apparaatjes breed worden ingezet, aldus een woordvoerder van het Ministerie van Veiligheid & Justitie. 'De wens is wel om dit mogelijk te maken, maar we moeten nu eerst kijken of alles goed werkt'.

Smartphone

Het vingerafdruk-apparaatje is een soort smartphone waar een verdachte zijn vinger op legt. De vingerafdruk wordt digitaal afgelezen en via een beveiligde verbinding doorgestuurd naar de landelijke database waar vingerafdrukken in zijn opgeslagen.

Illegalen

De apparaatjes worden onder meer ingezet voor de intensievere controle op illegale vreemdelingen, zo liet minister Leers (Integratie) onlangs al weten. Via een koppeling met de 'Basisvoorziening Vreemdelingenketen' kan in de toekomst een gewone agent op straat meteen nagaan of iemand rechtmatig in Nederland verblijft. Ook kunnen politiemensen binnenkort paspoorten en andere identiteitsbewijzen op straat digitaal uitlezen en op echtheid controleren, en nagaan of iemand nog een boete heeft openstaan. Mobiel werken bij de politie vindt steeds meer ingang: sinds kort lopen er ook al proeven met digitaal boetes uitschrijven op straat.

Identiteitsfraude

Identiteitsfraude is een groot probleem voor Justitie. In de databanken van politie, Justitie, Gevangeniswezen en Reclassering staan niet altijd de juiste gegevens. Soms betreft dat een simpele tikfout, soms gaat het verder en zijn hele identiteiten verwisseld. Zo komt het voor dat anderen dan de werkelijke dader een straf in de gevangenis proberen uit te zitten. Ook is identiteitsfraude vaak gekoppeld aan gevallen van oplichting: valse inschrijvingen bij de Kamer van Koophandel, of aankoop van onroerend goed met een vals identiteitsbewijs. Daarnaast is er nog de identiteitsfraude op internet. Een gekaapt DigiD kan voor het slachtoffer allerlei vormen van ellende teweegbrengen.

Jaarlijks worden in Nederland zo'n 250.000 identiteitsbewijzen ontvreemd. De meesten worden nooit teruggevonden.

PROGIS

Het Programma Informatievoorziening in de Strafrechtketen (PROGIS) is er op gericht een einde te maken aan alle vormen van identiteitsfraude. De eerste twee fases van dat in 2005 gestarte programma zijn inmiddels afgerond, de derde fase gaat nu van start.

GERELATEERDE ARTIKELEN

19-05 **Verwarring over vernietiging vingerafdrukken**

28-04 **Gemeenten mogen vingerafdrukken niet vernietigen**

27-04 **Dataopslag vingerafdrukken uitgesteld**

17-04 **Heilig geloof in databases is tanende**

01-03 **Ondernemer verliest vingerafdrukzaak**

Bron: http://www.binnenlandsbestuur.nl/digitaal-besturen/nieuws/nieuws/politie-scant-vingerafdruk-op-straat.1411906.lynkx.

© Copyright 2011 Kluwer. Alle rechten voorbehouden.