Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2009–2010

Aanhangsel van de Handelingen

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

2178

Vragen van het lid **Gerkens** (SP) aan de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *de veiligheid van DigiD* (ingezonden 17 maart 2010).

Antwoord van staatssecretaris **Bijleveld-Schouten** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 9 april 2010).

Vraag 1
Bent u op de hoogte van het feit dat het kinderspel is om iemands DigiD over te nemen, zoals blijkt uit bijgevoegde e-mail? Wat is uw mening over dit voorval?[1]

Antwoord 1
Het (opnieuw) aanvragen van een DigiD is zodanig ingericht dat de drempel om DigiD te gebruiken laag ligt. Burgers hoeven daarvoor bijvoorbeeld niet naar een loket. Voor kwaadwillenden is het niet onmogelijk om de DigiD van een ander aan te vragen. De kwaadwillende moet daarvoor de naam, het adres, de geboortedatum en het BSN kennen van degene wiens DigiD hij wil overnemen. Daarnaast moet *hij* de activeringsbrief voor DigiD onderscheppen. Deze brief wordt *altijd* naar het GBA-adres van de aanvrager gestuurd, dat de kwaadwillende dus ook moet kennen. Een dergelijk misbruik van DigiD is een misdrijf.

Vraag 2
Hoe vaak komt deze vorm van fraude voor? Hoeveel mensen hebben hier in voorgaande jaren aangifte van gedaan?

Antwoord 2
Bij Logius zijn geen gevallen bekend, waarin succesvol fraude heeft plaatsgevonden met een vals verkregen DigiD. Dat houdt in dat het niet is gelukt om met een vals verkregen DigiD een dienst af te nemen bij een overheidsorganisatie, daarvoor is reeds ingegrepen.
Er is recent een aantal samenlopende gevallen tot het vals verkrijgen van een DigiD aan het licht gekomen, die te herleiden zijn tot een of enkele daders. Daarnaast is nog een geval bekend waarin door derden geprobeerd is DigiD's van een ander te verkrijgen. In beide gevallen heeft Logius aangifte gedaan bij de politie.

[1] E-mail dhr. B. te Delft d.d. 11-03-2010, onderhands aan bewindspersoon verstrekt.

ah-tk-20092010-2178
ISSN 0921 - 7398
's-Gravenhage 2010

Vraag 3
Zijn deze zaken opgelost? Hoeveel mensen zijn er de afgelopen jaren veroordeeld voor het frauderen met DigiD?

Antwoord 3
De aangiftes zijn nu onderwerp van onderzoek door de politie en in een geval ook de FIOD. Er zijn in de afgelopen jaren geen mensen veroordeeld voor het vals verkrijgen van een DigiD. Overigens zijn alle betrokken burgers direct ingelicht en voorzien van aanvullende informatie en hulp.

Vraag 4
Zijn de betrokken instanties, zoals Logius, Belastingdienst en FIOD, voldoende op de hoogte van de mogelijkheden tot fraude, zodat zij gedupeerden snel en goed kunnen ondersteunen, om zo grotere schade te voorkomen?

Antwoord 4
De betrokken instanties zijn voldoende op de hoogte van de mogelijkheden tot fraude.
Bij een vermoeden van misbruik wordt direct gereageerd door Logius en de betreffende overheidsorganisatie die de dienst verleent, om schade bij burgers te voorkomen. Logius werkt daarbij nauw samen met de betrokken overheidsorganisaties.
Daarbij wordt aangetekend dat niet alleen DigiD een rol speelt bij het voorkomen van misbruik, maar ook de interne processen van de betrokken overheidsdienstverleners (zie ook het antwoord op vraag 7).
In individuele gevallen van misbruik adviseert Logius de slachtoffers altijd om aangifte te doen bij de politie. Bij vermoedens van grootschaliger misbruik, schakelt Logius daarnaast ook zelf de politie in.

Vraag 5
Wat gaat u doen om de hulpverlening en afhandeling richting slachtoffers te verbeteren?

Antwoord 5
DigiD kent een helpdesk die in desbetreffende gevallen de burger kan helpen en ondersteunen. Daarnaast kent Logius een calamiteitenteam dat in voorkomende gevallen direct en in overleg met overheidsdienstverleners in werking kan treden. In de voornoemde gevallen heeft Logius direct alle maatregelen genomen die nodig waren om misbruik van DigiD te voorkomen.
Naast de helpdesk DigiD is sinds 1 maart 2010 het Centraal Meld- en Informatiepunt Identiteitsfraude en -fouten (CMI) ingericht. Slachtoffers van identiteitsfraude, dus ook van fraude met DigiD, kunnen hier terecht. De eerstelijns helpdesk van het CMI is ingericht bij Postbus 51. Er is een ketenregisseur CMI ingesteld die ervoor zorg draagt dat problemen die op verschillende terreinen/organisaties spelen bezien blijven worden uit het perspectief van het slachtoffer.

Vraag 6
Zijn de opsporingsautoriteiten voldoende toegerust om deze vorm van criminaliteit snel en daadkrachtig aan te pakken? Zo nee, wat gaat u hieraan doen?

Antwoord 6
Mede voor deze problematiek is door de minister van Justitie, samen met de ministers van Binnenlandse Zaken en Koninkrijksrelaties (BZK), voor Jeugd en Gezin (J&G), voor Wonen, Werken en Integratie (WWI) en de Staatssecretarissen van Justitie en Onderwijs, Cultuur en Wetenschap (OC&W) het project «Veiligheid begint bij Voorkomen» in het leven geroepen. (TK 2007–2008, 28 684, nr. 119).

Vraag 7
Deelt u de mening dat er sprake is van een lek in de beveiliging van DigiD, dat zo snel mogelijk gedicht dient te worden? Zo nee, waarom niet?

Antwoord 7
Nee, er is geen sprake van een lek. Bij de introductie van DigiD is een afweging gemaakt tussen veiligheid en klantvriendelijkheid. Overheidsorganisaties die DigiD gebruiken zijn bekend met het uitgifteproces en bepalen op basis daarvan of een dienst met DigiD geleverd wordt of niet. Naast het steunen op de dienstverlening van DigiD moet een overheidsorganisatie die gebruikmaakt van DigiD aanvullende beveiligingsmaatregelen treffen om te komen tot aanvaardbare risico's rondom de eigen webdienst. Zie verder het antwoord op vraag 1.

Vraag 8
Is het waar dat bij de aanvraag van een nieuw DigiD wachtwoord er niet om bevestiging van de oude inlogcode en het oude wachtwoord wordt gevraagd? Zo ja, waarom gebeurt dit niet?

Antwoord 8
Het klopt dat er niet gevraagd wordt om de bevestiging van de oude inlogcode en het oude wachtwoord, als iemand een nieuwe DigiD aanvragen. Het betreft in dit geval namelijk mensen die hun wachtwoord en inlogcode (ook wel gebruikersnaam genoemd) zijn vergeten. Bij een nieuwe aanvraag kan dan ook niet om de oude inlognaam en wachtwoord worden gevraagd. Burgers die hun wachtwoord zijn vergeten, maar nog wel hun inlogcode weten, kunnen elektronisch een nieuw wachtwoord aanvragen als zij beschikken over een DigiD op niveau midden (SMS-authenticatie).

Vraag 9
Deelt u de mening dat dit de procedure al een stuk veiliger maakt? Bent u bereid deze tussenstap zo snel mogelijk in te voeren?

Antwoord 9
Ik verwijs u naar het antwoord op vraag 8.

Vraag 10
Ziet u mogelijkheden in het versturen van een waarschuwing via een sms-bericht naar de oorspronkelijke eigenaar van de DigiD op het moment dat er een nieuwe code wordt aangevraagd, zodat deze indien er sprake is van fraude, snel kan reageren? Zo ja, bent u bereid dit snel in te voeren? Zo nee, waarom niet?

Antwoord 10
Deze maatregel is alleen mogelijk voor burgers met een DigiD op niveau midden (waarvan dus het telefoonnummer bekend is). Daarmee wordt dus voor een grote groep burgers op het niveau DigiD basis een extra drempel opgeworpen, omdat zij dan over moeten gaan tot het gebruik van een mobiele telefoon. Tevens zijn er overheidsdienstverleners die voor hun processen slechts het niveau DigiD-basis vereisen op basis van hun eigen risico-inschatting. Vooralsnog ben ik daarom van mening dat een dergelijke maatregel – nog – niet nodig is maar ik neem deze suggestie wel mee in de reguliere kwetsbaarheidanalyses die voor DigiD worden uitgevoerd.

Vraag 11
Ziet u mogelijkheden om te werken met een zogenaamde «kruisidentificatie», waarbij de gegevens van de aanvrager van de DigiD code vergeleken worden met de aangeleverde rekeninggegevens, zoals dat bij banken al meer gebeurt? Zo ja, bent u bereid dit snel in te voeren? Zo nee, waarom niet?

Antwoord 11
Ik zie geen mogelijkheden om te werken met een zogenaamde «kruisidentificatie». De reden is dat overheidsorganisaties die DigiD gebruiken, na een geslaagde inlogpoging alleen het Burgerservicenummer ontvangen; dat is het enige gegeven waarover DigiD beschikt. DigiD heeft dus – mede uit privacyoverwegingen – geen andere informatie die voor kruisidentificatie gebruikt kan worden.

Vraag 12
Welke andere mogelijkheden ziet u om de beveiliging van DigiD te verbeteren?

Antwoord 12
DigiD kent juist meerdere niveaus van identificatie om publieke dienstverleners de mogelijkheid te bieden om het juiste niveau van beveiliging te kiezen voor de door hen gewenste elektronische dienstverleningsprocessen. Naast de huidige niveau's wordt nu gewerkt aan het EPD-DigiD niveau (zie het antwoord op vraag 13). Voor het hoogste niveau, de Elektronische Nederlandse Identiteitskaart (eNIK) is de mogelijkheid tot realisatie opgenomen in de aanbesteding voor de Nationale Identiteitskaart. Te zijner tijd zal ik u en uw Kamer inlichten of en hoe deze elektronische functionaliteit opgenomen zal worden.

Vraag 13
Deelt u de mening dat zolang de beveiliging van DigiD niet gegarandeerd kan worden, niet overgegaan moet worden tot koppeling van het Elektronisch Patiënten Dossier (EPD) aan DigiD? Zo ja, bent u bereid uw plannen hiertoe te bevriezen en eerst te werken aan een goede beveiliging van DigiD? Zo nee, waarom niet?

Antwoord 13
Nee, die mening deel ik niet. Over enkele maanden komt EPD-DigiD beschikbaar.
Invoering vindt plaats in overleg met mijn ambtgenoot van VWS. Burgers die een EPDDigiD aanvragen, kunnen deze alleen activeren door in persoon een brief met activeringscode op te halen. Legitimatie is daarbij verplicht, waardoor de betrouwbaarheid van het uitgifteproces verhoogd wordt.
EPD-DigiD is door de hogere betrouwbaarheid van het aanvraagproces een aanvulling op de bestaande DigiD niveaus basis en midden. Daardoor is misbruik als hier genoemd te voorkomen.
Het niveau EPD-DigiD is – op verzoek van de Minister van VWS – en naar aanleiding van het advies van onderzoekers van de Radboud Universiteit Nijmegen, de Universiteit van Tilburg en PWC (o.a. P 26, 37) juist ontwikkeld om een veilige toegang van de patiënt tot het EPD te waarborgen.

Vraag 14
Wat is uw mening over de gebrekkige procedure bij de politie om te komen tot aangifte van dit strafbare feit, zoals blijkt uit de e-mail van gedupeerde? Wat gaat u doen om de aangifteprocedure te verbeteren?

Antwoord 14
Uit de verstrekte informatie blijkt dat de burger extra moeite heeft moeten doen voor zijn aangifte, maar niet dat de aard van de aangifte in deze specifieke zaak tot problemen heeft geleid.
Om fraude en fouten met identiteiten te voorkomen en bestrijden, hebben de ministeries van BZK en Justitie in 2008 het programma VIPS[2] gestart. In het kader van dit programma wordt door het Ministerie van Justitie, in samenwerking met de politie en de Koninklijke Marechaussee, onder meer gewerkt aan een handreiking die ervoor moet zorgen dat gedupeerden die bij het politiebureau aankloppen om aangifte te doen van identiteitsfraude beter geholpen kunnen worden. In deze handreiking zal een overzicht worden opgenomen van de artikelen in het Wetboek van strafrecht die kunnen worden toegepast bij de bestrijding van identiteitsfraude. De handreiking zal verspreid worden in alle politiekorpsen en ook in de Politie Academie. Zie ook mijn antwoord op vraag 6.

[2] Programma VIPS = Programma Versterking Identiteitsketen Publieke Sector. Dit programma is voor het eerst aan de Tweede Kamer bekend gemaakt d.m.v. de voortgangsrapportage Veiligheid Begint Bij Voorkomen 2008. Kamerstuknummer: 28 684, nr. 178.