Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2010–2011 **Aanhangsel van de Handelingen**

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

2450

Vragen van de leden **Van der Burg, Hennis-Plasschaert** en **Neppérus** (allen VVD) aan de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Veiligheid en Justitie en de staatssecretaris van Financiën over *inbreuk op DigiD* (ingezonden 6 april 2011).

Antwoord van minister **Donner** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de minister van Veiligheid en Justitie en de staatssecretaris van Financiën (ontvangen 9 mei 2011).

Vraag 1
In hoeverre is het (nog steeds) mogelijk dat, als iemands NAW-gegevens (naam-, adres- en woonplaatsgegevens) en burgerservicenummer worden gestolen, een ander op zijn naam een DigiD kan aanvragen, met onder andere als gevolg dat teruggaven van de Belastingdienst op een verkeerde rekening terechtkomen?

Antwoord 1
Het is niet mogelijk om louter met de kennis van iemands burgerservicenummer (en geboortedatum en adres), ook zijn DigiD te verkrijgen.
Bij het aanvragen van een DigiD vult de aanvrager BSN, geboortedatum en postcode/huisnummer in op het aanvraagformulier. Hierna wordt een activeringscode verstuurd naar het GBA-adres van degene op wiens BSN een DigiD wordt aangevraagd. Misbruik is dus alleen mogelijk wanneer de kwaadwillende de naar het GBA-adres gestuurde brief met de activeringscode ook onderschept, en met deze code de DigiD activeert. Een DigiD werkt pas na activering.

Vraag 2
Welke omvang heeft het in vraag 1 genoemde probleem?

Antwoord 2
Het probleem dat kwaadwillenden – met louter de kennis van BSN en enkele andere gegevens – een DigiD van een ander kunnen verkrijgen, bestaat niet (zie vraag 1).
Het probleem dat kwaadwillenden de activeringsbrief onderscheppen komt – op een totaal van
circa 8 miljoen gebruikers en 37 miljoen transacties per jaar – slechts beperkt voor. Een precies cijfer is niet te geven.

ah-tk-20102011-2450
ISSN 0921 - 7398
's-Gravenhage 2011

Vraag 3
Hoe omvangrijk kan dit probleem worden, gegeven het feit dat het burgerservicenummer op elk paspoort en op elk rijbewijs staat afgedrukt en het ook relatief eenvoudig is de NAW-gegevens van iemand te achterhalen? Hoe verhoudt dit risico van oneigenlijk gebruik van het burgerservicenummer zich tot het gemak van het beschikbaar hebben van het burgerservicenummer op identificatiedocumenten voor burgers?

Antwoord 3
Daar het niet mogelijk is om met louter een BSN en NAW-gegevens een DigiD te verkrijgen, is er geen sprake van een probleem dat omvangrijk kan worden.
Over het risico van oneigenlijk gebruik van het BSN is het van belang te beseffen dat het burgerservicenummer geen beveiligingsmiddel is of authenticatiemiddel voor toegang tot de elektronische dienstverlening van de overheid. Een burgerservicenummer geeft op zich geen enkel recht aan een burger, noch legt het een plicht op. Overheidsorganisaties moeten de identiteit van een burger op een andere manier verifiëren, bijvoorbeeld met een geldig wettelijk identiteitsdocument.

Vraag 4
Is dergelijke fraude door diefstal van burgerservicenummers in combinatie met NAW-gegevens en aanvraag van DigiD ook bij andere overheidsinstanties, bijvoorbeeld uitkeringsinstanties, in de afgelopen jaren opgetreden? Zo ja, waar en hoe vaak?

Antwoord 4
Zie het antwoord op vraag 2.

Vraag 5
Waarom kan iemand «zijn» DigiD niet laten blokkeren, wanneer een inbreuk op die DigiD wordt vermoed, net zoals bij het vermoeden van misbruik van een bankpasje? Is het mogelijk om dit te regelen? Zo nee, waarom niet? Bent u bereid dit te regelen? Zo nee, waarom niet?

Antwoord 5
Het is wel degelijk mogelijk om een DigiD te laten blokkeren, zie het antwoord op vraag 7.
Daarnaast is het mogelijk om een DigiD te laten opheffen. Daarvoor bestaat een procedure bij de uitvoeringsorganisatie Logius.

Vraag 6
Wat bent u voornemens te doen om fraude met DigiD, als gevolg van gestolen NAW-gegevens en gestolen burgerservicenummers, te voorkomen? Hoe kan er voor worden gezorgd dat er sprake is van een waterdichte identificatie bij het aanvragen van een DigiD?

Antwoord 6
Zoals gezegd zijn er verschillende maatregelen genomen om de betrouwbaarheid van DigiD te waarborgen. Er is geen aanleiding om de aanvraag- en activeringsprocedure van DigiD te passen.
Wat hierbij wel opgemerkt kan worden is dat er verschillende betrouwbaarheidsniveaus zijn op het gebied van online authenticatiemiddelen. Het Europese STORK-project onderscheidt 4 niveaus. DigiD omvat niveau 2 (DigiD gebruikersnaam + wachtwoord) en niveau 3 (DigiD gebruikersnaam + wachtwoord + sms). Het hoogste niveau zou ingevuld kunnen worden door een elektronische Nederlandse identiteitskaart (eNIK). Een fors aantal landen beschikt inmiddels over een dergelijk middel. Momenteel wordt de wenselijkheid en haalbaarheid van het invoeren van een eNIK onderzocht. Rond de zomer van 2011 beoog ik de Kamer daarover verder te informeren.

Vraag 7
Vervalt door het aanvragen van een nieuwe DigiD de oude DigiD, ook als deze in handen van fraudeurs is? Zo nee, waarom niet?

Antwoord 7
Ja, bij het aanvragen van een nieuwe DigiD vervalt de oude DigiD.

Vraag 8
Hoe worden burgers die te maken hebben met fraude met hun NAW-gegevens en fraude met DigiD geholpen bij de ontstane problemen, onder meer bij de Belastingdienst? Wat doen de helpdesk DigiD en het Centraal Meld- en informatiepunt Identiteitsfraude en -fouten precies?

Antwoord 8
Burgers kunnen in eerste instantie contact opnemen met de overheidsdienstverlener, bij wiens dienst misbruik gemaakt is van de gegevens. Daarnaast kunnen zij in het geval van misbruik met DigiD contact opnemen met de helpdesk DigiD en in het geval van een vermoeden van fraude met het BSN met het BSN-punt. In het geval van verdenking van fraude heft Logius de DigiD-account op en adviseert de DigiD-helpdesk de burger een nieuw account aan te vragen. Vervolgens wordt de burger gevraagd contact op te nemen met de DigiD-helpdesk zodra hij de DigiD-aanvraag heeft gedaan; dit ter extra controle. Daarnaast wordt de burger geadviseerd aangifte te doen bij de politie.
Desgewenst kan een burger een melding doen bij het Centraal Meldpunt Identiteitsfraude en -fouten (CMI). Het meldpunt zorgt ervoor dat een melding wordt afgehandeld door haar partners, zoals de politie, de Koninklijke Marechaussee, het Ministerie van Veiligheid en Justitie en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Het CMI heeft verder goede afspraken gemaakt met de Belastingdienst om de fraudemeldingen ook daar te laten onderzoeken. De afspraken betreffen doorlooptijden en communicatie richting melder. Samen met de Belastingdienst wordt bovendien bekeken in welke bestanden foutieve gegevens terecht kunnen komen. Het CMI begeleidt de melder in dat geval om foutieve gegevens te laten corrigeren.

Vraag 9
Waarom worden betalingen, die op rekeningnummers worden gestort, waarvan men vermoedt of zelfs al weet dat ermee wordt gefraudeerd, niet onmogelijk gemaakt? Waarom kan er nu alleen achteraf worden teruggevorderd? Bent u bereid betalingen in de hier genoemde situaties te laten blokkeren? Zo nee, waarom niet?

Antwoord 9
Betalingen op rekeningnummers waarvan de Belastingdienst weet dat ermee is gefraudeerd worden geblokkeerd. Deze rekeningnummers worden doorgehaald in het systeem waarin de bankrekeningnummers staan geregistreerd. Betalingen op rekeningnummers waarvan de Belastingdienst vermoedt dat ermee is gefraudeerd, worden onderschept en gesignaleerd aan de regio's van de Belastingdienst en Toeslagen. Daar vindt een inhoudelijke toets plaats. Na geconstateerde fraude, wordt uitbetaling tegengehouden en de beschikking teruggedraaid. Met deze werkwijze worden onterechte betalingen voorkomen.