Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres

Aan de Voorzitter van de Tweede Kamer der Staten
Generaal
Postbus 20018
2500 EA Den Haag

Directie Burgerschap en Informatiebeleid

Turfmarkt 147
Den Haag

Kenmerk
2014-0000350206

Datum 9 juli 2014
Betreft Versterking en beveiliging DigiD

Hierbij informeer ik u over een aantal ontwikkelingen ten aanzien van DigiD; in het bijzonder over de voortgang van de uitvoering van de ICT-Beveiligingsassessments DigiD, de stappen die worden gezet om DigiD te versterken, alsmede de stand van zaken bij de uitvoering van de pilot voor DigiD Buitenland. In reactie op de vragen gesteld tijdens het Algemeen Overleg van 25 juni jl. door Kamerlid Verhoeven ga ik ook nader in op samenwerkingsverbanden.

ICT-Beveiligingsassesments DigiD

Voortgang
Naar aanleiding van een aantal beveiligingsincidenten in het najaar van 2011 (DigiNotar en Lektober) zijn de organisaties die DigiD gebruiken voor hun digitale dienstverlening verplicht gesteld om jaarlijks een ICT-Beveiligingsassessment DigiD uit te voeren. In 2012 gold deze verplichting al voor de grote afnemers van DigiD. Sinds 2013 geldt deze verplichting voor alle afnemers.

Voorop kan worden gesteld dat in mijn beleving het veiligheidsbewustzijn van publieke dienstverleners in de afgelopen jaren behoorlijk is toegenomen. Dit blijkt onder meer uit de serieusheid waarmee het proces voor de uitvoering van de assessments is opgepakt. Bij gemeenten heeft KING hier onder meer aan bijgedragen door de uitvoering van een ondersteuningsaanpak bij de voorbereiding en uitvoering van de assessments. Het algemene beeld is dat, mede door het proces van de uitvoering van de assessments bij overheidsorganisaties en andere afnemers van DigiD in het afgelopen jaar, bij die organisaties een ontwikkeling in gang is gezet om de beveiliging van hun ICT op orde te brengen, met name in relatie tot DigiD.

De assessmentronde heeft tot een flinke opschoning van de totale populatie DigiD aansluitingen geleid. Zo'n 200 aansluitingen zijn stopgezet, veelal op verzoek van de organisaties zelf omdat deze weinig tot niet werden gebruikt, bijvoorbeeld omdat ze meerdere aansluitingen hadden. Voor de overige aansluitingen, bijna 600, hebben de meeste organisaties aan de verplichting tot uitvoering van het assessment voor het einde van 2013 voldaan. Aan enkele organisaties is enige tijd uitstel verleend omdat zij bezig waren met een ingrijpende migratie van hun ICT-omgeving. In een enkel geval hield dit verband met een gemeentelijke fusie. In een beperkt aantal gevallen is de aansluiting op DigiD door Logius ontkoppeld omdat niet tijdig een assessmentrapport werd ontvangen.

Van de bijna 500 organisaties die zijn aangesloten op DigiD heeft niet één organisatie een resultaat laten zien waarbij er sprake was van een acuut beveiligingsrisico. Vrijwel alle organisaties die werken met een leverancier konden een positief Third Party Mededeling (TPM) leveren, een zogenaamde 'groene' verklaring waarmee zo'n 80 procent van de totale eisen positief scoorde. In een klein aantal gevallen is de leverancier, via de afnemer, geïnformeerd dat er verbeteringen moesten worden doorgevoerd. In 38% van de gevallen is een geheel bevindingvrije rapportage opgeleverd. In 5% van de gevallen was er, op grond van de auditresultaten, sprake van een dusdanig hoog risico dat dit zo snel mogelijk, binnen enkele weken, is opgelost. Voor de overige gevallen geldt dat deze organisaties er op zijn gewezen dat zij voor de bevindingen een verbetertraject moeten doorlopen en vervolgens een verbeterrapport moeten inleveren. De verwachting is dat de meeste organisaties dit traject in het najaar zullen afronden.

Risicocategorie	***Verbetertermijn***	***% assessments***
Zeer Hoog	1 maand	5%
Hoog	2 maanden	16%
Midden	4 maanden	39%
Laag	12 maanden	2%
Groen		38%
Totaal		*100%*

Algemene Rekenkamer
De Algemene Rekenkamer heeft in zijn rapport over het Jaarverslag 2013 van BZK enkele aanbevelingen gedaan ten aanzien van de uitvoering van de ICT-Beveiligingsassessments DigiD. Daarbij is onder meer gevraagd naar vervolgacties ten aanzien van organisaties die structureel niet voldoen aan de assessmentnormen. Als deze situatie zich voordoet dan wordt die organisatie daar op bestuurlijk niveau op aangesproken. Indien sprake is van een ernstig en acuut beveiligingsrisico dan wordt de aansluiting op DigiD (tijdelijk) opgeschort. Bij het treffen van maatregelen wordt de proportionaliteit van de maatregelen en het maatschappelijk belang van de voorzetting van de dienstverlening meegewogen.

Tevens is er door de Algemene Rekenkamer op aangedrongen dat de aangesloten organisaties concreter worden geïnformeerd over het vereiste niveau van authenticatie voor hun dienstverlening en dat organisaties er op worden gewezen als zij DigiD gebruiken voor processen waarvoor een hoger betrouwbaarheidsniveau noodzakelijk is. Hieraan zal gevolg worden gegeven door de "Handreiking betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten" van het Forum Standaardisatie nadrukkelijker onder de aandacht van de aangesloten organisaties te brengen. Op basis daarvan moeten de organisaties zelf bepalen welk authenticatieniveau voor hun dienstverlening is aangewezen. Dat is namelijk mede afhankelijk van de vraag hoe de betreffende overheidsorganisaties hun processen hebben ingericht en met name of er in die processen ook sprake is van extra controles of andere maatregelen die het verantwoord maken om van het beschikbare betrouwbaarheidsniveau gebruik te maken.

Vervolg assessments
Deze eerste volledige assessmentronde heeft een aantal leerpunten opgeleverd. Uit contacten met de VNG, individuele gemeenten en andere afnemers van DigiD, zijn signalen naar voren gekomen die aanleiding geven tot enige bijstellingen in het assessmentproces. Daarmee worden ook enkele vraagpunten uit de praktijk van de auditors beantwoord.

In dit verband is allereerst van belang om te benadrukken dat het Beveiligingsnormenkader DigiD vooralsnog ongewijzigd blijft. Weliswaar is denkbaar dat de beveiligingsrichtlijnen voor webapplicaties van het NCSC, waarop de DigiD-norm is gebaseerd, naar aanleiding van een evaluatie worden herijkt, maar zolang dat niet tot besluitvorming heeft geleid, is er geen aanleiding om het normenkader te wijzigen. Daarmee wordt zowel voor de afnemers van DigiD als voor de auditors voor de komende assessmentronde duidelijkheid geboden.

Gelet op het verloop van de eerste assessmentronde zie ik aanleiding om de uiterste inleverdatum voor het assessmentrapport in het vervolg te bepalen op 1 mei. Daarbij geldt tevens dat het assessmentrapport niet eerder dan 1 januari mag worden ingediend. Dit betekent concreet dat de aangesloten organisaties het eerstvolgende assessmentrapport moeten inleveren bij Logius vóór 1 mei 2015. Dit wordt mede ingegeven door het feit dat dit jaar (2014) veel organisaties bezig zijn met het oplossen van de bevindingen uit het eerste assessment. De verwachting is dat dit bij de tweede en volgende assessmentrondes in mindere mate aan de orde zal zijn. Aldus wordt tevens bereikt dat de last van de beoordeling van de assessments door Logius beter hanteerbaar wordt.

In samenhang met het voorgaande zullen nog enkele andere technische aspecten met betrekking tot de uitvoering en behandeling van de assessments worden geregeld en vastgelegd in de aansluitvoorwaarden voor DigiD. Dit ziet onder meer op het gebruik van Third Party Mededelingen (TPM) van ICT-leveranciers en de geldigheidsduur daarvan. Daarnaast zal worden bepaald dat nieuwe afnemers van DigiD binnen 2 maanden na aansluiting op DigiD een assessment dienen uit te voeren. De aangesloten organisaties zullen over deze wijzigingen zo spoedig mogelijk door Logius worden geïnformeerd.

Volledigheidshalve wijs ik er op dat ik -zoals al eerder aan de Kamer bericht- er naar streef om te komen tot eenduidige normenkaders, zoals de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). De Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID) (*vergaderjaar 2012 – 2013, Kamerstuk 26 643, nr. 269)* onderzoekt onder meer in welke mate de BIG overlap vertoont met audits die vanuit afzonderlijke departementen van toepassing zijn voor de gemeentelijke overheden en of deze auditverplichtingen op termijn kunnen worden samengevoegd of geheel of ten dele vervangen door één enkele informatiebeveiligingsaudit in plaats van de huidige verschillende losse audits. Een dergelijke enkelvoudige audit kan bijdragen om de lasten voor gemeenten en later mogelijke andere overheidsorganisaties met betrekking tot ICT-beveiliging, te beperken.

Versterking DigiD

Bij brief d.d. 10 januari 2014 (*Vergaderjaar 2013-2014, Kamerstuk 26 643, 302)* heb ik de Kamer geïnformeerd over het thuisbezorgen van activatiecodes voor DigiD voor gebieden waar sprake is van een verhoogd risico op fraude. Dit naar aanleiding van enkele incidenten waarbij DigiD-accounts door derden zijn ontvreemd (Groningen, Amsterdam Zuid Oost). Sinds de start van deze werkwijze zijn inmiddels ca. 2000 activatiecodes op deze wijze uitgereikt. Het eerste beeld is dat deze werkwijze in het algemeen door de betrokken burgers positief wordt ontvangen.

Bij genoemde brief is tevens aangekondigd dat nog verder onderzoek zal worden gedaan naar verbeteringen in het uitgifteproces van DigiD. In dat kader zal in de komende periode een oriëntatie plaatsvinden op de mogelijkheden om DigiD te combineren met een controle langs digitale weg op gegevens van bestaande wettelijke identiteitsdocumenten, met name het paspoort, de identiteitskaart en het rijbewijs. Daarmee kan dan in feite een hoger betrouwbaarheidsniveau worden

gecreëerd voor transacties waarbij dit van belang is.

Pilot DigiD Buitenland

Zoals toegezegd in het Algemeen Overleg DigiD van 5 maart jl. waarin de heer Sjoerdsma heeft gevraagd om informatie ten aanzien van een bredere uitrol van de voorziening DigiD Buitenland, met name in de top tien van landen waar Nederlanders zich veel bevinden, bericht ik u als volgt.

De pilot DigiD Buitenland is in mei 2013 van start gegaan. Inmiddels zijn ruim tienduizend Nederlandse burgers die woonachtig zijn in het buitenland, door één van de deelnemende baliepartijen (vijf gemeenten en het Nederlandse consulaat te Antwerpen) geholpen aan een DigiD die ook vanuit het buitenland te gebruiken is. Uit een eerste evaluatie is naar voren gekomen dat het aanvraag- en uitgifteproces van een DigiD via de balie -zoals deze momenteel is ingericht- als inefficiënt en -voor sommigen- (te) ingewikkeld wordt ervaren. In overleg met alle betrokken baliepartijen is daarom besloten het aanvraag- en uitgifteproces van DigiD via een balie te vereenvoudigen. Concreet betekent dit dat de aanvraag volledig digitaal zal gaan plaatsvinden en dat bij de uitgifte wordt volstaan met één baliecontact waarbij de aanvraag wordt gecontroleerd op juistheid en volledigheid en tevens de identiteit van de aanvrager wordt gecontroleerd en vastgesteld.

De pilot DigiD Buitenland is verlengd tot eind 2014 zodat in de tussenliggende periode het nieuwe proces kan worden ontworpen en de technische aanpassingen kunnen worden gerealiseerd. Het ligt in de verwachting dat begin 2015 het nieuwe proces in de pilot kan worden geïntroduceerd. Mede afhankelijk van een succesvolle implementatie zal deze extra dienstverlening voor Nederlandse niet-ingezetenen in de loop van 2015 een regulier DigiD proces zijn. Het is tevens het streven dat een aantal strategisch gekozen Nederlandse ambassades vanaf volgend jaar ook de uitgifte van DigiD's via de balie aan Nederlandse niet-ingezetenen gaat aanbieden. In overleg met het ministerie van Buitenlandse Zaken, de Belastingdienst en de Sociale Verzekeringsbank wordt onderzocht welke buitenlandse locaties hiervoor het meest in aanmerking komen en/of geschikt zijn.

Andere functionele ontwikkelingen en beveiligingsmaatregelen

Naast de hiervoor geschetste functionele ontwikkelingen zijn en worden ook andere aanpassingen ter hand genomen. In mei zijn de eisen voor DigiD-wachtwoorden verscherpt, waardoor gebruikers met een zwak wachtwoord een nieuw –sterker- wachtwoord moeten aanmaken. Voor nieuwe aanvragen gold deze eis al langer. Hiernaast zullen in september aanpassingen aan DigiD worden doorgevoerd waardoor de gebruiksvriendelijkheid wordt verhoogd. Dit moet er tevens toe leiden dat het aantal vragen bij de Helpdesk zal verminderen. Tevens is de weerbaarheid van DigiD tegen digitale verstoringen van buitenaf versterkt. Tenslotte wordt nog in 2014 een actieplan uitgevoerd om een aantal bevindingen van de Auditdienst Rijk op te lossen en de aanbevelingen van de Algemene Rekenkamer ten aanzien van DigiD tot uitvoering te brengen.

Gebruik maken van kennis van hackers (Motie Hachchi-El Fassed)

In 2011 heeft uw Kamer de regering opgeroepen "te onderzoeken hoe de overheid de beveiliging van haar computersystemen kan verbeteren door gebruik te maken van de kennis van hackers zonder dat hackers hier strafrechtelijke consequenties van ondervinden". Hieraan is gevolg gegeven door enkele hack evenementen te organiseren waarbij studenten van de Technische Universiteit Eindhoven en de Haagse Hogeschool betrokken zijn geweest. De reacties hierop waren zeer positief, ook bij deelnemende gemeenten. De hacktesten hebben mede de weg

bereid voor een Rijksbreed responsible disclosure beleid. Daarmee is er nu een permanent beleid voor het betrekken van de kennis en kunde van ict-experts en ethische hackers. De noodzaak voor speciale hackdagen is hiermee komen te vervallen. Ook Logius maakt bij haar producten gebruik van de zogenaamde 'ethische' hackers.

Samenwerkingsverbanden

Tijdens het Algemeen Overleg van 25 juni jl. vroeg uw Kamer naar de mogelijkheid om meer groepsaansluitingen te realiseren om op deze wijze de kosten voor gemeenten bij de assessments omlaag te brengen.

In de afgelopen periode heeft Logius zich om veiligheidsredenen terughoudend opgesteld bij groepsaansluitingen. Groepsaansluitingen worden tijdelijk niet meer toegestaan. Logius signaleerde een toename en diversiteit aan gedeelde aansluitingen op DigiD. Dit levert twee risico's op:

1. Door de grote diversiteit aan gedeelde aansluitingen is er bij Logius onvoldoende inzicht in de informatieveiligheidsrisico's die de gedeelde aansluitingen met zich mee (kunnen) brengen.
2. Door de grote diversiteit is er een afname van de zichtbaarheid van de achterliggende dienstaanbieders voor gebruikers. De burger weet niet meer in alle gevallen van wie hij/zij nu precies diensten afneemt.

Desondanks is er een duidelijke vraag naar groepsaansluitingen van samenwerkingsverbanden, waarbij de DigiD-aansluiting op verschillende manieren ingezet wordt. Het doel is om op een gedegen en toekomstvaste manier in deze behoefte te voorzien. Inmiddels heeft Logius stappen gezet in haar onderzoek. Randvoorwaardelijk hierbij is dat de informatieveiligheid van de DigiD-keten moet zijn geborgd en dat het voor de gebruiker te allen tijde duidelijk moet zijn bij welke gemeente hij/zij diensten afneemt. Belangrijk daarbij is dat de risico's afdoende worden gemitigeerd, ook in relatie tot de beveiligingseisen. Het is daarbij overigens nog niet duidelijk of er sprake kan zijn van kostenbesparing als gemeenten overgaan naar een gedeelde aansluiting. Dat moet nog worden onderzocht.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

dr. R.H.A. Plasterk