Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 372

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 23 november 2015

Inleiding

Het is de inzet van dit kabinet dat digitale dienstverlening van de Nederlandse overheid in de komende jaren een grote vlucht neemt. De voorziening DigiD, die burgers in staat stelt online hun identiteit aan te tonen, neemt daarin een heel belangrijke plaats in. In aanloop naar Idensys (voorheen het eID Stelsel) blijft DigiD de komende jaren een belangrijke voorziening waarop vertrouwd moet kunnen worden. Het huidige DigiD moet immers in de lucht blijven totdat alle afnemers gebruik maken van Idensys en burgers zich via Idensys goed kunnen identificeren voor publieke diensten.

Als Minister van BZK ben ik verantwoordelijk voor DigiD en is mij er veel aan gelegen het vertrouwen in DigiD te bevorderen. Kritieken op de veiligheid van DigiD neem ik daarom heel serieus.

De Algemene Rekenkamer (AR) concludeerde in haar verantwoordingsonderzoek over 2014 dat de DigiD-omgeving, naast de webomgevingen van meerdere afnemers, al enkele jaren niet volledig voldoet aan de belangrijkste beveiligingsnormen en dat de beveiliging onvoldoende bescherming biedt voor aanvallen op de webomgeving. Hierdoor is volgens de AR sprake van belangrijke beveiligingsrisico's.[1]

In 2014 al heb ik de beheerorganisatie Logius, onderdeel van mijn ministerie, de opdracht gegeven de veiligheid van DigiD grondig aan te pakken en te beginnen met het oplossen van de in 2014 geconstateerde bevindingen van de AR.

[1] Rapport «Resultaten verantwoordingsonderzoek bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties over 2014 (VII)», Algemene Rekenkamer, 20 mei 2015, Kamerstuk 34 200 VII, nr. 2

kst-26643-372
ISSN 0921 - 7371
's-Gravenhage 2015

In het Algemeen Overleg (AO) ICT-aangelegenheden van 20 mei jl. heb ik de toezegging gedaan uw Kamer een tussenrapportage te zenden over de stappen die worden genomen om de beveiliging van DigiD te verbeteren (Kamerstuk 26 643, nr. 366). In het vervolg van deze brief ga ik in op de resultaten en de stand van zaken van de inspanningen die vorig jaar en dit jaar hiertoe zijn en worden geleverd.

Stand van zaken

In mijn brief van 24 februari 2015 heb ik uw Kamer gemeld dat een taskforce bij Logius in 2014 uitvoering heeft gegeven aan een actieplan DigiD assessmentnormen dat primair gericht was op het oplossen van de bevindingen van de AR.[2]

Uit een rapport van een externe auditor van 1 juni 2015, dat op 6 juli jl. vertrouwelijk ter inzage aan uw Kamer is aangeboden, blijkt dat alle oorspronkelijke bevindingen uit 2014, waarover de AR rapporteerde in haar verantwoordingsonderzoek, zijn opgelost (Kamerstuk 26 643, nr. 364). Uit dit auditrapport bleek verder dat DigiD op dat moment nog slechts aan één norm niet voldeed. Dat betrof een nieuwe bevinding van de externe auditor, op basis van de bestaande kaders.
In juli zijn maatregelen genomen om ook aan die laatste norm te voldoen. Een andere dan bovengenoemde externe auditor heeft onlangs vastgesteld dat de laatste bevinding inderdaad qua opzet en bestaan is opgelost. De werking van de getroffen maatregelen over een periode van minimaal 6 maanden zal in 2016 moeten worden aangetoond.[3]

Zoals u weet zijn de afnemers van DigiD inmiddels jaarlijks onderwerp van een ICT-beveiligingsassessment. Dit jaar verloopt de afhandeling voorspoedig. Organisaties die in gebreke bleven, heb ik hier bestuurlijk op laten aanspreken. Bij niet tijdig voldoen aan de gestelde normen is de dienstverlening opgeschort, wat zich 7 keer heeft voorgedaan in 2015.

De AR verwacht van mij dat ik de afnemers concreter informeer over de betrouwbaarheidsniveaus van DigiD en afnemers er nadrukkelijker op wijs wanneer zij DigiD gebruiken voor processen waarvoor een hoger betrouwbaarheidsniveau noodzakelijk is.
Tijdens het aansluitproces op DigiD wordt de potentiële afnemer uitdrukkelijk gewezen op het belang om goed vast te stellen welk niveau van betrouwbaarheid van DigiD bij een bepaalde dienst hoort. Ik blijf erbij dat de afnemer zelf dit het best kan doen omdat daar de kennis aanwezig is over het specifieke proces waarvoor DigiD wordt ingezet. Daarnaast is het de verantwoordelijkheid van de afnemer, mede op grond van de Wet bescherming persoonsgegevens, om het voor een digitale dienst passend betrouwbaarheidsniveau van authenticatie toe te passen.
Wel ondersteun ik de afnemer om dit zorgvuldig te doen onder meer met de door het Forum Standaardisatie vastgestelde handreiking «Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten».

Project Arend

Informatiebeveiliging en daarmee ook de beveiliging van DigiD vraagt om niet aflatende alertheid. Daarom is Logius in 2015, als vervolg op bovengenoemd actieplan, het project Arend gestart.

---

[2] Kamerstuk 26 643, nr. 352.
[3] Opzet wil zeggen dat er een ontwerp is; bestaan wil zeggen dat de noodzakelijke processen zijn ingericht en werking wil zeggen dat de processen werken zoals ze zijn bedoeld.

Naast de verantwoordingsonderzoeken van de AR zijn door de Auditdienst Rijk en Logius in 2013 en 2014 onderzoeken gedaan naar de veiligheid van de DigiD-omgeving, gebaseerd op verschillende normenkaders. Daaruit zijn, los van de bevindingen van de AR, ruim honderd aanbevelingen naar voren gekomen, die verschillend zijn van aard en zwaarte.

Doelstelling van het project Arend is de originele bevindingen op te lossen en de aanbevelingen met meer dan een laag risico door te voeren. En de processen bij Logius, waar nodig, structureel hiervoor aan te passen. Het is de opdracht van Logius om DigiD aan alle vigerende normenkaders te laten voldoen. De snelle technologische en maatschappelijke ontwikkelingen gaan ondertussen door. Dat betekent dat ook na het project Arend de beveiliging van informatie een continu aandachtspunt zal blijven.

Op het moment van schrijven van deze brief zijn de laatste aanbevelingen in behandeling. De oplossingen van de laatste aanbevelingen zijn complex en hebben implicaties voor bestaande werkwijzen en afspraken met de leverancier van DigiD. Deze aanpassingen vragen daarom meer tijd. Het streven is en blijft de behandeling van alle aanbevelingen vóór het eind van 2015, in ieder geval qua opzet en bestaan, te hebben afgerond. Medio 2016 zal moeten blijken of alle getroffen maatregelen effectief zijn of dat er nog aanpassingen noodzakelijk zijn.

Slotwoord

Honderd procent veiligheid is niet te garanderen. Daarnaast evolueert de techniek voortdurend en worden de standaarden en normen voor informatiebeveiliging daarop aangepast. In 2016 zal Logius daarom onverkort, als onderdeel van de dagelijkse werkzaamheden, aandacht blijven besteden aan de beveiliging van de DigiD-omgeving en die van de webomgevingen van de afnemers.
Ik ben er van overtuigd dat door uitvoering van het actieplan in 2014 en het project Arend in 2015 de kwaliteit van de beschikbaarheid, integriteit en vertrouwelijkheid van DigiD verder is verbeterd en structureel continue aandacht krijgt. Daarbij wil ik er op wijzen dat er zich het afgelopen jaar geen noemenswaardige incidenten met DigiD hebben voorgedaan.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk