Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 332

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 7 november 2014

Bij brieven aan de Kamer[1] heb ik toegezegd om de Kamer nader te informeren over de mogelijkheden tot verdere versterking van DigiD. In deze brief schets ik de ontwikkelingen die mij daarbij voor ogen staan.

DigiD heeft op dit moment ca. 600 aangesloten afnemers en kent ca. 11 miljoen gebruikers. Deze genereerden in 2013 ca. 117 miljoen authenticaties. De prognose is dat in 2014 ca. 170 miljoen authenticaties worden bereikt. De beschikbaarheid voor DigiD lag tot en met augustus boven de met de leveranciers afgesproken norm van 99,95%.

Bovenstaande cijfers geven duidelijk het belang weer van DigiD. Het is belangrijk om met vereende kracht het hoofd te blijven bieden aan de steeds toenemende dreigingen voor de betrouwbaarheid en de continuïteit van een goede en veilige elektronische toegang tot de overheid. Om deze dienstverlening veilig te houden en tegelijk ook toekomstbestendig te maken, worden de nodige inspanningen verricht.

1. Bestaande maatregelen

– Bij ontdekking van zogeheten phishing-sites worden deze websites in samenwerking met de Belastingdienst en het Nationaal Cyber Security Center (NCSC) zo snel mogelijk uit de lucht gehaald. Dit jaar zijn er al 40 sites op deze manier uit de lucht gehaald.
– Op de website van DigiD wordt door Logius advies gegeven over het veilig omgaan met DigiD. Daarbij wordt onder meer gewezen op het belang dat de gebruiker controleert dat hij/zij daadwerkelijk inlogt op de echte inlogpagina van DigiD. Ook wordt gewaarschuwd voor valse e-mails waarin wordt gevraagd om inloggegevens in te vullen. Bovendien wordt uitgelegd hoe de gebruiker misbruik van zijn account kan herkennen en welke actie hij kan ondernemen bij geconstateerd

[1] Kamerstuk 26 643, nr. 323 en Kamerstuk 26 643, nr. 329.

kst-26643-332
ISSN 0921 - 7371
's-Gravenhage 2014

misbruik. Tenslotte wordt verwezen naar de ondersteuning die kan worden geboden onder meer via de helpdesk van DigiD, het Centraal Meldpunt Identiteitsfraude en het Meldpunt Slachtoffers Fraude van de Belastingdienst.
– In de Alert-Online-campagne wordt ook uitgebreid aandacht besteed aan veilig internetten.
– Burgers kunnen er nu ook al voor kiezen om standaard in te loggen op niveau Midden. Dat maakt hen – vanwege de tweede authenticatie door middel van SMS – minder kwetsbaar voor bijvoorbeeld phishing.

2. Recent doorgevoerde maatregelen

– Er worden voortaan e-mails verstuurd aan burgers bij belangrijke wijzigingen aan hun DigiD, zoals bij het wijzigen van een wachtwoord. Op die manier wordt het makkelijker voor burgers om misbruik van hun DigiD te herkennen.
– Op dit moment worden DigiD activeringscodes in kwetsbare postcodegebieden thuisbezorgd. In totaal zijn in 2014 ca. 7500 brieven thuisbezorgd per koerier.
– Er zijn maatregelen tegen DDoS-aanvallen genomen. Dit is belangrijk voor de beschikbaarheid en continuïteit van DigiD maar ook voor de veiligheid.
– Onlangs is DigiD beveiligd om het mogelijk te maken beter de integriteit en authenticiteit van de website te controleren en phishing te bemoeilijken.

3. Nog door te voeren maatregelen ter versterking van DigiD

Het komend jaar wordt er naar alternatieven voor de bestaande twee-factor authenticatie met SMS (DigiD Midden) gekeken, die tegen lagere kosten op grote schaal kunnen worden toegepast. Dit kan bijvoorbeeld een app zijn waarmee een extra verificatiecode op smartphone of tablet kan worden ontvangen. De eerste pilots starten naar verwachting medio 2015.

Om een nog grotere mate van zekerheid over iemands identiteit te verkrijgen bij het inloggen t.o.v. DigiD Midden met SMS, wordt er een aantal mogelijkheden onderzocht waarbij er een extra controle plaatsvindt, nadat iemand is ingelogd met DigiD, door het uitlezen van gegevens op de chip van een wettelijk identiteitsdocument (bv identiteitskaart, rijbewijs). Die gegevens worden vervolgens geverifieerd aan de hand van de betreffende documentregisters. Hiermee wordt het mogelijk om digitaal diensten aan te bieden die dat hogere betrouwbaarheidsniveau vereisen.

Mede naar aanleiding van de aanbeveling van de Algemene Rekenkamer, wordt ook uitvoering gegeven aan een Actieplan voor het oplossen van de bevindingen op DigiD. Hiermee zal de robuustheid van DigiD verder toenemen. Inmiddels zijn enkele van de bevindingen opgelost. Zoals eerder gemeld wordt er naar gestreefd ook de overige bevindingen vóór het einde van het jaar op te lossen.

4. Assessments

Voor het systeem van DigiD is het van belang dat afnemers volledig voldoen aan de ICT-beveiligingsassessments DigiD. Met de uitvoering van verbetertrajecten bij de afnemers naar aanleiding van de eerste ronde assessments, zijn inmiddels veel bevindingen opgelost. Logius blijft deze ontwikkeling monitoren. In de eerste helft van volgend jaar wordt de

tweede volledige assessmentronde uitgevoerd. De verwachting is dat dan een groter aantal organisaties direct aan alle assessmentnormen voldoet.

5. Aanpak fraude

In 2014 is een aantal maatregelen getroffen waardoor fraude of pogingen daartoe eerder en beter gedetecteerd kunnen worden. Logius heeft processen ingericht om signalen van mogelijk misbruik te genereren, te duiden en analyseren. Logius werkt hierbij intensief samen met belangrijke uitvoeringsorganisaties, wat succesvol is voor het vaststellen en tegengaan van bepaalde fraudevormen.
Voor slachtoffers van identiteitsfraude en -fouten is het van belang dat zij zich erkend voelen in hun probleem. De ervaringen van slachtoffers met het Centraal Meldpunt Identiteitsfraude en -fouten (CMI) zijn positief. De medewerkers van het CMI zijn getraind om goed door te vragen om de bron van de problemen te vinden. Vanaf dat punt kunnen zij gericht hulp bieden. Ook de Belastingdienst en het UWV hebben gespecialiseerde teams voor de begeleiding van burgers die in de problemen zijn geraakt (respectievelijk «Stella teams» en «Murphy teams»). Het CMI bespreekt de wijze van hulpverlening aan slachtoffers met diverse uitvoeringsorganisaties.

6. Toegankelijkheid DigiD

Het programma Digitaal 2017 streeft naar het digitaal mogelijk maken van het doen van allerlei zaken met de overheid. Voor sommige mensen vormt daarbij het gebruik van DigiD toch een drempel. Om die reden heb ik de Stichting Digisterker gevraagd een oefenmiddel te ontwikkelen: de DigiD oefentool. Mensen die een digivaardigheidscursus volgen kunnen in een veilige omgeving een DigiD leren aanvragen en gebruiken. Door te oefenen, wordt de drempel lager om DigiD aan te vragen en goed te gebruiken. De oefentool is naar verwachting in januari 2015 operationeel.

Voor toegang tot transacties met de overheid is het ook nodig dat websites voor grote groepen mensen toegankelijk zijn. DigiD voldoet aan de eisen die gesteld worden aan de toegankelijkheid van overheidswebsites, de zogenoemde webrichtlijnen.

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