Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 256

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 oktober 2012

Met deze brief wil ik u, conform mijn toezegging bij brief d.d. 2 februari 2012 (Kamerstukken II 2011/12, 26 643, nr. 242), informeren over de stand van zaken met betrekking tot de ICT-beveiligingsassessments DigiD.

Betrouwbare elektronische dienstverlening is van wezenlijk belang voor het functioneren van de Nederlandse samenleving en vereist voortdurende aandacht.
DigiD vervult hierin een cruciale rol, omdat DigiD het overheidsmiddel is waarmee burgers zich digitaal bekend maken. Om dit belang en het vertrouwen in DigiD te borgen, heb ik maatregelen rond de veiligheid van DigiD genomen, en informeer ik u hierbij over de stand van zaken.

Maatregelen beveiliging DigiD

De maatregelen die ik heb genomen houden in dat organisaties die gebruik maken van DigiD hun ICT-beveiliging, voor zover deze DigiD raakt, jaarlijks dienen te toetsen op basis van een ICT-beveiligingsassessment. Bij de uitvoering van het assessment wordt de «Norm ICT-beveiligingsassessments DigiD»[1] gehanteerd die 21 februari 2012 is vastgesteld. Deze norm is een selectie van de voor DigiD belangrijkste elementen uit het document «ICT-beveiligingsrichtlijnen voor webapplicaties» van het Nationaal Cyber Security Centrum (NCSC). Het gaat om elementen die de meeste impact hebben op de veiligheid van DigiD en de met DigiD ontsloten gegevens. Vanwege het generieke belang en de individuele verantwoordelijkheid van organisaties om de eigen ICT-beveiliging op orde te hebben, wordt DigiD gebruikende organisaties evenwel uitdrukkelijk geadviseerd om de hele set van richtlijnen van het NCSC toe te passen op hun ICT-beveiliging. Deze maatregelen zijn overigens niet de enige rond DigiD. De DigiD infrastructuur is inmiddels verbeterd met de oplevering van DigiD nieuwbouw en steeds meer organisaties en burgers kiezen voor het veiliger DigiD Midden. Met dat middel kunnen burgers zich extra legitimeren met behulp van een SMS. In

[1] Zie http://www.logius.nl/fileadmin/logius/product/digid/documenten/assessments/120221_norm_ict-beveiligingsassessments_digid.pdf.

kst-26643-256
ISSN 0921 - 7371
's-Gravenhage 2012

2012 zijn er ca. 400 000 extra DigiD Midden accounts aangemaakt. Tot slot heeft Logius opdracht gekregen om bij signalen van inbraak of onveiligheid over te gaan tot onmiddellijke afsluiting. In 2012 is dat instrument tot op heden niet nodig gebleken.

Procedure ICT-beveiligingsassessments DigiD

Vanwege het belang van een uniforme uitvoering van de ICT-beveiligingsassessments DigiD is bepaald dat het assessment wordt uitgevoerd door een Register EDP-auditor. Met de beroepsorganisatie van IT-auditors, NOREA, is overleg gevoerd over een standaard opdrachtbrief en een rapportageformat die zullen worden gebruikt bij het assessment. Met Logius[1], de beheerorganisatie van DigiD, heb ik afspraken gemaakt over het proces dat gevolgd zal worden in geval dat uit de rapportage blijkt dat DigiD gebruikende organisaties niet of nog niet geheel voldoen aan de gestelde eisen. Daarbij staat voorop dat er bij signalen van beveiligingsrisico's met mogelijke gevolgen voor DigiD altijd nader onderzoek wordt uitgevoerd. Daarnaast zal in geval van een geconstateerd serieus en acuut beveiligingsrisico door Logius meteen worden overgegaan tot het gecontroleerd afsluiten van DigiD bij de betreffende organisatie.

Grootgebruikers

Vanwege de vele miljoenen DigiD transacties die de grootgebruikers jaarlijks genereren, spelen zij een cruciale rol in de elektronische overheidsdienstverlening en zijn zij van groot belang voor de burger. Om die reden is intensief overleg gevoerd met deze gebruikers. De belastingdienst, DUO en UWV hebben inmiddels aangegeven dat zij het ICT-beveiligingsassessment DigiD naar verwachting nog in 2012 zullen hebben uitgevoerd. Daarmee wordt bewerkstelligd dat reeds dit jaar 73% van het totaal aantal DigiD transacties, plaatsvindt in een ICT-omgeving die middels het ICT-beveiligingsassessment is getoetst.

Medeoverheden en overige gebruikers

Ten aanzien van de medeoverheden heb ik met de Vereniging Nederlandse Gemeenten (VNG) afspraken gemaakt over de uitvoering van een door VNG gecoördineerde ondersteuningsaanpak voor gemeenten, die tevens ondersteuning aan provincies en waterschappen biedt. Deze aanpak ondersteunt de medeoverheden in de voorbereiding op en het uitvoeren van het assessment en zal onder meer bestaan uit een helpdesk, activiteiten rond het vergroten van de bewustwording en het opstellen van een draaiboek en standaarddocumenten.

Het belang van een gecoördineerde aanpak is ook gebleken uit de impactanalyse die het Kwaliteitsinstituut Nederlandse Gemeenten (KING) in opdracht van de VNG en mijn ministerie bij een aantal gemeenten en betrokken leveranciers heeft uitgevoerd naar de effecten van het assessment. De uitkomsten van de analyse tonen aan dat bundeling van werkzaamheden bij gemeenten en leveranciers mogelijk is, wat tijd en geld bespaart. Verder is gebleken dat bewustwording van informatiebeveiliging van cruciaal belang is.

KING is met de ondersteuningsactiviteiten gestart. De eerste regiosessies ICT-beveiligingassessments hebben reeds plaatsgevonden. Hiervoor zijn gemeenten, provincies en waterschapen uitgenodigd. Tijdens de regiosessies wordt aandacht besteed aan de bewustwording van informatiebeveiliging en wordt uitleg gegeven over de ondersteuningsaanpak. Daarnaast worden de medeoverheden opnieuw gewezen op de

[1] Logius is onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

urgentie van het uitvoeren van het ICT-beveiligingsassessment. Ook de VNG heeft deze urgentie middels een ledenbrief wederom onder de aandacht van gemeenten gebracht.

Daarnaast werkt de VNG aan de voorbereidingen rond de komst van een gemeentelijke informatiebeveiligingsdienst. Deze dienst zal gemeenten ondersteunen bij het optimaliseren van de gemeentelijke informatiebeveiliging en het afhandelen van beveiligingsincidenten. In dat verband zal VNG een baseline informatiebeveiliging voor gemeenten opstellen, naar analogie van de Baseline Informatiebeveiliging Rijksdienst die onlangs is vastgesteld. Ook de Unie van Waterschappen bereidt een baseline informatiebeveiliging voor, waarin ook het kwaliteitsniveau van de beveiliging van fysieke objecten zal worden meegenomen.
Het algemene beeld is dat de medeoverheden inmiddels zijn gestart met de voorbereiding op de assessments. Bij de uitvoering daarvan zal ook de capaciteit van auditors en pentesters een rol spelen.

Samenwerking hogescholen en universiteiten

In navolging op een voorstel van uw Kamer heb ik contact gelegd met een aantal hogescholen en universiteiten over het aangaan van een samenwerking over het uitvoeren van hacktesten bij overheden. Een aantal hogescholen en universiteiten heeft met enthousiasme hierop gereageerd. De vormen van deze samenwerking worden momenteel nader uitgewerkt. De intentie is om dit jaar al de eerste hacktesten door studenten te laten uitvoeren.

Eindrapport bedrijf Fox-IT over DigiNotar

Onlangs heeft het bedrijf Fox-IT het eindrapport over de digitale inbraak bij DigiNotar en het frauduleus aanmaken van valse certificaten opgeleverd. Het eindrapport bevat geen andere inzichten of conclusies ten opzichte van het interim rapport, dat u op 5 september 2011 is aangeboden (Kamerstuk 26 643, nr. 188). Wel geeft het veel gedetailleerdere informatie over de inbraak bij DigiNotar, gebaseerd op het forensisch onderzoek dat Fox-IT op de logbestanden van DigiNotar heeft gedaan. Conform de door mijn ambtsvoorganger gedane toezegging zend ik u het eindrapport met deze brief mee *).

De minister van Binnenlandse Zaken en Koninkrijksrelaties,
J. W. E. Spies

*) Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer