Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 269

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 22 maart 2013

Met deze brief informeer ik u over de stand van zaken ICT-beveiligingsassessments die inmiddels verplicht zijn bij organisaties die DigiD gebruiken en de oprichting van de Taskforce Bestuur en informatieveiligheid dienstverlening. In het Algemeen Overleg dat de vaste commissie voor Economische Zaken heeft gevoerd met minister Kamp van Economische Zaken over de digitale markt (13 februari 2013) heeft kamerlid mevrouw Mulder (CDA) gevraagd naar het voorstel voor de Taskforce, de tijdspanne en het informeren van de Tweede Kamer over de resultaten van de Taskforce.

ICT-beveiligingsassessments

Bij brief van 30 oktober 2012[1] bent u geïnformeerd over de stand van zaken met betrekking tot de voorbereidingen voor de uitvoering van de de ICT-beveiligingsassessments die worden ingezet bij organisaties die gebruikmaken van DigiD. Toen is onder meer bevestigd dat, zoals voorgeschreven, de zogeheten grootverbruikers van DigiD naar verwachting het ICT-beveiligingsassessment nog in 2012 zouden hebben uitgevoerd. Tevens is aangegeven dat de overige afnemers van DigiD voor eind 2013 het assessment op hun DigiD aansluiting moeten hebben uitgevoerd. De assessments zijn uitgevoerd door EDP auditors, op basis van de «Norm ICT-beveiligingsassessments DigiD», zoals deze sinds 21 februari 2012 geldt. De beroepsverenging van EDP-auditors, NOREA, heeft ten behoeve van haar leden een *guidance* opgesteld, aan de hand waarvan de toetsing van de normen in de praktijk nader kan worden geconcretiseerd.
De auditrapporten van de zes grootverbruikers zijn beoordeeld door het Agentschap Logius van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

[1] Kamerstuk 26 643, nr. 256

kst-26643-269
ISSN 0921 - 7371
's-Gravenhage 2013

Belangrijk is te constateren dat er bij geen van de grootverbruikers sprake is van een zodanig serieus en acuut beveiligingsrisico met mogelijke gevolgen voor DigiD, dat aanleiding zou bestaan dat direct afsluiten van de betreffende organisatie door Logius proportioneel is. Uit de auditrapporten komen wel bevindingen naar voren die aanleiding geven voor maatregelen tot verbetering op onderdelen. De betrokken organisaties hebben deze maatregelen inmiddels opgepakt.

Het is de eerste keer dat met de nieuwe en strengere eisen de assessments op de ICT-omgeving van afnemers van DigiD op deze wijze zijn uitgevoerd. Dit betekent dat het voor alle betrokken partijen een leerproces is, dat een grote -maar noodzakelijke- extra inspanning heeft gevraagd.

De eerste ervaringen met de grootverbruikers leveren leerpunten op voor zowel het proces als de inhoudelijke aanpak van de assessments die nu bij gemeenten en andere afnemers worden voorbereid en uitgevoerd. Ik heb met VNG en KING nadere afspraken gemaakt over een effectieve invoeringsstrategie van de ICT beveiligingsassessments bij gemeenten. Zij zullen zorgdragen voor de begeleiding van gemeenten met ondermeer een koplopergroep. KING heeft een ondersteuningsaanpak voor de uitvoering van assessments bij gemeenten en andere afnemers ontwikkeld. In dat kader zijn regiobijeenkomsten met afnemers gehouden waarbij het belang van assessments onder de aandacht is gebracht en tevens is geschetst op welke wijze voorbereidingen voor de assessments getroffen kunnen worden. Daarnaast wordt vanuit KING onder meer het initiatief genomen om zogeheten *Third Party Mededelingen* [TPM's] tot stand te brengen ten aanzien van leveranciers, zodat deze bij de assessments van meerdere gemeenten kunnen worden gebruikt. Bij een informatiebijeenkomst van KING voor leveranciers zijn de eerste stappen gezet om hierover tot concrete afspraken te komen.

Taskforce Bestuur en Informatieveiligheid Dienstverlening

Op 13 februari 2013 heb ik de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID) ingesteld om het onderwerp informatieveiligheid hoog op de agenda te krijgen bij bestuurders en topmanagement van alle overheidslagen. Zowel qua bewustwording als sturing. De Taskforce is uitvloeisel van de aanbevelingen van de Onderzoeksraad Voor Veiligheid in reactie op het diginotar-incident[2]. De Onderzoeksraad constateerde dat er een noodzaak is tot versterking van het bewustzijn van informatieveiligheid en gerelateerde risico's alsmede de sturing daarop en beveelde aan een programma te ontwikkelen om bestuurders te doordringen van het belang van digitale veiligheid en hen te voorzien van voldoende inzicht en vaardigheden. De Taskforce is ingericht voor een periode van twee jaar.

De Taskforce is met name gericht op bestuurders en het topmanagement van de individuele overheidslagen; waterschappen, provincies, gemeenten, zelfstandige bestuursorganen en rijksoverheid, alsook op de samenwerking daartussen. De Taskforce bouwt voort op de huidige initiatieven op informatieveiligheidsvlak van elk van de overheidslagen vanuit een intensieve samenwerking met de koepelorganisaties. Betrokken (koepel)organisaties zijn de Unie van Waterschappen, het IPO, de VNG, de Manifestgroep, en de Interdepartmentale Commissie Chief Information Officers. Bovendien wordt nauw samengewerkt met betrokken organisaties op informatieveiligheidsvlak, zoals het Nationaal Cyber Security Centrum (NCSC), het Centrum Informatiebeveiliging en

[2] Rapport: «Het diginotar-incident, waarom digitale veiligheid de bestuurstafel te weinig bereikt»

Privacybescherming (CIP), de Informatiebeveiligingsdienst voor gemeenten (IBD), het Waterschapshuis en Logius, het Agentschap van het Ministerie van BZK.

Het doel van de Taskforce is om versnelling teweeg te brengen in het bewustzijn van informatieveiligheid bij bestuurders en topmanagers van overheden, en om sturing op informatieveiligheid door deze bestuurders en topmanagers mogelijk te maken. Uiteindelijke doel is dat informatieveiligheid ook daadwerkelijk in de continuïteit van bedrijfsprocessen wordt geborgd en verankerd, en dat de risico's op incidenten zoals Diginotar tot een minimum beperkt worden.
Stip aan de horizon is uiteindelijk te komen tot verplichtende zelfregulering per overheidslaag als het gaat om informatieveiligheid. Iedere overheidslaag is en blijft zelf verantwoordelijk voor het op orde krijgen en houden van haar informatieveiligheid en om te komen tot die verplichtende zelfregulering.

Het onderwerp informatieveiligheid dient op de agenda te staan van ieder bestuur. Het is aanzienlijk effectiever dat de overheidslagen en organisaties daarbinnen dat zelf scherp en bewust sturen en reguleren, dan dat wetgeving hiertoe wordt ontwikkeld. Die zelfregulering mag echter niet vrijblijvend zijn. De opdracht aan de Taskforce is dan ook om de ontwikkeling naar zelfregulering met een verplichtend karakter te versterken en te faciliteren en werkt daartoe nauw samen met de koepelorganisaties. Naast het aanbieden van concrete sturingsmiddelen staat leren, ontwikkelen en verankeren bij die samenwerking centraal. De missie van de Taskforce is na twee jaar geslaagd wanneer alle overheidslagen en -organisaties gezamenlijk een solide basis hebben gelegd voor deze zelfregulering op het informatiebeveiligingsvlak. In iedere organisatie moet een jaarlijkse cyclus zijn geborgd waarin ambtelijke en bestuurlijke oordeelsvorming over de informatieveiligheid en de aanpak van verbeterpunten plaats vindt. Er moet sprake zijn van een voortgaand leerproces, mede gebaseerd op risicomanagement. De zelfregulering dient te geschieden op basis van de volgende uitgangspunten:

1. Een normatieve basis per organisatie en per overheidslaag (ISO 27001 en ISO 27002).
2. Een verankering van deze normatiek, ook als basis voor risicoanalyse. Elke betrokken organisatie regelt de informatieveiligheid op adequaat niveau. Op het niveau van de overheidslagen is er een stelsel van afspraken over de verantwoordelijkheid hierbij van koepelorganisaties. Op landelijk niveau belegde en daarvoor ingerichte voorzieningen faciliteren deze zelfregulering.
3. Auditing is hierbij een belangrijk instrument. De ontwikkeling van een stelsel van single audit is een stimulerende factor voor zelfregulering en vindt zo veel als mogelijk plaats.
4. Elke organisatie, nader ondersteund per overheidslaag, traint regulier op een actieve gerichtheid van bestuur, management, ICT-functionarissen en andere medewerkers op informatieveiligheid.
5. Voor elke organisatie en elke overheidslaag is een probleemanalyse en veranderplan opgesteld dat uiteindelijk leidt tot een verplichtende zelfregulering van informatieveiligheid.

Door de verschillende overheidslagen is nadrukkelijk de bereidheid uitgesproken om de komende periode tot een dergelijke aanpak te komen, waarbij in een aantal organisaties al sprake is van «best practices» inzake deze cyclische aanpak. Binnen de verschillende overheidslagen is daartoe

in samenwerking met de Taskforce initiatief genomen. Voor de Rijksoverheid geldt nu al dat per departement jaarlijks gerapporteerd gaat worden over de stand van de informatieveiligheid.

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