Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 344

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 18 december 2014

In het Algemeen Overleg van 27 maart 2013 over Beveiligingsaspecten en ICT heb ik uw Kamer toegezegd u te informeren over de voortgang van de Taskforce Bestuur & Informatieveiligheid Dienstverlening (Taskforce BID) (Kamerstuk 26 643, nr. 275).[1] Met deze brief geef ik invulling aan mijn toezegging. De Taskforce BID, die per 13 februari 2013 is ingesteld, was belast met het verhogen van het bewustzijn over het belang van en de kennis over informatieveiligheid bij bestuurders en topmanagers in het openbaar bestuur. Ik heb, in overeenstemming met de koepelvertegenwoordigers bij de overheid, de Taskforce BID ingesteld mede naar aanleiding van het rapport «Het DigiNotarincident» van de Onderzoeksraad voor Veiligheid (OvV), (Kamerstuk 26 643, nr. 257). Het rapport van de OvV constateerde onder meer dat er een noodzaak was tot versterking van het bewustzijn ten aanzien van informatieveiligheid en daaraan gerelateerde risico's, alsmede de sturing daarop.

De Taskforce BID kreeg verder als opdracht mee een systeem van verplichtende zelfregulering te helpen ontwikkelen en te faciliteren alsook de overheidsbrede coördinatie op informatieveiligheid bij het openbaar bestuur te bevorderen. De uitvoering van dit programma is in nauwe samenwerking met de koepels van de verschillende overheidslagen en enkele vakdepartementen (gemeenten, provincies, waterschappen en Rijk/ZBO's) opgepakt, met gebruikmaking van initiatieven die al gaande waren. De inzet van de Taskforce BID is niet gericht geweest op de informatieveiligheid van afzonderlijke overheidsorganisaties zelf, omdat deze in eerste instantie zelf verantwoordelijk zijn voor het op orde brengen en houden van informatieveiligheid in hun organisatie.

De Taskforce BID heeft voor verschillende overheidslagen een stelsel van verplichtende zelfregulering helpen (door)ontwikkelen en invoeren. De

[1] *Als bijlage bij deze brief treft u de voortgangsrapportage van de Taskforce BID aan.* Raadpleegbaar via www.tweedekamer.nl

kst-26643-344
ISSN 0921 - 7371
's-Gravenhage 2014

verplichtende zelfregulering is een niet vrijblijvend, samenhangend stelsel van normen, beleid en een set van afspraken over de naleving en toetsing daarvan. Op dit moment is binnen elke overheidslaag een norm afgesproken voor informatiebeveiliging, de zogenaamde baselines informatiebeveiliging.[2] Deze baselines zijn gebaseerd op breed geaccepteerde internationale standaarden.

Blijvende samenwerking en dialoog

De digitale dienstverlening bij de overheid en overheidsorganisaties is in sterke mate gebaseerd op met elkaar verweven netwerken. Onderling en met derden vindt dagelijks uitwisseling van gegevens plaats, met gebruik van gemeenschappelijke digitale voorzieningen en infrastructuur en in onderlinge samenwerking. Vanwege die onderlinge verwevenheid en samenwerking heeft de Taskforce BID zich ingezet voor het creëren van een blijvende samenwerking en dialoog tussen bestuurders en ambtelijke top van overheden en overheidsorganisaties ter verbetering van informatieveiligheid. Daarbij komen verschillende onderwerpen aan bod.

Speciale aandacht in deze dialoog gaat uit naar de wijze van verantwoording over informatieveiligheid. Belangrijk is dat bestuur en politiek inzicht kan krijgen in de stand van de informatieveiligheid bij overheidsorganisaties afzonderlijk, per overheidslaag en in het totaal. Daarbij is het uitgangspunt inzicht in de belangrijkste risico's van de organisaties en de aanpak, organisatiebreed en zelfs per overheidslaag, om die risico's te voorkomen. Konden we ons een paar jaar geleden nog moeilijk voorstellen dat bestuur en politiek zich zouden bezighouden met een onderwerp dat zich voornamelijk afspeelde bij de afdeling ICT, duidelijk is ondertussen dat dit niet alleen een technische kwestie is, maar ook een bestuurlijke die gaat over het functioneren van overheidsorganisaties in hun primaire processen; bestuurders moeten dus hun verantwoordelijkheid nemen voor de digitale veiligheid. En dat betekent ook het afleggen van verantwoording. Die verantwoording gaat dan niet alleen over veiligheid van afzonderlijke systemen, maar juist ook over aanpak in organisatie en netwerken en in processen en gedrag van de organisatie. Dit wordt momenteel nader uitgewerkt met de verschillende overheidslagen.

De interbestuurlijke visitatiecommissie

De gemeenten hebben tijdens de Bijzondere Algemene Leden Vergadering (B ALV) van de VNG op vrijdag 29 november 2013 de Resolutie «Informatieveiligheid, randvoorwaarde voor de professionele gemeente» aangenomen. In deze Resolutie geven gemeenten aan dat zij verder werken aan informatieveiligheid, onder andere door de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) te accepteren en uit te voeren en verantwoording goed in te richten op lokaal niveau.

In de resolutie is aangegeven dat een onafhankelijke interbestuurlijke visitatiecommissie de digitale veiligheid in gemeenten zal toetsen. Dat is een belangrijk besluit en een wezenlijk vervolg op het werk van de Taskforce BID. De gemeenten zijn sterk afhankelijk van informatiestromen, ook onderling, en moeten zorgvuldig omgaan met gegevens; een goede

---

[2] *De baselines vormen een instrument om de informatiehuishouding van overheidsorganisaties te verbeteren en zijn gebaseerd op andere algemeen geaccepteerde kaders, zoals de NEN-ISO-normen. Voor het Rijk is dat de Baseline Informatiebeveiliging Rijksdienst (BIR), voor provincies de Interprovinciale Baseline Informatiebeveiliging (IBI), voor gemeenten de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en voor waterschappen de Baseline Informatiebeveiliging Waterschappen (BIWA).*

informatieveiligheid is dus nodig en op lokaal niveau moet de uitvoeringskracht op dit gebied toenemen. Mijn ministerie is door de VNG gevraagd nauw betrokken te blijven bij het werk van de visitatiecommissie.

De verantwoordinglast voor gemeenten

In diezelfde Resolutie vragen gemeenten mij als Minister van BZK tevens onderzoek te doen naar de door gemeenten ervaren verantwoordingslast en de wijze waarop dit kan worden gestroomlijnd.

Verantwoording over informatieveiligheid wordt door gemeenten op dit moment afgelegd op verschillende onderwerpen en systemen van de gemeentelijke organisatie. Omdat het feitelijk steeds gaat om dezelfde soort verantwoording, en de gemeentelijke informatiestromen kunnen worden gezien als een netwerk, is de verantwoording aan vernieuwing en bundeling toe en kan de administratieve last worden teruggedrongen. Ik heb daartoe de Taskforce BID verzocht om in nauwe samenwerking met de VNG, de Informatiebeveiligingsdienst voor gemeenten (IBD), de Accountantsdienst Rijk (ADR) en vakdepartementen een onderzoek te verrichten naar de verantwoordinginspanning van gemeenten. Doel is te komen tot een eenduidige en enkelvoudige verantwoording. Daarbij wordt onderzocht of verantwoording kan worden afgelegd aan het bestuur van gemeenten in de vorm van een «in control statement». De Wet Revitalisering Generiek Toezicht wordt als uitgangspunt genomen. Om te toetsen of deze systematiek in praktijk effectief is, is een negental gemeenten gevraagd om mee te werken aan een pilot, waarvan de resultaten veelbelovend waren. Op dit moment wordt bezien hoe een vervolg kan worden gegeven aan deze pilot en op welke wijze de vermindering van de verantwoordingslast kan worden vormgegeven. Ik zal u in de loop van 2015 informeren over de voortgang van dit traject.

Overdracht taken Taskforce BID en vervolg op interbestuurlijke afspraken

De Taskforce BID eindigt begin 2015 en zorgt in goed overleg met de koepelorganisaties van de overheidslagen voor een overdracht van haar activiteiten en de ontwikkelde instrumenten. Eén van de overdrachtsmomenten heeft plaatsgevonden tijdens een bijeenkomst op 27 oktober 2014. Hierbij zijn vele bestuurders aanwezig geweest om hun verantwoordelijkheid voor en hun blijvende commitment aan informatieveiligheid te benadrukken. Tijdens deze bijeenkomst heb ik met de koepelvertegenwoordigers een verklaring getekend om ook na de beëindiging van de Taskforce BID de verdere verankering van een veilige en zorgvuldige verwerking van gegevens binnen de overheid actief op de agenda te houden, de actielijnen voor de komende periode te duiden en ook om de werkzaamheden van de Taskforce BID van de afgelopen periode te onderschrijven.

Om aan dit vervolg invulling te geven is ondermeer afgesproken dat na de beëindiging van de Taskforce BID structureel overleg blijft plaatsvinden over de voortgang op informatieveiligheid met de koepelvertegenwoordigers bij de overheid. Input hiervoor zijn onder meer de reeds beschikbare rapportages van de koepelorganisaties die jaarlijks tot stand worden gebracht. Alle koepelorganisaties van de overheidslagen geven in hun eigen rapportage(s) op hoofdlijnen weer welke stappen er zijn gezet. De afgelopen periode is hier reeds naar toe gewerkt per afzonderlijke overheidslaag. Voorbeelden zijn waarstaatjegemeente.nl, een monitoringstool informatiebeveiliging voor provincies en voor de waterschappen Waterschapspeil/Waterschapsspiegel.

Naast het voortzetten van de dialoog over informatieveiligheid is ook nodig dat de overheid adequaat reageert op incidenten en crises die de informatieveiligheid raken. Het gaat hierbij met name om het samenspel van organisaties in het openbaar bestuur, dat moet leiden tot een efficiënte en effectieve aanpak bij crisis of grootschalige dreigingen. Samen met het Nationaal Cyber Security Centrum (NCSC), de Informatiebeveiligingsdienst voor gemeenten (IBD) en de betrokken koepel/schakelorganisaties van de medeoverheden wordt gewerkt aan een netwerk waarin kennisdeling, melding van incidenten en lessons learned worden gedeeld. Adequate response en detectie van dreigingen zijn van groot belang voor de (Rijks)overheid. Hiertoe is actieve participatie in de ontwikkeling van initiatieven van het NCSC, zoals het Nationaal Respons Netwerk (NRN). [3] Daarnaast is voorzien in de oprichting van een platform (een zogenaamde ISAC) waarbinnen overheidsorganisaties in een vertrouwelijke omgeving kwetsbaarheden en dreigingen kunnen signaleren en daarmee komen tot gemeenschappelijke oplossingen. Door het delen van deze informatie over verschillende overheidsorganisaties heen, kunnen betere maatregelen worden genomen waarmee de digitale weerbaarheid van de overheid verder verhoogd kan worden.

Verankering in wet- en regelgeving

De afgelopen periode is met inzet van de Taskforce BID en alle betrokken partners bij de medeoverheden veel werk verzet. De aanpak werpt ook zijn vruchten af.[4] Als sluitstuk op de verplichtende zelfregulering, die de eigen verantwoordelijkheid van overheidsorganisaties vormgeeft, werk ik aan (kader)wetgeving waarin (minimum)eisen ten aanzien van informatieveiligheid worden vastgelegd. Welke eisen hierin dienen te worden opgenomen, wordt momenteel, met de betrokken partners bij de medeoverheden en vakdepartementen, nader verkend. De medeoverheden geven aan dat een wettelijke basis ondersteunend zal zijn aan het verder verbeteren van de informatieveiligheid binnen de overheid. [5]

Samen met de Minister van Economische Zaken (EZ) werk ik aan een gezamenlijke wetgevingsagenda voor elektronisch zakendoen voor burgers en bedrijven met de overheid. Informatieveiligheid is hiermee onlosmakelijk verbonden. Burgers en bedrijven moeten erop kunnen vertrouwen dat de gegevens die zij met de overheid uitwisselen, veilig zijn. Dit geldt ook voor de gegevensuitwisseling tussen overheden onderling. Op dit moment wordt bekeken of en hoe het generieke informatieveiligheidsbeleid een plaats kan krijgen in deze in voorbereiding zijnde wet. Van belang is voorts dat de Minister van Veiligheid & Justitie (V&J) een wetsvoorstel Wet gegevensverwerking en meldplicht cybersecurity voorbereidt, naar aanleiding van de motie Hennis-Plasschaert (vergaderjaar 2011–2012, Kamerstuk 26 643, nr. 202). In dit wetsvoorstel wordt onder andere voor de (rijks)overheid en de vitale sectoren geregeld welke organisaties meldingsplichtig zijn ingeval van een incident.

Tot slot

Het naar een hoger plan tillen van informatieveiligheid binnen overheidsorganisaties blijft de komende jaren één van mijn speerpunten. De digitale

---

[3] *Het NRN is een formeel samenwerkingsverband tussen het NCSC en publieke en private ICT-responsorganisaties uit verschillende sectoren. Het NRN heeft als doel de gezamenlijke respons op cybersecurity incidenten te versterken door capaciteiten te bundelen. Binnen het NRN kunnen responsorganisaties kennis en ervaringen delen en wederzijdse bijstand verlenen. Het NRN richt zich zowel op het organiseren van bestaande responscapaciteit als het stimuleren van nieuwe responscapaciteit binnen overheid en vitale sectoren.*

[4] *http://ictmagazine.nl/ict-breed/nederland-leert-van-diginotar/*

[5] *Ook de controle-, verantwoordings- en toezichtsystematiek zal hierin worden meegenomen.*

overheid is geen toekomst meer; het functioneren van de overheid is in sterke mate afhankelijk van een goede sturing op en gebruik van digitale voorzieningen en infrastructuur. Het goed regelen van informatieveiligheid is hier onlosmakelijk aan verbonden. Door dit binnen de overheid samen te doen, zodat kennis, producten en oplossingen voor informatieveiligheid over een weer worden gedeeld, helpt het effect te vergroten en beperkt tevens de kosten. Transparantie over de aanpak binnen de overheid helpt organisaties elkaar te vertrouwen: op informatieveiligheid moet je niet concurreren. Burgers, bedrijven en andere organisaties moeten kunnen blijven vertrouwen op de overheid, ook in het digitale tijdperk. Met digitaal 2017 en de drie decentralisaties is een adequate informatieveiligheid urgent en beleid en sturing hierop hoort op de bestuurstafel. Overheidsorganisaties zijn zelf verantwoordelijk voor de wijze waarop het informatieveiligheidsbeleid in hun organisatie gestalte krijgt. Mijn taak als Minister is kaderstellend en voorts ondersteunend, faciliterend en waar nodig aanjagend naar de overheidslagen.

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