Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 917

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 september 2022

Bij de begrotingsbehandeling BZK van 27 oktober 2021 heeft het lid Rajkowski (VVD) gevraagd naar de stand van zaken met betrekking tot een generiek kader voor vitale digitale overheidsvoorzieningen[1]. Dit naar aanleiding van de Kamerbrief *Voortgang informatieveiligheid bij de overheid* van mijn ambtsvoorganger[2], waarin is toegezegd een dergelijk kader op te stellen. Daarop is toegezegd dat de Tweede Kamer hierover aan het eind van het eerste kwartaal 2022 verder zou worden geïnformeerd.[3] Bij brief van 9 mei 2022[4] bent u geïnformeerd dat u hierover een meer inhoudelijke brief tegemoet zou kunnen zien. Met deze brief wil ik die belofte gestand doen.

Bestaande situatie

De digitale overheid is toegevoegd als een vitale sector in 2015, en daarmee opgenomen in de lijst van vitale infrastructuur van Nederland[5]. Een aantal voorzieningen van de digitale overheid is ook reeds als vitaal aangewezen. Om daarvoor in aanmerking te komen geldt dat bij verstoring, aantasting of uitval ten minste een van de volgende ondergrenzen moet worden geraakt:

- Economische gevolgen: > ca. 5 miljard euro schade of ca. 1,0% daling reëel inkomen;
- Fysieke gevolgen: meer dan 1.000 personen dood, ernstig gewond of chronisch ziek;

[1] Handelingen II 2021/22, nr. 14, items 3 en 7.
[2] Kamerstuk 26 643, nr. 749.
[3] Handelingen II 2021/22, nr. 15, item 11.
[4] Kamerstuk 26 643, nr. 846.
[5] Kamerstuk 30 821, nr. 23.

kst-26643-917
ISSN 0921 - 7371
's-Gravenhage 2022

- Sociaal maatschappelijke gevolgen: meer dan 100.000 personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen.[6]

Deze voorzieningen van de digitale overheid vallen onder het Besluit Beveiliging Netwerk en Informatiesystemen (Bbni) dat voortvloeit uit de Wet Beveiliging Netwerk en Informatiesystemen (Wbni) van de Minister van Justitie en Veiligheid (JenV).
Het overgrote deel van de als vitaal aangewezen processen van de sector Digitale overheid valt onder de Rijksdienst, zoals DigiD en Basisregistratie Personen (BRP). De basis voor informatiebeveiliging van alle informatieprocessen bij de Rijksdienst is geregeld in het Voorschrift Informatiebeveiliging Rijksdienst (VIR).[7] Voor het kiezen van maatregelen geldt met name de Baseline Informatiebeveiliging Overheid (BIO)[8] als uitwerking. De BIO bevat een grote hoeveelheid beveiligingsdoelen waarvoor passende maatregelen moeten worden gekozen, samen met een verplichte set aan basismaatregelen. Risicomanagement en proportionaliteit zijn bij al deze regelgeving de uitgangspunten. Het aantal processen dat bij de overheid vitaal is, is zo beperkt dat het niet zinvol is om hiervoor een generieke set eisen te maken in aanvulling op hierboven genoemde regelingen.

Een verhoogde digitale weerbaarheid

In de eerdergenoemde Kamerbrief *Voortgang informatieveiligheid bij de overheid* is aan uw Kamer gemeld dat het streven is om informatieveiligheid bij de overheid een wettelijke basis te geven.

Ik wil dit doen via een zorgplicht waaraan nadere regels kunnen worden gesteld, zoals de BIO. Door het wettelijk verplichten van de BIO is de vrijblijvendheid voorbij. Vanuit de rijksoverheid worden aan medeoverheden vanuit verschillende bronnen informatiebeveiligingseisen gesteld. Door op één plaats een algemene zorgplicht voor informatieveiligheid bij de overheid te regelen, bereik ik ook een vereenvoudiging van regels binnen de overheid. Daardoor komt de focus meer te liggen op het feitelijk beveiligen in plaats van administratief beveiligen.

Bij een dergelijke zorgplicht past ook aparte aandacht voor de belangrijkste processen. Dat zijn niet alleen de vitale processen, maar juist ook de hierboven genoemde processen die interbestuurlijke eisen stellen én interbestuurlijk toezicht uitoefenen[9]. Voor deze processen wil ik, samen met onze vitale processen en processen waar staatsgeheimen in rondgaan, een hogere mate van zorgvuldigheid bereiken.

Bij dit stelsel hoort ook een stelsel van toezicht. Ik wil daarom gaan toezien op informatieveiligheid bij de overheid, niet alleen op de naleving van algemene regels, zoals de BIO, maar ook op specifieke regels die vanuit vakdepartementen, aanvullend op de BIO worden gesteld. Hiermee wil ik ook bij het toezicht dubbel werk voorkomen. Het toezicht moet proportioneel zijn, dus veel aandacht voor de zorgvuldigheid bij het beveiligen van vitale processen en andere «kroonjuwelen». Ook zal gepaste interbestuurlijke handhaving hierin een plaats krijgen. Dit komt tegemoet aan mijn ambitie om de digitale weerbaarheid van de overheid te verhogen door óók in te zetten op wetgeving en daarop handhaving te organiseren.

---

[6] Artikel 3 Besluit Beveiliging Netwerk en Informatiesystemen (Bbni), sector Digitale overheid.
[7] Stcrt. 2007, nr. 122.
[8] Stcrt. 2019, nr. 26526.
[9] Enkele voorbeelden hiervan zijn art 5.22 van het Besluit SUWI, artikel 6 van het Besluit BRP, art. 6 en art 7 van de Regeling GDI, art. 5 onder 4 Regeling justitiële keteninformatisering Jeugdwet.

Bij dit alles geldt wel dat vakministers, gemeenten, provincies en waterschappen zelf verantwoordelijk zijn en blijven voor hun informatieveiligheid. Bij het opzetten van een overheidsbreed stelsel van normstelling en toezicht wil ik de verantwoording die wordt gedaan aan het eigen controlerend orgaan[10] meenemen. Ik wil deze zo normeren dat die verantwoording een goede basis is voor de interbestuurlijke verantwoording. Ook dat draagt bij aan een efficiënte verantwoording, terwijl het aan de andere kant administratieve lastendruk verlaagt en de feitelijke veiligheid van de overheid bevordert.

Vooruitblik en vervolgstappen

Intussen is in Europa een voorlopig politiek akkoord bereikt over een herziening van Netwerk- en Informatiebeveiligingsrichtlijn (NIB2-richtlijn).[11] Een belangrijke wijziging ten opzichte van de huidige richtlijn is dat overheidsdiensten binnen de reikwijdte van de richtlijn worden gebracht, en daarmee aan wettelijke verplichtingen voor de beveiliging van hun netwerk- en informatiesystemen moeten voldoen. Dit geldt in ieder geval voor de rijksoverheid. De conceptrichtlijn stelt verder dat regionale en lokale overheden na een risicobeoordeling kunnen worden aangewezen. Ik wil de daarbij geldende criteria als uitgangspunt nemen, zoals de hierboven genoemde vitaal criteria. Eerder vermeldde ik dat het aantal processen dat hieraan voldoet, beperkt is. Ik verwacht daarom niet dat medeoverheden categoraal binnen de scope van NIB2 gaan komen.

Na vaststelling van de richtlijn hebben lidstaten 21 maanden de tijd om deze in hun nationale wetgeving om te zetten. Mijn voornemen om tot wet- en regelgeving voor informatieveiligheid voor het openbaar bestuur te komen, laat ik samenlopen met het implementeren van de NIB2-richtlijn voor de overheid. Waar van toepassing, zal ik ook de bepalingen uit de NIB2-richtlijn moeten meenemen. Wat dit precies betekent, zal in nauwe samenwerking met het Ministerie van Justitie en Veiligheid worden bezien.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties
A.C. van Huffelen

[10] Tweede Kamer, Gemeenteraad, provinciale staten en Algemeen Bestuur Waterschap.
[11] Kamerstuk 21 501-33, nr. 931.