Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

887

Vragen van de leden **Rajkowski** en **Strolenberg** (beiden VVD) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *de Kamerbrief «Reactie op de motie van het lid Yesilgöz-Zegerius over een cyberverdedigingsprotocol voor gemeenten»* (ingezonden 20 oktober 2021).

Antwoord van Staatssecretaris **Knops** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 26 november 2021).

Vraag 1
Hoe beoordeelt u het feit dat verschillende gemeenten zoals Hof van Twente afgelopen jaren slachtoffer zijn geworden van cyberaanvallen waarbij veel gevoelige persoonsgegevens zijn buitgemaakt?[1]

Antwoord 1
Iedere digitale aanval op een overheidsorganisatie is er één te veel. De realiteit is dat digitale dreigingen toenemen. Vanuit mijn stelselverantwoordelijkheid voor de digitale overheid stel ik kaders en ondersteun ik waar nodig om het openbaar bestuur digitaal veilig te laten functioneren.

Vraag 2, 3 en 4
Hoe beoordeelt u het feit dat uit onderzoek blijkt dat een groot deel van de gemeenten nog geen draaiboek (protocol) heeft in het geval van een digitale aanval? Hoe beoordeelt u het feit dat gemeenten als gevolg hiervan geen kennis en kunde in huis hebben om de benodigde stappen te zetten na een digitale aanval en om de opgelopen schade te mitigeren?[2]
Hoe beoordeelt u het feit dat er wetenschappelijk en maatschappelijk consensus bestaat over de meerwaarde van een cyber protocol/draaiboek in het geval van een digitale aanval waarbij handelingsperspectief kan worden geboden aan organisaties en digitale aanvallen sneller kunnen worden verholpen?
Bent u het met ons eens dat digitale aanvallen nooit honderd procent voorkomen kunnen worden, maar dat het hebben van een cyber protocol/draaiboek indien een aanval zich voordoet wel van essentieel belang is om gemeentes de juiste stappen te laten zetten om zo goed mogelijk om te gaan met digitale aanvallen en om de schade zoveel mogelijk te beperken? Zo ja,

[1] Kamerstuk 26 643, nr. 786
[2] Cybersecurity onderzoek gemeenten: nog veel werk te doen – AG Connect

ah-tk-20212022-887
ISSN 0921 - 7398
's-Gravenhage 2021

bent u het dan ook eens dat het hebben van een cyber protocol/draaiboek een belangrijk hulpmiddel is in het zo goed mogelijk omgaan met digitale aanvallen? Zo nee, waarom niet?

Antwoord 2, 3 en 4
Ik deel het beeld dat op het terrein van informatieveiligheid binnen en buiten de overheid veel werk te doen is. De digitale dreiging is groeiende en alle organisaties wereldwijd kampen met dit vraagstuk. Het is een breed maatschappelijk vraagstuk waar naast gemeenten, ook andere publieke organisaties mee kampen.
Verder deel ik de mening dat overheidsorganisaties voorbereid moeten zijn op digitale aanvallen. Inderdaad zijn aanvallen nooit 100% te voorkomen. Vandaar dat ik uw Kamer graag wijs op de Baseline Informatiebeveiliging Overheid (BIO)[3]. Dit is het algemene basisnormenkader voor informatieveiligheid voor de gehele overheid, waarin ook eisen en maatregelen zijn opgenomen over het beheer van informatiebeveiligingsincidenten. Concreet stelt de BIO in hoofdstuk 16 «Beheer van informatiebeveiligingsincidenten» onder meer verplicht dat er verantwoordelijkheden en procedures tot op directieniveau zijn vastgesteld voor een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten. Er worden eisen gesteld aan het rapporteren van incidenten. Gezien het belang ervan zijn deze eisen in de BIO, conform de systematiek van de BIO[4], nader vertaald in maatregelen zoals de verplichting een intern meldloket te hebben met vastgestelde afhandelingsprocedures. En de meldingsprocedure moet voor iedereen in de organisatie kenbaar zijn. Ook beschrijft de BIO hoe afhankelijk van de ernst van een incident verder moet worden gereageerd. Draaiboeken en protocollen zijn daarmee impliciet onderdeel van een totaalpakket van de verplichtingen en aan maatregelen, die voortvloeien uit hoofdstuk 16 van de BIO.
Ik deel dan ook het standpunt dat het hebben van draaiboeken en protocollen van belang is om snel in te kunnen spelen op digitale ontwrichting. Gemeenten zijn verantwoordelijk voor hun informatieveiligheid binnen de geldende kaders, ook voor het opstellen van draaiboeken en protocollen voor incidenten. Het college van burgemeester & Wethouders draagt de eindverantwoordelijkheid voor hun gemeente en de gemeenteraad controleert.
Digitale aanvallen zijn niet allemaal hetzelfde. De kennis en kunde die nodig is om de nodige stappen te zetten, verschilt per aanval. Gemeenten kunnen indien nodig ondersteuning krijgen van de Informatiebeveiligingsdienst (IBD) van de Vereniging Nederlandse Gemeenten (VNG). Vanuit de kaderstellende en ondersteunende rol van BZK voert het Centrum Informatiebeveiliging een Privacybescherming (CIP) sinds 2019 een overheidsbreed ondersteuningsprogramma uit. Het voornaamste doel hiervan is adviezen en ondersteuningsmiddelen aanreiken aan overheden, gericht op het geïmplementeerd krijgen van de BIO.
Ten slotte maak ik u graag attent op de jaarlijkse overheidsbrede cyberoefening en de bijbehorende webinars[5] die erop zijn gericht op de digitale weerbaarheid van de overheid te vergroten. Aan deze oefening nemen veel verschillende overheidspartijen deel. De laatste cyberoefening met meer dan 1000 deelnemers vond op 1 november plaats.

Vraag 5
Bent u het met ons eens dat het hebben van een cyber protocol/draaiboek als een belangrijk aanvullend instrument kan worden in gezet in een breder pakket van bestaande maatregelen tegen digitale aanvallen? Zo ja, bent u alsnog bereid om de aangenomen motie Yesilgöz-Zegerius (Kamerstuk 26 643, nr. 753) uit te voeren en dus in samenwerking met de Vereniging Nederlandse Gemeenten (VNG) en de Informatiebeveiligingsdienst (IBD) cyber protocollen/draaiboeken op te stellen om gemeentes beter voor te bereiden op digitale aanvallen? Zo nee, waarom niet?

---

[3] *Stcrt.* 2020, 7857.

[4] De BIO stelt eisen die overeenkomen met de ISO27002 standaard, maar concretiseert deze voor de overheid met maatregelen op grond van wet- en regelgeving, vanwege de gemeenschappelijke veiligheid van informatieketens of omdat deze maatregelen fundamenteel zijn voor een betrouwbare c.q. professionele informatievoorziening.

[5] Zie https://www.weerbaredigitaleoverheid.nl/

Antwoord 5
In mijn reactiebrief[6] op de motie Yesilgöz-Zegerius[7] heb ik aangegeven hoe ik uitvoering geef aan de motie. Ik herhaal hier kort wat ik in mijn reactiebrief heb gesteld, namelijk dat ik in mijn beleid niet inzet op één cyberverdedigingsprotocol voor alle gemeenten, omdat de ene situatie niet de andere is. Hoe er daadwerkelijk moet worden gehandeld is weliswaar context-afhankelijk, maar wel onderworpen aan eisen. Zoals ik hierboven heb aangegeven stelt de BIO eisen aan het afhandelen van informatiebeveiligingsincidenten met inbegrip met vastgestelde procedures.
Naar aanleiding van het artikel van AG Connect wil ik hieraan nog een paar opmerkingen toevoegen. Ten eerste: informatieveiligheid is een gezamenlijke verantwoordelijkheid. Ik noemde eerder dat informatieveiligheid bij gemeenten onder de eindverantwoordelijkheid van het College van B&W valt. Het is van belang dat waar dat niet of onvoldoende gebeurt, zij hun verantwoordelijkheid nemen en gaan uitoefenen; de gemeenteraad dient hier ook op toe te zien. Gemeenten worden hierbij ondersteund door de VNG en de IBD voor gemeenten.
Ik ondersteun dit door de controlerende taak (het horizontale toezicht) van de gemeenteraad te versterken met onder andere de aanpak Eenduidige Normatiek Single Information Audit (ENSIA), waarover uw Kamer is geïnformeerd op 18 maart jl. in de Voortgangsbrief Informatieveiligheid.[8] ENSIA heeft tot doel te komen tot een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid bij gemeenten. De focus van ENSIA ligt op verantwoording richting de gemeenteraad, het hoogste politieke orgaan van de gemeente. Echter, omdat gemeenten ook verantwoording afleggen aan de rijksoverheid waar het gaat om het gebruik van landelijke voorzieningen, helpt ENSIA de gemeenten in één keer verantwoording af te leggen over informatieveiligheid gebaseerd op de normen die gelden voor de Nederlandse overheid, de BIO. Met ENSIA sluit de verantwoording over informatieveiligheid aan op de planning- en controlcyclus van de gemeente. Hierdoor heeft het gemeentebestuur meer overzicht over de informatieveiligheid van zijn gemeente en kan het beter sturen en verantwoording afleggen aan de gemeenteraad.
Ook de VNG ziet het belang en de urgentie van adequate digitale weerbaarheid toenemen. Ze biedt op het terrein van informatieveiligheid de gemeenten daarbij op allerlei wijzen ondersteuning, zoals ook op het terrein van incidentmanagement. VNG en IBD trekken lessen uit incidenten en stellen deze lessen openbaar beschikbaar. Dit geldt onder andere voor de geleerde lessen van de door u aangehaalde incidenten, de hacks bij de gemeenten Lochem en Hof van Twente en de Citrix-problematiek.
De IBD heeft voor gemeenten een aantal producten beschikbaar gesteld die ingaan op het voorkomen van digitale incidenten, maar ook op de wijze waarop een incident kan worden afgewikkeld. Het incident bij de gemeente Hof van Twente heeft onder andere geleid tot de ontwikkeling van het «kaartje in de meterkast» voor gemeentesecretarissen[9]. Dit document helpt de gemeente om vooraf de juiste stappen te bepalen in geval van een incident. Via de vakvereniging worden gemeentesecretarissen gewezen op dit initiatief.
Om gemeenten te helpen met het verhogen van de digitale weerbaarheid heeft de IBD een ondersteuningspakket ontwikkeld voor de processen en maatregelen uit de BIO met de hoogste prioriteit. In dit ondersteuningspakket wordt naast preventieve maatregelen en bewustwording ook ingezet op bedrijfscontinuïteitbeheer (BCM) en zijn concrete handreikingen voor incident en responsmanagement beschikbaar voor alle gemeenten. Zoals gesteld in mijn reactie op de motie Yesilgöz-Zegerius worden de Veiligheidsregio's betrokken bij crisis en incidenten volgens de Gecoördineerde Regionale Incidentbestrijdingsprocedure (GRIP) en kan opgeschaald worden naar de nationale crisisstructuur.
Met dit ondersteuningspakket zie ik dat de gemeenten voortvarend bezig zijn. Tegelijkertijd ben ik met de VNG, de rijksoverheid, de Unie van Waterschap-

---

[6] *Kamerstuk* 26 643, nr. 786
[7] *Kamerstuk* 26 643, nr. 753
[8] *Kamerstuk* 26 643 nr. 749
[9] https://www.informatiebeveiligingsdienst.nl/product/kaartje-in-de-meterkast-voor-de-gemeentesecretaris/

pen en het Interprovinciaal overleg doorlopend in gesprek om gezamenlijk de digitale weerbaarheid van de overheid te versterken tegen de telkens wijzigende dreigingen.