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

1852

Vragen van het lid **Kathmann** (PvdA) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *de digitale kwetsbaarheid van gemeenten* (ingezonden 20 januari 2022).

Antwoord van Staatssecretaris **Van Huffelen** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 24 februari 2022).

Vraag 1
Kent u het bericht «Digitale kwetsbaarheid van Eindhoven irriteert raad»?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u een overzicht geven van gemeenten die worstelen met de kwaliteit van hun ICT-toepassingen in de zin van dat de dienstverlening aan bewoners daaronder lijdt, de beveiliging niet op orde is en de privacy in het geding is?

Antwoord 2
Nee, ik beschik niet over een overzicht van de kwaliteit van ICT-systemen van gemeenten. Ook de Vereniging van Nederlandse Gemeenten (VNG) heeft een dergelijk overzicht niet. Gemeenten zijn zelf verantwoordelijk voor de kwaliteit van hun ICT-toepassingen, hun dienstverlening en de borging van privacy. Ze behoren dat echter wel binnen gestelde kaders te doen, zoals de Algemene Verordening Gegevensbescherming (AVG)[2] en de Baseline Informatieveiligheid Overheid (BIO)[3]. De BIO is het gemeenschappelijke, algemene, uniforme basisnormenkader voor informatiebeveiliging voor alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). De uitgangspunten van de BIO zijn onder andere risicomanagement en de eigen verantwoordelijkheid van overheidsorganisaties. Dat betekent dat organisaties zelf risicoafwegingen uitvoeren en maatregelen treffen in aanvulling op een minimumset van maatregelen die altijd verplicht zijn. In het antwoord op de volgende vraag ga

[1] Eindhovens Dagblad, 19 januari 2022
[2] Verordening (EU) 2016/679
[3] *Stcrt.* 2019, nr. 26526

ah-tk-20212022-1852
ISSN 0921 - 7398
's-Gravenhage 2022

ik in op de steun die ze daarbij krijgen[4]. De BIO is door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) in samenwerking met alle bestuurslagen samengesteld.
Gemeenten verantwoorden zich over de informatiebeveiliging naar hun eigen gemeenteraad. In samenwerking met het Ministerie van BZK is met de VNG voor alle gemeenten de Eenduidige Normatiek Single Information Audit (ENSIA) verantwoordingsmethodiek opgezet. De verantwoordingssystematieken van een aantal stelsels die gaan over informatiebeveiliging zijn in ENSIA samengevoegd en geharmoniseerd. Op die manier is één verantwoordingsproces gerealiseerd. ENSIA vormt de basis voor de verantwoording van het college aan de gemeenteraad.[5]

Vraag 3
Deelt u de mening dat het wenselijk is dat niet iedere gemeente alleen voor zichzelf oplossingen moet zoeken voor ICT-problemen, maar dat kennis en ervaring over de best practices gedeeld moet worden? Zo ja, welke rol speelt u vanuit uw coördinerende rol op het domein van de digitale overheid en de verantwoordelijkheid voor digitale weerbaarheid van de sector «overheid» hierin? Zo nee, waarom niet?

Antwoord 3
Ja, ik deel die mening. Ik zal ook steeds met de gemeenten blijven investeren in het verbeteren van de overheids-ICT.
In aanvulling op mijn antwoord in de vorige vraag worden gemeenten ondersteund, waar wenselijk en nodig. Het Ministerie van BZK stimuleert het kennis delen aan alle overheden onder meer door een bijdrage aan het Centrum voor Informatiebeveiliging en Privacybescherming (CIP), sinds het najaar van 2018. Het CIP ontwikkelt met die bijdrage bijvoorbeeld webinars, podcasts, workshops, games en handreikingen.[6]
Voor het Ministerie van BZK beheert het CIP tevens de website biooverheid.nl waarop veel informatie over informatiebeveiliging wordt gedeeld met alle overheden. Ook werkt het CIP aan een professionele community waarin beveiligings- en privacy-professionals van alle overheden van elkaar leren en elkaar (op dit moment vooral nog in digitale vorm) ontmoeten.
Een ander voorbeeld van het overheidsbrede delen van kennis is de jaarlijkse overheidsbrede cyberoefening[7] die door het Ministerie van BZK sinds 2019 in oktober – de maand van cybersecurity – wordt georganiseerd. Deze oefening, die is bedoeld voor Rijks- en uitvoeringsorganisaties, provincies, gemeenten en waterschappen, laat zich ieder jaar inspireren door recente en actuele dreigingen en cyberaanvallen (zoals op de gemeenten Lochem en Hof van Twente). Aan de hand van een gesimuleerde hackaanval oefenen alle partners in de publieke sector op crisispreparatie op verschillende niveaus van de organisaties met elkaar. Deze oefening wordt geflankeerd door webinars die ook later terug te kijken zijn.[8] Speciaal voor gemeenten heeft het Ministerie van BZK een drietal cyberoefenpakketten laten ontwikkelen door het Instituut voor Veiligheids- en Crisismanagement. Deze gemeentelijke cyberoefenpakketten zijn online raadpleegbaar en gratis af te nemen voor alle gemeenten.[9]
Verder worden alle gemeenten ondersteund door de Informatiebeveiligingsdienst (IBD) van de VNG. De IBD biedt een Integraal dienstverleningsaanbod voor informatiebeveiliging en privacy-expertise. Zo levert de IBD actuele producten en diensten ter ondersteuning van de BIO en verzorgt het programma Verhogen Digitale Weerbaarheid (VDW) voor gemeenten. De IBD houdt jaarlijks tientallen workshops, webinars, (be)spreekuren en expertgroep meetings, onder andere op het gebied van VDW en privacy, en bevordert het

---

[4] Meer informatie over de BIO en ondersteuning bij de toepassing ervan is te vinden op: https://www.bio-overheid.nl/
[5] Meer informatie over ENSIA is te vinden op: https://www.vngrealisatie.nl/ensia
[6] Op de website van het CIP zijn de diverse ontwikkelende producten te vinden: www.cip-overheid.nl
[7] https://www.weerbaredigitaleoverheid.nl/
[8] De webinars van de cyberoefening van 2021 zijn tot en met maart 2022 terug te kijken.
[9] Te vinden op de website van de Informatiebeveiligingsdienst gemeenten (IBD): https://www.informatiebeveiligingsdienst.nl/project/cyberoefenpakket-vngoefenscenariosdigitale-incidenten/

risico-denken op diverse niveaus binnen de gemeente. Ook organiseert de IBD intervisiesessies met Chief Information Security Officers (CISO's), Functionarissen Gegevensbescherming (FG's) en Privacy Officers. Verder biedt de IBD een platform voor gemeenten voor het delen van kennis en ervaring over best practices. Zo organiseert zij bijeenkomsten, zoals Code Rood sessies voor vertrouwde gemeentelijke contactpersonen over bevindingen bij recente incidenten. Tevens organiseert de IBD lunchuurtjes voor gemeentesecretarissen, zoals naar aanleiding van het Hof van Twente-ransomware-incident in 2020. De IBD draagt verder bij aan overheidsbrede programma's zoals de eerdergenoemde overheidsbrede cyberoefening en de activiteiten van het CIP.
De IBD is tevens het sectorale Computer Emergency Response Team/ Computer Security Incident Response Team (CERT/CSIRT) voor alle Nederlandse gemeenten. De IBD-CERT ondersteunt crisismanagementteams in het geval van incidenten. Zij oriënteert zich momenteel op verdere uitbreiding van haar dienstverlening in incident-response op locatie bij een gemeente. Tot slot werkt de IBD op het vlak van leveranciersmanagement aan standaardisatie waar dat een collectief en grootschalig effect heeft. Gemeenten kunnen zo beter veilige producten en diensten inkopen waarover zij de controle houden.

Vraag 4
Deelt u de mening dat de opgaven waar gemeenten voor staan om hun ICT-voorzieningen klantvriendelijk, veilig en privacyproof te maken en te houden groot zijn en dat zij daarbij meer ondersteuning vanuit het Rijk nodig hebben? Zo ja, hoe zorgt u voor die extra ondersteuning? Zo nee, waarom deelt u die mening niet?

Antwoord 4
Ik deel de mening dat het vraagstuk digitale weerbaarheid meer aandacht verdient, ook van gemeenteraden. Vanuit mijn rol heb ik een stelselverantwoordelijkheid voor de informatieveiligheid in het openbaar bestuur. Normeren door middel van kaderstelling zoals de BIO, aanjagen, stimuleren en faciliteren door middel van de genoemde initiatieven onder vragen 2 en 3 behoren daarbij tot de kerntaken van het Ministerie van BZK. Vanzelfsprekend vindt hierover overleg plaats met de VNG en de koepelorganisaties van de andere bestuurslagen. Ik wil samen met de gemeenten verder kijken naar de kaders en normen voor ICT die met name zorgen voor de bescherming van publieke waarden.
De individuele overheidsorganisaties moeten hun informatiebeveiliging primair zelf op orde hebben en houden, waarbij zij ondersteund worden door hun koepelorganisaties. De VNG ondersteunt de gemeentebestuurders hierbij met de Agenda Digitale Veiligheid. Begin 2021 werd tijdens een Bijzondere Algemene Ledenvergadering de Resolutie Digitale Veiligheid[10] vastgesteld, waaraan gemeenten zich gecommitteerd hebben. Hierin wordt de noodzaak onderstreept dat gemeenten hun digitale weerbaarheid versterken. Vanuit deze Agenda Digitale Veiligheid stimuleert de VNG dat er meer aandacht komt voor (bestuurlijke) awareness en voor oefenen met digitale ontwrichting. Vanuit het Ministerie van BZK is er nauw contact met de VNG en de IBD en wordt er gezamenlijk gewerkt aan het verhogen van de digitale weerbaarheid van gemeenten.

[10] https://vng.nl/sites/default/files/2020-12/resolutie-digitale-veiligheid-versie-3-december-2020.pdf