Datum
5 april 2022

Onderwerp
VNG Inbreng CD Online Veiligheid en Cybersecurity 7 april

Geachte woordvoerders digitale zaken,

Op donderdag 7 april debatteert u met de minister van J&V over online veiligheid en cybersecurity. De VNG is blij dat er voor dit debat onderwerpen van veel verschillende ministeries geagendeerd staan. Dat benadrukt maar weer hoe belangrijk het is dat één bewindspersoon de coördinatie over digitale veiligheid voert.

Hoofdlijnen digitale veiligheid voor gemeenten

Zoals gezegd is digitale veiligheid een onderwerp voor alle domeinen. Gemeenten hebben daarom met veel verschillende ministeries te maken in afstemming of bij regelgeving hieromtrent. Er komt veel op gemeenten af. De VNG zal in zijn contacten met het rijk doorlopend aandacht vragen om:

1. Initiatieven zoveel mogelijk gecoördineerd en in samenhang op te pakken;
2. Oog te hebben voor de gemeentelijke capaciteit en uitvoeringspraktijk;
3. Voldoende financiële middelen om de ambities te realiseren.

Deze drie hoofdlijnen zijn voor u als Kamer ook goed om in de gaten te houden bij uitwerking van wetgeving over digitale veiligheid of initiatieven om de online veiligheid in de samenleving te verbeteren.

Grondrechten en veiligheid

Het doet geen recht aan de digitale omgeving wanneer veiligheid enerzijds en grondrechten en ethiek anderzijds als twee losse onderwerpen worden behandeld. Bij de discussie over het bevorderen van digitale veiligheid moet ook worden stilgestaan bij de positie van inwoners en bedrijven in de digitale democratische samenleving.

Digitale veiligheid en digitale grondrechten en ethiek zijn twee kanten van dezelfde medaille. Het verhogen van digitale veiligheid kan tegelijkertijd een beperking van online bewegingsvrijheid opleveren. Bij het opstellen van kaders of normen dient u als Kamer oog te houden voor beide kanten van de medaille en een integrale blik op de digitale transitie te houden.

Informatiepositie gemeenten

Uit verschillende agendapunten van het debat op 7 april blijkt dat gemeenten een zeer beperkte informatiepositie hebben ten opzichte van de rijksoverheid of vitale sectoren. Dit speelt op verschillende fronten, maar heeft een direct effect op de fysieke en digitale veiligheid in Nederland. Voor lokaal bestuur is er in de gevolgeffecten en de actie daarop geen onderscheid of een vitale of niet-vitale sector digitaal verstoord worden.

Het voorbeeld van Kaspersky is uiterst confronterend: gemeenten moeten uit een wob-verzoek vernemen dat er risico's kleven aan het gebruik van de software. De aanwijzing hierover wordt enkel naar rijksorganisaties en vitale sectoren verstuurd. Vervolgens vraagt de samenleving wel een zelfde zorgvuldigheid bij het gebruik van mogelijk schadelijke software door gemeenten.

Het onderscheid van vitaal / niet vitaal doet geen recht aan hoe we Nederland hebben ingericht, zeker op digitaal vlak.

Hetzelfde treedt op wanneer de Rotterdamse haven wel vanuit de Inlichtingendiensten wordt gewaarschuwd voor digitale dreigingen naar aanleiding van de oorlog in Oekraïne, maar de CISO van de gemeente niet op de hoogte is van die eventuele dreigingen – en de maatregelen ertegen. Gemeenten zijn verantwoordelijk voor de openbare orde en veiligheid in hun gebied, maar kunnen hier niet de rol vervullen die de samenleving wel van ze verlangt. Het is belangrijk dat hier ook in de zogenaamde 'koude' fase – wanneer er geen dreiging is – aandacht voor is.

Met oog op de Nederlandse Cybersecuritystrategie (NLCS) doen wij enkele aanbevelingen om aan de positie van gemeenten te werken:

- het gelijktrekken van de informatiepositie van gemeenten
- het ontwikkelen van kennis en vaardigheden over digitale veiligheid bij verschillende doelgroepen (met bijzondere aandacht voor capaciteitsontwikkeling bij overheden)
- uitdagingen als digitale veiligheid en aandacht voor digitale grondrechten en ethiek zoveel mogelijk integraal te benaderen
- een heldere afbakening van verantwoordelijkheden op lokaal niveau ten opzichte van nationaal niveau
- inzichtelijk maken van (bestuurlijke) bevoegdheden in het digitale domein

Centrum voor Veiligheid en Digitalisering

Op gemeentelijk niveau zijn goede voorbeelden te vinden waar u als Kamer uw voordeel mee kunt doen en waar de rijksoverheid belangrijke lessen uit kan halen. Zo hebben de gemeenten Den Haag en Rotterdam onlangs hun beleidsplannen digitale veiligheid gepresenteerd, waarin duidelijk zichtbaar is dat lokaal het onderscheid vitaal/niet-vitaal minder relevant is. Gemeenten, VNG en politie werken daarnaast samen in de Impact Coalitie Safety & Security (ICSS).

En in Apeldoorn is vorig najaar het Centrum voor Veiligheid en Digitalisering van start gegaan: een nationaal centrum dat zich richt op het ontwikkelen en overdragen van kennis ten aanzien van digitale veiligheid, fraude, opsporing en het vergroten van bewustzijn. Het centrum is een samenwerking van hogeschool Saxion, de Politieacademie en de Universiteit Twente, ondersteund door de gemeente Apeldoorn en de provincie Gelderland. Zij werken samen in een ecosysteem met onder meer Koninklijke Marechaussee, Koninklijke Landmacht, Belastingdienst en het Kadaster.

Bij de begrotingsbehandeling J&V op 25 november 2021 heeft de kamer de regering verzocht (via de motie-Palland/Ellemeet) "te verkennen of aanhaken bij het initiatief van het Centrum voor Veiligheid en Digitalisering kan bijdragen aan het opbouwen van kennis en expertise terzake landelijke vraagstukken". De initiatiefnemers van het Centrum voor Veiligheid en Digitalisering zijn momenteel bezig met die verkenning en hebben daarover met verschillende rijksdiensten gesproken. Een vervolgstap is om de verschillende rijksdiensten, ook in het licht van het nieuwe regeerakkoord, verdiepend met elkaar in gesprek te laten gaan. De urgentie van het vraagstuk is alleen maar toegenomen met name op de opgaven rondom intelligence, cyberweerbaarheid en cybersecurity.

De verwachting is dat er voor de zomer voorgang te melden is op de uitvoering van deze motie.