Datum
8 december 2022

Onderwerp
VNG inbreng CD Nederlandse Cybersecuritystrategie (NLCS) 15 december

Geachte woordvoerders digitale zaken,

Op donderdag 15 december debatteert u over de Nederlandse Cybersecuritystrategie (NLCS). Een belangrijk product van het kabinet waarmee voor de komende jaren wordt geschetst hoe om te gaan met de enorme impact van digitale (on)veiligheid op onze samenleving.

In het kort:
Wat ons betreft zijn complimenten voor de Nederlandse Cybersecuritystrategie voor de minister op zijn plaats. Het betreft een ambitieuze en omvattende strategie waarvan wij verwachten dat deze Nederland concreet digitaal veiliger gaat maken.

Tegelijkertijd zien wij dat de NLCS vooral een rijksstrategie is en er te weinig rekening is gehouden met de gemeentelijke uitvoeringscapaciteit om aan de doelen van de NLCS bij te dragen. Dat vinden wij jammer. Ook manen wij de minister aan haast te maken met het bieden van duidelijkheid over nieuwe wet- en regelgeving zoals de NIB 2 richting medeoverheden.

Daarnaast zien wij op lokaal niveau drie systeemuitdagingen die zullen moeten worden aangepakt als de ambitie is om werkelijk tot een digitaal veilig Nederland te komen. Dat de minister heeft toegezegd om op de korte termijn met de gemeenten een convenant te ondertekenen om deze uitdagingen aan te pakken, vinden wij hoopgevend. Wij verwachten hier veel van.

Ambitieuze strategie
Wij zijn blij met de belangrijke stappen die met deze strategie worden gezet om te werken aan digitale veiligheid op nationaal niveau. In onze ogen is de strategie voldoende ambitieus en het valt te prijzen dat het rijk de focus heeft verlegd van symptoombestrijding naar het aanpakken van de oorzaken van digitale onveiligheid. Ook heeft de VNG in het verleden meermaals aangedrongen op een duidelijke regierol van het rijk ten aanzien van dit dossier en ook hierin worden belangrijke stappen vooruit gezet.

Daarnaast waarderen wij het dat het rijk zich bij de totstandkoming van de NLCS heeft ingespannen om de ambtelijke en bestuurlijke (inhoudelijke) inbreng vanuit gemeenten een plek in de strategie en de bijhorende operationele plannen te geven. Wij zien de strategie dan ook als een belangrijke stap vooruit om Nederland digitaal veiliger en weerbaarder te maken.

Hoge ambities
Incidenten & crises manifesteren zich voornamelijk op lokaal niveau, wat ook geldt voor de nog steeds toenemende digitale criminaliteit. Het is dan ook jammer dat gedurende deze kabinetsperiode geen additionele middelen zijn vrijgemaakt voor gemeenten om aan de doelen van

de NLCS bij te dragen. Het rijk laat hier een kans liggen om medeoverheden in staat te stellen om integraal aan de doelen van de strategie bij te dragen. Tegelijk is er bijna geen enkel digitaal proces meer dat zich beperkt tot één overheidslaag.

Daar komt bij dat het rijk steeds hogere eisen stelt aan de cybersecurity van medeoverheden, bijvoorbeeld via strengere wet- en regelgeving. Op zichzelf is dit zeer terecht. Tegelijkertijd moeten medeoverheden wel in staat worden gesteld om aan deze toenemende verwachtingen te voldoen. Dat lukt nog niet altijd, bijvoorbeeld omdat het gemeenten ontbreekt aan de noodzakelijke expertise en capaciteit. Voor gemeenten is dit een structureel knelpunt. Dan helpt het ook niet als het rijk niet helder is over in hoeverre nieuwe wet- en regelgeving, specifiek de NIB 2-richtlijn, van toepassing is op medeoverheden. Gemeenten kunnen nu niet inschatten wat de impact van deze richtlijn gaat zijn en zich hier dus ook niet adequaat op voorbereiden.

Convenant tussen rijk en gemeenten

Daarnaast zien wij ook dat in de NLCS de fundamentele uitdagingen voor digitale veiligheid op lokaal niveau nog onvoldoende geborgd zijn, ondanks de inspanningen van alle betrokken partijen. In onze ogen is de NLCS voornamelijk top-down georiënteerd, terwijl incidenten & crises en ook cybercriminaliteit zich vooral lokaal manifesteren. Het gemeentelijk perspectief op digitale veiligheid mist wat ons betreft dan ook nog.

Wij zien drie ontbrekende randvoorwaarden voor gemeenten om digitale onveiligheid effectief het hoofd te kunnen bieden:

1. Gemeenten hebben onvoldoende financiële middelen om voor de gemeentelijke organisatie en breder op lokaal niveau voldoende maatregelen te nemen. Structurele middelen zijn essentieel om de weerbaarheid en continuïteit van de gehele stad/gemeente op digitale veiligheid de komende jaren te verhogen;
2. Het fysieke veiligheidsstelsel is niet toereikend voor digitale incidenten en -crises. Hiervoor is een digitaal veiligheidsstelsel nodig om de verantwoordelijkheden, rollen, taken en bevoegdheden voor digitale veiligheid te organiseren;
3. De informatiepositie van gemeenten op digitale veiligheid is onvoldoende. Een situationeel beeld, dat duiding en inzicht geeft in aard en omvang van de weerbaarheid en problematiek op cruciale entiteiten in de gemeente en directe informatievoorziening bij dreigingen, incidenten en kwetsbaarheden helpt gemeenten om effectief, efficiënt en tijdig op te treden. Een gecombineerd cyberbeeld op de digitale en gedigitaliseerde criminaliteit maakt lokale interventies vanuit de driehoek effectiever.

We hebben als overheden de grootst mogelijke coalitie nodig om om te gaan met de grote impact van digitale (on)veiligheid op onze samenleving. Voor een krachtig verweer tegen digitale onveiligheid en om op te kunnen treden wanneer een crisis zich voordoet heeft de minister alle partners nodig. Ook gemeenten.

Het is dan ook een goede ontwikkeling dat gemeenten samen met het rijk nog voor het einde van dit jaar (2022) een bestuurlijk convenant tekenen om deze systeemuitdagingen aan te pakken. Wij hebben hier hoge verwachtingen van en zullen ons voor dit convenant inspannen. Gemeenten rekenen op het rijk als partner.