Datum
8 september 2022

Onderwerp
VNG inbreng CD online veiligheid en cybersecurity 14 september

Geachte woordvoerders digitale zaken,

Op woensdag 14 september debatteert u over online veiligheid en cybersecurity. U weet dat dit onderwerp bij gemeenten hoog op de bestuurlijke agenda staat. Enerzijds omdat gemeenten in hun rol als hoeder van de openbare orde en veiligheid in actie komen bij incidenten, anderzijds om het risico op incidenten te minimaliseren. Gemeenten voelen bij uitstek hun verantwoordelijkheid om inwoners, bedrijven en overheden digitaal veilig te houden, omdat zij draaien op data en in toenemende mate digitaliseren. Informatieveiligheid is ook essentieel voor de continuïteit en de kwaliteit van de dienstverlening in het fysieke domein.

Wij hopen dat u bij dit debat aandacht wil besteden aan de volgende vier onderwerpen die voor gemeenten van belang zijn:

Basis op orde

Digitale veiligheid is een kerntaak van gemeenten. Digitale dreigingen nemen toe en gemeenten beschikken lang niet altijd over de middelen of capaciteit om alle noodzakelijke maatregelen te treffen en de basis op orde te hebben. De financiële tekorten bij gemeenten werken door in de bedrijfsvoering en daarmee ook de inspanningen om de digitale gemeente te beveiligen. Voor alle bestuurslagen geldt de Baseline Informatiebeveiliging Overheid (BIO) als verplicht normenkader. Idealiter wordt dit thema risicogebaseerd opgepakt, waarbij de grootste risico's als eerste geadresseerd worden.

Coördinatie binnen cyberdomein

Tijdens de ALV van 29 juni jl. hebben gemeenten met een aangenomen motie bevestigd niet alleen verantwoordelijk te zijn voor de digitale veiligheid van de eigen organisatie, maar ook een verantwoordelijkheid te dragen over de digitale veiligheid op het niveau van de gemeente. Digitale dreigingen nemen hand over hand toe, maar gemeenten beschikken lang niet altijd over de middelen of capaciteit om de noodzakelijke maatregelen te treffen. Wat dan niet helpt, is dat het voor gemeenten nu niet duidelijk is wanneer zij hun informatieveiligheid effectief op orde hebben.

Verschillende departementen en autoriteiten voegen naast de BIO ongecoördineerd verschillende kaders toe. Wanneer gemeenten hier niet aan voldoen, kunnen zij vaak geen gebruik maken van noodzakelijke diensten.

Deze onduidelijkheid ervaren gemeenten ook in de verschillende proeftuinen, projecten en programma's die gemeenten worden aangeboden. Ten aanzien van cyberweerbaarheidsprogramma's voor het mkb bijvoorbeeld, werken gemeenten samen met departementen als J&V, BZK, EZK, maar ook met partijen als de politie, MKB Nederland, KvK, het CCV etc. Deze projecten en programma's zijn veel efficiënter en effectiever, wanneer deze gecoördineerd worden opgezet.

Nu heeft het kabinet duidelijk gemaakt dat de regie bij het NCSC komt te liggen. Dit wordt gefaseerd ingevoerd vanaf 2024. Een goed vooruitzicht, maar het is voor gemeenten wel van belang wat er vóór 2024 gaat gebeuren met lopende programma's. Daarnaast is nog niet duidelijk wat de coördinatie van

het NCSC straks betekent voor gemeenten: is de versnippering van aanspreekpunten dan verleden tijd?

Maak werk van een digitaal veiligheidsstelsel

Op het gebied van de fysieke openbare orde en veiligheid kent Nederland een functioneel stelsel met duidelijke afspraken tussen de betrokken partijen en helderheid over rollen, taken, verantwoordelijkheden en bevoegdheden. Binnen het fysieke veiligheidsdomein is voor alle betrokken partijen min of meer duidelijk voor welke van de schakels binnen de veiligheidsketen (proactie, preventie, preparatie, repressie en nazorg) zij verantwoordelijk zijn en hoe zij onderling moeten samenwerken. Voor het digitale veiligheidsdomein is dit nog lang niet altijd het geval, terwijl het risico bestaat dat een digitaal incident kan omslaan in een fysiek veiligheidsincident.

Zo heeft de burgemeester bijvoorbeeld de bevoegdheid om een straatverbod op te leggen aan een individu of aan een groep individuen wanneer hij/zij daartoe de noodzaak ziet. Voor het digitale domein bestaat die mogelijkheid niet, terwijl er toch scenario's denkbaar zijn dat deze bevoegdheid gewenst is. Hetzelfde geldt voor fysieke crises waarbij, afhankelijk van de aard en omvang, duidelijke handelingskaders over verantwoordelijkheden en voorwaarden voor op- of afschaling van inspanningen nodig zijn. Ook wanneer een digitale crisis een fysieke crisis wordt, gelden lang niet altijd dezelfde kaders en handelingsmogelijkheden. Zo legde de NotPetya-malware in 2017 niet alleen banken en energiemaatschappijen lam, maar ook busstations en het vliegverkeer.

Hoewel 100% veiligheid niet bestaat, is het wel van wezenlijk belang dat partijen binnen het veiligheidsdomein weten waarvoor ze aan de lat staan en hoe zij bij verschillende situaties dienen samen te werken. Dit geldt ook voor het uitwisselen van (dreigings-)informatie met en tussen de betrokken partijen. De regels en wetten die gelden die voor het fysieke domein gelden, zijn daarbij niet voldoende om de veiligheid ook in het digitale domein te borgen. Het is daarom noodzakelijk dat het fysieke veiligheidsstelsel een doorvertaling krijgt richting een digitaal veiligheidsstelsel.

Onduidelijkheid over wet- en regelgeving

Zoals hierboven geschreven gelden er verschillende normen voor gemeenten, naast de BIO. Het is voor gemeenten vrij helder of zij voldoen aan een bepaalde norm of niet. Hoe de verschillende normen zich echter tot elkaar verhouden en hoe dit bijdraagt aan de feitelijke veiligheid van de gemeentelijke organisatie, is minder duidelijk. Onduidelijke wet- en regelgeving zorgt hierbij voor extra verwarring. Zo is het niet helder in hoeverre de op Europees niveau recent bekrachtigde NIB-richtlijn (Netwerk- en Informatiebeveiliging richtlijn) gaat gelden voor gemeenten en op welke manier BZK en J&V de richtlijn gaan interpreteren. Zo lijken belangrijke gemeentelijke processen op het gebied van onder meer afvalwaterzuivering, verkeersregelsystemen en wegenbeheer binnen de scope van de NIB-richtlijn te vallen.

Voor gemeenten is het op dit moment echter onhelder, wat dit voor hen betekent in termen van zorgplicht, meldplicht en toezicht. Het is een reëel scenario dat de nationale implementatie van de NIB-richtlijn stevige extra inspanningen van gemeenten gaat vragen. Gemeenten willen weten wat de impact van de NIB-richtlijn gaat zijn voor gemeenten en hoe het proces omtrent implementatie eruit gaat zien.