Veiligheidsregio Drenthe

MEMO

aan Algemeen bestuur
van Suzanne Roijakkers
vergaderdatum 14 december 2022
onderwerp Nieuws uit het Veiligheidsberaad

Inleiding

In het reguliere Veiligheidsberaad van 10 oktober zijn onder andere de volgende zaken aan bod geweest.

Contourennota versterking crisisbeheersing en brandweerzorg
Het kabinet heeft eerder in haar standpunt over de evaluatie Wet veiligheidsregio's aangekondigd om mét behoud van het goede, zo spoedig mogelijk te komen tot een toekomstbestendig, samenhangend stelsel voor crisisbeheersing en brandweerzorg. Hiertoe wordt een contourennota opgesteld.

Deze contourennota schetst hoe de organisatiestructuur en samenwerking van betrokken partijen bij interregionale, nationale en internationale risico's en crises wordt vernieuwd. Ook gaat deze in op de veranderingen in de brandweerzorg. Daarbij worden bovenop de reeds in gang gezette verbeteringen nadrukkelijk de praktijkervaringen betrokken die in de afgelopen periode zijn opgedaan met de bestrijding van verschillende incidenten, rampen en crises. Ook waardevolle lessen en inzichten uit recente cyber-incidenten, oefeningen zoals Isidoor, specifieke crisisevaluaties, zoals het eerste deel van het onderzoek van de Onderzoeksraad voor Veiligheid naar de coronacrisis, en wetenschappelijke studies en rapporten borgt het kabinet waar mogelijk in het nieuwe wettelijk kader. De contourennota is een nadere uitwerking van het kabinetsstandpunt en schetst op hoofdlijnen de noodzakelijke vernieuwingen en veranderingen in het beoogde toekomstige stelsel van crisisbeheersing en van brandweerzorg.

Naar verwachting wordt de contourennota in december aangeboden aan de Tweede Kamer.

Ophoging BDUR met 83 miljoen
In de bestuurlijke afspraken doorstroom migratie is structureel € 83 miljoen toegezegd via de Brede Doeluitkering Rampenbestrijding (BDUR). In het Veiligheidsberaad is een verdeelsleutel afgesproken die nader wordt vertaald. De toegezegde gelden vormen een landelijke impuls voor crisisbeheersing en informatievoorziening. De wijze waarop de gelden in onze regio kunnen worden ingezet, komt terug op de bestuurlijke agenda.

Bestuurlijke bevoegdheden cyber
Vanuit het Veiligheidsberaad is een rapport opgesteld over de bestuurlijke bevoegdheden bij cyber. Het rapport verkent, op basis van vier scenario's, de interventiemogelijkheden van burgemeesters en/of voorzitters veiligheidsregio. Dit is onderzocht door middel van workshops met een gevarieerde groep van cyberexperts en professionals uit het werkveld.

Het rapport concludeert dat burgemeesters en/of voorzitters veiligheidsregio's geen bevoegdheden hebben waarmee zij specifiek bij cyberincidenten kunnen ingrijpen. Ze beschikken niet over wettelijke bevoegdheden op het gebied van cybersecurity. Op basis van de bestaande juridische bevoegdheden is het enkel mogelijk om in te grijpen bij een (dreigend) cyberincident als ten gevolge hiervan de openbare orde en/of veiligheid in het geding is. De taken en bevoegdheden zijn daarmee voornamelijk op gevolgbestrijding gericht.

Het rapport is ter kennisname bijgevoegd.

Versnellingsplan informatieveiligheid
Er is gesproken over de voortgang van het versnellingsplan informatieveiligheid.

Voortgang implementatie BIO (Baseline Informatiebeveiliging Overheid)
Bij de vaststelling van het Versnellingsplan in het Veiligheidsberaad (11 juni 2021) is afgesproken dat de veiligheidsregio's aan elkaar rapporteren over de voortgang van de implementatie van de BIO. Doel hiervan is de versterking van de kennisuitwisseling en om de basis van informatiebeveiliging op orde te krijgen (fase 1). Inmiddels hebben de veiligheidsregio's vier keer aan elkaar gerapporteerd over de voortgang van de BIO-implementatie in het POI. Drie van deze rapportages zijn besproken in de Bestuurlijke Adviescommissie IV.

Uit de vier rapportages is op te maken dat iedere regio hard aan de implementatie werkt. De beoogde versnelling is goed zichtbaar.

Cyberweerbaarheid door inrichting SOC en CERT
Fase 2 van het Versnellingsplan is gericht op weerbaarheid tegen cyberaanvallen. Een essentieel onderdeel daarvan is de inrichting van een goede monitoring (SOC) en incident respons (CERT).

Een SOC en CERT vormen samen met een ISAC (*Information Sharing and Analysis Center*) het cybersecuritynetwerk. Een ISAC voor de veiligheidsregio's (VR-ISAC) is reeds op 18 juni 2020 door de 25 directeuren veiligheidsregio (RCDV) ingesteld. Binnen het VR-ISAC wordt door en met de veiligheidsregio's informatie gedeeld betreffende cyberdreigingen en aanvallen. Door het inrichten van een SOC- en CERT-functie ontstaat er, samen met het VR-ISAC, een sluitende aanpak van informatieveiligheid.