

**Datum**

9 april 2024

**Onderwerp**

VNG- en G4-inbreng CD Online veiligheid en cybersecurity 11 april

Geachte woordvoerders Digitalisering,

Komende donderdag vindt het commissiedebat Online veiligheid en cybersecurity plaats. Via deze mail memoreren wij u graag aan de oproepen die gemeenten gedaan hebben tijdens het G4-werkbezoek digitale veiligheid van afgelopen najaar. Als gemeenten zien ook wij dat de digitale weerbaarheid van Nederland achterloopt op de dreiging. Daarom vragen wij aandacht voor de benodigde structurele financiering van 30-50 miljoen euro om onze steden weerbaarder te maken tegen digitale dreigingen. Daarnaast vragen wij u om de minister te verzoeken om de komende jaren de acties te blijven monitoren uit het 'Convenant digitale veiligheid rijk-gemeenten' en periodiek uw Kamer hierover te informeren.

## Openstaande rekening om gemeenten weerbaar te maken

Digitale dreiging loert in iedere gemeente. Zeker ook in de G4, met internationale havens, vliegvelden, gerechtshoven, enzovoorts, zijn de risico's van een nog grotere orde. Door de toenemende (afhankelijkheid van) digitalisering, maar ook de internationale spanningen, neemt het risico op cyberaanvallen en cybercrises toe en neemt criminaliteit in het digitale domein een vlucht. Voorbeelden uit binnen- en buitenland laten zien dat de kosten van succesvolle gijzelsoftware-aanvallen op gemeenten tot tientallen miljoenen kunnen oplopen. Om van de niet-financiële schade nog niet eens te spreken.

Om schade te voorkomen en als hele samenleving weerbaar te worden tegen de digitale dreiging van criminelen én statelijke actoren, moet ook de lokale overheid op dit onderwerp worden versterkt. Gemeenten hebben de afgelopen jaren een voortrekkersrol op zich genomen om het lokale perspectief op digitale veiligheid in nationale beleids- en besluitvorming beter onder de aandacht te brengen. Dat heeft er onder meer toe geleid dat rijk en gemeenten op 21 december 2022 het **convenant Digitale Veiligheid** sloten, als één van de acties uit de Nederlandse Cybersecuritystrategie. Dit convenant is erop gericht om belangrijkste knelpunten aan te pakken. De belangrijkste knelpunten zijn momenteel de onduidelijkheid over het stelsel, de rollen, verantwoordelijkheden en bevoegdheden maar ook de beperkte informatiepositie en het ontbreken van structurele (rijks)middelen voor digitale veiligheid op lokaal niveau.

Ondanks deze knelpunten zitten wij als gemeenten niet stil en werken we met beperkte incidentele middelen aan onze Agenda's Digitale Veiligheid. Voor meer en structurele impact is duurzame en structurele financiering noodzakelijk: minstens 30 tot 50 miljoen euro is per jaar structureel nodig om de digitale dreigingen het hoofd te bieden.

Deze behoefte aan financiering is extra urgent omdat gemeenten op dit moment geconfronteerd worden met een veelheid aan (urgente) maatschappelijke vraagstukken (zoals t.a.v. woningbouw, stikstof en asiel) die veel vragen van de schaarse lokale middelen en capaciteit. Daarbij zijn in het Regeerakkoord en vanuit het rijk nog geen middelen voor digitale veiligheid van gemeenten beschikbaar gesteld. Gebrek aan financiële middelen zal ten koste gegaan van de aandacht voor de digitale veiligheid op lokaal niveau en het risico op onveilige situaties doen toenemen. Bij digitale veiligheid geldt dat criminelen zich richten op de zwakste schakel in de keten.

Een eerste interne inventarisatie van de VNG en G4 laat zien dat er de komende jaren voor digitale veiligheid op lokaal niveau ten minste tussen de 30 en 50 miljoen euro aan structurele financiering per jaar extra nodig is. Het gaat daarbij om benodigde investeringen ter verhoging van de digitale weerbaarheid van de gemeentelijke organisaties, het implementeren van aankomende wet- en regelgeving en het aanstellen van coördinatoren bij de gemeenten met meer dan 100.000 inwoners die zich richten op effecten van digitale dreigingen, incidenten en crisis op de openbare orde en veiligheid in de stad. Deze inventarisatie wordt nog verder uitgewerkt, maar de eerste cijfers zijn reden tot zorg.

## Houd vinger aan de pols: structurele monitoring van lokale dreiging noodzakelijk

Eén van de geagendeerde stukken is het 'Evaluatiekader en nulmeting NLCS' dat door Dialogic is opgesteld in opdracht van het WODC. In dit document stelt Dialogic dat de 'activiteit' bestuurlijk convenant is afgerond en dus niet gemonitord hoeft te worden. Wij benadrukken echter dat met het sluiten van het convenant slechts een eerste (proces)stap is gezet. Maar met processtappen worden wij niet weerbaarder, met acties wel. Wij vragen daarom om juist de voortgang van de acties uit het convenant te blijven monitoren en daarmee het lokale perspectief op digitale veiligheid in zicht te houden.