Datum
30 januari 2025

Onderwerp
VNG-inbreng CD online veiligheid en cybersecurity 5 februari

Geachte woordvoerders digitale veiligheid,

Op 5 februari debatteert u over online veiligheid en cybersecurity. Op de agenda staan voortgangsbrieven van de Ministers van J&V en EZ. Daarover geven wij het gemeentelijk perspectief mee om de haalbaarheid van de Nederlandse Cybersecuritystrategie (NLCS) te waarborgen.

1. Gevolgen niet-tijdige implementatie NIS2- en CER-richtlijn
2. Toekomstvisie Cyberweerbaarheidsnetwerk
3. Cybersecuritybeeld Nederland 2024 en Voortgang Nederlandse Cybersecuritystrategie
4. Nationale Technologiestrategie - Agenda Cybersecurity Technologies

1. Haalbaarheid, betaalbaarheid en uitvoerbaarheid van de NIS2- en CER-implementatiewetten
De gemeenten werken hard aan het verhogen van de digitale weerbaarheid om de systemen en infrastructuur veilig te houden en de privacygevoelige gegevens van inwoners te beschermen.
De wettelijke kaders hiervoor in de Cyberbeveiligingswet (Cbw) en Wet weerbaarheid kritieke entiteiten (Wwke) zijn in Nederland naar verwachting in september 2025 van kracht.
Sinds de aankondiging van de wetten adviseren wij gemeenten om niet te wachten met voorbereidingen op de inwerkingtreding. Ondanks dat de inwerkingtreding is opgeschoven, blijkt het nog onvoldoende haalbaar, betaalbaar en uitvoerbaar voor gemeenten, omdat er nog veel onduidelijk is, zowel over de Cbw, als ook over de Wwke.

Of gemeenten moeten voldoen aan de Wwke wordt pas duidelijk na de risicobeoordeling van het Ministerie van I&W dat rond juli 2026 zal plaatsvinden. Dit is lang na de consultaties en inwerkingtreding van de Wwke. Dit betekent dat de medeoverheden niet goed kunnen reageren op het wetsvoorstel en het risico lopen dat zij de Wwke in een kort tijdbestek moeten implementeren, wat zowel onpraktisch als inefficiënt is. Daarnaast betekent de Cbw een taakverzwaring op het gebied van zorgplicht, governance, registratieplicht en meldplicht.

We vragen de minister om rekening te houden met de inbreng van de decentrale overheden bij de consultatie van de Cbw en de Wwke. Zo moet er, in overeenstemming met artikel 2 van de Financiële-verhoudingswet, voor adequate financiële dekking worden gezorgd om de vereiste zorg-, meld- en toezichtplicht maatregelen te implementeren. De grote financiële problemen voor het jaar 2026, het ravijnjaar en de onzekerheid die daarbij komt, heeft ook invloed op de prioriteit die aan informatiebeveiliging wordt gegeven.

Wij vragen u daarom:

Aandacht te vragen voor de haalbaarheid, betaalbaarheid en uitvoerbaarheid van de NIS2- en CER-implementatiewetten, gezien de taakverzwaring en de beperkte implementatietermijn.

2. Schaalbaarheid van het Cyberweerbaarheidsnetwerk (CWN)
Om de digitale weerbaarheid van de gemeentelijke organisatie en van de gemeenten te verhogen, zetten gemeenten in op meer oefenen en trainen. De uitwerking van het Rapport Toekomstvisie Cyberweerbaarheidsnetwerk stelt ook dat opleiden, trainen en oefenen (OTO) één van de kernfuncties van het CWN is, met als doel de digitale weerbaarheid van organisaties te vergroten. Wij ondersteunen deze aanpak. Het volwassenheidsniveau van gemeenten op dit gebied verschilt en dat zorgt vooral bij kleinere gemeenten voor problemen, vanwege hun kwetsbaarheid voor grote cyberaanvallen.

Het vraagt echter ook een flinke investering om structureel opleidingen, trainingen en oefeningen te kunnen volgen. Gemeenten kunnen deze investering lang niet altijd doen, vanwege de grote financiële problemen en de samenwerking die nodig is om het CWN op te schalen. Het is belangrijk dat de OTO-functie tot een uitvoerbaar en efficiëntere opleidingslast leidt. De functie moet zo dicht mogelijk op het fysieke domein van openbare orde en veiligheid aansluiten en gefocust zijn op maatschappelijke gevolgen.

Wij vragen u daarom:
- Tijd en ruimte te maken zodat álle gemeenten het benodigde volwassenheidsniveau kunnen bereiken.
- Voldoende middelen vrij te maken gerelateerd aan een efficiëntere opleidingslast voor gemeenten.

3. Meer inzicht in het tekort van cybersecuritypersoneel
Het lukt gemeenten niet of nauwelijks om voldoende gekwalificeerd cybersecuritypersoneel te vinden (*als* ze er al middelen voor vrij kunnen maken). De NLCS benadrukt het belang van een arbeidsmarkt die aan de toenemende vraag naar cybersecurity-experts kan voldoen. Gezien de verwachte implementatielast van de NIS2- en CER-richtlijnen moet er meer aandacht worden besteed aan personeelsbehoeften, vooral bij kleine en middelgrote gemeenten die sowieso minder arbeidskracht en middelen hebben om dezelfde taken als grote gemeenten uit te moeten voeren.

Het helpt dat het ministerie van EZ informatie over de huidige stand van de cybersecuritymarkt inzichtelijk maakt. De interventies vanuit de Human Capital Agenda Cybersecurity worden nu uitgewerkt. Om het tekort op lange termijn aan te pakken is er echter meer inzicht nodig in de ontwikkeling van de vraag naar cybersecuritypersoneel en gerichte interventies voor efficiëntere en flexibelere arbeidsinzet in de gemeentelijke sector.

Wij vragen u daarom:
- De huidige informatiemiddelen uit te breiden voor gericht inzicht in de ontwikkeling van de vraag naar personeel voor digitale veiligheid.
- Gerichte interventies voor efficiëntere en flexibelere arbeidsinzet in de gemeentelijke sector.

4. Leveranciersmanagement voor post-quantum cryptografie digitale veiligheid
Wij zien dat de ontwikkeling van strategische cybersecuritytechnologie en het toepassen van de benodigde PQC-oplossingen als een goede en noodzakelijke ontwikkeling vòòr 2030 moet zijn ingevuld. Deze verantwoordelijkheid kan volgens ons niet alleen bij de opdrachtgeverskant liggen. Met name kleine en middelgrote gemeenten hebben die kennis en capaciteit niet. Dit vereist schaarse expertise op té veel plaatsen en dat is een ongewenst en onhaalbaar beeld.
De Nederlandse Technologiestrategie (NTS) benadrukt het belang van onderzoek naar en innovatie in post-quantum cryptografie (PQC) om de toegepaste cryptografie van organisaties op langere termijn veiliger te maken. De kennis en capaciteiten om deze ambitie te bereiken bestaan echter grotendeels bij producenten, waardoor gemeenten van anderen afhankelijk zijn om zelf binnen afzienbare termijn quantumveilige dienstverlening te bevorderen en implementeren. Wij ondersteunen de prioritering van PQC in de NTS en vragen om een gezamenlijke verantwoordelijkheid met leveranciers en producenten van PQC in te richten.

De rijksoverheid heeft de opdracht gekregen om een PQC-aanpak voor alle overheden uit te werken. Wij zien in de prioritering van leveranciersmanagement in de Europese Cyberresilience Act (CRA) mogelijkheden voor een gedeelde verantwoordelijkheid op PQC met de producenten en leveranciers, om zo gezamenlijk de veiligheid in de hele levenscyclus te waarborgen.

Wij vragen u daarom:

> De minister te vragen naar een gezamenlijke verantwoordelijkheid met leveranciers en producenten voor strategische cybersecurity technologieën zoals PQC.