

Punt 4: Mogelijkheid tot het stellen van vragen

Indiener: B. de Groot (VVD)

Vragen over de brief VNG Lbrf 25-017 Gevolgen Cyberbeveiligingswet voor gemeenten

De websites van verschillende Nederlandse gemeenten en provincies werden maandagochtend 28/4 getroffen door een grootschalige cyberaanval. Hierdoor waren ze urenlang niet bereikbaar. Midden-Delfland gelukkig niet. Naar aanleiding hiervan en de brief van de VNG van 26 maart 2025, met nummer: B 25048, heeft de VVD een aantal vragen.

VRAAG 1

Is het college bekend met de inhoud van beide brieven van de VNG over de Cyberbeveiligingswet?

Zo ja, hoe beoordeelt het college de signalen en zorgen die hierin worden geuit door de VNG met betrekking tot de uitvoering en impact voor de gemeente zelf?

ANTWOORD

Het college heeft kennisgenomen van de inhoud van de brieven en laat zich ten aanzien van de inhoudelijke aspecten informeren door de vakinhoudelijke medewerkers. Naar aanleiding van beide brieven van de VNG wordt op het gebied van informatiebeveiliging door onze Chief Information Security Officer (CISO) en Information Security Officer (ISO) een memo voorbereid voor het college.

De verwachting is dat deze memo volgende week wordt aangeboden aan het college.

Hierin staan de gevolgen van de nieuwe wet- en regelgeving voor onze gemeente.

Als gemeente commiteren wij ons al aan de huidige Baseline Informatiebeveiliging Overheden (BIO). Op basis daarvan hebben we al aanzienlijke maatregelen genomen om onze informatiebeveiliging op orde te houden en te verbeteren. De taken en normen in nieuwe wetgeving is op dat vlak strenger, maar uitvoerbaar.

VRAAG 2

Wat zijn volgens het college de (verwachte) implicaties van de Cyberbeveiligingswet voor onze gemeentelijke organisatie? Wordt onze gemeente als 'essentiële' of 'belangrijke' entiteit aangemerkt onder de nieuwe wetgeving, en wat betekent dit concreet voor onze informatiebeveiliging?

ANTWOORD

Onze gemeente wordt als aangemerkt als essentiële entiteit binnen de Cyberbeveiligingswet. De invoering van de wet heeft implicaties voor ons als gemeente als het gaat om informatiebeveiliging. De wet introduceert een aantal belangrijke verplichtingen:

- **Zorgplicht:** Gemeenten zijn expliciet verantwoordelijk geworden voor het beheersen van cyberrisico's. Dit betekent dat informatiebeveiliging structureel onderdeel moet zijn van het risicomanagement. Besluitvorming over bijvoorbeeld te nemen maatregelen die nu als bedrijfsvoeringonderdeel via het DT loopt, loopt dan via het college.
- **Meldplicht:** Ernstige digitale incidenten moeten gemeld worden aan de Informatiebeveiligingsdienst (IBD). Dit was in de praktijk al vormgegeven en dit wordt met deze wetgeving alleen geformaliseerd. De exacte regels hierover zijn nu nog niet bekend. De VNG heeft het Rijk vragen gesteld hierover.
- **Toezicht:** De Rijksinspectie Digitale Infrastructuur (RDI) houdt toezicht op naleving. De gemeenteraad gaat primair toezicht houden op de naleving van de wet. Dit gebeurt door het vervullen van de kaderstellende en controlerende rol, waarbij voldoende budget voor te nemen maatregelen moet worden geborgd.

- **Bestuurdersverantwoordelijkheid:** Collegeleden (B&W) moeten verplichte trainingen volgen over cyber risico's. Niet-naleving kan leiden tot persoonlijke boetes tot €25.000.

Daarnaast voorzien we dat de scope wordt uitgebreid met de komst van de Cyberbeveiligingswet. Denk hierbij aan **SCADA-systemen** (Supervisory Control and Data Acquisition), die worden gebruikt voor het aansturen en monitoren van fysieke processen zoals:

- Brugopeningen.
- Rioolgemalen.
- Verkeerslichten.
- Waterbeheer.

Deze systemen zijn vaak kwetsbaar voor cyberaanvallen en vallen daarom onder de verhoogde aandacht van zowel de Cyberbeveiligingswet als BIO 2.0. Dit vraagt extra aandacht van de gemeente op het gebied van risicomanagement en de mogelijk te nemen maatregelen.

Praktische gevolgen voor ons als gemeenten zijn:

- Inventarisatie van alle SCADA-systemen.
- Toetsen op risicomanagement en het mogelijk nemen van beveiligingsmaatregelen, zoals netwerksegmentatie, monitoring, en incidentresponsplannen.
- Audits en rapportageverplichtingen richting toezichthouders.
- Training en bewustwording bij personeel.

VRAAG 3

Is onze gemeente momenteel voldoende voorbereid op de aanvullende eisen die de wet stelt aan onder andere risicobeheer, incidentmeldingen en toezicht? Zo nee, welke stappen worden er genomen om hier alsnog aan te voldoen?

ANTWOORD

Ja, de gemeente is voldoende voorbereid op de aanvullende eisen die de wet stelt. Met de VNG resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" van 2013 hebben de gemeenten afgesproken de Baseline Informatieveiligheid Gemeenten (vanaf 2020 overgegaan in de BIO) te implementeren. Daar commiteert de gemeente zich nu al aan. Met de Cyberbeveiligingswet wordt dit nu formele wetgeving. De huidige Baseline Informatiebeveiliging Overheden vraagt al om risicomanagement. Het betekent wel dat er meer getoetst gaat worden op werking van maatregelen.

VRAAG 4

Welke rol speelt of verwacht het college van de VNG en/of de Informatiebeveiligingsdienst (IBD) in de ondersteuning van gemeenten bij de implementatie van de Cyberbeveiligingswet? Is het college van mening dat de ondersteuning vanuit deze organisaties toereikend is?

ANTWOORD

De VNG en IBD ondersteunt gemeenten al op basis van de huidige BIO. Zij bieden diverse hulpmiddelen om gemeenten te helpen te voldoen aan de nieuwe wet- en regelgeving. Daarnaast geven ze ook al advies bij incidenten.

Of de ondersteuning vanuit de VNG en IBD toereikend is in het kader van de nieuwe strengere wetgeving moet uiteindelijk nog blijken.

VRAAG 5

Kan het college aangeven welke (extra) middelen, menskracht of investeringen nodig zijn om te voldoen aan de eisen van de wet? Is het college voornemens om hiervoor aanvullende financiering aan te vragen of vrij te maken?

ANTWOORD

Op basis van de externe audit van de ENSIA (Eenduidige Normatiek Single Information Audit) zijn wellicht extra middelen benodigd, maar deze lijken vooralsnog marginaal. Deze middelen dekken we voorlopig uit de lopende begroting. We vragen wanneer nodig gericht om extra middelen als deze in een concrete behoefte voorzien. Dit hebben we bijvoorbeeld ook op deze manier gedaan bij de aanbesteding van het SIEM&SOC

(Security Operations Center/ Security Information & Event Management). Sinds mei dit jaar is er naast onze CISO ook een ISO aangesteld om onder andere bij de verhoogde auditlast te ondersteunen en bij te dragen aan het risicomanagement en operationeel beleid op te stellen. We kijken voorlopig of we nog uit de voeten kunnen met de huidige formatie. Het moet in de praktijk nog blijken in hoeverre nog extra middelen benodigd zijn. Vooralsnog loopt dit nog in lijn.