

Toezicht in het kader van de Cyberbeveiligingswet

In deze mededeling wordt u geïnformeerd over de uitkomsten van het rapport naar toezicht op de digitale veiligheid binnen de decentrale overheden.

De komst van de Cyberbeveiligingswet is van invloed op de organisatie van het waterschap, maar ook op het bestuur daarvan. Het bestuur moet zorgen dat de organisatie afdoende maatregelen treft, zodat het waterschap de digitale veiligheid op orde heeft. In de Cyberbeveiligingswet zijn nieuwe regels over governance en handhaving genomen. Artikel 24 van de wet geeft aan hoe de governance wordt ingericht en op basis van artikel 78 kan een bestuurder geschorst worden als een waterschap de digitale veiligheid niet op orde heeft. Gezien dit toezichtregime op basis van de Cyberbeveiligingswet hebben de Vereniging van Nederlandse Gemeenten (VNG), het Interprovinciaal Overleg (IPO) en de Unie van Waterschappen (Unie) PBLQ gevraagd onderzoek te doen naar het toezicht binnen de decentrale overheid. Doel was mogelijkheden in beeld te krijgen om het toezicht op digitale veiligheid bij deze bestuurslagen te versterken. Hierbij gaat het zowel om het interbestuurlijke, verticale toezicht als om het horizontale toezicht.

Aandachtspunten rapport

Eerste aandachtspunt in de opdracht was te onderzoeken hoe generieke toezichtinstrumenten kunnen worden ingezet om de digitale veiligheid bij de gemeenten, waterschappen en provincies te versterken. Eveneens was er aandacht voor de vraag hoe het horizontale toezicht op digitale veiligheid kan worden versterkt. Ook is aandacht besteed aan de mogelijke bijdrage van decentrale rekenkamers aan het versterken van het horizontale toezicht op informatiebeveiliging.

In het rapport wordt in beeld gebracht hoe op dit moment het toezicht op informatieveiligheid is ingericht. Op basis van deze praktijk konden er uitspraken worden gedaan over hoe het toezicht het best kan worden ingericht teneinde de digitale veiligheid van decentrale overheden te versterken.

Bij de waterschappen houdt het Algemeen Bestuur toezicht op het Dagelijks Bestuur, het horizontaal toezicht. Daarnaast is er sprake van verticaal toezicht, waarbij een hogere bestuurslaag (in het geval van de waterschappen de provincie en/of Rijk) toezicht houdt op een lagere bestuurslaag.

Uitkomsten rapport

Op basis van het voor het rapport uitgevoerde onderzoek blijkt dat het horizontaal toezicht op digitale veiligheid soms tekortschiet. Volgens het onderzoeksbureau heeft dat drie belangrijke oorzaken:

- er wordt onvoldoende prioriteit toegekend aan dit onderwerp door het toezichthoudend orgaan;
- er is onvoldoende kennis aanwezig over digitale veiligheid om toezicht te kunnen houden;
- het toezichthoudend orgaan wordt onvoldoende in stelling gebracht om toezicht op digitale veiligheid te kunnen uitoefenen.

Om het horizontaal toezicht te verbeteren, worden in het rapport suggesties aangereikt: zoals opleidingen tot verbetering van de informatiepositie en van de goedkeuring van bestuurlijke rapportages door een onafhankelijke auditor tot aandacht voor digitale veiligheid bij inwerkprogramma's voor nieuwe volksvertegenwoordigers. Hierbij kunnen de verschillende bestuurslagen en hun koepels veel van elkaar leren. Geadviseerd wordt om aan kennisuitwisseling te doen¹.

¹ Na oplevering van het rapport hebben de Unie en het Waterschapshuis nog met VNG en IPO gedeeld hoe er door de waterschappen wordt gewerkt met een volwassenheidsniveau op de Baseline Informatieveiligheid Overheid (BIO). Bij de gemeenten en provincies is de monitoring op het voldoen aan de BIO op dit moment nog zo ingericht dat er aan een verplichting wel/niet wordt voldaan. Door net zoals de waterschappen met een volwassenheidsniveau te werken, wordt duidelijker wat deze bestuurslagen al allemaal doen in het kader van het verbeteren van de digitale veiligheid.



In het rapport is aandacht besteed aan de rol van rekenkamers bij de uitvoering van horizontaal toezicht. De conclusie is dat rekenkamers geen structurele rol kunnen spelen bij het horizontaal toezicht. Zij zijn onafhankelijk en de rol van toezichthouder past hun niet. Ook beschikken zij niet over de vereiste kennis.

Op het gebied van digitale veiligheid worden horizontaal- en verticaal toezicht gezien als 'communicerende vaten'. Als het horizontaal toezicht goed functioneert, kan het verticale toezicht daar gebruik van maken. Andersom geldt natuurlijk ook dat bij afwezigheid van horizontaal toezicht meer verticaal toezicht nodig is.

Aanbevelingen

Het adviesbureau geeft uiteindelijk vier aanbevelingen op basis van de bevindingen:

1. Versterk de kennis over digitale veiligheid in alle bestuurslagen;
2. Ontwikkel een toezichtstelsel waarin horizontaal en verticaal toezicht elkaar aanvullen;
3. Voorkom verdere bureaucratisering en zorg dat toezicht de digitale veiligheid daadwerkelijk versterkt;
4. Zorg voor structurele kennisuitwisseling bij het ontwerp en de implementatie van het nieuwe toezichtstelsel.

Het Uniebureau beraadt zich momenteel over opvolging van het onderzoek.