Reactie op internetconsultatie Cyberbeveiligingsbesluit
Datum: 28 maart 2025
Van: G4-gemeenten (Amsterdam, Den Haag, Rotterdam, Utrecht)

Met veel interesse hebben wij meegelezen op de concepttekst van het Cyberbeveiligingsbesluit, als Algemene Maatregel van Bestuur bij de Cyberbeveiligingswet, en de concept Ministeriële Regeling. Onze zorgen, opmerkingen en behoeften maken we met deze inbreng kenbaar.

Algemene reactie Cyberbeveiligingsbesluit & Ministeriële Regeling

- De in dit Cyberbeveiligingsbesluit bijgevoegde Ministeriële Regeling is niet van toepassing op de overheid. Kunt u aangeven wanneer de Ministeriële Regelingen die voor gemeenten gelden bekend zijn, zodat wij ons als G4-gemeenten kunnen voorbereiden in de korte tijd die ons daarvoor nog rest tot van kracht worden van de Cyberbeveiligingswet (naar verwachting derde kwartaal 2025)?
- De bijgevoegde Ministeriële Regeling is gericht op de sectoren energie, digitale infra, etc. De in de Ministeriële Regeling opgenomen voorschriften gaan niet in op eventuele specifieke risico's of eisen die voor die sectoren gaan gelden; de regeling doet zeer generiek aan. Wij adviseren om de Ministeriële Regeling die van toepassing wordt voor de overheid, voor de gemeenten, wel specifiek te maken.
- Wanneer komen de overige Ministeriële Regelingen beschikbaar die van toepassing zijn op de overheid, de zorgsector, de watersector, en andere sectoren die een relatie hebben met de G4-gemeenten? En hoe anders zullen deze zijn ten opzichte van de nu gepubliceerde regeling?
- Hoe wordt er gezorgd voor samenhang en harmonisatie tussen de verschillende Ministeriële Regelingen en onderliggende normenkaders vanuit de rijksoverheid, waarin daadwerkelijke beveiligingseisen worden geconcretiseerd?. Hierbij enkele voorbeelden daarvan:
    - Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft het concept van de BIO2 gepubliceerd
    - In de zorgsector geldt de NEN7510 als norm (onder andere voor de gemeentelijke gezondheidsdiensten)
    - Voor operationele technologie/ industriële automatisering moeten we voldoen aan het normenkader IEC62443 en heeft het ministerie van Infrastructuur en Waterstaat zowel de norm CSIR als BIACS ontwikkeld
    - Voor DigiD geldt het specifieke normenkader van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties/Logius

  De G4-gemeenten moeten aan al deze nomen voldoen en hebben dringend behoefte aan duidelijkheid over de harmonisatie en samenhang.
- Als lokale overheid hebben we te maken met de Gemeenschappelijke Regelingen en Verbonden Partijen/Deelnemingen die deels als zelfstandige eenheid onder de

Cyberbeveiligingswet vallen. Als er veel verschillen zijn tussen de Ministeriële Regelingen, neemt de complexiteit verder toe.

- Ten aanzien van de meldplicht hebben we van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties begrepen dat er bewust voor gekozen is om de Cyberbeveiligingswet letterlijk te vertalen en toevoegingen/verduidelijking te verwerken in de Algemene Maatregel van Bestuur omdat deze dan makkelijker aan te passen is (in tegenstelling tot een wetswijziging vanwege lange doorlooptijd). Maar ook in de Cyberbeveiligingswet staat dat de criteria (dus drempelwaarde) voor meldingen per sector, subsector en soorten entiteit aangepast kan worden door de Ministeriële Regeling van de vakminister. Hierdoor kunnen de drempelwaarden om te melden per sector verschillen. We vinden het een gemiste kans, vanuit cybergevolgbestrijding en het cyberrisicoprofiel van de gemeente, om dit niet in de Algemene Maatregel van Bestuur te regelen. Ook omdat opnemen per Ministeriële Regeling mogelijk een wettelijke grondslag mist om informatie te delen, tenzij dat weer als plicht in de Ministeriële Regeling opgenomen wordt.
- Onduidelijkheid is er ten aanzien van de manier van toezicht op de hiervoor genoemde verschillende normenkaders, hoe wordt dit bijvoorbeeld voor de OT systemen vormgegeven? Hoe wordt in het algemeen de toezichtrol geharmoniseerd?
- Wij willen de noodzaak benadrukken van harmonisatie tussen deze Algemene Maatregel van Bestuur, Ministeriële Regelingen en de eisen vanuit de toezichthouders. Om dit te bereiken verzoeken wij u hier een integrale regeling over op te nemen in het Cyberbeveiligingsbesluit, waarbij duidelijkheid wordt gegeven over hoe risicogebaseerd toezicht onder de Cyberbeveiligingswet zodanig wordt ingericht dat het specifiek, meetbaar, acceptabel, realistisch en tijdgebonden is.

Hoofdstuk 4 – Zorgplicht

Artikel 5 - uitvoering van artikel 21 van de wet

Hoofdstuk 4 bevat concrete verplichtingen ten aanzien van de zorgplicht. Voor overheden geldt dat de zorgplicht wordt ingevuld door de Baseline Informatieveiligheid Overheid (BIO). De in het Cyberbeveiligingsbesluit uitgewerkte zorgplicht betreft een subset van de onderwerpen uit de BIO. De vraag rijst welke waarde wordt gehecht aan de BIO-maatregelen die in het Cyberbeveiligingsbesluit worden genoemd, vergeleken met de BIO-maatregelen die niet zijn opgenomen, gezien de Ministeriële Regeling van BZK nog niet publiek is.
Blijft een deel van de BIO zelfregulering? En wat betekent dit voor toezicht, handhaving en mogelijke sanctionering?
Het bovenstaande heeft gevolgen voor prioritering, het cyberrisicoprofiel en de risicoacceptatie(s) door gemeenten. Het lijkt nu dat gemeenten ten minste moeten doen wat in het Cyberbeveiligingsbesluit staat, en dat daar bovenop passend is wat verder in de BIO staat. Dit levert een ander managementsysteem op met meer en minder essentiële BIO-maatregelen. In deze zelfde lijn wordt meermaals gesproken over aantoonbaarheid. De vraag is dan: aantoonbaar voor wie? Als het gaat om aantoonbaarheid voor het eigen bestuur, vergt dat een andere invulling van het managementsysteem dan aantoonbaarheid voor landelijk toezichthouders.
Eisen aantoonbaarheid zijn nu niet bekend. Wij verzoeken u hiervan duidelijke omschrijvingen op te nemen in de Ministeriële Regeling(en) voor de overheid.

Artikel 9 Bedrijfscontinuïteit en crisisbeheer

In dit Cyberbeveiligingsbesluit wordt ervoor gekozen om de eisen rond continuïteit puur in het perspectief van netwerk- en informatiesystemen te zien. Dat staat haaks op de '*all hazards*-benadering' die in de Cyberbeveiligingswet de basis vormt voor risicomanagement en maatregelen. Waarom is ervoor gekozen hier de eisen zo specifiek te maken? En wat betekent dat voor toezicht bij incidenten? Ook hier wordt er niet specifiek ingegaan op OT-systemen waarvan de levenscyclus afwijkt van IT systemen en mogelijk specifiek zijn.

In sub 3c bij artikel 9 wordt beveiligde noodcommunicatie benoemd. In geval van een GRIP-situatie is de Veiligheidsregio de partij om te voorzien in communicatiemiddelen ten behoeve van het functioneren van de leiding en coördinatie binnen dat spectrum. Zo is er een noodvoorziening voor het regionaal crisiscentrum. Kunt u aangeven waarom voor de beschrijving in sub 3c is gekozen zonder relatie te leggen met de Gecoördineerde Regionale Incidentbestrijdingsprocedure (GRIP)?

Hoofdstuk 5 - Training

Artikel 20 t/m 23 Eisen aan de training, het certificaat en aan de trainer

Artikel 20 geeft aan dat de training elk lid van het bestuur van de essentiële entiteit of belangrijke entiteit in staat stelt om risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren en de gevolgen daarvan voor de diensten die door de entiteit worden verleend te kunnen beoordelen.
Wij vinden het identificeren en beoordelen van risico's primair een taak van de organisatie zelf, waar het bestuur uiteraard goed moet worden geïnformeerd.

De artikelen lijken ook toegeschreven aan IT-omgevingen. De gemeenten beschikken ook over voor OT en moeten voor OT voldoen aan diverse eisen en normeringen. Dit vereist ook een andere aanpak dan voor IT. Wij adviseren om de trainingsartikelen duidelijk voor de OT-omgevingen inhoud te geven.

Wij vinden het opvallend dat hier gekozen wordt voor een onafhankelijke en gekwalificeerde trainer. Daarbij zien wij een aantal aandachtspunten:

- Door eisen te stellen aan een trainer wordt hier impliciet vereist dat de training wordt gegeven door een persoon; wij geven wellicht de voorkeur aan een training in combinatie met gaming, e-learning, of andere (virtuele) technieken.
- Door specifieke eisen aan de training en certificaat mee te geven, zal een markt ontstaan voor onafhankelijke trainingsbureaus en zullen gemeenten een trainer moeten inhuren om onafhankelijkheid aan te tonen. Is dat ook de bedoeling van dit besluit? Zal een toezichthouder vragen stellen als een eigen gekwalificeerde medewerker de training verzorgt? Wij hebben als G4-gemeenten voldoende onafhankelijke ambtenaren die gedegen toelichting en training zouden kunnen verzorgen. Bovendien geven wij de voorkeur aan eigen trainers in combinatie met duurzame en digitale leermiddelen. Zo kan meer specifiek op de eigen organisatie worden ingegaan, met de eigen specifieke risico's, dreigingen en verbetermaatregelen, en wordt het onderdeel van de planning & control-cyclus.
- Voor een benadering vanuit een integrale veiligheidscultuur geven wij de voorkeur aan een *integrale* (bredere) training waarin ook cyberveiligheid met bijbehorende risico's wordt opgenomen.

- Wij stellen voor dat de rijksoverheid centraal de vereiste opleiding aan gemeenten beschikbaar stelt.

Hoofdstuk 6 - Meldingen van significante incidenten, incidenten, bijna-incidenten, significante cyberdreigingen, cyberdreigingen en kwetsbaarheden

Artikel 24 Significante incidenten

De drempelwaarde voor het melden van significante incidenten wordt later nog door de verschillende vakministers vastgelegd in Ministeriële Regelingen. Voor de G4-gemeenten is het belangrijk om vroegtijdig te beschikken over deze drempelwaarden en niet pas vlak voor of na het van kracht worden van de Cyberbeveiligingswet, zodat we ons goed kunnen voorbereiden op het inrichten van de meldplicht.
Kunt u aangeven hoeveel Ministeriële Regelingen wij als gemeenten mogen verwachten en wanneer deze beschikbaar zijn? Daarnaast verzoeken wij om harmonisatie aan te brengen in de omschrijving van drempelwaarden.

Vanuit lokale cybercrisisbeheersing, is in eerdere consultatie op de Cyberbeveiligingswet vanuit het perspectief van G4-OOV (Openbare Orde en Veiligheid) geadviseerd om organisaties niet alleen te laten melden bij effecten op de digitale organisatie en bij effecten op de continuïteit van de dienstverlening, maar ook bij (mogelijke) effecten op de fysieke veiligheid en openbare orde, zodat we ons voor kunnen bereiden op cybergevolgbestrijding. Dit derde criterium is niet overgenomen in het Cyberbeveiligingsbesluit, waarmee het wel of niet toevoegen van dit criterium afhankelijk is per minister en Ministeriële Regeling. Dit lijkt ons niet wenselijk.
Tot slot is er met het ontbreken van dit derde criterium in het Cyberbeveiligingsbesluit ook geen wettelijke grondslag voor de lokale overheid en bevoegd gezag om informatie over (mogelijke) gevolgen voor de fysieke veiligheid en openbare orde te ontvangen. Ook dit is iets wat volgens ons centraal georganiseerd moet worden, in plaats van per Ministeriële Regeling.

Artikel 30 Bewaartermijnen persoonsgegevens

In beginsel voldoet het artikel aan de gestelde eisen om een bewaartermijn van max 60 maanden te geven. Veel loggegevens worden bij leveranciers opgeslagen die het beheer over cybersecuritymaatregelen voeren. Langdurig opslaan van grote hoeveelheden logbestanden gaat gepaard met hoge kosten.
In het Cyberbeveiligingsbesluit wordt voor alle gegevens ook één maximale bewaartermijn vastgesteld maar niet bij alle data wordt goed weergegeven waarom dat echt noodzakelijk is. Dit is wel nodig.
Tevens adviseren wij om per soort data de bewaartermijnen vast te stellen (bijvoorbeeld: loggegevens maximaal 2 jaar, incidentrapportages maximaal 5 jaar, forensisch bewijsmateriaal maximaal 5 tot 7 jaar etc.). Hiermee wordt niet voldaan aan de eisen van dataminimalisatie (zie Algemene verordening gegevensbescherming, Avg) en tegelijkertijd is er een risico dat voor bepaalde dossiers dit misschien wel een te korte bewaartermijn is. Er zou hier dus een balans in moeten komen door een gedifferentieerde aanpak. Wij vragen hier duidelijkheid over aan te brengen, ook in de Ministeriële Regeling van BZK, in lijn met de eisen uit de Archiefwet en de Avg.