Gemeente Amsterdam | Den Haag | Gemeente Rotterdam | Gemeente Utrecht

Reactie op internetconsultatie Cyberbeveiligingswet
Datum: 29 juni 2024
Van: G4-gemeenten (Amsterdam, Den Haag, Rotterdam, Utrecht)

Digitale dreiging vraagt om hoger niveau digitale veiligheid
Digitale dreiging loert in iedere gemeente en in de G4-gemeenten zijn de risico's van een nog grotere orde, onder meer vanwege het grote aantal inwoners, het regionale zorggebied, de internationale havens, vliegvelden en gerechtshoven. Door de toenemende digitalisering en de afhankelijkheid daarvan, maar ook door internationale spanningen, neemt het risico op cyberaanvallen en cybercrises toe en neemt criminaliteit in het digitale domein een vlucht. We zijn daarom blij met de intentie van de Europese NIS2-richtlijn en de nationale vertaling daarvan naar de Cyberbeveiligingswet (hierna: Cbw) om een hoog (gezamenlijk) niveau van cyberbeveiliging in Nederland en de Europese Unie te bereiken.
Met veel interesse hebben we dan ook meegelezen op de concepttekst van de Cbw. Onze zorgen, opmerkingen en behoeften maken we met deze inbreng kenbaar.

In het belang van IT, OT én Openbare Orde & Veiligheid
Deze G4-reactie richt zich enerzijds op de implementatie van de wet door ons als gemeenten ten behoeve van de digitale veiligheid van de interne organisatie en gemeentelijke dienstverlening in de stad en anderzijds op de openbare orde en veiligheid, met inachtneming van de huidige en bijbehorende bevoegdheden, rollen en processen. Het is voor bedrijven, instellingen, bezoekers en bewoners onwenselijk dat er digitale incidenten en crises in onze steden plaatsvindt.

Samengevat richt deze reactie zich op de volgende drie punten:

1. Vanuit het perspectief van de beveiliging van Informatie (IT) en Operationele Technologie (OT) van de gemeente zijn er verschillende op- en aanmerkingen ten aanzien van benodigde randvoorwaarden, de zorgplicht, meldplicht, het toezicht en daarbij de governance:

Randvoorwaarden
Vanuit het landelijk toezicht maakt de Cbw niet voldoende duidelijk hoe de verantwoordelijkheden en aansprakelijkheden bij gemeenten worden belegd. Het is onduidelijk hoe ‘het bestuur’ hier geïnterpreteerd moet worden – ambtelijk of bestuurlijk.
Het doel van NIS2 is onder andere harmonisatie in toepassing van de wet binnen de EU, maar lidstaten passen NIS2 verschillend toe als het gaat om decentrale overheden. Dat vormt een risico.
Er is bij de Cbw onduidelijkheid in normenkaders en standaarden, waardoor uitvoering van de wet niet goed kan worden ingeschat.
Het ontbreken van middelen voor implementatiekosten voor decentrale overheden blijft onderbelicht.
Een uitvoeringstoets is noodzakelijk, maar ontbreekt in het huidige voorstel.

Zorgplicht en meldplicht
De wet, en dus ook de zorgplicht, heeft alleen betrekking op netwerk- en informatiesystemen. Dat zien wij als een gemiste kans, we hadden graag gezien dat alle digitale infrastructuur expliciet onderdeel was geweest van de wet.
De maatregelen worden vastgesteld per Algemene Maatregel van Bestuur (hierna: AMvB), waar wij het risicomanagement willen laten prevaleren.
Er zijn zorgen over de uitvoerbaarheid van de meldplicht zoals deze in de Cbw wordt voorgesteld. Wij verzoeken u de meldplicht zoveel mogelijk te vereenvoudigen en efficiënt in te richten.

Toezicht en governance
Naast benodigde verhoogde aandacht voor digitale dreigingen zien we ook de verhoogde

administratieve last voor toezicht en compliance. We moeten oog blijven houden voor de balans tussen het primaire proces en de bedrijfsvoering rond digitale weerbaarheid. Daarnaast is de governance onduidelijk. Kwetsbaarheden in de toeleveringsketen is een groot risico, maar de eisen rondom toezicht door een gemeente op alle leveranciers en hun onderaannemers op het niveau van specifieke kwetsbaarheden zoals dat nu wordt voorgesteld is niet uitvoerbaar.

2. Vanuit het perspectief van openbare orde en veiligheid (hierna: OOV) in de steden:

Gemeentelijke en regionale crisisorganisaties, bestaande uit de hulpdiensten en gemeenten binnen die veiligheidsregio, opererend onder het gezag van de burgemeester of voorzitter veiligheidsregio, dienen in het belang van de lokale en regionale openbare orde en veiligheid in staat te worden gebracht om invulling te geven aan (de voorbereiding op) cybergevolgbestrijding. Het wettelijk kader dient hiervoor de juiste bevoegdheden en mogelijkheden voor informatiedeling te bevatten, maar duidelijkheid over bijvoorbeeld de wettelijke grondslag om lokale overheid en bevoegd gezag informatie over (mogelijke) gevolgen voor de fysieke veiligheid en openbare orde te ontvangen lijkt in de Cbw concepttekst te ontbreken. In het geval van de Cbw concepttekst gaat het ten minste om de in de bijlage benoemde aandachtspunten.

De Cbw zal in de huidige opzet van toepassing zijn op een groot aantal organisaties binnen de gemeentegrenzen van de G4. Tegelijkertijd zijn er nog veel meer organisaties binnen de gemeenten, waarvan een groot deel MKB, die niet rechtstreeks onder de Cbw vallen. Deze organisaties zijn wellicht op Europees of nationaal niveau niet ‘essentieel’ of ‘belangrijk’, maar kunnen lokaal wél van cruciaal belang zijn voor onze inwoners en het ordentelijk functioneren van de stad. Onlangs bracht de Cyber Security Raad een advies uit waarin zij waarschuwen voor deze cyberweerbaarheidskloof en het risico hiervan op maatschappelijke ontwrichting. Op welke ondersteuning mogen deze organisaties rekenen vanuit de samenwerkende overheden? Wat is het minimumniveau waaraan deze organisaties voor cyberbeveiliging moeten voldoen? Is het mogelijk om in deze wet ook aandacht te besteden aan deze groep organisaties en de rol van de overheid richting deze groep?

3. Vanuit het perspectief van financiële middelen en risico's:

In algemene zin geldt dat het voor instemming met deze wet randvoorwaardelijk is dat de decentrale overheden ook financieel in staat worden gesteld om te zorgen voor de implementatie van de Cbw. Dit punt is in de conceptwettekst helaas nog onderbelicht, terwijl het op dit moment aan de middelen voor implementatie ontbreekt. Middels een uitvoeringstoets op de uiteindelijke Cbw en de bijbehorende AMvB’s kan pas worden onderzocht hoeveel middelen er exact nodig zijn. Een eerste inschatting op basis van de kengetallen uit de praktijk toont dat er extra middelen nodig zijn om op lokaal niveau de digitale veiligheid te verhogen.

We zien de reactie op onze inbreng in deze internetconsultatie van harte tegemoet en gaan indien gewenst graag nader in gesprek om onze punten verder toe te lichten.

Namens de G4-gemeenten,

CIO’s en OOV-directeuren gemeente Amsterdam, Den Haag, Rotterdam, Utrecht

In de bijlage vindt u deze punten uitgewerkt in de delen Randvoorwaarden, Zorgplicht, Meldplicht en Toezicht en Governance.

BIJLAGE

- Deel 1: Opmerkingen rondom randvoorwaarden
- Deel 2: Opmerkingen rondom zorgplicht
- Deel 3: Opmerkingen rondom meldplicht
- Deel 4: Opmerkingen rondom toezicht en governance

Deel 1: Randvoorwaarden

Geen harmonisatie in toepassing van de wet voor decentrale overheden *(perspectief: informatieveiligheid)*
Als doel bij de Cbw wordt het streven uit de NIS2-richtlijn tot verdere marktharmonisatie als centraal thema in paragraaf 2.1 benoemd. De gefragmenteerde interpretatie vanuit de NIS1-richtlijn wordt expliciet onwenselijk verklaard. In dit kader kijken wij met enige verbazing naar de manier waarop deze wet bij verschillende lidstaten van toepassing wordt verklaard op decentrale overheidspartijen. Hoewel wij slechts de beschikking hebben tot een beperkt aantal conceptteksten valt het op dat bijvoorbeeld Duitsland deze vraag doorspeelt aan de individuele bondsstaten.

Hoewel de G4-steden een betere verankering van cyberveiligheidseisen toejuichen, vragen wij ons af in hoeverre er stilgestaan is bij het effect dat deze keuzes hebben voor het centrale thema van marktharmonisatie. Nederlandse gemeenten hebben een groot aantal leveranciers, zowel op het gebied van ICT als andere dienstverlening die door deze keuze onderworpen gaan worden aan veel strengere leveringseisen. Door hier geen eenduidige Europese keuze in te maken ontstaat een serieus risico op ernstige marktverstoring doordat leveranciers in Nederland aan hogere eisen worden onderworpen dan in andere EU-lidstaten. Dit lijkt niet consistent met de doelstellingen zoals opgenomen in de Memorie van Toelichting (hierna: MvT).

Onduidelijkheid in normenkaders en standaarden *(perspectief: informatieveiligheid)*
Wij merken meerdere onduidelijkheden op en verzoeken u deze nader toe te lichten.
In de MvT 4.11 (Hoofdlijnen in de wet, nadere uitwerking in lagere (sectorale) regelgeving) wordt de mogelijkheid voor sectorspecifieke regels genoemd, zoals sectorspecifieke drempelwaarden voor het bepalen van incidenten die meldplichtig zijn. In MvT 5.3.6 (Europese en internationale normen) staat dat entiteiten eigen normenkaders kunnen ontwikkelen, gewoonlijk te baseren op de standaard ISO 27000-serie. Tevens staat er *“Het voldoen aan een eigen normenkader betekent op zichzelf niet dat een entiteit aan de zorgplicht van artikel 23 van dit wetsvoorstel voldoet.”*

In MvT 5.3.5 (Delegatie van regelgevende bevoegdheid) wordt beschreven dat voor de zorgplicht onder de Cbw bijvoorbeeld ook de NEN-7510 normen als verplichting kunnen worden toegevoegd voor de zorgsector. Gemeenten vallen deels onder de zorgsector en deels onder de zorgplicht van andere AMvB’s.

In de MvT wordt tevens aangegeven dat *“het is aan de toezichthouder om te beoordelen of de maatregelen die entiteiten hebben genomen om hun weerbaarheid te waarborgen voldoende zijn om de risico’s te mitigeren”.*
In dat geval is het wenselijk dat de criteria waaraan moet worden voldaan duidelijk is.

Gemeenten werken met de Baseline Informatiebeveiliging Overheid (BIO) v1.4, welke op dit moment wordt geactualiseerd naar de BIO 2.0. De opzet en structuur van de BIO2.0 is cf de internationale IB standaard 27001. Inhoudelijk wordt in de BIO2.0 op diverse normen verwezen naar “basishygiëne NIS2”. In de Cbw wordt dat niet expliciet benoemd.

Artikel 5.7.9. (Bindende aanwezig) beschrijft dat er een bindende aanwijzing kan komen om te voldoen aan een norm. Hierbij is niet uitgewerkt aan welk normenkader wordt getoetst, de Cbw, de ISO27001 of de sectorspecifieke normenset kan van toepassing zijn en verschillen.

Voor gemeenten zijn nog andere normenkaders van belang:

- De CSIR wordt gebruikt als vastgestelde implementatie richtlijn voor Operationele Technologie (OT).
- De IEC 62443 wordt gebruikt voor industriële controlesystemen (ICS/PA)
- De NEN7510 en NTA 7516 worden gebruikt voor het zorgdomein.
- De SSD, NPR5326, IEC25010 en de ICT-beveiligingsrichtlijnen voor webapplicaties en de aansluitvoorwaarden DigiD worden gebruikt voor het veilig ontwikkelen van software en voor het ontwikkelen van veilige en toegankelijke websites.

Het is niet duidelijk welke normenset als leidend gezien moet worden om te voldoen aan de zorgplicht onder de Cbw. Is een sectorale normenset die qua opzet gelijk is aan de internationale standaard in die vorm geschikt om toe te voegen?

Wellicht wordt artikel 21, tweede lid van de NIS2-richtlijn, waarin de maatregelen voor het beheer van cyberbeveiligingsrisico's worden benoemd, bij artikel 23 lid 1 Cbw betrokken. Een entiteit moet weten aan welke vereisten moet worden voldaan.

Rollen & verantwoordelijkheden *(perspectief: informatieveiligheid)*
De invoering van de Algemene Verordening Gegevensbescherming (AVG) heeft destijds een groot aantal vragen opgeworpen over de manier waarop organisaties informatie met elkaar mogen uitwisselen en samen mogen verwerken. Veel van deze vragen zijn tot de dag van vandaag slechts in beperkte mate beantwoord.

Artikel 6 roept de situatie in het leven waar partijen die niet onder de NIS2 vallen (zoals politie) samen moeten werken en informatie moeten uitwisselen met partijen die hier wel onder vallen (zoals gemeenten). Om onduidelijkheden zoals deze onder de AVG bestaan te voorkomen zou het wenselijk te zijn ergens in de MvT het uitgangspunt op te nemen dat de Cbw niet poogt om beperkingen op te leggen aan dergelijke informatie-uitwisselingen. Dan wel dat partijen die wel onder de NIS2 vallen er vanuit mogen gaan dat partijen die onder artikel 6 van de Cbw vallen aan een met de NIS2 vergelijkbaar regime zijn onderworpen.

In de BIO worden de rollen en verantwoordelijkheden benoemd voor een aantal functies. Wij vinden het vreemd dat dit niet is opgenomen in de wet zelf. Specifiek de CISO-rol, bijvoorbeeld zoals opgenomen in de BIO: *"Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel en deze CISO heeft een onafhankelijke positie binnen de organisatie hiërarchie t.o.v. het lijnmanagement zodat de CISO vrij kan rapporteren aan het bestuur en of het controlerend orgaan."*
Daarnaast is ook de rol van de toezichthouder (controlerend orgaan) en het stelsel van toezicht niet helder omgeschreven. Wij hadden dat wel verwacht in de Memorie van Toelichting.

Ontbreken van aandacht voor uitvoeringslast en hoge implementatiekosten *(perspectief: informatieveiligheid)*
Met de Cbw wordt voor gemeenten voor het eerst een organisatiebreed wettelijk afdwingbaar kader vastgesteld die de informatieveiligheid bij gemeenten regelt. Gemeenten zien zich daarbij geconfronteerd met een aantal stapelende omstandigheden:

- De toetsing op het onderliggende kaders en normen, zoals de BIO of ISO27001 en/of de NEN7510 en/of de CSIR of meer, wordt de komende jaren aangescherpt met uitbreiding naar werking;
- Een groot gedeelte van de toeleverancierskketen van gemeenten worstelt nu al met het voldoen aan de gestelde normen (leveranciersproblematiek);

- De gemeenten worden zelf geconfronteerd met forse bezuinigingen;

Deze omstandigheden leiden er samen toe dat naar ons inzicht de gestelde toename van kosten van naar alle waarschijnlijkheid onvoldoende zal zijn om aan de gestelde norm te voldoen. Een aanzienlijke toename van budgetten voor het verhogen van de digitale weerbaarheid zal noodzakelijk zijn om het door de Europese Commissie als noodzakelijke investeringsniveau te realiseren. In een tijd van bezuinigen is dit lastig te realiseren.

Daarbij zijn wij van mening dat de uitvoeringslast voor decentrale overheden in de MvT onderbelicht blijft. We verwachten dat dit gebrek significante gevolgen zal hebben voor de mate waarin wij als gemeenten in staat zullen zijn deze wetgeving te implementeren. We roepen daarom op om in overleg met de VNG passende middelen vrij te maken om deze implementatie te ondersteunen. Daarbij kan een uitvoeringstoets op niveau van gemeenten helpen. In het stuk van de Europese Commissie is hiervoor een methode1 benoemd.

Aansprakelijkheid en financieel risico (*Perspectief van Openbare Orde en Veiligheid/cybergevolgbestrijding)*
Hoe is aansprakelijkheid en financieel risico geregeld met partijen waar wij als lokale overheid aandeelhouder van zijn? Bijvoorbeeld bij de vervoersbedrijven.

Deel 2: Zorgplicht

Artikel 23 – OT en IT *(perspectief: informatieveiligheid)*
In de definities en in artikel 23 lid 1 wordt duidelijk dat de wet, en dus ook de zorgplicht, alleen betrekking heeft op netwerk- en informatiesystemen. Dat zien wij als een gemiste kans, we hadden graag gezien dat alle digitale infrastructuur expliciet onderdeel was geweest van de wet. Wel geeft de MvT aan dat zowel IT als OT bedoeld wordt, maar dat volgt niet duidelijk uit de wet.

Artikel 23 – maatregelen versus risico's *(perspectief: informatieveiligheid)*
Zoals toegelicht is de impact van de Cbw op gemeenten groot. Het is daarbij onwenselijk dat aan de voorkant onduidelijk is welke eisen er precies aan gemeenten gesteld gaan worden. We begrijpen de keuze voor de AMvB maar tegelijkertijd blijft lid 4 als een zwaard van Damocles boven het onderwerp hangen. Gezien de budgettaire druk die aanvullende eisen in veel gevallen zullen opleveren is het gepast dat de extra maatregelen die genomen moeten worden, ook goedgekeurd worden in het democratische proces. De doelstelling van de wetgeving – meer harmonisatie en basis beveiligingsmaatregelen – wordt daarmee niet gehaald. Iedere sector, subsector en type entiteit krijgt een of meerder eigen set(s) aan beveiligingsmaatregelen waaraan voldaan moet gaan worden. Dat is onwenselijk en niet in lijn met de evaluatie van de huidige BIO.

Tegelijkertijd zien wij hier een mogelijkheid om verschil te maken in de regeldruk tussen de grotere en kleinere gemeenten. Het is bijvoorbeeld niet realistisch om de kleinste gemeenten aan dezelfde eisen te onderwerpen als de G4-gemeenten en gezien de risico's waarschijnlijk ook niet nodig. Risicomanagement zoals genoemd in het 2e en 3e lid moeten prevaleren boven afvinklijstjes. Wij roepen op tot het (toewerken naar) toepassen van een eenduidige Europese aanpak voor risicomanagement die aansluit bij internationale standaarden, zoals het ENISA framework of ISO/IEC 27x.

Artikel 23 – toeleveringsketen *(perspectief: informatieveiligheid)*
In de Memorie van Toelichting wordt aangegeven dat de zorgplicht ook geldt voor de directe toeleveringsketen

[1] Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union | Shaping Europe's digital future (europa.eu)

en dat essentiële entiteiten rekening moeten houden met specifieke kwetsbaarheden, kwaliteit en risicobeoordelingen van de directe leveranciers. Dat is niet reëel en doet bovendien af aan de verantwoordelijkheid van deze leveranciers zelf. Als opdrachtgever zouden wij de kwaliteit en het managementsysteem moeten toetsen in een periodieke cyclus (zoals nu al verplicht onder de BIO), maar de uitbreiding naar specifieke kwetsbaarheden en eigen risicobeoordelingen is een te grote administratieve lastenverzwaring die bovendien weinig extra veiligheid oplevert.

Ten aanzien van de beveiliging van de toeleveringsketen (punt d) wordt in artikel 21, tweede lid, onderdeel d, en derde lid, NIS2-richtlijn aangegeven dat dit met inbegrip is van aan beveiliging gerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners. Wanneer essentiële entiteiten en belangrijke entiteiten overwegen welke maatregelen in dit verband passend zijn, moeten zij rekening houden met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures. Ook houden zij rekening met de resultaten van gecoördineerde risicobeoordelingen van kritieke toeleveringsketens als bedoeld in artikel 22 NIS2- richtlijn. Ten aanzien van de beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen (punt e) is in artikel 21, tweede lid, onderdeel e, NIS2-richtlijn bepaald dat dit 22 met inbegrip is van de respons op en de bekendmaking van kwetsbaarheden.
Dit betekent een forse impact op de gemeentelijke processen rondom inkoop en contractmanagement. Een tijdspad wanneer gemeenten zouden moeten voldoen is echter niet gegeven.

Deel 3: Meldplicht

Artikel 17 - Aanwijzing en taken CSIRT *(perspectief: openbare orde en veiligheid)*
Op te merken is dat wanneer een belangrijke of essentiële entiteit kennis heeft gekregen van een significant incident, zij dit bij hun Computer Security Incident Response Team (hierna: CSIRT) binnen 72 uur moeten melden. Het lijkt ons wenselijk dat de CSIRT dergelijke melding binnen een korte periode afhandelt, zodat (dreigings)informatie binnen de CSIRT snel gedeeld kan worden. Er staat echter geen tijdsaanduiding bij waaruit blijkt dat informatie wordt teruggegeven binnen de CSIRT, dit bevelen wij wel aan om de impact van een incident zoveel mogelijk in te perken.

Artikel 22 - Nationaal register van entiteiten *(perspectief: openbare orde en veiligheid)*
Er wordt een nationaal register van entiteiten opgesteld van essentiële en belangrijke entiteiten. Wij vragen ons echter af of het voldoende geborgd is dat essentiële en belangrijke bedrijven zich melden bij de CSIRTS? Hoe zorgt het Rijk dat bedrijven die eerder niet onder NIS1, maar wel onder NIS2, vallen weten dat ze zich moeten registeren?

Binnen de nationale crisisstructuur wordt van de regionale crisisorganisaties, bestaande uit de hulpdiensten en gemeenten binnen die veiligheidsregio, verwacht dat zij bevorderen dat risicovolle objecten en partners in haar regio zelf zorgdragen voor een goede digitale weerbaarheid en herstelvermogen. Tevens wordt verwacht dat regionale crisisorganisaties in samenwerking met partners de mogelijke maatschappelijke impact van een digitaal incident in hun regio duiden. Om deze activiteiten uit te kunnen voeren dienen lokale overheden toegang te hebben tot het register van belangrijke en essentiële entiteiten, zodat zij hun regionaal en stedelijk risicoprofiel compleet kunnen maken, risicoanalyses uit kunnen voeren en zich goed voor kunnen bereiden op cybergevolgbestrijding. Dit raakt eveneens aan de voor gemeenten benodigde informatievoorziening zoals besproken in artikelen 27, 29 en 41 (zie onderstaand).

Artikel 27 en verder *(perspectief: informatieveiligheid)*
Uiteraard onderschrijven we het nut van het snel inlichten van het verantwoordelijke Cert om schade bij andere organisaties te voorkomen of beperken. Maar de impact van deze maatregel op organisaties blijft nu onderbelicht.

De wettekst is onduidelijk over de uitvoerbaarheid van de meldplicht. In de Memorie van Toelichting op de wet staat vermeld dat meerdere artikelen, zoals die over de meldplicht, een delegatiegrondslag bevatten voor het bij of krachtens algemene maatregel van bestuur kunnen stellen van regels. Die grondslag biedt mogelijkheden om met sectorspecifieke regels te komen. Een dergelijke uitwerking van de meldplicht is nog niet beschikbaar, waardoor wij uitvoerbaarheid van de meldplicht niet goed kunnen inschatten.
Wij hebben meerdere zorgen en/of opmerkingen over deze onduidelijkheden, die wij hieronder nader omschrijven:

- **Melden binnen 24 of 72 uur niet realistisch**
  Bij ontdekking van een cyberbeveiligingsincident is het niet altijd mogelijk om snel de significantie van het incident in te schatten. Alleen al om die reden lijkt het verplichten om een melding binnen 24 uur of zelfs binnen 72 uur te doen ons niet realistisch. Daarnaast zijn er veel leveranciers/dienstverleners die geen 24x7 ondersteuning kunnen bieden, of waarbij de die ondersteuning extra kosten met zich meebrengt. Vanaf de ontdekking van een cyberbeveiligingsincident, zal alle capaciteit zich moeten richten op het beperken van de impact. Een korte meldingsplichttermijn zorgt voor het onnodig wegtrekken van capaciteit uit het crisisteam.
- **Drempelwaarde voor significante meldingen onbekend**
  Onduidelijk is wanneer een incident een significant incident betreft. Wilt u dat verduidelijken zodat wij het uitvoering geven aan deze meldplicht kunnen inschatten.
- **Melden van niet-significante meldingen onduidelijk**
  Gemeenten melden tot nu toe informatiebeveiligingsincidenten die mogelijk ook effect hebben op andere gemeenten of organisaties bij de sectorale CSIRT, de Informatiebeveiligingsdienst voor gemeenten (IBD). Het is onduidelijk hoe het melden van cyberincidenten onder de Cbw gaat plaatshebben, bijvoorbeeld in gevallen waarbij een incident in eerste instantie niet significant lijkt te zijn maar dat later wel blijkt te zijn, of als het gaat om cyberincidenten die niet typische informatiebeveiligingsincidenten blijken te zijn.
  Maak duidelijk wat in welke situaties bij welke instantie gemeld moet worden. Daarbij geven de G4-gemeenten vanwege eenduidigheid de voorkeur aan het melden van alle cyberincidenten bij één meldpunt, namelijk het Nationaal Cyber Security Centrum (hierna: NCSC) als nationale CSIRT.
- **Melden bij meerdere instanties niet efficiënt**
  Er wordt uitgegaan van het melden van significante incidenten aan zowel de sectorale CSIRTs, de landelijke CSIRT, als de toezichthouder(s). In de MvT wordt gesproken over een dubbele meldplicht. Daarnaast kan het ook nog zo zijn dat het incident een datalek betreft, waardoor ook aan de Autoriteit Persoonsgegevens een melding moet worden gedaan.
  Dit is een ongewenste situatie. Wanneer zich een al dan niet significant incident voordoet, is er doorgaans geen tijd voor zoveel administratieve lasten. Wij verzoeken u de meldplicht efficiënt in te regelen zodat wij als gemeenten aan de meldplicht kunnen voldoen.
- **Meldplicht is onduidelijk bij een incident in een toeleveringsketen**
  De wet is onduidelijk wie meldplichtig is bij een al dan niet significant incident dat zich in een toeleveringsketen voordoet. Als een dienstverlener in de toeleveringsketen zelf meldplichtig is, bij wie wordt dan gemeld? De sectorale of de landelijke CSIRT? Wilt u dat verduidelijken?
- **Gegevensdeling tussen CSIRTS en mogelijk andere organisaties onbekend**
  Welke gegevens worden gedeeld tussen nationale CSIRT, een of meerdere sectorale CSIRTs en internationale CSIRTs op basis van gedane meldingen? Mogelijk betreft het hoog gevoelige kwetsbaarheden. Welke classificatie is van toepassing? Wie wordt geïnformeerd als er gegevens

worden gedeeld? In welke taal worden gegevens gedeeld en op welke wijze wordt omgegaan met verschillende talen bij gegevensdeling?

- **Bewaren van de meldingsinformatie onbekend**
  De wet is onduidelijk over hoe lang de informatie van een melding wordt bewaard en wanneer die wordt verwijderd, ook in het geval dat de informatie met andere instanties wordt gedeeld.
  En welke classificatie is van toepassing? Wilt u dat verduidelijken?
- **Mogelijkheden voor incident-respons onduidelijk**
  Het is onduidelijk welke mogelijkheden het NCSC en sectorale CSIRTs bieden op het gebied van incident-respons. Wilt u dit verduidelijken?
- **Mogelijkheden voor makkelijk melden onduidelijk**
  Voor een efficiënt proces ten aanzien van melden zou een Application Program Interface (api) gewenst zijn. Dit voorkomt meervoudig registreren. Een incident is uiteraard al eerder intern bij een organisatie geregistreerd.
  Wilt u aangeven of het mogelijk is meldsystemen met elkaar te verbinden?
- **Eindverslag melding**
  In een eindverslag staan mogelijk hoog gevoelige kwetsbaarheden of gevoelige informatie vermeld. Welke classificatie wordt gehanteerd bij het delen van deze informatie? Wie wordt geïnformeerd als er een eindverslag wordt gedeeld? Op welke wijze kan deze informatie veilig worden gedeeld?
  Hoe lang worden gegevens bewaard?

Artikel 27 – Meldplicht significante incidenten: ontbreken (mogelijke) effecten op de fysieke veiligheid en openbare orde) *(perspectief: openbare orde en veiligheid)*
Om te bepalen of een incident significant is, zijn in artikel 23, derde lid, NIS2-richtlijn drie parameters opgenomen. Deze parameters zien toe op een (mogelijke) ernstige operationele verstoring van de diensten, (mogelijke) financiële verliezen voor de betrokken entiteit en het (mogelijk) treffen van andere natuurlijke personen of rechtspersonen door aanzienlijke materiële of immateriële schade. Of een verstoring van diensten ernstig is, is bedrijfs- en ketenafhankelijk. Daarnaast missen wij in deze parameters de impact van het incident op de openbare orde en veiligheid. In het landelijk crisisplan digitaal (LCD) wordt aangegeven dat bij melding van een incident dient uitgegaan te worden van:

- Effecten op de digitale organisatie
- Effect op de continuïteit van de dienstverlening en
- (Mogelijke) effecten op de fysieke veiligheid en openbare orde

Wij missen deze laatste parameter in de meldplicht van significante incidenten en adviseren met klem om deze toe te voegen.

Artikel 29 - Melding, update en initiële beoordeling *(perspectief: openbare orde en veiligheid)*
De melding van een significant incident bij desbetreffende CSIRT en bevoegde autoriteit is erg gericht op de sectorale aanpak. Hoe verhoudt deze zich tot de verantwoordelijkheden zoals beschreven in de gemeentewet of de wet veiligheidsregio's?

Artikel 41 - Informatieverstrekking over gemelde significante incidenten, incidenten, bijna incidenten en cyberdreigingen: missen duiding voor (mogelijke) gevolgen voor openbare orde en grondslag om informatie te ontvangen als lokale overheid *(perspectief: openbare orde en veiligheid)*
De melding en afhandeling bij CSIRT is volgens ons gericht op de technische incidentresponse. De melding die gedaan wordt bij het NCSC als centraal contactpunt, moet in onze ogen ook getoetst zijn op de mogelijke effecten op de fysieke veiligheid en nadere duiding van de openbare orde (zie opmerking onder artikel 27). Een

CSIRT kan deze gevolgen in de openbare ruimte niet altijd overzien. Het lijkt ons daarom wenselijk om het proces zo in te richten dat deze duiding gemaakt wordt en CSIRT hierbij geholpen wordt.

Daarnaast willen we als gemeentelijke en regionale crisisorganisaties, bestaande uit de hulpdiensten en gemeenten binnen die veiligheidsregio, opererend onder het gezag van de burgemeester of voorzitter veiligheidsregio, bovengenoemde meldingen (dat wil zeggen: meldingen met betrekking op (mogelijke) effecten op de fysieke veiligheid en openbare orde) ontvangen om invulling te geven aan (de voorbereiding op) cybergevolgbestrijding. In de Cbw zien wij echter niet terug van welke wettelijke grondslag wij gebruik mogen maken om als lokale overheid en bevoegd gezag deze informatie te ontvangen van het NCSC om, situationeel afhankelijk in samenwerking met de veiligheidsregio's, de cybergevolg bestrijding goed in te richten. Wij zien deze grondslag graag toegevoegd, om te zorgen dat wij als lokale overheid de juiste bevoegdheden en mogelijkheden voor informatiedeling hebben. Zie ook opmerking bij artikel 29.

Deel 4: Toezicht & governance

De uitvoering van de Cbw betekent voor gemeenten een aanzienlijke administratieve lastenverzwaring om aantoonbaar te kunnen voldoen. Een groeipad hiervoor ontbreekt. Wij verzoeken u een realistisch tijdspad aan te geven, ook in relatie tot het toezicht van de landelijk toezichthouder.

Artikel 26 - Governance *(perspectief: informatieveiligheid)*

Artikel 26 lid 8 regelt dat de verplichtingen uit artikel 26 lid 2 tot en met 6 liggen bij de ambtelijke top. De onderbouwing in de memorie van toelichting beschouwend zetten wij vraagtekens bij de manier waarop het nu in de Cbw terecht is gekomen:

- De MvT stelt onder 5.4 onder *Bestuur overheidsorganisaties* dat het bestuur risicobeheersingsmaatregelen goedkeurt en toeziet op de uitvoering hiervan. Verder stelt het dat deze verplichtingen niet goed passen bij politiek benoemde ambtsdragers en dat het ook niet past om politiek benoemde ambtsdragers te sanctioneren bij het niet voldoen aan de richtlijn.
- De kanttekening die kan worden gemaakt bij het beleggen van verantwoordelijkheid bij de ambtelijke leiding is dat de ambtelijke leiding niet gaat over de beschikbare budgetten van de gemeente; dit blijft voorbehouden aan het college van B&W en gemeenteraad. De ambtelijke leiding krijgt via deze wet extra verplichtingen, maar is voor een goede nakoming van deze verplichtingen afhankelijk van budgettaire beslissingen van het college en raad.
- In de volgende alinea stelt de MvT dat "Het feit dat deze organen zijn aangemerkt als het bestuur van die overheidsinstanties, brengt dus geen wijziging in het aansprakelijkheidsregime voor die organen". Voor zover de wetgever het dus niet gepast vindt dat politiek benoemde ambtsdragers gesanctioneerd kunnen worden, maakt het dus niet uit of ze al dan niet als bestuurder onder de Cbw worden aangemerkt. Immers het verandert niets aan het al bestaande regime.
  Belangrijker is echter dat artikel 26 lid 1 en 7 uitgezonderd zijn van artikel 26 lid 8. Artikel 26 lid 1 regelt wie verantwoordelijk is voor het daadwerkelijk vaststellen van maatregelen. Nu artikel 26 lid 1 expliciet geen onderdeel van artikel 26 lid 8 is kunnen wij niet anders dan concluderen dat het de bedoeling is geweest van de wetgever om die bevoegdheid expliciet niet neer te leggen bij de ambtelijk top.
  Verder regelt artikel 26 lid 7 dat de verplichtingen uit 26 lid 2, 3 en 4 hoofdelijk rust op elk lid van het bestuur. Door dit niet onderdeel te laten zijn van artikel 26 lid 8 kunnen wij niet anders dan redeneren dat het de bedoeling is om deze verplichtingen niet op elk lid van de ambtelijke top van toepassing te verklaren. Daarmee menen wij dat artikel 26 lid 8 per abuis het tweede tot en met zesde lid aanwijst waar het eerste tot en met zevende lid had moeten staan.

- Artikel 26 gaat over de verplichtingen van het bestuur (en de leden) van een essentiële (voor de gemeente van belang) entiteit. Er ontstaat verwarring nu de gebruikte terminologie anders is dan in artikel 20, het governance artikel, van de Nis2-richtlijn. In dat artikel wordt gesproken over bestuursorganen en dus niet het bestuur. Uit artikel 26 lid 8 Cbw blijkt dat het bestuur bestaat uit de ambtelijke leiding. Voor de Rijksoverheid is dit de Secretaris Generaal en in gemeenten is dat de gemeentesecretaris (algemeen directeur) en de concerndirecteur (zie hiervoor artikel 1 van de regeling organisatie 2016 | Lokale wet- en regelgeving (overheid.nl).
- Daarnaast zetten we vraagtekens bij het uitgangspunt dat het niet passend is om ambtsdragers zoals wethouders te onderwerpen aan een cursus informatieveiligheid. Al jaren wordt er in het maatschappelijke debat beklag gedaan over de beperkte IT-kennis bij bestuurders op alle niveaus. Deze wet geeft een geweldige kans om hier verandering in te brengen.
- Daarnaast is het de vraag of de opgelegde verplichtingen (waaronder het opleggen van het volgen van een opleiding, de vereiste mate van deskundigheid aan de ambtelijke leiding effectief en wenselijk is. De taak van het management is toch een andere. Het is wenselijk als duidelijkheid wordt gegeven hoe 'het bestuur' geïnterpreteerd moet worden.

Aansprakelijkheid: tegenstrijdigheid in de richtlijn

Ten aanzien van de aansprakelijkheid merken we het volgende op: de richtlijn zorgt enerzijds dat de leden van het bestuur aansprakelijk gesteld moeten kunnen worden (art. 20 lid 1 en 32 lid 6), en anderzijds dat de nationale regels voor aansprakelijkheid van overheidsfunctionarissen niet veranderen door de richtlijn.