Aan de leden

Datum
14 augustus 2026

Ons kenmerk
U202600341
Lbr. 26/031

Telefoon
070-3738393

Onderwerp
Inwerkingtreding van de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten - gevolgen voor gemeenten bestuurders en organisatie

Geachte leden van college en gemeenteraad,

De Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke) treden op 15 augustus 2026 gelijktijdig in werking. Met deze wetten zijn de Europese NIS2-richtlijn (Network and Information Security Directive) en de CER-richtlijn (Critical Entities Resilience Directive) in Nederland ingevoerd.

De wetgeving past in een bredere Europese ontwikkeling. Overheden en essentiële organisaties moeten beter bestand zijn tegen cyberdreigingen, digitale verstoringen en sabotage. Internationale spanningen laten zien hoe belangrijk digitale en fysieke weerbaarheid zijn voor een goed werkende overheid en voor de continuïteit van maatschappelijke dienstverlening.

Gemeenten spelen hierin een belangrijke rol. Zij voeren maatschappelijke taken uit en zijn sterk afhankelijk van digitale dienstverlening, leveranciers en ketenpartners. De wetgeving brengt nieuwe verantwoordelijkheden met zich mee. Tegelijk biedt zij gemeenten de kans om hun dienstverlening blijvend veiliger, betrouwbaarder en weerbaarder te maken.

De wetgeving kent geen overgangstermijn. Vanaf de datum van inwerkingtreding gelden alle verplichtingen direct. Niet-naleving kan leiden tot sancties en gevolgen hebben voor de digitale weerbaarheid van uw gemeente. Met deze brief informeren we u over wat dit betekent voor het college van burgemeester en wethouders en voor de gemeenteraad.

Impact op de gemeentelijke dienstverlening

Digitale verstoringen kunnen de gemeentelijke dienstverlening en publieke voorzieningen ernstig raken. Het gaat daarbij niet alleen om IT-systemen, zoals burgerzaken- en financiële systemen. Ook operationele technologie (OT) speelt een rol: digitale systemen die fysieke processen aansturen, zoals verkeersregelinstallaties, bruggen en sluizen. Als deze systemen uitvallen of verstoord raken, kan dat direct gevolgen hebben voor inwoners en ondernemers, de uitvoering van gemeentelijke taken en de openbare orde en veiligheid.

Ook incidenten bij leveranciers en ketenpartners kunnen grote gevolgen hebben voor de dienstverlening en bedrijfsvoering van gemeenten. De nieuwe wetten vragen expliciet aandacht

voor de beveiliging en continuïteit van zowel IT- als OT-systemen en voor het beheersen van risico's in de keten.

Wat betekent dit voor u als bestuurder?

Voor het college van burgemeester en wethouders
Het college is primair verantwoordelijk voor de naleving van de wetten. Daarmee is het ook verantwoordelijk voor de bestuurlijke sturing op digitale weerbaarheid en de continuïteit van gemeentelijke processen en dienstverlening. Dit vraagt om actieve sturing op cyberrisico's, als onderdeel van het integrale risicobeheer, de governance en de bestuurlijke besluitvorming.

Het college is verantwoordelijk voor passend beleid met een duidelijke visie op digitale weerbaarheid. Het zorgt ervoor dat in de begrotingscyclus voldoende financiële en personele middelen beschikbaar zijn. Daarnaast richt het de organisatie zo in dat verantwoordelijkheden helder zijn belegd en de benodigde deskundigheid aanwezig is. Het college treedt op als risico-eigenaar, stelt de risicobereidheid vast en keurt de benodigde risicobeheersmaatregelen goed.

Alle collegeleden moeten verplicht een training volgen. Hieronder leest u daar meer over.

Voor de gemeenteraad
De gemeenteraad vervult een kaderstellende en controlerende rol. Van de raad wordt verwacht dat zij richting geeft aan het beleid rond digitale weerbaarheid en toeziet op de uitvoering daarvan. Dit vraagt om voldoende inzicht in de risico's, beschikbare maatregelen en benodigde investeringen. Digitale weerbaarheid moet structureel een plek krijgen in de planning- en controlcyclus. Zo kunnen risico's, kosten en maatschappelijke impact zorgvuldig tegen elkaar worden afgewogen.

Nieuwe verplichtingen voor digitale weerbaarheid

De Cyberbeveiligingswet scherpt de eisen voor informatiebeveiliging aanzienlijk aan. Gemeenten en een aantal gemeenschappelijke regelingen worden daarbij aangemerkt als 'essentiële entiteit'. Dat betekent dat digitale veiligheid een vaste plek moet krijgen in de reguliere bedrijfsvoering, de werkprocessen en het integrale risicobeheer. De wet brengt diverse verplichtingen met zich mee:

Zorgplicht
De Cbw verplicht gemeenten om een brede cyberrisicoanalyse uit te voeren en passende technische, organisatorische en operationele maatregelen te nemen voor de eigen ICT-systemen en in de samenwerking met leveranciers. Ook de mogelijke maatschappelijke gevolgen van verstoringen moeten daarbij worden meegewogen. De Baseline Informatiebeveiliging Overheid (BIO) was al het gezamenlijke normenkader voor informatiebeveiliging binnen gemeenten. Met de invoering van de BIO2 krijgt dit normenkader een expliciete juridische basis als invulling van de zorgplicht.

Meldplicht
Significante cyberincidenten die de continuïteit van de dienstverlening bedreigen, moeten binnen 24 uur na kennisname worden gemeld via het portaal van het Nationaal Cyber Security Centrum (NCSC). In eerste instantie volstaat een voorlopige melding. De melding wordt vervolgens doorgeleid naar de bevoegde toezichthouder en, waar van toepassing, het aangewezen Computer Security Incident Response Team (CSIRT).

Voor gemeenten en Cbw-plichtige gemeenschappelijke regelingen is tot op heden geen sectoraal CSIRT aangewezen. Het NCSC voert vanaf de inwerkingtreding de wettelijke CSIRT-taken uit.

Registratieplicht
Daarnaast geldt een registratieplicht: alle gemeenten en Cbw-plichtige gemeenschappelijke regelingen moeten zich inschrijven in het landelijke entiteitenregister via het portaal van het

NCSC. Dit moet voor de inwerkingtreding van de wet afgerond zijn. De verantwoordelijkheid hiervoor ligt bij het bestuur.

Trainingsplicht
Alle leden van het college moeten een verplichte training volgen. Aan de training zijn wettelijke eisen gesteld. Ook het behalen van een certificaat en het actueel houden van de kennis zijn verplicht. De training helpt collegeleden om cyberrisico's te begrijpen, beheersmaatregelen te beoordelen en de gevolgen voor de dienstverlening af te wegen. Binnen twee jaar na inwerkingtreding van de Cbw moet ieder collegelid aan deze verplichting voldoen. Het is belangrijk om de training tijdig te agenderen en structureel onderdeel te maken van bestuurlijke professionalisering.

De VNG heeft een syllabus ontwikkeld die gemeenten een praktische, uniforme basis biedt voor de invulling van deze training, en werkt daarnaast samen met het rijk aan overheidsbrede initiatieven. Gemeenten worden hierover geïnformeerd zodra er meer duidelijkheid is.

Toezicht
De Rijksinspectie Digitale Infrastructuur (RDI) houdt risicogericht toezicht op de naleving van de Cbw door gemeenten, met als doel de digitale weerbaarheid te vergroten. Daarbij ligt de nadruk op het bevorderen van naleving, het stimuleren van continue verbetering en het delen van kennis.

Gemeenten en gemeenschappelijke regelingen die onder de Cbw vallen, zijn zelf verantwoordelijk voor het naleven van de verplichtingen uit de Cbw. De RDI kan hiervoor informatie opvragen, inspecties uitvoeren en, indien nodig, onderzoek doen naar aanleiding van een incident en eventueel handhavend optreden.

Gemeenschappelijke regelingen, relatie met gemeenten en samenwerking in de keten

De continuïteit van de gemeentelijke dienstverlening is mede afhankelijk van organisaties waarmee gemeenten samenwerken. Daarom is het belangrijk om inzicht te hebben in de risico's en afhankelijkheden binnen deze samenwerkingsrelaties.

Gemeenschappelijke regelingen
Gemeenschappelijke regelingen (GR'en) kunnen zelfstandig onder de Cyberbeveiligingswet vallen. Dat geldt niet automatisch voor iedere gemeenschappelijke regeling. Een GR moet zelf beoordelen of zij voldoet aan de overheidscriteria uit de wet. Het ministerie van BZK heeft GR'en opgeroepen deze beoordeling uit te voeren door de toepasselijkheid van de criteria te verifiëren.

Relatie met gemeenten
Wanneer een gemeenschappelijke regeling onder de Cyberbeveiligingswet valt, is zij zelfstandig verantwoordelijk voor de naleving van de wettelijke verplichtingen. De deelnemende gemeente(n) zijn hiervoor niet verantwoordelijk. Gemeenten blijven echter wel afhankelijk van de dienstverlening van gemeenschappelijke regelingen voor de uitvoering van hun eigen taken. Daarom is het belangrijk om, ongeacht of een GR onder de Cbw valt, afspraken te maken over risicobeheersing, incidentafhandeling, informatie-uitwisseling en continuïteit van dienstverlening.

Samenwerking in de keten
Gemeenten werken daarnaast samen met veel uitvoeringsorganisaties, leveranciers en andere ketenpartners. Verstoringen bij deze organisaties kunnen gevolgen hebben voor de gemeentelijke dienstverlening. Daarom is het belangrijk dat gemeenten inzicht hebben in deze afhankelijkheden en passende afspraken maken.

Het gaat daarbij niet alleen om contractuele of juridische verantwoordelijkheden, maar ook om inzicht in de onderlinge afhankelijkheden van informatievoorziening, digitale systemen en bedrijfsprocessen die essentieel zijn voor de continuïteit van de gemeentelijke dienstverlening.

Weerbaarheid essentiële diensten en ketenafhankelijkheid

De Wet weerbaarheid kritieke entiteiten heeft als doel om de weerbaarheid te verhogen van organisaties die essentiële diensten verlenen. Het gaat om de weerbaarheid tegen uiteenlopende dreigingen en risico's, zoals natuurrampen en ongevallen, maar ook terroristische misdrijven en sabotage, die de levering van essentiële diensten aanzienlijk kunnen verstoren.

De wet richt zich op sectoren als energie, drinkwater, afvalwater, vervoer en telecom. Organisaties die van groot belang zijn voor de continuïteit van deze diensten kunnen worden aangewezen als kritieke entiteit. In dat geval moeten ze onder meer een sectorale risicobeoordeling uitvoeren, passende maatregelen treffen en ernstige incidenten melden.

Sommige essentiële diensten zijn ook gemeentelijke taken. Per essentiële dienst wordt bekeken of gemeenten hierin een kritieke rol hebben en zo ja, welke gemeenten dat zijn. Gemeenten die als kritieke entiteit worden aangewezen, worden hierover rechtstreeks benaderd door het ministerie van Infrastructuur en Waterstaat (IenW). Alleen gemeenten waarvoor een aanwijzingsprocedure wordt gestart, ontvangen hierover bericht. Gemeenten die op dat moment niet in aanmerking komen voor aanwijzing, ontvangen hierover geen afzonderlijke kennisgeving vanuit het ministerie.

De aanwijzing van kritieke entiteiten is een zorgvuldig proces. Dit vindt gefaseerd plaats en kent per sector een eigen planning. Het proces van aanwijzing kan ook na de inwerkingtreding van de wet starten. Aangewezen gemeenten krijgen negen maanden de tijd om een sectorale risicobeoordeling uit te voeren, op grond van de sectorale risicoanalyse van het vakministerie.

Ook gemeenten die niet als kritieke entiteit worden aangewezen, doen er goed aan om inzicht te hebben in de afhankelijkheden van kritieke infrastructuur en ketenpartners.

Bestuurlijke urgentie: voorbereiding noodzakelijk

We adviseren gemeenten om op korte termijn te beoordelen of het huidige beleid, de organisatie en de beschikbare middelen aansluiten op de nieuwe wettelijke eisen. Voor veel gemeenten zijn aanvullende stappen nodig op het gebied van governance, capaciteit, deskundigheid en technische weerbaarheid. Denk aan het actualiseren van risicoanalyses, het versterken van rapportagelijnen, het borgen van voldoende capaciteit en expertise, het opnemen van middelen in de begroting, het organiseren van oefeningen en samenwerking met ketenpartners.

Cruciale rol van de ambtelijke organisatie

De ambtelijke organisatie heeft een belangrijke rol in de uitvoering van de verplichtingen uit de Cbw. De gemeentesecretaris zorgt voor een goede organisatorische inbedding van informatiebeveiliging in de reguliere bedrijfsvoering en risicobeheersing. Daarbij horen duidelijke afspraken over sturing, voldoende capaciteit en goede rapportagelijnen richting bestuur.

De Chief Information Security Officer (CISO) heeft een onafhankelijke en adviserende taak. De CISO signaleert risico's, adviseert over passende maatregelen, bewaakt de voortgang en coördineert de aanpak bij digitale incidenten. De verantwoordelijkheid voor risico's en maatregelen binnen processen ligt bij de lijnmanagers en proceseigenaren. Zij besluiten over risicoacceptatie en continuïteit. Het college blijft altijd eindverantwoordelijk.

Ondersteuning

De VNG ondersteunt gemeenten bij de implementatie van de nieuwe wetgeving, onder meer met actuele informatie, hulpmiddelen en bijeenkomsten over de uitvoering van de verplichtingen.

Informatiebeveiligingsdienst

De Informatiebeveiligingsdienst (IBD) blijft na 15 augustus het aanspreekpunt voor gemeenten op het gebied van informatiebeveiliging en privacy. Gemeenten kunnen bij de IBD terecht voor onder meer BIO2-ondersteuning, kennisproducten over informatiebeveiliging en privacy, informatiebeveiligings- en privacyadviezen en ondersteuning bij vragen.

ENSIA
De jaarlijkse ENSIA-rapportage is het instrument waarmee gemeenten inzicht krijgen in de staat van hun informatiebeveiliging en daarover verantwoording afleggen. ENSIA helpt gemeenten om richting raad, stelselhouders en toezichthouders te laten zien dat zij 'in control' zijn. Daarnaast maakt ENSIA jaarlijks duidelijk welke risico's aandacht vragen en waar gemeenten hun informatiebeveiliging verder kunnen verbeteren.

Gemeenten kunnen met de ENSIA-rapportage aantonen in hoeverre zij voldoen aan de zorgplicht. De RDI heeft als toezichthouder recht op deze informatie. Hoe de RDI deze informatie gebruikt binnen haar toezicht, wordt momenteel verder uitgewerkt. Ook daarom is het belangrijk om binnen college en raad het goede gesprek te voeren over de staat van de informatiebeveiliging.

Rijk
Ook het rijk ondersteunt gemeenten en gemeenschappelijke regelingen bij de implementatie van de Cyberbeveiligingswet. Het ministerie van BZK stuurt tevens een informatiebrief aan alle gemeenten en gemeenschappelijke regelingen over de implementatie van de Cbw.

Vragen

Heeft u vragen? Neemt u dan contact op met het Klantcontactcentrum van de VNG via telefoonnummer 070-373 83 93 of e-mail via info@vng.nl.

Met vriendelijke groet,

Vereniging van Nederlandse Gemeenten

dr. mr. L.K. Geluk
Algemeen directeur