Aan de leden

Datum
26 maart 2025
Ons kenmerk
U202500124
Lbr. 25/017
Telefoon
070-3738393
Bijlage(n)

Onderwerp: Gevolgen Cyberbeveiligingswet voor gemeenten

Geachte leden van college en gemeenteraad,

Met deze brief informeren we u over de stand van zaken rondom de invoering van de Cyberbeveiligingswet (Cbw) en hoe u zich hier als bestuurder met uw gemeente op kunt voorbereiden. De wet hangt samen met de Wet Weerbaarheid Kritieke Entiteiten, hierover wordt u later geïnformeerd.

Digitale weerbaarheid
De nieuwe wetten hebben belangrijke implicaties voor gemeenten als het gaat om informatiebeveiliging. Door de naleving van deze wetten kunnen essentiële processen in de maatschappij beter beschermd worden tegen digitale dreigingen, waaronder hacks en aanvallen met ransomware. Dit geldt ook voor uw gemeente, waar processen zoals financiële administratie, burgerzaken, en de aansturing van bruggen en verkeersregelsystemen beter beschermd zullen zijn. Zonder goede informatiebeveiliging loopt uw gemeente risico op verstoringen van vitale diensten, financiële verliezen, schade aan de openbare veiligheid en verlies van vertrouwen van inwoners. Het versterken van digitale weerbaarheid helpt deze risico's te minimaliseren en zorgt voor een veilige omgeving voor uw inwoners.

NIS2- en CER-richtlijnen
De Europese Unie heeft twee richtlijnen aangenomen om de fysieke, digitale en economische weerbaarheid te versterken: de Network and Information Security Directive (NIS2-richtlijn) en de Critical Entities Resilliance Directive (CER-richtlijn). Sinds januari 2023 werkt de rijksoverheid aan de doorvertaling hiervan naar nationale wetgeving**,** de Cyberbeveiligingswet (Cbw) en de Wet Weerbaarheid Kritieke Entiteiten. Deze wetten worden naar verwachting in het vierde kwartaal van 2025 ingevoerd.

Vereniging van Nederlandse Gemeenten
Nassaulaan 12 Den Haag | Postbus 30435 | 2500 GK Den Haag
070 - 373 83 93 | info@vng.nl

Veranderingen rondom zorgplicht, meldplicht en toezicht
In vergelijking met de huidige wetgeving zal voor gemeenten, en voor u, de gemeentelijke bestuurder, een aantal zaken veranderen als het gaat om de zorgplicht, meldplicht en toezicht op informatiebeveiliging.

Zorgplicht
Zodra de wet ingaat, worden gemeenten expliciet verantwoordelijk voor de beheersing van cyberrisico's. Dat betekent dat een analyse van cyberrisico's onderdeel moet zijn van het bredere, reguliere risicobeheer, net als financiële, juridische en politieke risico's. De bestuurders hebben hierin een belangrijke rol. Voor gemeenten houdt dit in dat het college van burgemeester en wethouders verplicht is om informatiebeveiligingsmaatregelen goed te keuren en een training te volgen. Deze training stelt u in staat om risico's te identificeren, risicobeheersmaatregelen te evalueren en de impact van zowel de risico's als de beheersmaatregelen te beoordelen. De Cbw brengt voor overheidsbestuurders (in tegenstelling tot private bestuurders) geen nieuwe aansprakelijkheden met zich mee.

Meldplicht
De Informatiebeveiligingsdienst (IBD) blijft het Computer Emergency Response Team, of Computer Security Incident Response Team (CERT/CSIRT) voor alle Nederlandse gemeenten. Gemeenten betalen de IBD uit het GGU-fonds. Het recht op ondersteuning wordt wettelijk verankerd in de Cbw. De IBD en haar partners binnen het Cyberweerbaarheidsnetwerk ondersteunen gemeenten bij het voorkomen en herstellen van digitale incidenten. Nieuw is dat er ook een meldplicht komt voor ernstige incidenten.

Toezicht
Binnen de gemeente is het van belang dat primair de gemeenteraad toezicht houdt op de naleving van de wet. De raad doet dit door het oppakken van zijn kaderstellende en controlerende rol en het borgen van voldoende budget. Naar aanleiding van de ENSIA-rapportage en rondom voorjaars- en najaarsnota’s kunnen de wethouders en ambtelijk verantwoordelijken, zoals de CISO, gesprekken voeren over de stand van zaken en benodigde acties.

De Rijksinspectie Digitale Infrastructuur (RDI) houdt toezicht op de naleving van de Cbw door de gehele overheid. Op de informatiebeveiliging van enkele gemeentelijke processen, zoals zorg of infrastructuur, kunnen ook andere toezichthouders een rol spelen, zoals de Inspectie Gezondheidszorg en Jeugd en de Inspectie Leefomgeving en Transport nu al doen op hun domeinen. Deze toezichthouders werken nauw met elkaar samen.

Sancties bij gebreken
De RDI heeft als toezichthouder ook de mogelijkheid om sancties op te leggen. Het gaat dan niet alleen om sancties voor de gemeentelijke organisatie, maar ook om persoonlijke sancties voor bestuurders (burgemeester en wethouder) die in gebreke blijven. Bij inbreuken op de zorgplicht en meldplicht kan de toezichthouder de gemeente een bestuurlijke boete opleggen van maximaal € 10 miljoen. Voor overtredingen van andere verplichtingen in de Cyberbeveiligingswet, zoals de registratieplicht, kan de boete oplopen tot € 1 miljoen. Burgemeesters en wethouders kunnen individueel een boete van maximaal € 25.000 krijgen als zij de verplichte training niet volgen.

Concrete voorbereiding
Gemeenten kunnen zich op verschillende manieren voorbereiden op de aankomende Cyberbeveiligingswet.

Baseline Informatiebeveiliging Overheid (BIO)
Blijf werken volgens de BIO-standaarden. De eisen van NIS2 worden hierin opgenomen, dus het is belangrijk om de cyclus van plannen, uitvoeren, controleren en bijstellen te blijven volgen.

ISMS-systeem
Werk gestructureerd volgens een Informatie Security Management Systeem (ISMS) om de status van de informatiebeveiliging te monitoren en te verbeteren. Dit plan-do-check-act systeem helpt bij het naleven van de verschillende normenkaders en maakt continue verbetering mogelijk. Zo wordt de organisatie en de bestuurder in het bijzonder in staat gesteld om de juiste afwegingen te maken.

Bewustwording en training
Zoals hierboven toegelicht (onder *zorgplicht*), stelt de Cbw een training over informatiebeveiliging voor bestuurders (burgemeester en wethouders) verplicht. Een dergelijke training helpt u als bestuurder om de juiste vragen te stellen aan de organisatie om de voorgestelde beveiligingsmaatregelen af te kunnen wegen in relatie tot het risico voor de continuïteit van de gemeentelijke dienstverlening. Wij raden aan om nog geen trainingen te volgen van commerciële partijen, omdat de eisen nog niet zijn vastgesteld. De besluitvorming over de eisen aan de opleiding is op dit moment nog lopende. De insteek van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties is dat de trainingsverplichting voor de overheid zo uniform en efficiënt mogelijk wordt ingericht. Het ministerie hoopt tegen de zomer meer duidelijkheid te kunnen verschaffen. Bovendien is er voldoende tijd. Na de inwerkingtreding hebben bestuurders twee jaar de tijd om aan de opleidingsverplichting te voldoen.

Samenwerking met de VNG en IBD
Maak gebruik van de ondersteuning die de VNG biedt bij de implementatie van de wetgeving. De IBD ondersteunt bij incidenten op het gebied van informatiebeveiliging. U kunt de IBD benaderen bij alle soorten informatiebeveiligingsincidenten waar de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en systemen in het geding is.

ENSIA-rapportage
De jaarlijkse ENSIA-rapportage in mei/juni is hét verantwoordingsinstrument over de staat van informatiebeveiliging. Onder de nieuwe Cyberbeveiligingswet wordt de ENSIA-rapportage nog belangrijker, omdat de gemeente daarmee aan de raad, de stelselhouders en de toezichthouders binnen de rijksoverheid kan aantonen dat zij ‘in control’ is en dus of ze voldoet aan de zorgplicht. Stimuleer het goede gesprek over de staat van de informatiebeveiliging in het college en de raad.

Uitnodiging webinar voor bestuurders
Om u naar aanleiding van deze brief verder te informeren en vragen te beantwoorden nodigen wij u uit voor een webinar op donderdag 15 mei om 10:00. Dit webinar is speciaal bedoeld voor bestuurders. Aanmelden kan via deze link: https://vng.webinargeek.com/optimale-voorbereiding-cyberbeveiligingswet.

Meer informatie

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.

Tot slot

De VNG blijft zich inzetten om gemeenten optimaal te ondersteunen. De haalbaarheid, betaalbaarheid en uitvoerbaarheid van de nieuwe wetten staan in onze lobby richting het rijk voorop. Om te kunnen voldoen aan de Cbw is een eerste randvoorwaarde dat, in overeenstemming met artikel 2 van de Financiële-verhoudingswet, de rijksoverheid zorgt voor adequate financiële dekking van de extra uitvoeringskosten die gemeenten moeten maken voor de naleving van de nieuwe regelgeving voor het beveiligen van netwerk- en informatiesystemen. Er is nauw contact met onder meer de betrokken ministeries over de uitwerking en implicaties van de wetten voor lokale overheden.

Met vriendelijke groet,
Vereniging van Nederlandse Gemeenten

Mr L.K. Geluk
Algemeen directeur