Raadsbrief

Onderwerp	Cyberbeveiligingswet (NIS2)
Zaaknummer	778393
Datum	17 december 2024
Portefeuillehouder	drs. H.A.M. Nauta-van Moorsel MPM
Medewerker	Kluitmans, P. (Peter)

Doel
Ter informatie

Aanleiding
De Network and Information Security directive, of NIS2-richtlijn, is de opvolger van de NIS-richtlijn. Deze richtlijn is vastgesteld door de Europese Unie (EU) en bedoeld om de cyberbeveiliging en weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren.

De NIS2-richtlijn vergroot de reikwijdte van de NIS-richtlijn door meer sectoren te omvatten. Ook stelt de richtlijn strengere beveiligingsnormen en meldingsvereisten voor incidenten. De NIS2-richtlijn wordt momenteel vertaald naar Nederlandse wetgeving.

Deze wetgeving ging officieel in per 17 oktober 2024, maar wordt in Nederland pas rond augustus 2025 omgezet in nationale wetgeving. In de tussenliggende tijd, waarin de richtlijn van kracht is maar de wet nog niet, geldt een bijzondere situatie waarin organisaties die onder de richtlijn vallen al wel rechten hebben, maar nog geen wettelijke plichten.

De afgelopen jaren zetten ontwikkelingen als de covid-19-epidemie, de oorlog in Oekraïne, cyberdreigingen en de gevolgen van klimaatverandering, de veiligheid van onze maatschappij en economie in toenemende mate onder druk. In het licht hiervan is er sinds 2020 vanuit de EU gewerkt aan de NIS2-richtlijn. De richtlijn is gericht op het verbeteren van de digitale en economische weerbaarheid van Europese lidstaten.

De NIS2-richtlijn gaat in op de risico's die netwerk- en informatiesystemen bedreigen, zoals cyberbeveiligingsrisico's. Dit moet bijdragen aan meer Europese harmonisatie en een hoger niveau van cybersecurity bij bedrijven en organisaties in de EU. In 2022 is de EU-richtlijn Netwerk- en Informatiesystemen (NIS2) aangenomen. De gemeente is aangewezen als essentiële entiteit en valt hiermee onder deze richtlijn. De NIS2-richtlijn wordt vertaald in de Cyberbeveiligingswet (Cbw). In deze raadsbrief schetsen wij op hoofdlijnen de strekking van de nieuwe Cyberbeveiligingswet.

Inhoudelijke boodschap

Welke verplichtingen schrijft de NIS2-richtlijn voor?
De gemeente wordt verplicht om meer maatregelen te nemen om cyberbeveiligingsrisico's te beheersen. Zo moeten we aan strengere beveiligings- en rapportagevereisten voldoen.

Zorgplicht – De richtlijn bevat een zorgplicht die organisaties verplicht zelf een risicobeoordeling uit te voeren. Op basis van deze risicobeoordeling nemen zij passende maatregelen om de continuïteit van hun diensten zoveel mogelijk te waarborgen en de gebruikte informatie te beschermen. Vanuit de verschillende sectoren van NIS2 worden nadere regels gesteld aan de zorgplicht. Voor de gemeente omvat dit in elk geval het voldoen aan de Baseline Informatiebeveiliging Overheid (BIO) 2.0.

De plicht om digitale risico's te beheersen strekt zich uit tot voorbij de kantoorautomatisering en gaat ook over fysieke processen met een digitale aansturing zoals verkeerslichten, openbare verlichting, riolering en afvalverwerking.

Meldplicht – De richtlijn schrijft voor dat we incidenten binnen 24 uur moeten melden bij de toezichthouder. Het gaat om incidenten die de continuïteit van dienstverlening van de gemeente aanzienlijk (kunnen) verstoren. In het geval van een cyberincident moet het ook gemeld worden bij het Computer Security Incident Response Team (CSIRT), die hulp- en bijstand kan leveren. Voor de gemeente zal de Informatiebeveiligingsdienst (IBD) van de Vereniging Nederlandse Gemeenten als CSIRT optreden.
Factoren die een incident meldingswaardig maken, zijn bijvoorbeeld het aantal personen dat door de verstoring is geraakt, de tijdsduur van een verstoring en de mogelijke financiële verliezen. De drempelwaarden in specifieke sectoren wordt in nadere regelgeving verder uitgewerkt.

Registratieplicht - De NIS2 bevat een registratieplicht voor gemeenten. Deze geldt voor Nederlandse gemeenten nadrukkelijk pas bij de inwerkingtreding van de Cbw. Aangeraden wordt om registratie uit te stellen totdat alle functionaliteiten van het landelijke registratieportaal gereed zijn. Dit om fouten en een kans op mismatch tussen de landelijke systemen en die van de IBD en de administratieve lasten tot een minimum te beperken.

Toezicht – Organisaties die onder de richtlijn vallen, krijgen ook verplicht toezicht. De NIS2-richtlijn schrijft voor dat een onafhankelijk toezichthouder (niet te verwarren met interbestuurlijk toezicht in het geval van medeoverheden) kijkt naar de naleving van de verplichtingen uit de richtlijn, zoals de zorg- en meldplicht. Voor de overheid wordt de Rijksinspectie Digitale Infrastructuur (RDI) aangewezen als toezichthouder. De RDI maakt voor het toezicht op NIS2 voor de overheid gebruik van bestaande verantwoordingsstructuren. Dit om mogelijke administratieve lasten van het toezicht tot een minimum te beperken. Als verantwoordingsstructuur voor de gemeente zal de Eenduidige Normatiek Single Information Audit (ENSIA)-verantwoording waarschijnlijk worden gebruikt.

Opleiding - Om een goed oordeel te kunnen geven over de risicobeheersmaatregelen op het gebied van cyberbeveiliging en de uitvoering ervan, moet het bestuur over voldoende kennis en vaardigheden beschikken om de risico's voor de beveiliging van de netwerk- en informatiesystemen van de gemeente te kunnen identificeren, de risicobeheerspraktijken te kunnen beoordelen en de gevolgen van die praktijken voor de door de gemeente aangeboden diensten te kunnen beoordelen.
Bestuursleden spelen een cruciale rol in het neerzetten van een sterke cyberweerbaarheidscultuur. Naast de beoordeling van de digitale gezondheid is het ook daarom van belang dat bestuursleden een training volgen. Vanuit die voorbeeldfunctie dragen ze cyberbewustheid uit, en moedigen werknemers binnen hun organisatie aan soortgelijke trainingen te volgen. In de Cbw is bepaald dat de ambtelijke leiding van een gemeente wordt aangemerkt als het bestuur van die overheidsinstantie.

Voor welke instanties geldt de NIS2?
Voor Nederland geldt dat lokale overheden onder de richtlijn worden aangewezen als essentiële entiteiten. Medeoverheden zijn ook verantwoordelijk voor het aanbieden van meerdere essentiële diensten, zoals het wegbeheer of de afvalwatervoorziening, en vallen om die reden ook onder de reikwijdte van de NIS2. Tevens vallen gemeenschappelijke regelingen onder de werking van de richtlijn, voor zover zij voldoen aan de criteria die NIS2 hanteert om een overheidsentiteit te zijn.
De NIS2-richtlijn biedt een uitzondering voor overheidsinstanties die hoofdzakelijk activiteiten uitvoeren op het gebied van openbare veiligheid. Dit betekent bijvoorbeeld dat de veiligheidsregio's en de politie zijn uitgesloten van de NIS2-richtlijn.

Wat kunnen we doen om ons voor te bereiden?
Voor de gemeente geldt dat zij momenteel al moeten voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). De BIO wordt onderdeel van de zorgplicht van NIS2 voor de overheid. Het voldoen aan de BIO en andere bestaande kaders voor informatiebeveiliging bij de overheid, is dus een belangrijk beginpunt.

De NIS2-richtlijn brengt enkele andere maatregelen met zich mee die nu nog geen onderdeel zijn van de BIO. De BIO wordt geüpdatet naar de BIO 2.0. Deze nieuwe versie is gebaseerd op internationale afspraken (NEN/ISO 27001 en 27002), die aangeven hoe risico's rondom informatiebeveiliging moeten worden beheerd.

Met de BIO 2.0 wordt invulling gegeven aan de NIS2-richtlijn, die extra eisen stelt aan de beveiliging van belangrijke netwerken en systemen. De BIO 2.0 zal als normenkader voor de zorgplicht worden aangewezen.

De ISO 27001 gaat over het risicomanagement van de gegevensbescherming. Dit houdt in dat we een Information Security Management System (ISMS) moeten inrichten om het overzicht te krijgen en te bewaren. Dit systeem draagt bij aan de bescherming van de kritieke processen van de gemeente tegen mogelijke risico's. In het eerste kwartaal van 2025 komt een generieke risicoanalyse op de kritieke processen beschikbaar.

Juridische gevolgen
De toezichthoudende instantie Rijksdienst voor Digitale Infrastructuur (RDI) is bevoegd tot het opleggen van een last onder bestuursdwang ten aanzien van de gemeente. Daarnaast voorziet de wet in de bevoegdheid voor de RDI om een bestuurlijke boete op te leggen aan de gemeente.

Consequenties voor Hof van Twente
Gezien het feit dat we nu al een zorgplicht (voldoen aan de BIO), een meldplicht (incidenten melden aan de Informatiebeveiligingsdienst, IBD) en toezicht (verantwoording via de Eenduidige Normatiek Single Information Audit (ENSIA) hebben, zal de impact van de Cyberbeveiligingswet afhankelijk zijn van de mate waarin we nu al gedocumenteerd voldoen aan de BIO. Op dit moment voldoen we niet geheel aan de BIO. Daarom is het cruciaal dat we door blijven gaan met de cyclus van plannen, uitvoeren, controleren en bijstellen rondom de complete BIO.

Conclusie
Om te voldoen aan de eisen die de Cyberbeveiligingswet naar verwachting gaat stellen zullen we moeten blijven werken aan de implementatie van technische en organisatorische maatregelen. Dit zoals opgenomen in ons gemeentelijke informatiebeveiligingsbeleid en het verbeterplan n.a.v. de externe audit 2023. Daarbij is het van belang om te (blijven) beschikken over voldoende kwalitatieve en kwantitatieve capaciteit. Via de raadscommissie informatieveiligheid houden we de raad op de hoogte van de ontwikkelingen.

Burgemeester en wethouders van Hof van Twente,

de secretaris,	de burgemeester,
drs. D. Lacroix	drs. H.A.M. Nauta-van Moorsel MPM