Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

T.a.v. koepelvertegenwoordigers: Interprovinciaal Overleg (IPO), Vereniging Nederlandse Gemeenten (VNG) en Unie van Waterschappen (UvW)

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag

Kenmerk
2023-0000564311

Datum 20 NOV 2023
Betreft NIS2 bij de overheid

Geachte koepelvertegenwoordiger,

De wet- en regelgeving die de herziene Europese richtlijn Network and Information Security Directive (NIS2) uitwerkt, moet door Nederland uiterlijk 17 oktober 2024 in nationale wetgeving worden omgezet. Hoewel momenteel nog hard wordt gewerkt aan deze omzetting, wil ik u in deze brief reeds nader informeren over het voorgenomen besluit om in dit verband de medeoverheden onder de reikwijdte te plaatsen van de wet ter implementatie van de NIS2-richtlijn. Verder wil ik u informeren over de betekenis daarvan, de nadere invulling van het toezicht voor de publieke sector, de meldplicht en de zorgplicht en u verzoeken deze informatie te delen met uw achterban.

Wetgevingstraject NIS2-richtlijn
Het kabinet werkt onder coördinatie van de minister van Justitie en Veiligheid aan een wetsvoorstel ter implementatie van de NIS2-richtlijn. Binnen het kabinet ben ik stelselverantwoordelijk voor de sector overheid. In die hoedanigheid vertaal ik de kaders uit de NIS2-richtlijn naar regelgeving voor de sector overheid. In deze brief wil ik u meenemen in mijn voorgenomen invulling van deze kaders, onder voorbehoud van verdere besluitvorming in het wetgevingsproces.

Medeoverheden binnen reikwijdte NIS2
NIS2 brengt voor veel sectoren de wettelijke verplichting met zich mee om passende en evenredige maatregelen te nemen om cyberbeveiligingsrisico's te beheersen. De overheid gaat daarop ook toezien.

De overheid zelf heeft de maatschappelijke taak om op een zorgvuldige manier om te gaan met gegevens van onze burgers en bedrijven. Burgers en bedrijven zijn bovendien veelal verplicht hun gegevens te delen met de overheid. Ook heeft de overheid simpelweg een voorbeeldfunctie. Ik wil daarom dat de gehele overheid aan dezelfde vereisten voldoet als andere sectoren binnen NIS2. Behoudens enkele uitzonderingen, zullen alle bestuurslagen in Nederland in de implementatiewet NIS2 dan ook worden aangemerkt als essentiële entiteit.

Dit betekent dat de centrale overheid in de richtlijn als essentieel is aangemerkt. Dit is met inbegrip van zelfstandige Bestuursorganen (ZBO's) op wie de Kaderwet Zelfstandige Bestuursorganen van toepassing is. Tevens worden alle medeoverheden als essentiële entiteit aangewezen. Overheden zijn ook verantwoordelijk voor het aanbieden van meerdere essentiële diensten, zoals het wegbeheer of de afvalwater-voorziening, 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.

Overheidsorganisaties die behoren tot de rechterlijke macht, het parlement en de centrale bank zijn van de richtlijn uitgezonderd. Ook overheidsorganisaties die in hoofdzaak activiteiten uitvoeren op het terrein van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving zijn uitgezonderd. Voor deze organisaties moet op andere wijze worden geregeld dat zij zich adequaat beveiligen.

Toezicht en verantwoording

NIS2 verplicht dat onafhankelijk toezicht wordt uitgeoefend. Op dit moment bestaat er voor de sector overheid geen aparte centrale toezichthouder voor digitalisering bij de overheid. Ik wil daarom maximaal gebruik maken van bestaande toezichts- en verantwoordingsinstrumenten en waar nodig deze instrumenten versterken en optimaal op elkaar laten aansluiten. Dat minimaliseert ook eventuele extra lastendruk.

Dat betekent dat ik onder meer de Eenduidige Normatiek Single Information Audit ENSIA[1]-systematiek samen met de Vereniging Nederlandse Gemeenten (VNG) verder wil versterken, zodat lokale verantwoording en toezicht op informatieveiligheid worden gebundeld. Het verkennen van de ENSIA-systematiek richting provincies en waterschappen is daarbij ook het uitgangspunt, altijd in combinatie met de al bestaande horizontale verantwoordingsmechanismen. Verder is ook de onafhankelijkheid van lokale, decentrale rekenkamers recent versterkt met de Wet versterking decentrale rekenkamers[2], waarover mijn collega de minister van Binnenlandse Zaken u per brief[3] heeft geïnformeerd.

Bij de rijksoverheid wordt jaarlijks een Informatiebeveiligingsbeeld opgesteld door de Audit Dienst Rijk (ADR) en rapporteert de Algemene Rekenkamer (ARK) jaarlijks aan de Tweede Kamer in het kader van het Rechtmatigheidsonderzoek. De Rijksinspectie Digitale Infrastructuur (RDI) gaat toezicht houden op het hele stelsel van informatieveiligheid voor de sector overheid en baseert zich daarbij mede op de informatie die voortkomt uit de bestaande verantwoordings- en toezichtstructuren.

---

[1] Gemeenten verantwoorden zich over informatiebeveiliging en kwaliteit middels ENSIA. De focus van ENSIA ligt op verantwoording richting de gemeenteraad, het hoogste politieke orgaan van de gemeente. Parallel hieraan leggen gemeenten verantwoording af aan de rijksoverheid waar het gaat om het gebruik van landelijke voorzieningen.
[2] *Stb* 2022, 430
[3] Brief van 29 november 2022 aan alle decentrale overheden met kenmerk 2022-0000536640

De NIS2-richtlijn kent diverse bepalingen op het terrein van handhaving. Op dit moment wordt nog gesproken over de verdere invulling van de handhavingsbepaling in de NIS2 voor de sector overheid.

Meldplicht
NIS2 verplicht lidstaten om in nationale wet- en regelgeving te voorzien in een meldplicht bij cybersecurityincidenten "met aanzienlijke gevolgen".[4] Er moet worden gemeld aan de toezichthouder en aan het eigen Computer Security Incident Response Team (CSIRT). Naar verwachting zal dat het Nationaal Cyber Security Centrum (NCSC) zijn voor de Rijksoverheid, de Informatiebeveiligingsdienst (IBD) voor gemeenten en CERT-Watermanagement (CERT-WM) voor de waterschappen. De provincies zijn momenteel in de laatste fase van besluitvorming of zij aansluiten bij een bestaand CSIRT of zelf een CSIRT voor de provinciale bestuurslaag gaan inrichten. De gezamenlijke provincies en IPO hebben een business case uitgevoerd waarin meerdere scenario's zijn onderzocht. In een bestuursvergadering van het IPO-bestuur van 14 december wordt hierover besloten.

Consequentie zorgplicht informatieveiligheid
De NIS2-implementatiewet is wetgeving voor alle entiteiten die binnen de reikwijdte van de richtlijn vallen. Ook voor overheden gaat dus een zorgplicht voor informatieveiligheid gelden. De NIS2 biedt wel ruimte om aanvullende sectorale wetgeving op te stellen.

Voor de overheidssector geldt nu al de Baseline Informatiebeveiliging Overheid (BIO). Ik ben voornemens om in de al geplande modernisering van de BIO de eisen van de NIS2 mee te nemen. De BIO wordt wettelijk verankerd als sectoraal kader voor de gehele overheid onder NIS2. Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is hiervoor verantwoordelijk. De wettelijke verankering van de BIO is daarmee in versnelling gekomen en vervangt de bestaande, zogenoemde "verplichtende zelfregulering" van de BIO.

Uit een analyse van BZK en vertegenwoordigers van de koepels is gebleken dat de huidige BIO een groot inhoudelijk deel van de aanstaande NIS2 vereisten afdekt. Deze analyse is beschikbaar via de website van Digitale Overheid: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/mapping-nis2-maatregelen

Ik wil u dan ook oproepen om aan uw achterban te communiceren, dat daar waar dat nog niet het geval is, prioriteit te maken van het toepassen van de huidige BIO. Daarmee bent u bezig met wat de overheid zichzelf al heeft opgelegd (de "verplichtende zelfregulering" van de BIO), alsook bent u proactief bezig met de NIS2 maatregelen.

[4] Wat aanzienlijke gevolgen zijn, wordt nog nader uitgewerkt.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Kenmerk
2023-0000564311

Tot slot wil ik u erop wijzen dat op 12 oktober, volgend op het eerste webinar van 10 maart, het tweede webinar over de laatste stand van zaken van NIS2 bij de overheid heeft plaatsgevonden. Via de website Weerbare Digitale Overheid kunt u dit webinar terugkijken:
https://www.weerbaredigitaleoverheid.nl/programma-onderdelen/sessie/259c8281/

Ik hoop u voor dit moment voldoende te hebben geïnformeerd. Zodra nadere uitwerking beschikbaar is, zal ik u hierover informeren.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
Digitalisering en Koninkrijksrelaties

Alexandra C. van Huffelen