Beleidskompasformulier voor **internetconsultatie**

Titel:

Regeling cyberbeveiliging EZ

∞ Wie zijn belanghebbenden en waarom?

Toelichting

Hulpvragen

- Wie zijn direct of indirect belanghebbenden bij het betreffende vraagstuk?
  De essentiële en belangrijke entiteiten die onder het toepassingsbereik van deze regeling komen te vallen behoren tot de volgende (sub)sectoren:
    - *de aanbieders van internetknooppunten*
    - *aanbieders van openbare elektronische communicatienetwerken*
    - *aanbieders van elektronische communicatiediensten*
    - *ruimtevaart*
    - *post- en koerierdiensten*
    - *vervaardiging. Bij de sector vervaardiging gaat het om de subsectoren a) vervaardiging van informaticaproducten en van elektronische en optische producten b) vervaardiging van elektrische apparatuur c) vervaardiging van machines, apparaten en werktuigen, niet elders geclassificeerd d) vervaardiging van motorvoertuigen, aanhangers en opleggers e) vervaardiging van andere transportmiddelen.*
    - *Onderzoeksector voor zover deze onder de verantwoordelijkheid van de Minister van Economische Zaken valt.*
- *Deze regeling geldt alleen voor middelgrote en grote entiteiten in de genoemde sectoren; in de Cyberbeveiligingswet is nader gedefinieerd wat hieronder wordt verstaan. Alleen voor aanbieders van openbare elektronische communicatienetwerken en -diensten geldt een uitzondering; deze regeling geldt voor alle aanbieders in deze sector ongeacht hun omvang.*

  Het Ministerie van Economische Zaken is belanghebbende als opsteller van de regeling. Het Ministerie van Justitie en Veiligheid is belanghebbende; het Nationaal Cyber Security Centrum (NCSC) is als CSIRT verantwoordelijk voor de EZ-sectoren . De Rijksinspectie Digitale Infrastructuur (RDI) ziet als toezichthouder toe op de naleving van deze regeling en is daarmee ook belanghebbende.

- Wie beschikken er over relevante kennis over en ervaring met het vraagstuk?

Zie voorgaand antwoord.

- Op welke wijze zijn belanghebbenden tot nu toe in de verschillende fasen van het beleidstraject betrokken?
  De concept-Cyberbeveiligingswet en het concept-Cyberbeveiligingsbesluit zijn eerder openbaar gemaakt ten behoeve van een internetconsultatie. Verder heeft er ten behoeve van deze concept-regeling overleg plaats gevonden met meerdere bedrijven en brancheorganisaties uit bovenvermelde sectoren.
  Met de overheidspartijen is zo goed mogelijk afstemming gezocht middels reguliere overleggen.

1. Wat is het probleem?

Toelichting

Hulpvragen

a) Wat is het probleem?
De NIS2-richtlijn (Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148, PbEU 2022, L 333) bevat maatregelen om de cyberbeveiliging van essentiële en belangrijke entiteiten binnen de Europese Unie naar een hoger gemeenschappelijk niveau te brengen. De NIS2-richtlijn wordt in Nederland geïmplementeerd in de Cyberbeveiligingswet (Cbw). De ontwerp-Cyberbeveiligingswet (Cbb) ligt momenteel (november 2025) voor behandeling in de Tweede Kamer. Verschillende onderdelen van de Cyberbeveiligingswet worden nader uitgewerkt in het Cyberbeveiligingsbesluit en in regelingen van verschillende ministeries. Het ontwerp-Cyberbeveiligingsbesluit zal naar verwachting eind 2025 voor advies aan de Raad van State worden verzonden.

Nadere uitwerking van een aantal maatregelen uit de Cbw en het Cbb in deze regelingen is noodzakelijk om een hoger niveau van cyberbeveiliging te realiseren en om ook duidelijkheid te bieden aan essentiële en belangrijke entiteiten in de EZ-sectoren.

b) Wat zijn de oorzaken van het probleem?
Zie het antwoord op vraag 1a.

c) Wat is de omvang van het probleem?
Zie het antwoord op vraag 1a en de vraag over de belanghebbenden.

d) Wat is het huidige beleid en wat heeft de evaluatie opgeleverd?
In het beleidskompas die bij de consultatieversie van de Cyberbeveiligingswet op deze website is gepubliceerd is nader ingegaan op de noodzaak tot herziening van de NIS-richtlijn.

e) Wat gebeurt er als de overheid niets doet (Nuloptie)? Wat rechtvaardigt overheidsinterventie?

Nederland is verplicht om richtlijnen van de Europese Unie te implementeren. Ten aanzien van de NIS2-richtlijn geldt dat overheidsoptreden is gerechtvaardigd doordat in dezen een publiek belang bestaat, namelijk het waarborgen van de levering van essentiële diensten in de interne markt.

Deze concept-regeling draagt bij aan het verbeteren van de cyberbeveiliging van de relevante entiteiten door de beveiligingsmaatregelen nader uit te werken en de criteria voor het melden van incidenten te verduidelijken.

2. Wat is het beoogde doel?

Toelichting

Hulpvragen

a) Wat zijn de beleidsdoelen?
De NIS2-richtlijn beoogt een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie te bereiken, teneinde de werking van de interne markt te verbeteren. Deze richtlijn beoogt dit doel te bereiken door de verschillen weg te nemen die tussen lidstaten bestaan op het gebied van de cyberbeveiligingseisen die worden gesteld aan entiteiten die economisch belangrijke activiteiten of diensten verrichten. De richtlijn tracht dit doel te bereiken door onder meer regels vast te stellen over entiteiten die van rechtswege, zonder tussenkomst van een lidstaat, onder het toepassingsbereik van de richtlijn komen te vallen, en door te voorzien in doeltreffende voorzieningen ten aanzien van de cyberbeveiligingseisen waar entiteiten aan moeten voldoen en het toezicht op de naleving van de verplichtingen die voortvloeien uit de richtlijn.

Deze conceptregeling vormt een nadere uitwerking van het bij de Tweede Kamer ingediende wetsvoorstel. Voor dat wetsvoorstel is in een eerder stadium een beleidskompas opgesteld. De inhoudelijke keuzes die aan deze regeling ten grondslag liggen, zijn in dat kader reeds gemaakt. Met de inwerkingtreding van de Cbw, wordt beoogd een stevige impuls te geven aan de versterking van de digitale weerbaarheid van Nederland. Dit gebeurt door entiteiten, op wie de wet van toepassing is, te verplichten cyberbeveiligingsmaatregelen te treffen en ernstige incidenten te melden.

b) Aan welke duurzame ontwikkelingsdoelen (sustainable development goals, SDG's) en brede welvaartsuitkomsten dragen de doelen bij?
N.v.t.

3. Wat zijn opties om het doel te realiseren?

Toelichting

Hulpvragen

a) Wat zijn kansrijke aangrijpingspunten om het doel te realiseren?

Om een hoger niveau van cyberbeveiliging te bereiken en duidelijkheid te bieden aan essentiële en belangrijke entiteiten, is het noodzakelijk om bepaalde maatregelen uit de Cbw en het Cbb nader uit te werken. Deze conceptregeling vormt voor de genomen EZ-sectoren een nadere uitwerking van beveiligingsmaatregelen en van de criteria aan de hand waarvan wordt bepaald of sprake is van een significant incident. Daarnaast voorziet de regeling in de aanwijzing van autoriteiten waarmee de NIS2-instanties informatie kunnen uitwisselen.

Mbt de beveiligingsmaatregelen:

Het doel van deze nadere invulling is om de algemene normen uit de wet en het besluit verder te concretiseren op onderdelen die van groot belang worden gezien voor de beveiliging van netwerk- en informatiesystemen. Daarmee wordt meer duidelijkheid geboden aan essentiële en belangrijke entiteiten en wordt bijgedragen aan een hoger gemeenschappelijk niveau van de beveiliging van netwerk- en informatiesystemen. Het gaat hierbij onder andere om maatregelen op het gebied van bedrijfscontinuïteit en toegangsbeheer. Hierdoor ontstaat er ook meer duidelijkheid over het kader waarop de toezichthouder toezieten een gelijk speelveld tussen sectoren waarin concurrentie een rol speelt.

Mbt de meldplicht:

Het doel van deze nadere invulling is om de algemene meldcriteria uit de wet verder te concretiseren. Deze criteria hebben in deze concept-regeling met name een sectorspecifieke uitwerking gekregen. Dit biedt niet alleen duidelijkheid aan essentiële en belangrijke entiteiten over welke incidenten als significant worden beschouwd en derhalve moeten worden gemeld, maar ook aan het CSIRT en de toezichthouder over de aard en reikwijdte van de meldplicht. Bij het vaststellen van de criteria is eveneens gestreefd naar uitvoerbaarheid voor de entiteit. Daarnaast kunnen meldingen over incidenten ook nuttige informatie bevatten voor andere entiteiten die mogelijk met vergelijkbare incidenten te maken kunnen krijgen. Een CSIRT en andere ontvangers (beleidsdepartementen) van meldingen kunnen deze informatie gebruiken voor hun waarschuwende en ondersteunende taken. Dit draagt bij aan een gemeenschappelijk hoger niveau van cyberweerbaarheid.

Mbt aanwijzing autoriteiten:

Voor een aantal wetten geldt dat deze nauwe raakvlakken hebben met de Cyberbeveiligingswet. Het is daarom gewenst dat de bevoegde autoriteiten, CSIRT's en het centrale contactpunt onder de Cbw voor de doeltreffende en doelmatige uitvoering van hun taken samenwerken en informatie uitwisselen met de autoriteiten die toezicht houden op

de naleving van deze andere wetgeving. Hiertoe zijn in deze concept-regeling autoriteiten aangewezen die uit hoofde van sectorale regelgeving een rol hebben in het toezicht op entiteiten die ook onder toepassing van de Cyberbeveiligingswet vallen.

b) Wat zijn, gegeven de aangrijpingspunten, kansrijke beleidsopties?
n.v.t.

c) Wat is de beleidstheorie (doelenboom) per kansrijke beleidsoptie?
n.v.t.

4. Wat zijn de gevolgen van de opties?

Toelichting

Hulpvragen

a) Wat zijn de verwachte gevolgen per beleidsoptie?
Deze regeling veroorzaakt geen nieuwe regeldruk ten opzichte van de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit. Voor de meldplicht is de regeldruk voor alle relevante sectoren verantwoord in de memorie van toelichting bij het wetsvoorstel. Betreffende de zorgplicht is regeldruk in de nota van toelichting bij het besluit uitgewerkt. Zowel de meldplicht als de zorgplicht kennen een nadere invulling in deze regeling, maar deze leveren geen aanvullende regeldruk op.

b) Welke verplichte toetsen zijn van toepassing en wat zijn daarvan de uitkomsten (voor zover bekend)?
De Rijksinspectie Digitale Infrastructuur zal de concept-regeling toetsen op uitvoerbaarheid en handhaafbaarheid. Daarnaast wordt de concept-regeling ook aan het Adviescollege Toetsing Regeldruk (ATR) voor de algemene toets regeldruk voorgelegd.

5. Wat is de voorkeursoptie?

Toelichting

Hulpvragen

a) Wat is het voorstel?

Deze concept-regeling ziet op de verdere uitwerking van met name de zorg- en meldplicht die als verplichtingen voortvloeien uit de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit.

b) Hoe houdt het voorstel rekening met:

- doeltreffendheid en doelmatigheid;
- uitvoerbaarheid voor alle relevante partijen (inclusief doenvermogen, regeldruk en handhaving);
- brede maatschappelijke impact?

Door de nadere uitwerking van de beveiligingsmaatregelen krijgen de entiteiten duidelijkheid over welke maatregelen ze moeten treffen alsmede wanneer ze een incidenten moeten melden. Ook zullen er toetsen worden uitgevoerd om de regelgeving te toetsen op uitvoerbaarheid en handhaafbaarheid.

c) Wat zijn de risico's en onzekerheden van dit voorstel?

Bij het opstellen van het wetsvoorstel is een inschatting gemaakt van het aantal entiteiten dat onder het toepassingsbereik van de Cyberbeveiligingswet vallen en daarmee oa recht hebben op bijstand van de CSIRT. Welke entiteiten onder deze wetgeving vallen is mede afhankelijk van de grootte en omvang van entiteiten en dat blijkt moeilijk in te schatten.

d) Hoe ziet de voorgenomen monitoring en evaluatie eruit?

In de concept-cyberbeveiligingswet is opgenomen dat de Minister van Justitie en Veiligheid binnen vijf jaar na de inwerkingtreding van de wet een evaluatieverslag aan de Staten-Generaal zal sturen en vervolgens elke drie jaar.