Beleidskompasformulier voor **internetconsultatie**

Titel:

Regeling cyberbeveiliging en weerbaarheid kritieke entiteiten energiesector van de Minister van Klimaat en Groene Groei

∞ Wie zijn belanghebbenden en waarom?

Toelichting

Hulpvragen

- Wie zijn direct of indirect belanghebbenden bij het betreffende vraagstuk?

De Minister van Klimaat en Groene Groei, de Minister van Justitie en Veiligheid, de Minister van Binnenlandse Zaken en Koninkrijksrelaties, de Minister van Economische Zaken, de Minister van Financiën, de Minister van Infrastructuur en Waterstaat, de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur, de Minister van Onderwijs, Cultuur en Wetenschap, de Minister van Defensie en de Minister van Volksgezondheid, Welzijn en Sport.

De entiteiten in de energiesector die onder het toepassingsbereik van de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten komen te vallen en brancheorganisaties. Dit zijn bijvoorbeeld systeembeheerders, elektriciteitsbedrijven, producenten, exploitanten van oliepijpleidingen, aardgasbedrijven en exploitanten van stadsverwarming of stadskoeling.

De bevoegde autoriteiten die toezicht zullen houden op de naleving van de verplichtingen uit de Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten.

De computer security incident response teams (CSIRT's) die ondersteuning zullen leveren aan entiteiten.

- 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 belanghebbenden zijn betrokken geweest bij de voorbereidingen van de regeling cyberbeveiliging en weerbaarheid kritieke entiteiten energiesector van de Minister van Klimaat en Groene Groei onder meer middels (gezamenlijke) overleggen. Tevens is deze internetconsultatie ook een manier om waardevolle input van belanghebbenden op te halen.

1. Wat is het probleem?

Toelichting

Hulpvragen

a) Wat is het probleem?

De zogeheten ECI-richtlijn (Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren) voorziet in een procedure voor het aanwijzen van Europese kritieke infrastructuren in de sectoren energie en vervoer, waarvan de ontwrichting of vernietiging aanzienlijke grensoverschrijdende gevolgen zou hebben voor ten minste twee lidstaten. Die richtlijn is uitsluitend gericht op de bescherming van dergelijke infrastructuren. De ECI-richtlijn is in 2019 geëvalueerd. Daaruit bleek dat door de steeds sterkere verwevenheid en grensoverschrijdende aard van activiteiten waarbij gebruik wordt gemaakt van allerlei kritieke infrastructuur, de in de ECI-richtlijn opgenomen maatregelen te beperkt zijn om de vitale maatschappelijke functies of economische activiteiten op de Europese interne markt voldoende te beschermen. De ECI/CER richtlijn wordt in Nederland omgezet in de Wet weerbaarheid kritieke entiteiten. Veel bepalingen zijn omgezet in deze wet en het onderliggende Besluit weerbaarheid kritieke entiteiten. Ten behoeve van de nationale implementatie van de richtlijn, is nadere sectorale invulling van een aantal van deze bepalingen nodig. Deze regeling geeft deze nadere sectorale invulling voor de energiesector.

De zogeheten NIS1-richtlijn (Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie,) biedt de lidstaten van de Europese Unie een ruime discretionaire bevoegdheid bij de uitvoering van de daarin opgenomen verplichtingen over cyberbeveiliging en het melden van ICT- incidenten. Ook wordt het aan de lidstaten gelaten om aanbieders aan te wijzen die onder het NIS1-regime komen te vallen. Uit een evaluatie van de NIS1-richtlijn is gebleken dat lidstaten de richtlijn op uiteenlopende wijze uitvoeren. Zo zijn de hiervoor genoemde verplichtingen op nationaal niveau op aanzienlijk verschillende wijze uitgevoerd, waardoor er verschillen zijn op het gebied van het type maatregel en het detailniveau. Dit geldt ook voor de bepalingen uit de richtlijnen over toezicht en handhaving. Verder zijn er tussen de lidstaten verschillen op het gebied van de aanwijzingen van aanbieders die onder het NIS1-regime vallen. Deze verschillen tussen lidstaten leiden tot een versnippering van de interne markt en kunnen een nadelig effect hebben op het functioneren van de interne markt, met gevolgen voor onder meer de grensoverschrijdende dienstverlening. De NIS2-richtlijn wordt in Nederland geïmplementeerd in de Cyberbeveiligingswet. Veel bepalingen zijn omgezet in deze wet en het onderliggende Cyberbeveiligingsbesluit (amvb). Ten behoeve van de nationale implementatie van de richtlijn, is nadere sectorale invulling van een aantal van deze bepalingen nodig. Deze regeling geeft deze nadere sectorale invulling voor de energiesector.

b) Wat zijn de oorzaken van het probleem?

Zie het antwoord op vraag 1.

c) Wat is de omvang van het probleem?

Zie het antwoord op vraag 1.

d) Wat is het huidige beleid en wat heeft de evaluatie opgeleverd?

De evaluatie van de ECI-richtlijn heeft geleid tot de zogeheten CER-richtlijn (Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende deweerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad). De CER-richtlijn beoogt de weerbaarheid te bevorderen van entiteiten die van kritiek belang zijn voor een goede werking van de Europese interne markt ten aanzien van alle relevante risico's. Verder voorziet de CER-richtlijn in de intrekking van de ECI-richtlijn. De CER-richtlijn wordt in Nederland geïmplementeerd in de Wet weerbaarheid kritieke entiteiten, het Besluit weerbaarheid kritieke entiteiten en onderliggende regelgeving.

De bij vraag 1A genoemde verschillen die uit de evaluatie van de NIS1-richtlijn naar voren zijn gekomen, in relatie tot de toename van digitale dreigingen en technologische ontwikkelingen, hebben geleid tot 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). De NIS2-richtlijn 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 en onderliggende regelgeving.

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

Nederland is verplicht om richtlijnen van de Europese Unie te implementeren. In dit geval is overheidsoptreden gerechtvaardigd omdat een publiek belang bestaat, namelijk het waarborgen van de levering van essentiële diensten in de interne markt, waaronder de levering van energie.

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. Zowel de NIS2- richtlijn en CER-richtlijn hebben als doel het waarborgen van de levering van essentiële diensten in de interne Europese markt en daarmee het beschermen van de nationale veiligheid, onder meer door verplichtingen aan bedrijven die essentiële diensten leveren voor te schrijven en ondersteuning te verlenen in geval van incidenten. Dit gaat bijvoorbeeld over het treffen van adequate beveiligingsmaatregelen, het melden van incidenten en het borgen van informatie-uitwisseling tussen betrokken partijen. Zowel de Wet weerbaarheid kritieke entiteiten als de Cyberbeveiligingswet bevatten een bijlage waarin deze bedrijven die essentiële diensten leveren vermeld staan. Zie; Cyberbeveiligingswet | Overheid.nl | Wetgevingskalender en Wet weerbaarheid kritieke entiteiten | Overheid.nl | Wetgevingskalender.

In aanvulling op de Cyberbeveiligingswet, de Wet weerbaarheid kritieke entiteiten en bijbehorende besluiten, biedt de onderhavige Regeling cyberbeveiliging en weerbaarheid kritieke entiteiten energiesector een nadere sectorale invulling voor de energiesector.

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?

De Cyberbeveiligingswet, het Cyberbeveiligingsbesluit en onderliggende regelgeving zorgen voor een wettelijke verankering die aansluit op de doelen die zijn gesteld in de Cybersecuritystrategie 2022-2028. De Wet weerbaarheid kritieke entiteiten, het Besluit weerbaarheid kritieke entiteiten en onderliggende regelgeving zorgen voor een wettelijke verankering van de Aanpak Vitaal. Onder coördinatie van het ministerie van Justitie en Veiligheid, richt de Aanpak Vitaal zich op het voorkomen van verstoring van vitale processen en het verhogen van de weerbaarheid. De Aanpak Vitaal biedt een integrale, adaptieve en richtinggevende aanpak om risico's binnen de vitale infrastructuur het hoofd te blijven bieden. Het doel wordt bereikt met regels over onder meer het uitvoeren van risicobeoordelingen, het treffen van passende en evenredige beveiligingsmaatregelen, het uitwisselen van informatie, het melden van incidenten, het inregelen van toezicht en het inregelen van bijstand voor entiteiten in geval van incidenten.

Om entiteiten (bedrijven) die onder deze wetgeving zullen vallen voor te bereiden zijn er verschillende communicatiemiddelen vanuit de overheid ingezet om deze doelgroep en belanghebbenden te informeren en tijdig te betrekken bij het implementatietraject. Zo hebben er meerdere Webinars plaatsgevonden, zijn er stakeholder sessies georganiseerd, presentaties gegeven bij verschillende netwerkbijeenkomsten en communicatieproducten (zoals informatie sheets en brochures) ontwikkeld. Meer informatie hierover is te vinden op de website van de Rijksoverheid: Cyberbeveiligingswet | Nationaal Coördinator Terrorismebestrijding en Veiligheid en Wet weerbaarheid kritieke entiteiten | Nationaal Coördinator Terrorismebestrijding en Veiligheid.

b) Wat zijn, gegeven de aangrijpingspunten, kansrijke beleidsopties?

Zie 3a.

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?

Een verhoogde digitale en fysieke weerbaarheid van overheidsorganisaties en organisaties uit vitale sectoren.

Er ontstaan regeldrukeffecten voor de entiteiten die onder het toepassingsbereik van deze implementatiewet- en regelgeving komen te vallen. Zij moeten investeringen doen en inspanningen verrichten om te voldoen aan de verplichtingen die daaruit voortvloeien. Naar verwachting veroorzaakt deze regeling geen nieuwe regeldruk ten opzichte van de Wet weerbaarheid kritieke entiteiten, het Besluit weerbaarheid kritieke entiteiten, de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit. De regeldruk voor kritieke, essentiële en belangrijke entiteiten is verantwoord in de bijbehorende toelichtingen bij de wetsvoorstellen en besluiten.

Voor bevoegde autoriteiten zijn er toezichts- en handhavingskosten.

Voor zogeheten Computer security incident response teams (CSIRT's), zoals het Nationaal Cyber Security Centrum, zijn er uitvoeringseffecten en -kosten.

b) Welke verplichte toetsen zijn van toepassing en wat zijn daarvan de uitkomsten (voor zover bekend)?

Voor deze regeling zal een uitvoerings- en handhaafbaarheidstoets bij de toezichthoudende instanties worden aangevraagd dat gelijktijdig zal lopen met de internetconsultatie.

Deze regeling zal hierna worden voorgelegd aan het Adviescollege toetsing regeldruk. Zoals vermeld bij 4A veroorzaakt deze regeling naar verwachtring geen nieuwe regeldruk ten opzichte van de beide wetten en onderliggende besluiten.

5. Wat is de voorkeursoptie?

Toelichting

Hulpvragen

a) Wat is het voorstel?

Nederland moet de NIS2- en CER richtlijn implementeren. Voor veel bepalingen uit de richtlijnen geschiedt dat middels de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten, in elk geval voor wat betreft het opleggen van verplichtingen aan entiteiten, omdat dat een wettelijke grondslag vereist. In de onderhavige algemene maatregelen van bestuur (Cyberbeveiligingsbesluit en Besluit weerbaarheid kritieke entiteiten) worden de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten verder uitgewerkt, onder meer met een uitwerking van de meldplicht en de maatregelen die moeten worden genomen in het kader van de zorgplicht. De Minister van Klimaat en Groene Groei is beleidsverantwoordelijk voor de implementatie van deze richtlijnen voor de energiesector en heeft een ministeriële regeling opgesteld met nadere regels passend bij de kenmerken van deze sector.

Deze regeling bevat nadere regels voor zowel het Besluit weerbaarheid kritieke entiteiten als het Cyberbeveiligingsbesluit en is onderdeel van de implementatie van de Richtlijn (EU) 2022/2557 betreffende de weerbaarheid van kritieke entiteiten (CER) en de richtlijn (EU) 2022/2555 betreffende de cyberbeveiliging van netwerk- en informatiesystemen (NIS2).

In deze regeling zijn verschillende onderwerpen nader uitgewerkt. Hierbij wordt voor de Wet weerbaarheid kritieke entiteiten de meldplicht nader ingevuld. Voor de Cyberbeveiligingswet worden de volgende onderwerpen verder uitgewerkt: 1) meldplicht, 2) zorgplicht, 3) aanwijzen van autoriteiten.

b) Hoe houdt het voorstel rekening met:

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

Ja.

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

N.v.t.

d) Hoe ziet de voorgenomen monitoring en evaluatie eruit?

Deze regeling zal periodiek worden geëvalueerd en waar nodig aangepast of aangevuld worden. De Minister van Klimaat en Groene Groei evalueert ten minste elke vier jaar de doeltreffendheid van de nadere regels van de meldplicht en de effecten daarvan in de praktijk en zal indien nodig aanpassingen doorvoeren.

Daarnaast zal de Europese Commissie controleren of de CER- en NIS2-richtlijn adequaat zijn geïmplementeerd in Nederland. Mede op basis daarvan zal ook door de Minister van Justitie en Veiligheid worden beoordeeld of de wet en onderliggende regelgeving, zoals deze regeling, voldoende efficiënt en effectief functioneert. Dit zal in overleg gebeuren met de betrokken bewindspersonen, zoals de Minister van Klimaat en Groene Groei.