Beleidskompasformulier

Titel:

Cyberbeveiligingsbesluit

∞ Wie zijn belanghebbenden en waarom?

Toelichting

Hulpvragen

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

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

  De entiteiten die onder het toepassingsbereik van de Cyberbeveiligingswet komen te vallen, brancheorganisaties en de koepels van provincies, gemeenten en waterschappen.

  De bevoegde autoriteiten die toezicht zullen houden op de naleving van de verplichtingen uit de Cyberbeveiligingswet.

  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 het Cyberbeveiligingsbesluit, onder meer middels gezamenlijke overleggen.

1. Wat is het probleem?

Toelichting

Hulpvragen

a) Wat is het probleem?

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, *PbEU* 2016, L 194) 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.

b) Wat zijn de oorzaken van het probleem?

De lidstaten van de Europese Unie voeren de NIS1-richtlijn op uiteenlopende wijze uit.

c) Wat is de omvang van het probleem?

Zie het antwoord op vraag 1a.

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

De hiervoor 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.

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.

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. Het doel wordt bereikt door onder meer plichten op te leggen aan entiteiten, zoals de verplichting tot het treffen van adequate ICT-maatregelen en het melden van ICT-incidenten. Naast plichten zijn er ook rechten, zoals het recht op bijstand.

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 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.

Voor bevoegde autoriteiten zijn er toezichts- en handhavingskosten.

Voor het centrale contactpunt zijn er uitvoeringseffecten en -kosten.

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)?

Administratieve lastentoets / regeldrukkosten (Adviescollege toetsing regeldruk).

5. Wat is de voorkeursoptie?

Toelichting

Hulpvragen

a) Wat is het voorstel?

Nederland moet de NIS2-richtlijn implementeren. Voor veel bepalingen uit de richtlijn geschiedt dat middels de Cyberbeveiligingswet, in elk geval voor wat betreft het opleggen van verplichtingen aan entiteiten, omdat dat een wettelijke grondslag vereist. In de onderhavige algemene maatregel van bestuur (Cyberbeveiligingsbesluit) wordt de Cyberbeveiligingswet verder uitgewerkt, onder meer met een uitwerking van de maatregelen die moeten worden genomen in het kader van de zorgplicht.

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?

n.v.t.