Beleidskompasformulier voor **internetconsultatie**

.

Titel:

(Vul hier de publicatietitel van de internetconsultatie in)

Regeling van de Staatssecretaris van Minister van Binnenlandse Zaken en Koninkrijksrelaties van 10 november 2025 houdende regels ten aanzien van de beveiliging van netwerk- en informatiesystemen van entiteiten voor de sector overheid ter uitvoering van de cyberbeveiligingswet (Cyberbeveiligingsregeling sector overheid).

∞ Wie zijn belanghebbenden en waarom?

Toelichting

Hulpvragen

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

Entiteiten van de overheid die onder de reikwijdte van de Cyberbeveiligingswet (Cbw) vallen (hierna te noemen: overheidsentiteiten); - Van de centrale overheid: Ministeries en zelfstandige bestuursorganen (voor zover zij kwalificeren als 'overheidsinstantie' onder de Cbw) - Van de decentrale overheid: gemeenten, provincies en gemeenschappelijke regelingen (voor zover zij kwalificeren als 'overheidsinstantie' onder de Cbw). Waterschappen via het ministerie van Infrastructuur en Waterstaat (IenW) Daarnaast zijn ook de bevoegde autoriteiten die toezicht zullen houden op de naleving van de verplichtingen uit de Cyberbeveiligingswet en de Computer Security Incident Response Teams (CSIRTs) die ondersteuning zullen leveren aan entiteiten, directe belanghebbenden. Organisaties met indirect belang kunnen zijn de toeleveranciers van overheidsentiteiten, burgers en bedrijven en organisaties die hun informatie aan de overheid toevertrouwen.

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

Zie directe belanghebbenden bij 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 bestaande bestuurlijke overleggen. Dit gaat onder meer over de werkgroep BIO, Werkgroep Informatiebeveiliging Overheid (IBO), via overleggen met koepelorganisaties van medeoverheden en interdepartementale overleggen zoals de NIS2-werkgroep Rijk van de CISO-raad.

1. Wat is het probleem?

Toelichting

Hulpvragen

a) Wat is het probleem?

De NIS2-richtlijn verplicht tot het implementeren van regels over de beveiliging van netwerk- en informatiesystemen van essentiële en belangrijke entiteiten (de zorgplicht) en de daarvoor benodigde governance binnen de entiteiten. Daarnaast wordt er een meldplicht voor significante incidenten bij de daarvoor aangewezen Computer Security Incident Response Teams (CSIRTs) ingesteld en wordt toezicht en handhaving op de voorgenoemde regels ingevoerd. Deze regels zijn omgezet in het voorstel voor de Cyberbeveiligingswet (Cbw) en het Cyberbeveiligingsbesluit (Cbb), de Algemene Maatregel van Bestuur onder de Cbw. Daarin zijn een aantal grondslagen opgenomen voor het stellen van nadere regels voor de verschillende essentiële en belangrijke sectoren (en eventueel voor subsectoren en entiteiten. Entiteiten in de sector overheid, zowel op centraal- als decentraal niveau, zijn in de Cbw aangewezen als essentiële entiteiten. In het Cbb is een aantal grondslagen opgenomen om per ministeriële regeling nadere regels te stellen. Deze zien toe op het aanwijzen van een ander CSIRT dan het Nationaal Cyber Security Centrum (NCSC), het stellen van nadere regels voor de zorgplicht en het opnemen van sectorspecifieke drempelwaarden voor de meldplicht. Dit moet uitgewerkt worden in een sectorspecifieke ministeriële regeling.

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.

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

n.v.t.

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

De Cyberbeveiligingswet en het Cyberbeveiligingsbesluit verplicht voor een aantal onderwerpen regels nader uit te werken in sectorspecifieke ministeriële regelingen. Wanneer hiertoe niet wordt besloten, wordt daar niet aan voldaan. Bovendien is Nederland verplicht om richtlijnen vanuit 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. Het risico bestaat dat Nederland niet volledig voldoet aan de verplichting tot het implementeren van de richtlijnen wanneer deze niet nader zijn uitgewerkt in de ministeriële regeling.

2. Wat is het beoogde doel?

Toelichting

Hulpvragen

a) Wat zijn de beleidsdoelen?

Het doel is om voor de sector overheid, zowel voor de centrale als de decentrale overheden, een sectorspecifieke regeling vast te stellen. Deze dient nadere regels te stellen voor de zorgplicht en de drempelwaarden voor de meldplicht en het aanwijzen van een CSIRT voor entiteiten die niet onder het NCSC moeten vallen. Uiteindelijk dient deze regeling, als onderdeel van de implementatie van de NIS2-richtlijn ten doel om een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie te bereiken, teneinde de werking van de interne markt te verbeteren.

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 nadere regels te kunnen stellen onder de Cbw en het Cbb is het maken van een sectorspecifieke ministeriële regeling de enige optie. Bij de invulling van deze ministeriële regeling zijn er nog wel enkele keuzes te maken ten aanzien van de invulling voor de aanwijzing van het CSIRT, de zorgplicht en drempelwaarden voor de meldplicht. De mogelijkheden hiervoor worden hieronder toegelicht.

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

Aanwijzing CSIRT
Er kan gekozen worden om geen ander CSIRT voor (sub)sectoren van de overheid aan te wijzen per ministeriële regeling. In dat geval zou het NCSC het CSIRT zijn voor de gehele overheid. Er is ook de optie om een CSIRT voor de sector, subsector of voor entiteiten aan te wijzen via deze ministeriële regeling. Daarnaast laat het Cbb de mogelijkheid om per ministeriële regeling nadere vereisten, zoals functionele, financiële, technische en organisatorische eisen te stellen aan de organisaties die als CSIRT worden aangewezen.

Zorgplicht
De Cbw en het Cbb geven een algemene zorgplicht voor een groot aantal maatschappelijke sectoren, waaronder de overheid. Over de onderwerpen waarop de zorgplicht ziet zijn dan ook verschillende bepalingen opgenomen. Naast de grondslag om deze onderwerpen nader uit te werken, biedt de delegatiegrondslag van het Cbb de ruimte om per ministeriële regeling ook zorgplichtbepalingen op te nemen over andere dan de genoemde onderwerpen. Dit geeft verschillende mogelijkheden voor het invullen van de zorgplicht:

1. Geen nadere invulling van de zorgplicht per ministeriële regeling. De zorgplicht bestaat dan uit bepalingen van de Cbw en het Cbb.
2. Aansluiting bij de invulling van de zorgplicht in de voorziene de ministeriële regelingen van EZ, KGG, IenW en LVVN. Deze invulling is gebaseerd op de Uitvoeringsverordening die van toepassing is op een specifieke groep normadressaten (o.a. digitale infrastructuur).
3. Het invullen van de zorgplicht voor de sector overheid door middel van normen die via rijksbrede afspraken al zijn voorgeschreven voor de rijksdienst en decentrale overheden, de ISO27001 en 27002-standaarden en de Baseline Informatiebeveiliging Overheid (BIO). Waarmee wordt gezorgd voor een wettelijke verankering van deze geldende regels.

Drempelwaarden voor de meldplicht
De Cbw verplicht entiteiten tot het melden van significante incidenten bij het CSIRT en de toezichthouder. Een incident is een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt. In het Cbb is een delegatiegrondslag opgenomen om bij ministeriële regeling per sector invulling te geven aan de drempelwaarden voor het bepalen wanneer sprake is van een significant incident. Hiervoor wordt gekeken naar de gevolgen van een incident in de zin van een operationele verstoring van de diensten van de entiteit, financiële schade voor de eigen entiteit, en materiële en immateriële schade aan andere natuurlijke of rechtspersonen. In de uitwerking van de drempelwaarden voor de meldplicht voor de overheid is zoveel mogelijk aangesloten bij de bestaande praktijk.

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?

Aanwijzen CSIRT
De entiteiten zullen op basis van de Cbw significante incidenten moeten melden bij het CSIRT. Daarnaast wordt het mogelijk gemaakt dat ze vrijwillig melding doen van incidenten die de drempelwaarden niet overstijgen. In principe is het NCSC aangewezen als het CSIRT voor alle (sub)sectoren en entiteiten waarvoor er niet per ministeriële regeling een ander CSIRT is aangewezen. Voor het aanwijzen van een CSIRT per ministeriële regeling kan gekozen worden om meer aan te sluiten bij een bestaande situatie, waarin sommige (sub)sectoren of entiteiten al samenwerken met een bestaande organisatie als CSIRT. Op die manier is het niet nodig om nieuwe samenwerkingen in te regelen, en worden uitvoeringslasten voor organisaties beperkt.

Zorgplicht
Met het stellen van nadere regels onder de zorgplicht ontstaat er voor overheidsinstanties, zowel op centraal als decentraal niveau, een wettelijk uniform en afdwingbaar kader met betrekking tot de zorgplicht voor de beveiliging van netwerk- en informatiesystemen.

1. Indien het Cbb niet nader wordt ingevuld vullen in de ministeriële regeling, blijft naar verwachting het belang van behoud van de BIO als interbestuurlijk convenant bestaan. Net als de andere informatiebeveiligingseisen die vanuit verschillende stelsels zoals vanuit Wet SUWI worden gesteld. Met als gevolg dat verschillende kaders voor informatiebeveiliging blijven bestaan, inclusief bijbehorende uitvoeringslasten voor overheden. Daarnaast kan de uitvoering van de maatregelen, vanwege het abstractieniveau van de zorgplichtbepalingen in de Cbw en Cbb, uiteen gaan lopen. Dit is niet praktisch, gelet op de samenwerking binnen en tussen de verschillende overheidslagen. Overigens is met deze optie de vraag of wordt voldaan aan de verplichte implementatie van alle onderdelen van de NIS2-richtlijn. Mogelijk dienen aspecten nog nader uitgewerkt te worden.
2. Het aansluiten bij de uitwerking van de zorgplicht zoals in de Uitvoeringsverordening heeft ook verschillende gevolgen voor overheden. In principe is deze uitvoeringsverordening geschreven voor andere sectoren dan de sector overheid, waardoor het niet goed aansluit bij de overheidspraktijk. Zij zullen zich daarom moeten aanpassen aan deze nieuwe methodieken op het terrein van informatiebeveiliging met bijbehorende uitvoeringslasten. Bovendien heeft dit grote gevolgen voor de status van de BIO, die via zorgvuldige afstemming samen met de overheden tot stand is gekomen.
3. De wettelijke verankering van de BIO in de ministeriële regeling sluit aan bij de bestaande situatie, waarin de verschillende overheden de BIO al toepassen. Hiermee zijn de uitvoeringslasten van de regeling beperkt. Dit is tevens in overeenstemming met wensen vanuit overheidsorganisaties. Immers, op 23 september 2025 is door het Overheidsbreed Beleidsoverleg Digitalisering Overheid (OBDO) akkoord gegeven op BIO2 en het verzoek gedaan aan de staatssecretaris van BZK om de BIO2 mee te nemen in de nadere regelgeving onder de Cyberbeveiligingswet.

Meldplicht
Met het opstellen van de drempelwaarden voor significante incidenten wordt de lastendruk ten aanzien van de meldplicht voor organisaties bepaald. Lage drempelcriteria zorgen mogelijk voor grotere administratieve lasten voor overheidsorganisaties, die het meldproces moeten doorlopen. Tegelijkertijd kunnen te hoge drempelcriteria ervoor zorgen dat incidenten niet gemeld worden, terwijl signalering van deze incidenten door het CSIRT en toezichthouder wel van belang was geweest. Bijvoorbeeld omdat incidenten organisatie-overstijgende gevolgen hebben binnen sectoren.

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

Uitvoerbaarheid- en handhaafbaarheidstoets (UHT)
De bevoegde autoriteit voor de overheid (RDI) wordt gevraagd een Uitvoerbaarheid- en handhaafbaarheidstoets uit te voeren op de Cyberbeveiligingsregeling voor de sector overheid.

Uitvoeringstoets CSIRT
De IBD zal worden gevraagd een uitvoeringstoets uit te voeren voor de uitvoering van haar taken op grond van de Cbw en onderliggende regelgeving. Inzichten hieruit kunnen waar nodig worden meegenomen in de ministeriële regeling, waar een grondslag is opgenomen om functionele, financiële, technische en organisatorische vereisten aan organisaties die als CSIRT worden aangewezen, vast te leggen.

Uitvoerbaarheidstoets Decentrale Overheden (UDO)
Gedurende de looptijd van het implementatietraject is uitvoering gegeven aan de Uitvoerbaarheidstoets Decentrale Overheden (UDO). Medeoverheden zijn actief betrokken bij het wetgevingsproces, zo ook bij de totstandkoming van de onderdelen die in deze ministeriële regeling worden geregeld. Conform de handreiking UDO, wordt de uitwerking van de UDO zo veel mogelijk opgenomen in reguliere documenten in het beleids- of wetgevingsproces zoals de toelichting op de ministeriële regeling. Bovendien zijn de koepels VNG, IPO en UvW in het kader van de formele consultatie op grond van de Code Interbestuurlijke Verhoudingen actief geconsulteerd.

5. Wat is de voorkeursoptie?

Toelichting

Hulpvragen

a) Wat is het voorstel?

Aanwijzen CSIRT
Het Nationaal Cyber Security Centrum (NCSC) is in beginsel het verantwoordelijke CSIRT voor de (sub)sectoren, tenzij in de ministeriële regeling een andere organisatie hiertoe wordt aangewezen. Voor de gemeenten en gemeenschappelijke regeling waar ten minste één gemeente aan deelneemt, is de voorkeursoptie om de Informatiebeveiligingsdienst (IBD) van de VNG aan te wijzen als CSIRT. Dit CSIRT vervult deze rol op dit moment al voor de gemeenten, waardoor het voor de uitvoeringsconsequenties het meest logisch is om de huidige samenwerking voort te zetten. Voor de overige overheidsentiteiten onder de verantwoordelijkheid van BZK zal het NCSC als CSIRT zal fungeren.

Zorgplicht
Het heeft de voorkeur om voor de zorgplicht aan te sluiten bij de regels die via een rijksbrede afspraak al zijn voorgeschreven. Dit betekent dat in de ministeriële regeling wordt opgenomen dat organisaties de internationale standaard voor informatiebeveiliging, de ISO27001- standaard dienen toe te passen, met daarbij de verplichting om de beheersmaatregelen van de ISO27002 te volgen. Daarnaast zijn ze verplicht tot het toepassen van ten minste de overheidsmaatregelen van de Baseline Informatiebeveiliging Overheid (BIO) 2 die gerelateerd zijn aan de ISO27002 standaard. De BIO beschrijft generieke informatieveiligheidsnormen en -maatregelen. Deze is op dit moment voor de rijksdienst geldend in de vorm van een ministerraadsbesluit en voor de decentrale overheden via een interbestuurlijk convenant (zelfregulering).

Deze keuze wordt gemaakt om de volgende redenen:
1. Beperken implementatiedruk van de Cbw bij medeoverheden: Met het aansluiten bij reeds bestaande normenkaders voor informatiebeveiliging van de overheid worden administratieve lasten van implementatie voor overheidsorganisaties beperkt. Zij dienen immers te voldoen aan normen die zij zich eerder zelf al hebben opgelegd. Bovendien hebben alle koepelorganisaties van medeoverheden in hun consultatiereacties op de Cbw en het Cbb reeds aangegeven graag de Baseline Informatiebeveiliging Overheid (BIO) te hanteren als invulling van de zorgplicht.
2. Hanteren van één methodiek binnen de overheid: Het uitgangspunt is om binnen de overheid één werkwijze te hanteren. Zodat overheidspartijen eenzelfde uitgangspunt hebben bij het maken van ketenafspraken en dezelfde taal en denkwereld hanteren richting burger en bedrijfsleven.
3. Als (lange-termijn)instrument voor mogelijk terugdringen administratieve lastendruk: In de Nederlandse Cybersecurity Strategie (NLCS) is de wens naar voren gekomen om de BIO wettelijk te verankeren. Met als reden dat dit de noodzaak verkleint om vanuit verschillende (wettelijke) stelsels, denk aan SUWI, eisen te stellen aan de informatiebeveiliging voor overheden. Op dit moment is dat niet mogelijk, omdat de BIO nog een interbestuurlijk convenant is dat niet dezelfde status heeft als een van de te vervangen wettelijke regelingen. Door de verankering van de BIO in deze ministeriële regeling zou echter op termijn wel een versimpeling kunnen worden aangebracht in het aantal van toepassing zijnde wettelijke regelingen ten aanzien van informatiebeveiliging, waardoor verantwoordings- en toezichtlasten voor overheden kunnen worden teruggedrongen.

Daarnaast wordt er in de zorgplicht een bepaling opgenomen die het identificeren van de kernprocessen voor de centrale en decentrale overheden verplicht stelt, door middel bestaande methoden hiervoor. Te weten de Te Beschermen Belangen (TBB's) en de impact tabel voor de gemeenten die de IBD heeft gepubliceerd. Op deze manier kan van tevoren al een inschatting worden gemaakt over de vraag of de uitval van bepaalde diensten en systemen meldenswaardig is. Deze bepaling helpt een deel van de uitvoeringslasten voor de meldplicht te beperken doordat de meldplicht wordt toegespitst op essentiële diensten. Het is immers wenselijk dat een incident op een van deze diensten eerder wordt gemeld dan binnen diensten die minder belangrijk zijn voor de organisatie.

Drempelwaarden voor de meldplicht
In ministeriële regeling wordt nader uitgewerkt wanneer sprake is van een significant incident binnen de sector overheid. De drempelwaarden voor de meldplicht voor de overheid zijn zoveel mogelijk in lijn gebracht met reeds bestaande criteria. Voor de sector overheid gaat dit om de Te Beschermen Belangen (TBB's). Zowel Rijksorganisaties als gemeenten gebruiken (afgeleiden van) deze criteria, alleen verschilt invulling ervan, zoals aangegeven in het bovenstaande over het identificeren van de kernprocessen. De Rijksoverheid kent 4 niveaus binnen de TBB-tabel, gemeenten spreken over 5 impactniveaus. Beide modellen gaan in op de volgende criteria:

1. Schade aan personen, denk aan doden of ernstig gewonden als gevolg van het incident.
2. Materiële schade, denk aan financieel verlies dat niet binnen de reguliere begroting van de organisatie is op te vangen.
3. Integriteit en vertrouwelijkheid, denk aan de openbaarmaking van het niveau Confidentieel of hoger of de openbaarmaking van verzamelingen aan informatie op het niveau Departementaal-Vertrouwelijk.
4. Beschikbaarheid, denk aan uitval van dienstverlening van kernprocessen die een bepaalde tijd voortduurt en waardoor een minimaal aantal personen wordt gehinderd. Of herstel dat niet binnen afzienbare tijd mogelijk is.

Vanuit de zorgplicht dienen overheidsorganisaties hun essentiële diensten te classificeren. Systemen op categorie TBB3, TBB2 en TBB1 binnen de centrale overheid en categorie 'hoog' of 'zeer hoog' voor decentrale overheden worden gekenmerkt als essentiële diensten. Op voorhand is de inschatting gemaakt dat uitval of verstoring van deze diensten grote impact heeft voor de organisatie. Daarnaast kunnen ook incidenten op niet-essentiële diensten grote impact hebben. Om die reden zijn ook incidenten op deze niet-essentiële diensten meldplichtig indien de inschatting is dat er wordt voldaan aan de concrete impactcriteria. Het staat organisaties bovendien vrij om naast de verplichte melding ook vrijwillig melding te maken van incidenten. Dat kan wanneer incidenten niet voldoen aan de criteria, maar volgens de organisatie wel meldingswaardig zijn.

b) Hoe houdt het voorstel rekening met:

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

Er wordt er zoveel mogelijk aangesloten bij bestaande instrumenten en praktijken om de uitvoeringslasten tot een minimum te beperken.

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.