Beleidskompasformulier internetconsultatie ‘Cyberbeveiligingsregeling IenW’

∞ Wie zijn belanghebbenden en waarom?

Wie zijn direct of indirect belanghebbenden bij het betreffende vraagstuk?

De belangrijke en essentiële entiteiten die in de scope vallen van de Cyberbeveiligingswet en werkzaamheden verrichten in de sectoren:

- Vervoer: over de weg, spoor of water, of door de lucht;
- Drinkwater en afvalwater;
- Chemische industrie;
- Afvalstoffenbeheer;
- Nucleaire installaties;
- Waterkwantiteitsmanagement;
- Meteorologie.

Een deel van deze entiteiten zijn overheden (agentschappen, ZBO’s) of medeoverheden (gemeenten, provincies waterschappen, gemeenschappelijke regelingen).

Verder zijn van belang:

- Kritieke entiteiten op grond van de Wwke;
- Ministeries I&W, DGWB, DGMo, DGMI en DGLM;
- ILT, ANVS, NVWA;
- Verschillende departementen in verband met hun verantwoordelijkheden: MinJenV en in verband met overlappende entiteiten in sectoren: MinBZK, MinVWS, MinEZ, MinKGG, MinLVVN.

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

- Vewin;
- FERM (Haven Rotterdam);
- VNG, IPO en Unie van Waterschappen;
- BPVS (Luchtvaart).

Op welke wijze zijn belanghebbenden tot nu toe in de verschillende fasen van het beleidstraject betrokken?

- De inhoud van de zorgplicht en de inhoud van de drempelwaarden voor een significant incident kunnen met vertegenwoordigers van de sector worden besproken.
- De concept-regeling met zorgplichtbepalingen en drempelwaarden wordt interdepartementaal besproken en zo mogelijk op elkaar afgestemd.
- De concept-regeling wordt via internet geconsulteerd.

1. Wat is het probleem?

a) Wat is het probleem?

Meldingen over incidenten bevatten nuttige informatie. Deze informatie kan anderen helpen vergelijkbare incidenten te voorkomen. Toch wordt er weinig gemeld, omdat de drempel hiervoor te hoog is. Dat geldt voor diegenen die al meldplichten over cyberincidenten hebben (bijvoorbeeld op grond van de Wet beveiliging netwerk- en informatiesystemen). Daardoor missen CSIRTS (Computer Security Incident Response Team) en toezichthouders relevante informatie. Hierdoor kunnen CSIRTS en de toezichthouders de entiteit zelf en anderen niet goed ondersteunen bij het voorkomen en beheersen van incidenten. Op grond van artikel 27, eerste lid, van het Cyberbeveiligingsbesluit (hierna Cbb) moeten drempelwaarden worden vastgesteld. Deze drempelwaarden zijn nodig om te kunnen bepalen wanneer sprake is van een 'incident met significante gevolgen'. Voor dit soort incidenten geldt een meldplicht (artikelen 27 tot en met 31 van de Cyberbeveiligingswet). Wanneer deze drempel niet helder of concreet is, voeren de entiteiten de drempel verschillend uit. Dit maakt handhaven van de drempel lastiger.

Het Cbb beschrijft de te nemen maatregelen op grond van artikel 23, vierde lid, van de Cyberbeveiligingswet vaak in termen van 'het vastgesteld hebben van beleid op bepaalde domeinen'. De praktische toepassing of een minimum-niveau is daarbij nog niet voorgeschreven. Op grond van artikel 5.15 van het Cbb kan de Minister nadere regels stellen over de maatregelen, die een essentiële of belangrijke entiteit moet nemen, om weerbaar te zijn voor verstoringen van de dienst die de entiteit levert (de zorgplicht). Het Cbb is op onderdelen minder concreet. Hierdoor ontstaat een verschil in weerbaarheid. Bij ministeriële regeling kunnen voorschriften geconcretiseerd worden. In meerdere sectoren is daar voor een aantal voorschriften behoefte aan. Zo ontstaat er duidelijkheid waarop de toezichthouder toeziet. En er ontstaat een gelijk speelveld voor sectoren waar concurrentie een rol speelt.

De Minister van BZK en van IenW hebben het voornemen gehad de BIO(2) voor overheidsinstanties verplicht te stellen. Het Cbb doet dat nog niet.

Het CERT-watermanagement (CERT-wm) heeft momenteel al een essentiële rol in het cyberweerbaar maken van waterschappen voor hun watertaken. Het voornemen is dat deze CERT-Wm ook wordt aangewezen als CSIRT op grond van artikel 2, tweede lid, van het Cbb. Als deze aanwijzing niet plaatsvindt, dan is de NCSC de standaard CSIRT voor enkele specifieke taken. De door CERT-Wm opgebouwde expertise is dan niet beschikbaar voor deze taken.

b) Wat zijn de oorzaken van het probleem?

Het Cyberbeveiligingsbesluit delegeert de regels over concrete drempelwaarden naar het niveau van ministeriële regeling. Het Cyberbeveiligingsbesluit bevat een discretionaire bevoegdheid van de minister. Op grond van deze bevoegdheid kan de minister regels vaststellen over de maatregelen die een essentiële of belangrijke entiteit moet nemen.

Essentiële en belangrijke entiteiten kunnen werkzaamheden verrichten in meerdere sectoren. Deze sectoren kunnen onder verschillende ministeries vallen, en daarom verschillende maatregelen voorschrijven. Vanuit de belangen van de entiteiten is het daarom wenselijk de concrete invulling

van de zorgplicht goed af te stemmen tussen de verschillende sectoren waar overlap zich voordoet. Met het concretiseren van de verplichting, wordt zowel voor de normaddressaat als voor de verschillende toezichthouders duidelijk wat het minimum-niveau is. Daar vereisen dan alleen heel specifieke sectoren een aanvullende maatregel.

Gemeenten, provincies, waterschappen en de Rijksoverheid passen momenteel al het BIO (1) toe voor communicatie met de rijksoverheid. Deze is gemoderniseerd naar BIO2. Het gebruik van BIO2 (en de ISO 27001 en 27002) wordt door BZK voorgeschreven voor alle overheidsinstanties

Het Cyberbeveiligingsbesluit bevat een discretionaire bevoegdheid van de minister om bij regeling een ander CSIRT aan te wijzen.

c) Wat is de omvang van het probleem?

1100 entiteiten in de IenW sectoren moeten weten wanneer een incident meldplichtig is en welke maatregelen (als onderdeel van de zorgplicht) moeten worden getroffen.

Het aanwijzen van de CSIRT voor specifieke watertaken van de waterschappen treft 21 waterschappen en mogelijk ook Rijkswaterstaat.

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

Voor een deel van de entiteiten (voor IenW ongeveer 30) die onder de Cyberbeveiligingswet gaan vallen geldt nu al de Wet beveiliging netwerk- en informatiesystemen (Wbni). Op grond van deze Wbni zijn er ook drempelwaarden vastgesteld voor incidenten waarvoor een meldplicht geldt. De drempelwaarde is in de afgelopen jaren nog nooit overschreden. De meldplicht heeft voor geen enkel incident gegolden. De huidige drempelwaarde is daarmee te hoog, waardoor de doelen van de meldplicht niet worden bereikt.

Op grond van de Wbni geldt ook een zorgplicht. Voor IenW sectoren is de zorgplicht geconcretiseerd in een regeling (Ministeriële regeling beveiliging netwerk- en informatiesystemen IenW). Deze regeling is tot stand gekomen als gevolg van behoeften, die leefden bij de toezichthouder en onder toezichtstaanden, voor een concretere invulling van het (abstractere) Besluit beveiliging netwerk- en informatiesystemen. Deze regeling is niet geëvalueerd. Maar de veronderstelling is te rechtvaardigen, dat dezelfde behoefte bestaat onder de Cyberbeveiligingswet.

Momenteel is op grond van de Regeling aanwijzing schakelorganisaties cybersecurity het CERT-wm (onderdeel van het Waterschapshuis) het CSIRT voor waterschappen. Deze partij heeft geïnvesteerd in het opbouwen van kennis over de gebruikte systemen en processen van waterschappen. Wel moeten voorafgaand aan de aanwijzing nog afspraken gemaakt worden over de bekostiging en de governance van deze entiteit.

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

- Dan is het niet duidelijk wanneer een incident significant is en gemeld moet worden.

- Er blijft onduidelijkheid bestaan over de concrete invulling van de maatregelen die nodig zijn in het kader van de zorgplicht. Deze onduidelijkheid kan leiden tot verschillen in de wijze van naleven. Hierdoor wordt een hoog gemeenschappelijk niveau van weerbaarheid niet of niet volledig behaald. Ook blijft hierdoor veel meer ruimte voor een andere interpretatie van de wettelijke verplichting bestaan, waardoor verschillen ontstaan in de handhaving bij verschillende toezichthouders. Dat is onwenselijk.
- Dan is het CERT-Wm niet aangewezen voor waterschappen. De taken van het CSIRT worden dan uitgevoerd door het NCSC.

2. Wat is het beoogde doel?

a) Wat zijn de beleidsdoelen?

- Waarborgen van de cyberveiligheid en weerbaarheid van essentiële en belangrijke entiteiten.
  - Door het melden kan een bedreiging eerder ondervangen worden (bij entiteiten die hetzelfde risico lopen).
  - Door het melden kan ondersteuning worden geboden door een Cybersecurity-incident respons team (CSIRT).
  - Een drempelwaarde draagt bij aan de selectie van relevante dreigingen.
  - Een geconcretiseerde zorgplicht draagt direct bij aan een hoog niveau van cyberveiligheid en weerbaarheid. Maar draagt ook bij aan een gelijk speelveld (binnen Nederland) voor entiteiten met een commerciële insteek (die niet uit publieke middelen bekostigd worden).

b) Aan welke duurzame ontwikkelingsdoelen (sustainable development goals, SDG's) en brede welvaartsuitkomsten dragen de doelen bij?

- SDG 6: Schoon water en afvalwater
- SDG 9: Investeren in industrie, innovatie en infrastructuur

3. Wat zijn opties om het doel te realiseren?

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

Voor de meldplicht beschrijven we (verwachte) consequenties van een hypothetisch incident. Zowel in effecten op de entiteit (schade, omzetderving) als in effecten op de maatschappij als gevolg van uitval van de dienst van de entiteit. Er worden meerdere consequenties beschreven. Als al één daarvan gerealiseerd wordt (en dus de drempelwaarde wordt overschreden), dan is er sprake van een incident met significante gevolgen. Dat incident moet dan gemeld worden.

Voor de zorgplicht worden concrete(re) maatregelen beschreven, die de entiteit moet nemen. Deze maatregelen sluiten aan bij wat (het beleid) op grond van het Cyberbeveiligingsbesluit moet worden opgesteld, en vormt een invulling van dat beleid.

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

Alternatieven voor regulering van de drempelwaarde in een ministeriële regeling (bijvoorbeeld als gevolg van onderhandelde afspraken of individuele beschikkingen) stuiten af op:

a) de omvang van de groep normadressaten; en
b) de potentiële ongelijke behandeling die daaruit voortvloeit.

Een goed geoperationaliseerde drempelwaarde voor een significant incident geeft rechtszekerheid en leidt tot een behapbaar aantal meldingen per jaar over de meest relevante verstoringen.

Sectorspecifieke drempelwaarden (als aantallen getroffen aansluitingen, uren uitval of aansluiten bij andere bestaande meldplichten) zijn effectiever dan generieke drempelwaarden. Ze zijn namelijk concreet en onmiddellijk toepasbaar in die sector.

Voor de invulling van de zorgplicht is gekeken naar bestaande standaarden.

c) Wat is de beleidstheorie (doelenboom) per kansrijke beleidsoptie?

Een goedgekozen drempelwaarde leidt tot een beheersbaar en uitvoerbaar aantal meldingen. Een deel daarvan bevat relevantie informatie voor derden. Door ondersteuning vanuit het CSIRT kan daar opvolging aan worden gegeven. CSIRT, en andere ontvangers (beleidsdepartement) van de melding, kunnen deze informatie beoordelen en benutten voor hun ondersteunende en waarschuwende taak. Daarmee leren die derden van 'fouten en kwetsbaarheden' en kunnen zij maatregelen treffen om vergelijkbare incidenten te voorkomen of de gevolgen ervan te beheersen. Dat draagt bij aan een gemeenschappelijk ho(o)g(er) niveau van cyberweerbaarheid.

Als concrete regels worden vastgesteld over de te nemen maatregelen, dan gaan essentiële en belangrijke entiteiten investeringen doen om deze maatregelen te nemen. Door de regels ontstaat er een gelijk speelveld voor concurrerende entiteiten. Als alle essentiële en belangrijke entiteiten binnen een sector de maatregelen nemen, dan bereikt de sector een hoog niveau van cyberweerbaarheid.

4. Wat zijn de gevolgen van de opties?

a) Wat zijn de verwachte gevolgen per beleidsoptie?

Een toename van het aantal meldingen over incidenten binnen de IenW-sectoren. Dit aantal komt ongeveer tussen de 10 en de 100 meldingen per jaar te liggen.

Essentiele en belangrijke entiteiten in IenW-sectoren stellen beleid vast over de cyberweerbaarheidsmaatregelen, op basis van hun riskappetite. Daarbij hebben ze aandacht voor relevante aspecten die in de regeling genoemd worden.

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

- UDO voor medeoverheden;
- ATR;

- UHT (door ILT);
- Uitvoeringstoetsen voor overige overheden.

5. Wat is de voorkeursoptie?

a) Wat is het voorstel?

Vaststellen van een ministeriële regeling waarin:

1) de zorgplicht wordt uitgewerkt;
2) de drempelwaardes voor een meldplicht worden opgenomen; en
3) een CSIRT wordt aangewezen.

De zorgplicht wordt uniform ingevuld met de departementen waarbinnen entiteiten zijn die ook in IenW-sectoren werkzaamheden verrichten. Deze invulling moet het merendeel van de zorgplicht afdekken.

Wel blijft er op onderdelen behoefte aan de mogelijkheid om heel sectorspecifiek een incidentele maatregel voor te schrijven.

b) Hoe houdt het voorstel rekening met doeltreffendheid en doelmatigheid?

Relevante informatie over incidenten wordt snel gedeeld door meldingen. Irrelevante informatie blijft achterwege (drempelwaarde meldplicht).

Doelmatige zorgplicht draagt bij aan een gelijk speelveld, voorspelbaarheid gedrag toezichthouder en bereiken van een hoog niveau van cyberweerbaarheid (minder incidenten of verstoringen).

c) Hoe houdt het voorstel rekening met uitvoerbaarheid voor alle relevante partijen (inclusief doenvermogen, regeldruk en handhaving)?

Uitvoeringslasten zijn hoger bij lage drempelwaarde. Dit leidt bij zowel de kant van de melder als de ontvanger tot meer meldingen.

Bij strengere eisen aan de te treffen maatregelen in het kader van de zorgplicht zijn de uitvoeringslasten hoger.

Bij concrete regels kunnen de handhavingslasten afnemen. Controle door en onderbouwing van de overtreding door de ILT zal eenvoudiger te onderbouwen zijn.

d) Hoe houdt het voorstel rekening met brede maatschappelijke impact?

Een hoog niveau van cyberweerbaarheid vermindert het risico op maatschappelijke verstoringen. Tegelijkertijd moeten de kosten van dat hogere niveau ook gedragen worden door de maatschappij. De afweging is dat deze kosten te rechtvaardigen zijn, in het licht van de consequenties van een verstoring van de dienstverlening.

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

Te lage drempelwaarden leiden tot hoge aantallen meldingen waarvan de behandeling veel capaciteit vergt. Het doen van een melding neemt capaciteit weg van het oplossen van een incident.

Generieke voorschriften om maatregelen te treffen, ontnemen entiteiten de keuze om deze maatregelen te beoordelen op noodzakelijkheid en proportionaliteit. Mogelijk leidt dat tot (onnodige) belasting van die entiteiten.

De voorgeschreven maatregelen zijn overwegend rule-based. In dat geval worden specifieke risico's voor een entiteit te weinig meegewogen (te weinig risk-based). De maatregel is dan niet passend (gaat te ver of juist niet ver genoeg).

f) Hoe ziet de voorgenomen monitoring en evaluatie eruit?

Nog nader te bepalen.