Adviescollege Toetsing Regeldruk

Aan de staatssecretaris van Veiligheid en Justitie
De heer dr. K.H.D.M. Dijkhoff
Postbus 20301
2500 EH DEN HAAG

Datum
8 september 2017

Onderwerp
Cybersecuritywet

Uw kenmerk

Ons kenmerk
MvH/RvZ/HS/MF/2017
-U028

Bijlage(n)

Geachte heer Dijkhoff,

Op 23 augustus heeft ATR, de rechtsopvolger van Actal, het wetvoorstel Regels ter implementatie van richtlijn (EU) 2016/1148 (Cybersecuritywet) ter toetsing ontvangen. De Cybersecuritywet (hierna: Csw) strekt ter uitvoering van de zogenoemde NIB-richtlijn van de Europese Unie (hierna: de richtlijn).[1] Het doel van de NIB-richtlijn is om eenheid en samenhang te brengen in het Europese beleid voor netwerk- en informatiebeveiliging om op deze wijze het functioneren van de Europese economie en samenleving te versterken. Om het beoogde doel te bereiken verplicht de NIB-richtlijn de lidstaten ertoe hun digitale paraatheid te verbeteren en om beter met elkaar samen te werken. Onder meer vraagt de richtlijn van aanbieders van essentiële diensten (hierna: AED's) en digitale dienstverleners om maatregelen nemen om hun ICT adequaat te beveiligen tegen inbreuken van buitenaf en ter voorkoming en minimalisering van cyberincidenten. Verder dienen zij in het vervolg incidenten met aanzienlijke gevolgen te melden bij de bevoegde autoriteit of het computer security incident response team (CSIRT).

ATR heeft de regeldrukgevolgen van het voorstel getoetst. Hieronder treft u het advies van ATR aan.

Toetsingskader

ATR beoordeelt de gevolgen voor de regeldruk aan de hand van het volgende toetsingskader:

1. Nut en noodzaak: is er een taak voor de overheid en is wetgeving het meest aangewezen instrument?
2. Zijn er minder belastende alternatieven mogelijk?
3. Is gekozen voor een uitvoeringswijze die werkbaar is voor de doelgroepen die de wetgeving moeten naleven?
4. Zijn de gevolgen voor de regeldruk volledig en juist in beeld gebracht?

[1] 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).

Contact
Rijnstraat 50
2515 XP Den Haag
Postbus 16228
2500 BE Den Haag
T (070) 310 86 66
info@atr-regeldruk.nl
www.atr-regeldruk.nl

Bevindingen

1. Onderbouwing nut en noodzaak

Algemeen
De Csw strekt ter uitvoering van de Europese NIB-richtlijn. De afweging en onderbouwing van nut en noodzaak heeft op Europees niveau plaatsgevonden en de ruimte om hier nationaal van af te wijken is om die reden beperkt. Dat neemt niet weg dat in de memorie van toelichting nader wordt ingegaan op het belang van aanvullende regelgeving om beter geëquipeerd te zijn tegen ernstige cyberincidenten. Uit de publieke consultaties op het wetsvoorstel blijkt verder dat het nut van aanvullende wetgeving, de verdergaande harmonisering en internationale samenwerking worden onderschreven.

Artikel 19 lid 7
Artikel 19 bevat een bijzondere openbaarheidsbepalingsregeling voor vertrouwelijke, herleidbare gegevens, die afwijkt van de Wet openbaarheid van bestuur (WOB). In het artikel 19 lid 7 wordt dit buiten twijfel gesteld door de WOB niet van toepassing te verklaren op dit type gegevens. Het artikel is overgenomen uit de Wet gegevensbescherming meldplicht cybersecurity (Wgmc). De destijds gekozen uitzondering wordt hiermee voortgezet in de Csw. Dat neemt niet weg dat niet duidelijk wordt waarom de WOB in dit geval onvoldoende bescherming zou bieden. Mogelijk vloeit de bepaling voort uit een zorg van het veld over een WOB-procedure. Alhoewel een dergelijke zorg op zich voor te stellen is, hoeft deze nog niet gerechtvaardigd te zijn. De WOB bevat immers ook uitzonderingsbepalingen die bedoeld zijn om de vertrouwelijkheid van gegevens te borgen.

1.1 Het college adviseert om nader te onderbouwen waarom de WOB in dit geval onvoldoende bescherming biedt en buiten toepassing moet worden verklaard.

2. Minder belastende alternatieven

Invoering dubbele meldplicht
AED's en digitale dienstverleners moeten volgens de richtlijn ernstige ICT-incidenten melden bij de bevoegde autoriteit of het CSIRT.[2] Bij de implementatie is gekozen voor een dubbele melding bij zowel de bevoegde autoriteit als het CSIRT. In tegenstelling tot andere landen heeft Nederland de advies- en toezichthoudende functie apart ondergebracht bij het CSIRT (advies) en de bevoegde autoriteit (toezicht). Bovendien is het nodig dat de meldingen zo snel mogelijk de instanties bereiken. Om die reden is niet gekozen voor een getrapte melding. Om de regeldruk zoveel mogelijk te beperken zal de dubbele meldplicht zo worden vormgegeven, dat de indiener desgewenst met een formulier (een handeling) aan beide meldplichten kan voldoen.

Het college is van mening dat de additionele regeldruk van een dubbele meldplicht op deze manier inderdaad aanzienlijk wordt beperkt. Tegelijkertijd blijft het wel zo dat organisaties

[2] Artikel 14 lid 3 en artikel 16 lid 3.

hetzelfde incident tweemaal aan de overheid moeten melden. Een dubbele meldplicht zal bovendien in de tijd wellicht toch uitnodigen tot verschillende uitvragen van beide organisaties.
De vraag is of de scheiding van functies een gezamenlijk postbusfunctie, uitsluitend voor dit type meldingen, daadwerkelijk in de weg te staat. De melding is namelijk gelijk voor beide organisaties en wordt op hetzelfde moment gedaan. Het is technisch mogelijk om ingekomen berichten gelijktijdig door te geleiden naar meerdere organisaties, zonder afbreuk te doen aan de gewenste organisatorische scheiding.

Bedrijven en organisaties kunnen daarnaast bij cyberincidenten te maken hebben aanvullende meldplichten, zoals die aan de Autoriteit Persoonsgegevens in het geval van een data-lek. Meerdere partijen in het veld hebben in dat licht gewezen op de wenselijkheid van een onderzoek naar een integraal meldingssysteem, waardoor bedrijven slechts één keer hoeven te melden.

2.1 Het college adviseert om een enkele meldplicht in de wet op te nemen, die bijvoorbeeld in de praktijk de vorm heeft van een gezamenlijk postbusfunctie uitsluitend voor dit type meldingen.

2.2 Ook vraagt het college om in te gaan op de vraag hoe wordt geborgd dat de informatievereisten in het geval van een dubbele meldingsplicht in de tijd toch niet uiteen gaan lopen.

2.3 Het college adviseert tot slot om na te gaan met welke meldplichten organisaties naar verwachting nog meer te maken zullen hebben bij een ernstig cyberincident. En of een integraal meldingssysteem kan bijdragen aan een efficiëntere melding en afhandeling daarvan.

3. Merkbare regeldruk

In de consultatie is meerdere keren melding gemaakt van onduidelijkheden in de definitie van digitale dienstverlener. Onduidelijkheid in definities kan ervoor zorgen dat bedrijven niet goed weten of ze wel of niet vallen onder nieuwe wetgeving, met het risico dat ze het zekere voor het onzekere nemen en toch kosten maken om aan de nieuwe regels te voldoen (nalevingsoverschot). De memorie van toelichting is op dit punt nu verduidelijkt.

De onduidelijkheid zou kunnen worden voorkomen door – net als in Denemarken –bedrijven te informeren of ze als digitale dienstverlener zijn aangemerkt. In de memorie van toelichting wordt als reactie op de consultatie geen bereidheid getoond om te zijner tijd dit minder belastende voorbeeld te volgen. De reden die hiervoor wordt gegeven, is dat het benodigde inzicht in de doelgroep zou ontbreken. Deze argumentatie miskent dat aangeschreven bedrijven wel helderheid krijgen of ze wel of niet onder vallen onder de nieuwe regels, ook al is deze aanschrijving niet 100% dekkend. Verder wekt het gebrek aan inzicht de indruk dat de regelgever onvoldoende scherp heeft hoe groot de doelgroep is die te maken krijgt met de nieuwe wetgeving. Dit gebrek aan inzicht belemmert een goed zicht op de totale omvang van de regeldrukeffecten.

3.1 Het college adviseert om de digitale dienstverleners, die onder de reikwijdte van de richtlijn vallen, aan te schrijven.

De Csw bevat open normen voor de maatregelen die aanbieders moeten treffen voor de beveiliging van hun netwerk en informatiesystemen. Deze open normen kunnen verder uitgewerkt worden bij algemene AMvB of in sectorale wetgeving. Om te zorgen dat de concretisering van de normen zo goed aansluit bij de praktijk van AED's is het zaak om deze in overleg met de betrokken sectoren nader uit te werken, uiteraard zonder afbreuk te doen aan het gewenste niveau van beveiliging.

3.2 Het college adviseert om beveiligingseisen verder uit te werken in overleg met de betreffende sectoren zodat deze goed aansluiten bij de gangbare praktijk en systemen.

De Csw overlapt mogelijk met andere sectorspecifieke wetgeving, zoals de Wet financieel toezicht. Mocht dit het geval zijn, dan biedt de Csw de mogelijkheid om bepaalde bij of krachtens de wet vastgestelde voorschriften buiten toepassing te laten. In de memorie van toelichting is een eerste inventarisatie gemaakt van de mogelijke overlap met sectorale wetgeving. Om te voorkomen dat sectoren te maken krijgen met dubbele of wellicht strijdige beveiligingsnormen, is inzicht in eventuele overlap met sectorale wetgeving gewenst. Ook is het nodig om richting de betreffende sectoren duidelijk te maken welke artikelen prevaleren, in ieder geval voorafgaand aan de feitelijke inwerkingtreding van de nieuwe wetgeving.

3.3 Om onduidelijkheden en een nalevingsoverschot te voorkomen is het van belang om voor inwerkingtreding helderheid te bieden of er overlap is tussen de Csw en andere sectorale wetgeving en om daarbij aan te geven welke wetgeving in dat geval leidend is.

4. Berekening regeldruk

De nieuwe verplichtingen omvatten de meldplicht voor ernstige ICT-incidenten, de wettelijke beveiligingseisen, de eenmalige kennisname kosten en de (structurele) toezichtlasten. In de toelichting is opgenomen dat de stijging van de regeldruk naar verwachting beperkt is. Het college heeft voor wat betreft de volledigheid weergave van de regeldrukeffecten de volgende opmerkingen:

- De stijging van de regeldruk als gevolg van de meldplicht is naar verwachting beperkt vanwege het beperkte aantal (10-20 per jaar). ATR deelt deze zienswijze. Om over-compliance te voorkomen is het wel zaak dat helder is wanneer bedrijven wel en niet moeten melden.
- Aanbieders moeten mogelijk (technische en organisatorische) beveiligingsmaatregelen treffen als gevolg van de nieuwe wet. Een inschatting van de nalevingskosten kan volgens de toelichting pas goed gemaakt worden wanneer deze doelvoorschriften verder uitgewerkt worden bij AMvB of in sectorale regelgeving.
  ATR volgt deze redenering. De verwachting dat de kosten te zijner tijd geheel overeenkomen met de "business as usual costs" kan op basis van de beschikbare informatie alleen nog niet worden aangenomen. De aanname dat de nalevingskosten van de implementatie van de wettelijke beveiligingseisen derhalve nul bedragen ook niet. Dit is afhankelijk van de mate

waarin de beveiligingseisen overeenkomen met wat reeds wordt toegepast. Een eerste inschatting van eventuele kosten kan desgewenst gemaakt worden door korte navraag bij een aantal AED's en digitale dienstverleners. Gevraagd wordt om de memorie van toelichting op dat vlak aan te passen.

- In de regeldrukparagraaf ontbreekt nog een inschatting van de hoeveelheid AED's en digitale dienstverleners die onder de wet vallen (de "q"). De reden is onder meer dat AED's nog aangewezen moeten worden en een exacte inschatting nog niet gemaakt kan worden. Digitale dienstverleners vallen alleen wel direct onder de richtlijn. Voor een goede weergave van de regeldrukeffecten is het nodig om in ieder geval een inschatting te maken van het aantal digitale dienstverleners. Verder is het ten behoeve van de politieke besluitvorming ook nu al mogelijk om een "educated quess" te maken van de hoeveelheid AED's, ook al is het exacte aantal nu nog niet bekend. Verwacht mag worden dat vakdepartementen inzicht hebben in de bedrijven en organisaties die het mogelijk treft. Daarnaast bevat het Europese Impact Assessment ook informatie over het aantal organisaties, uitgesplitst naar sector en land, wat als basis mag dienen voor de berekeningen.
- De "business as usual costs" zijn kosten die bedrijven en organisaties al maken voor de eigen interne bedrijfsvoering. De tijd die een bedrijf kwijt is aan het zoeken en aanleveren van de gewenste informatie voor de meldplicht, valt niet onder de zgn. 'business as usual costs'. De meldplicht vloeit direct voort uit de wet en de tijd die een bedrijf kwijt is aan het verzamelen van de informatie valt onder de kosten van regeldruk. Gevraagd wordt om de paragraaf op dat punt aan te passen.

4.1 Het college adviseert om de regeldrukparagraaf conform bovenstaande punten aan te passen ten behoeve van een volledig beeld van de regeldruk-effecten.

5. Dictum

Het college is van mening dat het wetvoorstel nut en noodzaak van de nieuwe regels voldoende onderbouwt. Wel geeft het college mee om na te gaan of het buiten toepassing verklaren van de WOB nodig is en zo ja, dit nader te motiveren in de memorie van toelichting. Het voorstel laat ook zien dat is nagedacht over een lastenluwe vormgeving van de dubbele meldplicht. Dat neemt niet weg dat het college mogelijkheden ziet voor een nog eenvoudiger vormgeving. De regeldrukparagraaf geeft verder een goed inzicht in de diverse verplichtingen van het wetsvoorstel. Een meer principieel punt is dat het wetsvoorstel geen inschatting geeft van de omvang van de doelgroep, in het bijzonder die van de digitale dienstverleners. Zij worden niet bij AMvB aangewezen en vallen direct onder de richtlijn. Zonder inzicht voor de orde van grootte van de doelgroep is het ook niet goed mogelijk om een gevoel te krijgen voor de regeldrukgevolgen van een wetsvoorstel. Door deze onvolkomenheid kan bij normadressanten onduidelijkheid ontstaan of zij al dan niet als zodanig worden gezien. En de onduidelijkheid kan ertoe leiden dat partijen die géén normadressant zijn, zich wel als zodanig gaan gedragen, met een nalevingsoverschot als gevolg. Gelet hierop luidt het dictum van het college over de Cybersecuritywet:

Het wetsvoorstel niet indienen, tenzij met de adviespunten rekening is gehouden.

Het college vertrouwt erop u hiermee voldoende te hebben geïnformeerd. Het verneemt graag van u op welke wijze u met de adviespunten rekening hebt gehouden.

Hoogachtend,

w.g.

M.A. van Hees
Voorzitter

R.W. van Zijp
Secretaris