Adviescollege toetsing regeldruk

> **Retouradres** Postbus 16228 2500 BE Den Haag

Aan de minister van Justitie en Veiligheid
De heer mr. dr. F.B.J. Grapperhaus
Postbus 20301
2500 EH DEN HAAG

ATR, Adviescollege toetsing regeldruk
Rijnstraat 50
2515 XP Den Haag

Postbus 16228
2500 BE Den Haag

T 070 310 86 66
E info@atr-regeldruk.nl
www.atr-regeldruk.nl

Onze referentie MvH/RvZ/AvE/bs/ATR01018/2020-U023
Uw referentie

Datum 26 februari 2020
Betreft Wijziging Besluit beveiliging netwerk- en informatiesystemen

Geachte heer Grapperhaus,

Op 12 februari 2020 is aan het Adviescollege toetsing regeldruk (ATR) voor advies aangeboden het wijzigingsvoorstel Besluit beveiliging netwerk- en informatiesystemen (Bbni).
Als uitwerking van een Europese Richtlijn uit 2016 (de NIB-richtlijn)[1] zijn eerder al de Wet beveiliging netwerk- en informatiesystemen (Wbni) en het Bbni in werking getreden. Aanbieders van een essentiële dienst (AED's) en andere aangewezen vitale aanbieders[2] zijn op grond van de Wbni en het Bbni verplicht om ernstige ICT-incidenten te melden bij het Nationaal Cyber Security Centrum (NCSC). Voor AED's geldt bij ernstige incidenten ook de meldplicht bij de sectorale toezichthouder. Daarnaast moeten AED's zich houden aan de beveiligingseisen uit de wet.
Het voorstel voegt enkele AED's toe waarop het Bbni van toepassing is. Deze toevoegingen betreffen de sector energie en dan specifiek de sectoren elektriciteit en gas. Tevens bevat het voorstel wijzigingen voor de deelsector spoor- en wegvervoer. Verder worden met dit voorstel voorzieningen die behoren tot de digitale overheidsvoorzieningen aangewezen als een vitale aanbieder. Dat betekent concreet dat deze aanbieder ernstige ICT-incidenten moet melden bij het NCSC. Te denken valt aan de Kamer van Koophandel voor de dienst Handelsregister, de centrale voorzieningen van de Basisregistratie Personen (BRP) en DigiD.
Naast genoemde toevoegingen geeft het Besluit nadere regels over de door AED's te nemen beveiligingsmaatregelen. Deze maatregelen betreffen de beheersing van de risico's voor de beveiliging van hun netwerk- en informatiesystemen en om ernstige ICT-incidenten te voorkomen en de gevolgen van dergelijke incidenten zo veel mogelijk te beperken.

[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).
[2] Zie voor de aanwijzing van vitale aanbieders: https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/voor-wie-geldt-de-wbni/vitale-aanbieders.

Toetsingskader

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

1. Nuloptie (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. Nut en noodzaak

Het doel van de uitbreiding van de AED's in de sectoren elektriciteit en gas is met name om de risico's van de onderlinge afhankelijkheid in de keten te verkleinen. Zo vallen voortaan ook grote producenten en een beheerder van een (grensoverschrijdende) interconnector onder het besluit. De toelichting vermeldt dat de aanwijzingen van deze nieuwe AED's zijn besproken met de betrokken marktpartijen. De toevoegingen uit de sector spoor- en wegvervoer komen voort uit een nieuwe vitaliteitsbeoordeling. De toevoeging van de genoemde digitale overheidsvoorzieningen volgt uit de overweging dat uitval of compromittering van deze voorzieningen leidt tot een maatschappelijk ongewenste verstoring van de dienstverlening of het economisch verkeer.
Met de nadere uitwerking van de zorgplicht voor beveiligingsmaatregelen geeft het besluit een gemeenschappelijk kader voor de aangewezen AED's. Volgens de toelichting bevordert dit de rechtszekerheid. Ook draagt het bij aan effectief toezicht. Deze maatregelen, die een AED in ieder geval moet nemen, hebben primair tot doel de digitale weerbaarheid te verhogen.
Het college vindt nut en noodzaak van de wijziging voldoende onderbouwd en heeft geen opmerkingen op dit punt.

2. Minder belastende alternatieven

De wijzigingen uit dit besluit veroorzaken regeldruk. De (nieuw aangewezen) AED's moeten ernstige incidenten melden bij het NCSC en bij de bevoegde autoriteit. De andere aangewezen vitale aanbieders hoeven alleen te melden bij het NCSC. De meldplicht geldt alleen voor incidenten met aanzienlijke gevolgen voor de continuïteit van de door de AED verleende dienst. Een melding kan schriftelijk of telefonisch worden gedaan.
Daarnaast moeten de AED's beveiligingsmaatregelen treffen. Deze beveiligingsmaatregelen hebben betrekking op de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van de netwerk- en informatiesystemen die een essentiële dienst ondersteunen. Het besluit bevat de minimale eisen. De toelichting geeft aan dat ook zonder wetgeving AED's al de nodige beveiligingsmaatregelen hebben getroffen. De toelichting vermeldt dat uit gevoerde gesprekken met AED's blijkt dat enkele van deze nieuwe AED's verwachten dat hun beveiligingsmaatregelen nu reeds of nagenoeg op het niveau van de Wbni en het Bbni zijn, waardoor de additionele kosten beperkt zullen zijn. Voor andere producenten geldt echter dat hun aanwijzing als AED de belangrijkste reden is om extra beveiligingsmaatregelen te treffen. Dit levert dus een divers beeld op voor wat betreft de consequenties van de gestelde eisen. De toelichting geeft tevens aan dat waar gewenst de maatregelen verder kunnen worden uitgewerkt bij regeling van de sectoraal verantwoordelijke bewindspersoon of in beleidsregels van de bevoegde toezichthouder.

Het college ziet, binnen het licht van de gewenste beveiliging van essentiële diensten, geen minder belastende alternatieven.

3. Werkbaarheid

De aangewezen AED's moeten voldoen aan de beveiligingseisen uit dit Besluit. Deze eisen vloeien voort uit de wettelijke zorgplicht die een essentiële dienst heeft voor veilige netwerk- en informatiesystemen. De toelichting vermeldt dat is gekozen voor een invulling die de benodigde ruimte laat aan de AED en de toezichthouder om tot een voor de sector passende invulling te komen. Ook is er zo veel mogelijk ruimte om aan te sluiten bij bestaande en eventuele nieuwe normenkaders. Hiervoor is gekozen omdat de zorgplicht van toepassing is op diverse sectoren met elk een eigen risicoprofiel van de beveiliging van netwerk- en informatiesystemen. De toelichting geeft tevens aan dat de regeldruk deels afhangt van de uitleg die de bevoegde autoriteit de komende jaren zal geven aan de concrete invulling van de beveiligingseisen. Het college geeft in overweging om de bevoegde autoriteiten te verzoeken om, in goed overleg met de sectoren, spoedig met een nadere invulling van de beveiligingseisen te komen, zodat de uitvoerders weten wat van hen concreet wordt verwacht.
De toelichting vermeldt voorts dat het besluit de mogelijkheid geeft om het tijdstip van inwerkingtreding van deze Bbni-wijziging voor de verschillende artikelen of onderdelen daarvan verschillend vast te stellen. Het college merkt op dat dit positief is, omdat het de uitvoerbaarheid van het besluit kan bevorderen.

4. Gevolgen regeldruk

De toelichting bevat een uitgebreide regeldrukparagraaf. Daarin wordt een onderscheid gemaakt in eenmalige en structurele lasten. De regeldrukgevolgen zijn van tevoren besproken met de nieuwe AED's en voorgelegd aan bestaande AED's.
Voor wat betreft het doen van een melding wordt uitgegaan van (300 minuten x 2 meldingen per jaar x 60,- euro) € 3.600,- per jaar.
Om te voldoen aan de beveiligingseisen uit het besluit moeten de nieuwe AED's extra capaciteit en expertise inzetten. Voor de eerste twee jaar gaat het voor alle producenten samen om ongeveer € 7,9 miljoen (€ 4 miljoen per jaar). Daarnaast verwachten de producenten in de eerste twee jaar ook zo'n € 4,5 miljoen (€ 2,3 miljoen per jaar) aan eenmalige investeringen te moeten doen in informatietechnologie (IT) en operationele technologie (OT).
Naar schatting van de producenten is er structureel voor hen samen circa 16 fte noodzakelijk om blijvend te voldoen aan de beveiligingseisen van de Wbni en het Bbni. Dit komt uit op een bedrag van circa € 1,9 miljoen per jaar. Voor onderhouds- en vervangingskosten als gevolg van de gedane investeringen in IT en OT wordt structureel een bedrag van circa € 0,4 miljoen per jaar geschat.
De eenmalige kennisnamekosten bedragen € 960,- per organisatie, de toezichtlasten € 960,- per organisatie per jaar.
Voor wat betreft de gevolgen voor de regeldruk voor bestaande AED's vermeldt de toelichting dat de meeste AED's aangeven dat de extra regeldruk als gevolg van de eisen uit het Bbni relatief beperkt zullen zijn, omdat de eisen aansluiten bij de maatregelen die in de sectoren al worden toegepast. Afhankelijk van de reeds gedane investeringen is de hoogte van de *extra* investeringen per organisatie als gevolg van dit besluit variabel.

Het college merkt op dat de regeldrukgevolgen goed en volledig in beeld zijn gebracht, en heeft hierbij geen opmerkingen.

Dictum

Gelet op bovengenoemde bevindingen is het eindoordeel ten aanzien van de consultatie-versie van dit voorstel:

Het voorstel indienen / vaststellen.

In de verwachting u hiermee voldoende te hebben geïnformeerd,

Hoogachtend,

w.g.

M.A. van Hees
Voorzitter

R.W. van Zijp
Secretaris