Consultatieverslag wetsvoorstel uitvoeringswet cyberbeveiligingsverordening

17 augustus 2020

Het ontwerp-wetsvoorstel (in het kort: de uitvoeringswet cyberbeveiligingsverordening) tot uitvoering van Verordening (EU) nr. 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (hierna: de cyberbeveiligingsverordening), is geconsulteerd via internetconsultatie.nl. De consultatie vond plaats van 25 juni 2020 tot en met 16 augustus 2020. Op deze consultatie zijn in totaal 7 reacties ontvangen, waarvan 5 openbaar zijn (zie https://www.internetconsultatie.nl/uitvoeringswetcyberbeveiligingsverordening).

Het overgrote deel van de reacties is afkomstig vanuit het bedrijfsleven. De overige reacties zijn afkomstig van particulieren. De opmerkingen zijn bekeken en zo veel mogelijk verwerkt.

Goedkeuringsprocedure

Een aantal organisaties hadden een aantal opmerkingen over de goedkeuringsprocedure. Hieronder worden de opmerkingen op hoofdlijnen behandeld.

Een organisatie stelt dat artikel 3 van de uitvoeringswet, de melding, geen toegevoegde waarde heeft en tot vertraging kan leiden. In reactie hierop wil het kabinet benadrukken dat de nationale autoriteit met deze melding voorbereidingen kan treffen voor de stapsgewijze goedkeuringsprocedure en dat dit naar verwachting ten goede komt aan de doorlooptijd van de goedkeuringsprocedure.

Een organisatie stelt voor om de nationale autoriteit het onderzoeksplan a priori te laten goedkeuren, en pas na het uitbrengen van de conformiteitsverklaring te laten toetsen. Het kabinet acht aanpassing van het ontwerpwetsvoorstel hierop niet wenselijk. In het wetsvoorstel is bewust gekozen voor het goedkeuringsmodel met stapsgewijze goedkeuring, waarbij de nationale autoriteit het onderzoeksplan niet zonder beoordeling goedkeurt. Het gaat immers om ICT-producten, -diensten, en -processen met hoge veiligheidsrisico's. Dit neemt niet weg dat er voor bepaalde categorieën ICT-producten, -diensten, en -processen omstandigheden kunnen zijn die aanleiding kunnen geven om van deze hoofdregel af te wijken. Dit dient bij ministeriële regeling geregeld te worden (artikel 4 lid 2 van de uitvoeringswet).

Kiwa Nederland BV ziet toegevoegde waarde in de procedure rondom het goedkeuringsbesluit, de autoriteit kan immers, indien nodig, tijdig interveniëren in het certificatietraject. Kiwa Nederland BV suggereert om vormvereisten verder te regelen in artikel 4 van de uitvoeringswet. Het kabinet merkt op dat het de voorkeur heeft om vormvereisten niet in een formele wet, maar in lagere regelgeving te regelen. Dit komt onder meer tot uitdrukking in artikel 4, vijfde lid van de uitvoeringswet. Tevens kunnen vormvereisten rechtstreeks uit een Europese cyberbeveiligingscertificeringsregeling volgen.

Twee organisaties merken op dat de beslistermijnen van de goedkeuringsprocedure (artikelen 4 en 5 van de uitvoeringswet) tot onnodige vertraging zullen leiden. Hierdoor kan mogelijk negatieve marktwerking in Nederland optreden. Daarbij roepen de organisaties op om voor bepaalde categorieën van ICT-producten, -diensten en -processen standaardprocedures te ontwikkelen met een vlotte doorlooptijd. Met betrekking tot de beslistermijnen merkt het kabinet op dat de gekozen termijnen maximale termijnen betreffen. De Awb stelt dat een besluit binnen een redelijke termijn genomen dient te worden en dat een termijn van acht weken als een redelijke termijn beschouwd kan worden. De nationale autoriteit dient binnen de gestelde termijn een besluit te nemen. Dit betekent dat de autoriteit eerder een besluit kan nemen. Het is daarbij de insteek dat de besluitvormingsprocessen binnen de autoriteit niet tot onnodige vertraging zullen gaan leiden. Verder zal de autoriteit standaardprocedures ontwikkelen, voor zover dit mogelijk is gelet op de betreffende certificeringsregeling.

Een organisatie vraagt of er gedurende de goedkeuringsprocedure contact kan plaatsvinden tussen de conformiteitsbeoordelingsinstantie en de nationale autoriteit. Hierop geeft het kabinet mee dat het mogelijk moet zijn dat een conformiteitsbeoordelingsinstantie en de nationale autoriteit informeel contact kunnen hebben.

Updates, hacks of patches

Kiwa Nederland BV stelt dat artikel 7 van de uitvoeringswet zou moeten worden aangevuld met aanvullende regels waarbij wordt vastgesteld hoe er omgegaan wordt met bepaald situaties, zoals *updates*, *hacks* of *patches*.
Het kabinet acht aanpassing van de uitvoeringswet hierop niet nodig. De regels omtrent het beschikbaar stellen en uitvoeren van updates en de naleving ervan zullen een onderdeel van iedere certificeringsregeling zijn. De op grond van de cyberbeveiligingsverordening vastgestelde certificeringsregelingen hebben onder meer als doelstelling dat ICT-producten, -diensten en –processen worden geleverd met actuele software en hardware die geen algemeen bekende kwetsbaarheden bevatten, en met mechanismen voor beveiligde updates (artikel 51, aanhef en onder j, van de cyberbeveiligingsverordening). Daarnaast zal bij de uitwerking van deze certificeringsregelingen per regeling nader ingegaan worden op onder andere de wijze waarop voorheen onopgemerkte kwetsbaarheden, zoals hacks, in de cyberbeveiliging moeten worden aangepakt (artikel 54, eerste lid, aanhef en onder m, van de cyberbeveiligingsverordening).
De regels inzake updates, hacks of patches en de gevolgen van de updates, hacks of patches voor het zekerheidsniveau en het afgegeven certificaat zullen per afzonderlijke Europese cyberveiligheidscertificeringsregeling moeten worden bepaald. Het is dan ook niet de doelstelling om dergelijke *updates*, *hacks* of *patches* in de uitvoeringswet te regelen, maar indien een Europese cyberbeveiligingscertificeringsregeling dit vereist kan dit middels een ministeriële regeling nader uitgewerkt worden.

Overig

Ook brengt Kiwa Nederland BV op dat hoofdstuk 4 van de uitvoeringswet niet ingaat op concepten zoals *continuous compliance* en *market surveillance activities*. Ten aanzien hiervan merkt het kabinet op dat de cyberbeveiligingsverordening de nationale autoriteit niet beperkt in haar methodiek omtrent toezicht. De nationale autoriteit zal dan ook onverkort de hedendaagse methodes kunnen toepassen.

Cyberveilig Nederland merkt op dat de nationale autoriteit over voldoende personele middelen dient te beschikken. Ook merkt Cyberveilig Nederland op dat kwaliteitseisen aan certificaten zoveel mogelijk in wet- en regelgeving vastgelegd moeten worden. Daarnaast dient certificering van zekerheidsniveau hoog verplicht te worden. Met betrekking tot personele middelen spant het kabinet zich in om de nationale autoriteit over voldoende capaciteit te laten beschikken. De kwaliteitseisen van certificaten zullen naar verwachting volgen uit de betreffende Europese cyberbeveiligingscertificeringsregelingen. Verder zal het kabinet in Europees verband zich ertoe inspannen dat de betreffende cyberbeveiligingscertificeringsregelingen een verplicht karakter krijgen. Hierbij moet opgemerkt worden dat de Europese Commissie ook eerder dan 31 december 2023 certificeringsregelingen verplicht kan stellen.