Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 3451

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 29 juni 2022

De vaste commissie voor Digitale Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Justitie en Veiligheid over:

– het Fiche: Verordening cyberbeveiliging van instellingen, organen en instanties van de Europese Unie (Kamerstuk 22 112, nr. 3406) en
– het Fiche: Verordening Informatiebeveiliging in de instellingen, organen en instanties van de Unie (Kamerstuk 22 112, nr. 3405)

De vragen en opmerkingen zijn op 30 mei 2022 aan de Minister van Justitie en Veiligheid voorgelegd. Bij brief van 27 juni 2022 zijn de vragen beantwoord.

De voorzitter van de commissie,
Kamminga

De adjunct-griffier van de commissie,
Van Tilburg

kst-22112-3451
ISSN 0921 - 7371
's-Gravenhage 2022

Vragen en antwoorden

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de stukken voor het schriftelijk overleg: BNC-fiches inzake Verordening Informatiebeveiliging en cybersecurity in de instellingen, organen en instanties van de Unie. Deze leden onderschrijven de doelstellingen van de verordeningen en hebben hierover nog enkele vragen en opmerkingen.

Fiche: Verordening cyberbeveiliging van instellingen, organen en instanties van de Europese Unie

De leden van de VVD-fractie lezen dat digitale weerbaarheid wat het kabinet betreft niet meer vrijblijvendheid kan zijn. Op welke manieren kan dit voldoende worden gewaarborgd in het deze verordening? Hoe verhoudt deze verordening zich tot de NIS 2-richtlijn?

Het voorstel voor de verordening biedt een aantal bepalingen op basis waarvan de instellingen, organen en instanties van de EU (EU IOA's) verplicht worden maatregelen te nemen ten behoeve van hun digitale weerbaarheid. Zo zijn er verplichtingen voor de EU IOA's tot het opzetten van een intern kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's en verplichtingen inzake risicobeheer en rapportage op het gebied van cyberbeveiliging. Daarnaast houdt het voorstel voorschriften over de organisatie en werking van het cyberbeveiligingscentrum voor de EU IOA's (CERT-EU) en een interinstitutionele raad voor cyberbeveiliging (IICB). Hiermee wordt naar het oordeel van het kabinet het niveau van cyberbeveiliging van de EU IOA's verhoogd.

Zowel dit voorstel als het voorstel voor de herziening van de Netwerk- en informatiebeveiligingsrichtlijn (NIB2) heeft tot doel de digitale weerbaarheid binnen de EU te verhogen. Wat betreft reikwijdte en systematiek verschillen beide initiatieven echter. Het eerste voorstel ziet specifiek op de cyberbeveiliging van de IOA's van de EU, terwijl het voorstel voor de NIB2-richtlijn betrekking heeft op de beveiliging van systemen van essentiële en belangrijke entiteiten binnen de EU-lidstaten, waaronder delen van het bedrijfsleven en overheden van lidstaten, en niet ook op IOA's van de EU. De systematiek van het voorstel voor de verordening houdt in dat de EU IOA's gehouden zijn specifieke maatregelen te implementeren en te rapporteren aan de IICB. De NIB2-richtlijn gaat daarentegen uit van een zorgplicht, waar ook toezicht op wordt gehouden door een toezichthouder.

Het kabinet acht het van belang dat het voorstel een met de NIB2-richtlijn vergelijkbaar niveau van eisen met betrekking tot digitale weerbaarheid bewerkstelligt en zal daarop inzetten in gesprekken met de Europese Commissie en andere lidstaten.

De leden van de VVD-fractie lezen dat de instellingen, organen en instanties van de Unie (EU-IOA's) eigen kaders mogen opstellen die betrekking hebben op cybersecurity. Deze leden begrijpen dat er verschillen in de kaders kunnen zijn tussen de verschillende EU-IOA's, maar zouden een wirwar van kaders ook een risico kunnen zijn voor bestuurbaarheid en digitale veiligheid? Digitale veiligheid is zo sterk als de zwakste schakel.

Omdat iedere EU IOA een andere opdracht heeft en andere soorten gegevens verwerkt, heeft het kabinet begrip voor het uitgangspunt dat de EU IOA's een eigen kader opstellen met betrekking tot hun cybersecurity. Een risicogebaseerde en proportionele aanpak acht het kabinet dan ook passend.

Desalniettemin erkent het kabinet het risico van een te grote verscheidenheid aan maatregelen. Om de bestuurbaarheid van het geheel te kunnen overzien is het van belang dat er een duidelijke, gelijksoortige opdracht ligt die geldt voor alle EU IOA's. Daartoe vormt het huidige voorstel een basis. De inzet van het kabinet is om te waarborgen dat er voldoende uniformiteit en flexibiliteit is om de digitale weerbaarheid van alle EU IOA's op een passend niveau te hebben.

Is het kabinet het met deze leden eens dat in alle kaders minimale veiligheidseisen geborgd moeten worden? Zo ja, gaat het kabinet dit meenemen bij de behandeling van deze verordening? Zo nee, waarom niet?

Het kabinet is het eens met de VVD-fractie dat er minimale veiligheidseisen gewaarborgd moeten worden. Het voorstel voorziet hier ook in: in Annex I van het voorstel is een lijst opgenomen met domeinen die door iedere EU IOA dienen te worden geadresseerd. In Annex II staan verder concrete stappen waar de EU IOA's aandacht aan dienen te besteden. Het kabinet zal erop inzetten dat minimale veiligheidseisen onderdeel blijven van het voorstel.

Fiche: Verordening Informatiebeveiliging in de instellingen, organen en instanties van de Unie

De leden van de VVD-fractie onderschrijven de beoordeling van het kabinet over de eigen merkingen van EU-IOA's. Deze leden onderschrijven ook de inzet van het kabinet over het verwijderen van de categorie «niet gerubriceerde informatie» uit de verordening. Wat is het standpunt van andere lidstaten over het verwijderen van de categorie «niet gerubriceerde informatie»?

De meerderheid van de lidstaten lijkt de zorg van het kabinet te delen over het ontbreken van een (juridisch) systeem in de lidstaten voor de beveiliging van deze categorie informatie, indien deze informatie met lidstaten gedeeld wordt. Tevens verwacht het kabinet dat de meerderheid van de lidstaten de positie van het kabinet deelt dat de introductie van de categorie «niet gerubriceerde informatie» bij de EU-IOA's kan leiden tot een toename in administratieve lasten en het verkeerd rubriceren van informatie.

Op welke manier kan de slagkracht van de veiligheidsdirectoraten van de EU-IOA's beter gepositioneerd en verbeterd worden zodat informatie beter beveiligd kan worden?

Het kabinet verwacht dat de slagkracht van de veiligheidsdirectoraten van de EU IOA's verbeterd kan worden door de organisatorische inbedding van de veiligheidsdirectoraten te versterken en hun budgetten te verhogen.

Vragen en opmerkingen van de leden van de SP-fractie

De leden van de SP-fractie hebben kennisgenomen van de BNC-fiches die gaan over de verbetering van de informatiebeveiliging van EU-instellingen, organen en instanties, alsmede de verbetering van de

cyberbeveiliging. Over de twee verordeningen hebben deze leden los wat vragen, maar ook wat algemene overkoepelende vragen.

De leden van de SP-fractie vragen of het mogelijk is aan te geven wat nu de stand van zaken is bij de verschillende EU-instellingen, organen en instanties.

De Europese Rekenkamer (ERK) heeft in maart 2022 een rapport gepubliceerd over de cyberweerbaarheid van EU IOA's.[1] Uit dit onderzoek blijkt dat het aantal significante cyberincidenten bij EU IOA's sinds 2018 is vertienvoudigd. De conclusie van de ERK is dat het bereikte niveau van cyberparaatheid in de gemeenschap van EUIOA's niet in verhouding staat tot de dreigingen waaraan zij is blootgesteld. Ook concludeert de ERK dat de goede praktijken op het gebied van cyberbeveiliging, waaronder bepaalde essentiële controles, niet altijd worden toegepast, en dat enkele EU IOA's duidelijk te weinig middelen uittrekken voor cyberbeveiliging.

Op dit moment zijn de EU IOA's zelf verantwoordelijk voor het opstellen en implementeren van regels voor informatiebeveiliging. Dit heeft geleid tot fragmentatie van regelgeving voor informatiebeveiliging en in enkele gevallen tot het ontbreken hiervan. Deze situatie bemoeilijkt het uitwisselen van informatie tussen de EU IOA's en vergroot de kans op informatiebeveiligingsincidenten.

Het kabinet verwelkomt daarom ook de voorstellen om de cyberbeveiliging en informatiebeveiliging van de EU IOA's sterk te verbeteren.

Het verwondert deze leden dat er een verordening nodig is om de informatiebeveiliging op orde te krijgen. Kan het kabinet aangeven waarom dit niet intrinsiek als opdracht wordt ervaren?

Het kabinet kan geen inschatting geven van de intrinsieke ervaring van specifiek de EU IOA's. In het algemeen geldt dat digitale weerbaarheid, waaronder zowel informatiebeveiliging als cyberbeveiliging, vaak niet de urgentie krijgt die het verdient. Zo wordt ook in het Cybersecuritybeeld Nederland 2021 (CSBN 2021) geconcludeerd dat organisaties niet of niet voldoende basismaatregelen nemen van tegen de digitale dreiging.[2] Het is mogelijk dat dit ook geldt voor sommige EU IOA's. Daarom verwelkomt het kabinet dat de Europese Commissie daar middels voorliggende voorstellen verandering in wil brengen. Deze voorstellen kunnen fungeren als aansporing voor de EU IOA's om hier voldoende middelen voor beschikbaar te stellen.

Deze leden vragen hetzelfde over de verordening cyberbeveiliging; welke EU-instellingen, organen en instanties zijn kwetsbaar en hoe komt dat?

Het kabinet kan geen precies beeld geven van specifieke EU IOA's waarvan de cyberbeveiliging kwetsbaar is. Algemeen kan worden gesteld, onder meer op basis van voornoemd ERK-rapport, dat er werk aan de winkel is om het cybersecurityniveau van alle EU-IOA's op het niveau te krijgen dat proportioneel is aan de risico's en dreiging.

De leden van de SP-fractie zijn er van overtuigd dat als er nu een goede analyse wordt gemaakt, het daarmee ook mogelijk is voortgang in de informatiebeveiliging en cyberbeveiliging te volgen. Hoe ziet het kabinet dit?

---

[1] https://www.eca.europa.eu/Lists/ECADocuments/SR22_05/SR_cybersecurity-EU-institutions_NL.pdf.

[2] Cybersecuritybeeld Nederland 2021, Kamerstuk 26 643, nr. 767.

Zoals reeds benoemd heeft de Europese Rekenkamer in maart 2022 een uitgebreid rapport gepubliceerd over de cyberweerbaarheid van EU IOA's. Het kabinet ziet dit rapport als een goede nulmeting om de voortgang in de toekomst te volgen. Tevens dient iedere EU IOA periodiek een maturiteitsbeoordeling uit te voeren. Het kabinet is van mening dat hiermee op gedegen wijze de voortgang kan worden beoordeeld.

De leden van de SP-fractie zijn voor zowel de informatie- als de cyberbeveiliging benieuwd naar het speelveld van de verschillende lidstaten en de Nederlandse positie. Waar staat Nederland (redelijk) alleen en waar niet?

In geval van beide verordeningen lijken andere lidstaten in grote mate de positie van Nederland te steunen. Zo lijkt er steun voor bijvoorbeeld een sterkere samenhang met de NIB2-richtlijn en in de vraag of de IICB voldoende bevoegdheden krijgt. Er zijn nog geen punten gebleken waarop Nederland alleen staat. De Europese Raad heeft in zijn conclusies de afgelopen jaren verschillende keren aandacht gevraagd voor een hoog niveau van cybersecurity en informatiebeveiliging van EU IOA's met oog op vergaande digitalisering en de toenemende dreiging.[3] Lidstaten zullen dus naar verwachting, net als het kabinet, inzetten op verordeningen die een hoog niveau van informatie- en cyberbeveiliging van EU IOA's bewerkstelligen.

Hoe ziet het kabinet haar rol in het agenderen van hogere standaarden van beveiliging?

Digitale weerbaarheid is randvoorwaarde voor het ongestoord functioneren van onze steeds verder gedigitaliseerde maatschappij. Hiertoe moeten burgers, bedrijven en overheden inspanningen leveren. Voor het agenderen hiervan ziet het kabinet een belangrijke rol voor zichzelf weggelegd. Dit wordt nader uitgewerkt in de Nederlandse Cybersecuritystrategie (NLCS) die na afronding met de Tweede Kamer zal worden gedeeld.

Wat betreft informatiebeveiliging geldt dat de lidstaten toezicht houden op de beveiliging van gerubriceerde EU informatie. Hiertoe neemt de Nederlandse Nationale Veiligheidsautoriteit (NSA) deel aan het Beveiligingscomité van de Raad, het Beveiligingscomité van de Europese Dienst voor Extern Optreden en de Werkgroep Veiligheidsexperts van de Commissie. In deze gremia vraagt Nederland aandacht voor hoge standaarden van beveiliging.

Het gebruik van standaarden kan in algemene zin bijdragen aan hoger niveau van digitale veiligheid. Het kabinet zet in op het zo veel mogelijk harmoniseren van de verschillende standaardisatie-initiatieven. Het kabinet omarmt dan ook Europese wetgeving zoals de Europese cyberbeveiligingsverordening, die een Europees raamwerk voor cyberbeveiligingscertificeringsschema's introduceert en daarmee ook tot meer uniformiteit in standaardisatie leidt. De cyberbeveiligingscertificeringsschema's bevatten immers beveiligingsnormen die mede gebaseerd zijn op internationale standaarden. Ook bij de totstandkoming van de Europese Cyber Resilience Act bepleit het kabinet dat daarin aan fabrikanten en leveranciers van alle digitale producten, diensten en processen die in de EU op de markt worden gebracht, minimale beveili-

[3] Recent n.a.v. de informele Telecom Raad (9 maart jl.) heeft de Raad gesteld dat: «Strongly believe that EU institutions, agencies and bodies should take measures to further strengthen their cyber and information security as the EU has become a key strategic player whose role on the international stage requires to secure its data and networks against cyber threats.»

gingseisen worden opgelegd, waarmee ook uniformiteit inzake standaarden wordt bevorderd.

Hoe leren EU-IOA's van een datalek of een cyberaanval bij één van hen?

Op basis van het voorstel voor de cyberbeveiligingsverordening kan CERT-EU informatie over incidenten die zich hebben voorgedaan bij een van de EU IOA's delen met andere EU IOA's. Indien die informatie de identiteit van de getroffen EU IOA onthult, vereist dat toestemming van die EU IOA. Tevens is er in het voorstel een verplichting opgenomen voor EU IOA's om significante incidenten binnen 24 uur te melden bij CERT-EU. CERT-EU kan die informatie verspreiden onder de andere EU IOA's om hun systemen te helpen beschermen tegen soortgelijke incidenten, dreigingen en kwetsbaarheden.

Op dit moment werken de lidstaten daarnaast reeds samen met CERT-EU via het Europese CSIRT-netwerk, zoals bedoeld in de NIB-richtlijn – een netwerk van Computer Security Incident Response Teams (CSIRTs) van de EU-lidstaten en CERT-EU. In dit netwerk wordt ook waar mogelijk informatie over concrete cyberdreigingen en -aanvallen gedeeld. In geval van dreigingen en incidenten die verband houden met de nationale veiligheid geldt voorts dat inlichtingen- en veiligheidsdiensten van de lidstaten kunnen samenwerken met de EU IOA's. Deze samenwerking zal plaatsvinden op basis van door de lidstaten te stellen voorwaarden voor wat betreft de vertrouwelijkheid van de bilaterale samenwerking.

Is er met de nieuwe voorstellen rond het uitwisselen van informatie en het instellen van het Cyberbeveiligingscentrum sprake van overlappende taken met nationale cyberbeveiligingsinstellingen of juist van braakliggend terrein? Kan het kabinet daar op ingaan?

CERT-EU is een al bestaande organisatie waarmee al sinds de inwerkingtreding van de huidige Netwerk- en informatieveiligheidsrichtlijn door lidstaten wordt samengewerkt voor de uitwisseling van informatie. Dit gebeurt via het bovengenoemde CSIRT-netwerk. Er is dus geen sprake van braakliggend terrein. Doelgroep van CERT-EU zijn de EU IOA's, terwijl de CSIRTs van de lidstaten op basis van de huidige NIB-richtlijn aanbieders van essentiële diensten en digitale dienstverleners tot doelgroep hebben. Daar vallen de EU IOA's niet onder, en in die zin is er dus ook geen sprake van overlap.

Tot slot vragen de leden van de SP-fractie hoe het kabinet ervoor wil zorgen dat dit inhoudelijke, maar zeker ook technische onderwerp, voldoende geborgd is als het bij de Raad Algemene Zaken wordt besproken? Kan het kabinet daar een bespiegeling op geven?

De Horizontale Raadswerkgroep Cyber is primair verantwoordelijk voor het voorbereiden van de Raadspositie op dit onderwerp en zal in deze hoedanigheid ook de uiteindelijke besluitvorming in de Raad Algemene Zaken voorbereiden. Deze Raadswerkgroep vormt een horizontaal platform voor harmonisatie en een uniforme aanpak van cybervraagstukken waarin verschillende perspectieven op dit vraagstuk samengebracht worden. Vereiste technische expertise zal dus ook via deze werkgroep ten goede komen aan de Raad Algemene Zaken.

Daarnaast adviseert het Beveiligingscomité van de Raad over informatieveiligheid en de beveiliging van gerubriceerde EU-informatie, en doet zo nodig aanbevelingen aan de Raad.

Vragen en opmerkingen van de leden van de GroenLinks-fractie

Fiche: Verordening cyberbeveiliging van instellingen, organen en instanties van de Europese Unie

De leden van de GroenLinks-fractie zien cybersecurity als randvoorwaarde van een digitaliserende samenleving en overheid. Dit is natuurlijk ook van toepassing op Europese instellingen, organen en instanties (EU-IOA's).

Deze leden lezen dat EU-IOA's ten minste om de drie jaar een maturiteitsbeoordeling van hun cyberbeveiliging dienen uit te voeren. Weet het kabinet waar deze tijdsspanne op gebaseerd is? Is het kabinet het ermee eens dat veranderingen in de cyberwereld in een hoog tempo gaan, en de voorgestelde tijdsspanne tussen maturiteitsbeoordeling wellicht te lang is?

Het standpunt van het kabinet is dat drie jaar een logische termijn is, die niet afwijkt van wat gangbaar is. Deze termijn geeft tijd om uitvoering te geven aan de aanbevelingen die uit de maturiteitsbeoordeling voortkomen. Dergelijke maatregelen kunnen zo ingrijpend in de werkwijze van de organisatie zijn dat deze tijd nodig is. De uit een maturiteitsbeoordeling voortkomende aanbevelingen kunnen bovendien variëren in vereiste implementatietermijn. Het is dus geenszins de bedoeling dat in een dergelijke periode niets gebeurt, maar juist dat er maatregelen worden genomen ter bevordering van de digitale weerbaarheid.

De leden van de GroenLinks-fractie lezen ook dat de interinstitutionele raad voor cyberbeveiliging (IICB) slechts niet-bindende waarschuwingen kan geven en audits kan aanbevelen. Denkt het kabinet dat dit voldoende effect heeft op EU-IOA's? Deze leden lezen namelijk ook dat de Europese Rekenkamer geconcludeerd heeft dat het paraatheidsniveau van de EU-IOA's over het algemeen niet in verhouding staat tot de dreiging.[4] Deze leden hopen op een kritische houding richting de EU-IOA's met betrekking tot dit thema.

Zoals in het BNC-fiche over het voorstel tot een Verordening cyberbeveiliging van instellingen, organen en instanties van de Europese Unie is aangegeven leeft ook bij het kabinet de vraag in hoeverre de IICB voldoende bevoegdheden zal hebben om naleving van de verordening te bevorderen.[5] Het is van belang daarbij te benadrukken dat een balans dient te worden gezocht tussen de autonome positie van de EU IOA's en het belang om over de gehele linie de digitale weerbaarheid te verhogen. Het is daarnaast de vraag in hoeverre er een juridische grondslag is op basis waarvan er strengere eisen kunnen worden gesteld aan de EU IOA's. Het kabinet is hierover in de Europese Raad in gesprek met de andere EU-lidstaten.

De leden van de GroenLinks-fractie stellen vast dat CERT-EU, onder andere, ook de bevoegdheid tot het delen van informatie met nationale instanties van lidstaten en tot het samenwerken met derde landen krijgt. Wordt er ook toezicht gehouden op deze bevoegdheden? Hoe ziet het kabinet de controlerende rol van het Europees Parlement als democratisch gekozen volksvertegenwoordigers in bredere zin in dit dossier?

---

[4] Europese Rekenkamer, 2022, Speciaal verslag, «Cyberbeveiliging van EU-instellingen, -organen en -agentschappen, Paraatheidsniveau staat over het algemeen niet in verhouding tot dreigingen» (https://www.eca.europa.eu/Lists/ECADocuments/SR22_05/SR_cybersecurity-EU-institutions_NL.pdf).

[5] BNC-fiche Verordening cyberbeveiliging van instellingen, organen en instanties van de Europese Unie, Kamerstuk 22 112, nr. 3406.

Op basis van het huidige voorstel zal de IICB toezicht houden op de uitvoering van de algemene prioriteiten en doelstellingen van CERT-EU. Ook is op basis van het voorstel goedkeuring van de IICB nodig in geval van samenwerkingsovereenkomsten met derde landen. In de IICB zullen vertegenwoordigers van verschillende EU IOA's plaatsnemen, waaronder van het Europees Parlement. Het kabinet hecht er belang aan dat het Europees Parlement deze rol vervult, zowel omdat het de taak van volksvertegenwoordiging heeft, als omdat het een prominente EU IOA betreft. Het voorstel voorziet niet uitdrukkelijk in een andere toezichthoudende rol voor het Europees Parlement.

Fiche: Verordening Informatiebeveiliging in de instellingen, organen en instanties van de Unie

De leden van de GroenLinks-fractie zien het als nuttig en waardevol dat er een voorstel ligt voor een gemeenschappelijk niveau van informatiebeveiliging. Deze leden lezen dat ieder EU-IOA een eigen intern informatiebeveiligingsbeleid kan opzetten. Deze leden vragen wat het kabinet ervan vindt dat hierbij elk EU-IOA een «eigen wiel» zal moeten uitvinden, in plaats van dat er gekozen is voor harmonisatie van informatiehuishouding tussen instellingen, organen en instanties. Hoe wordt er door het Nederlandse kabinet gepleit voor meer harmonisering?

Met deze verordening wordt gepoogd de regelgeving voor informatiebeveiliging te harmoniseren door algemene regelgeving voor informatiebeveiliging op te stellen die voor alle EU IOA's geldt. Dit voorkomt dat elk EU IOA een «eigen wiel» moet uitvinden. In aanvulling hierop deze regelgeving kunnen EU IOA's eigen informatiebeveiligingsregels stellen. Omdat dit de harmonisatie van informatiebeveiligingsregelgeving negatief kan beïnvloeden, is het kabinet hier geen voorstander van. Dit standpunt wordt door de Nederlandse Nationale Veiligheidsautoriteit (NSA) uitgedragen in het Beveiligingscomité van de Raad en de Werkgroep Veiligheidsexperts van de Commissie.

De leden van de GroenLinks-fractie lezen dat er een interinstitutionele coördinatiegroep voor informatiebeveiliging wordt opgericht, waarin de beveiligingsautoriteiten van de EU-IOA's vertegenwoordigd zijn. Deze leden zijn benieuwd of het Europees Parlement hier ook bij betrokken is. Hier werkt ook een grote groep mensen met mogelijk gevoelige informatie. Deze leden vinden het wenselijk dat medewerkers van het Europees Parlement ook geïnformeerd worden over het belang van informatiehuishouding en dat het Europees Parlement kan meebeslissen over informatiebeveiliging.

Het kabinet deelt de wens over de betrokkenheid van het Europees Parlement. De verordening stelt dat elk van de instellingen en organen van de Unie op passende wijze wordt vertegenwoordigd in de coördinatiegroep.

De leden van de GroenLinks-fractie delen de zorgen van het kabinet over tot in hoeverre de beveiliging van informatie in de categorie niet-gerubriceerde informatie op de voorgestelde manier niet gewaarborgd is.

Vragen en opmerkingen van het lid van de BBB-fractie

Het lid van de BBB-fractie heeft met interesse kennisgenomen van de BNC-fiches inzake Verordening Informatiebeveiliging en cybersecurity in de instellingen, organen en instanties van de Unie. Het kabinet vraagt zich af of de IICB wel voldoende bevoegdheden krijgt om goed te kunnen

bijdragen aan een hoger en gemeenschappelijker niveau van de digitale weerbaarheid, aangezien de IICB enkel niet-bindende waarschuwingen kan geven en audits kan aanbevelen. Ook vraagt het kabinet zich af in hoeverre de EU-lidstaten voldoende vertegenwoordigd zijn in de IICB, aangezien de veiligheid van de EU-IOA's ook de belangen van de lidstaten raakt

Het lid van de BBB-fractie heeft daarom de volgende vragen aan de Minister. Wat is de reden dat de termijn van 24 uur voor het melden van significante cyberdreigingen, kwetsbaarheden of incidenten aan het CERT-EU onderhavig is aan discussie? Wat zijn mogelijke uitzonderingsgronden om van deze termijn af te wijken?

Zoals reeds aangekondigd in het BNC-fiche over het voorstel tot een Verordening cyberbeveiliging van instellingen, organen en instanties van de Europese Unie heeft het kabinet de Commissie inmiddels om toelichting gevraagd over de nadere invulling van de uitzonderingsgrond bij de plicht voor EU IOA's om significante cyberdreigingen, kwetsbaarheden of incidenten binnen 24 uur na ontdekking hiervan te delen met CERT-EU.[6] Hierover is op dit moment nog geen antwoord ontvangen.

In algemene zin geldt dat er steeds een balans moet worden gezocht tussen de snelheid en de volledigheid van een melding, wat maakt dat een precieze termijn onderwerp van discussie kan zijn.

Welke extra bevoegdheden ziet het kabinet concreet voor het IICB? Wat is het standpunt van andere lidstaten hierover?

Net als van het kabinet is de zienswijze van veel lidstaten dat de vrijblijvendheid op gebied van digitale weerbaarheid voorbij zou moeten zijn. Ook wat toezicht betreft zou dat moeten gelden. Bezien moet worden wat er in dit kader concreet mogelijk is, mede met oog op de wettelijke grondslag van het voorstel en de autonome positie van de EU IOA's. Het kabinet is nog in gesprek met andere lidstaten over de mogelijkheden.

Welke lidstaten delen het standpunt van het kabinet dat lidstaten voldoende vertegenwoordigd moeten zijn in de IICB?

Naar verwachting zullen lidstaten het standpunt van het kabinet delen, aangezien lidstaten er over het algemeen belang aan hechten dat lidstaten in voldoende mate vertegenwoordigd zijn in dergelijke organen om sturing te kunnen geven.

Europese landen zijn vaak afhankelijk van buitenlandse leveranciers voor cyberbeveiligingsdiensten, waaronder Amerikaanse bedrijven. In hoeverre borgt dit voorstel de veiligheid van EU-IOA's als deze bedrijven niet aan dezelfde veiligheidsregels worden onderworpen?

In Annex I van het voorstel met betrekking tot cyberbeveiliging wordt een aantal domeinen benoemd waar aandacht aan moet worden besteed door de EU IOA's in het kader van het basisniveau van cyberbeveiliging. Daaronder vallen onder andere de acquisitie van systemen en de relatie met leveranciers. In Annex II, waarin wordt gespecificeerd welke maatregelen de EU IOA's ten minste moeten nemen, wordt daarnaast het bewerkstelligen van de veiligheid van de leveranciersketen van software benoemd. Er is dus expliciet aandacht in het voorstel voor eventuele risico's in de leveranciersketen.

---

[6] BNC-fiche Verordening cyberbeveiliging van instellingen, organen en instanties van de Europese Unie, Kamerstuk 22 112, nr. 3406.