2022D21936

INBRENG VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Binnen de vaste commissie voor Digitale Zaken hebben enkele fracties de behoefte om enkele vragen en opmerkingen voor te leggen aan de Minister van Justitie en Veiligheid en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties 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 voorzitter van de commissie,
Kamminga

De adjunct-griffier van de commissie,
Van Tilburg

Inhoudsopgave **Blz.**

I Vragen en opmerkingen vanuit de fracties

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?

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. 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?

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»? 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?

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

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?

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? Hoe ziet het kabinet haar rol in het agenderen van hogere standaarden van beveiliging? Hoe leren EU-IOA's van een datalek of een cyberaanval bij één van hen? 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?

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?

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?

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.[1] Deze leden hopen op een kritische houding richting de EU-IOA's met betrekking tot dit thema.

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.

---

[1] 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).

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?

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?

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.

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? Welke extra bevoegdheden ziet het kabinet concreet voor het IICB? Wat is het standpunt van andere lidstaten hierover? Welke lidstaten delen het standpunt van het kabinet dat lidstaten voldoende vertegenwoordigd moeten zijn in de IICB? 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?

II Antwoord / Reactie van de Minister