22112 **Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie**

Nr. **Verslag van een schriftelijk overleg**

Vastgesteld

Binnen de vaste commissie voor Digitale Zaken hebben enkele fracties de behoefte om enkele vragen en opmerkingen voor te leggen aan de minister voor Economische Zaken en Klimaat over het Fiche: Verordening Cyber Resilience Act (CRA).

Bij brief van ……zijn deze vragen en opmerkingen beantwoord. Vragen en antwoorden zijn hierna afgedrukt.

Voorzitter van de commissie,

Kamminga

Adjunct-griffier van de commissie,

Van Tilburg

Inhoudsopgave

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben kennisgenomen van de kabinetspositie inzake de Verordening Cyber Resilience Act (CRA) en hebben hierover nog enkele vragen en opmerkingen.

De leden van de VVD-fractie achten het positief dat vanuit Europa het initiatief wordt genomen om slimme apparaten (IoT apparaten) veiliger te maken zodat het aantal cyberaanvallen verminderd kan worden. Deze leden zijn het eens met de constatering dat helaas te vaak nog cyberaanvallen kunnen worden uitgevoerd via zwakke plekken in de software en hardware van IoT apparaten. Deze leden achten het dan ook van belang om de beveiligingstandaarden van IoT apparaten te verhogen om digitale deuren beter op slot te houden voor cybercriminelen.

De leden van de VVD-fractie lezen dat Standalone software, apps en Software als een service (SaaS) niet onder de reikwijdte van de CRA vallen. Deze leden delen de twijfel van het kabinet omtrent deze uitzondering. Gegeven dat bovenstaande digitale middelen niet onder de CRA vallen, onder welke

wettelijke scope wordt hun digitale beveiliging wel voldoende geborgd? Wordt dit bijvoorbeeld geborgd via de NIS2-richtlijn? Welke analyse vormt de basis van deze verdeling? In hoeverre zijn deze verordeningen toereikend als het gaat om Standalone software, apps en Saas?

Daarnaast lezen de leden van de VVD-fractie dat de verantwoordelijkheid voor het verhogen van de beveiligingseisen van slimme apparaten komt te liggen bij fabrikanten die producten ontwikkelen, ontwerpen en beschikbaar stellen en leveranciers en importeurs die de producten beschikbaar stellen in de interne markt. Hoe verhoudt deze verantwoordelijkheid zich tot producten van buiten de Europese Unie die niet aan de gestelde beveiligingseisen voldoen? In het geval er sprake is van niet veilige producten, wordt dan de betrokken importeur van de producten verantwoordelijk gehouden? Zo ja, betekent dit ook dat deze importeurs verplicht een toets moeten doen op de veiligheidseisen van slimme apparaten vanuit derde landen? Moeten zij op basis van deze toets ook slimme apparaten vanuit derde landen weigeren? Kan het kabinet de hier geldende procedure verduidelijken?

Naast dat het van belang is dat de cyberbeveiligingseisen voor slimme apparaten verhoogd moeten worden, willen de leden van de VVD-fractie wijzen op de belangrijke complementaire verantwoordelijkheid van consumenten om veilig en bewust om te gaan met (huidige) slimme apparaten. Is het kabinet dit met deze leden eens? Zo ja, is zij bereid om parallel aan de implementatie van de CRA in te zetten op een voorlichting/bewustwordingscampagne rondom het verantwoordelijk gebruiken van slimme apparaten om consumenten tegelijkertijd ook weerbaarder te maken? Zo nee, waarom niet?

Is het kabinet het met de leden van de VVD-fractie eens dat het net zo belangrijk is om de beveiligingseisen van huidige slimme apparaten die al op de markt zijn gebracht, te verhogen? Zo ja, welke mogelijkheden ziet zij, al dan niet via de CRA, om de beveiligingseisen niet alleen voor toekomstige maar ook voor huidige slimme apparaten te verhogen? Is zij ook voornemens om deze voorstellen kenbaar te maken in de onderhandelingen? Zo nee, waarom niet?

Tevens lezen de leden van de VVD-fractie dat fabrikanten conform de CRA zonder onnodige vertraging en binnen 24 uur ontdekte kwetsbaarheden in producten moeten melden bij de European Union Agency for Cybersecurity (ENISA). Wat wordt bedoeld met ‘onnodige vertraging’ en hoe haalbaar acht het kabinet deze tijdspanne, in het bijzonder voor middelkleine en kleine fabrikanten die deze meldingen moeten maken gegeven de nalevings- en handhavingskosten die dit met zich meebrengt? Kunt het kabinet dit toelichten?

In het kader van de uitvoerbaarheid en proportionaliteit voor ondernemers hebben de leden van de VVD-fractie de nodige zorgen en stellen daarom graag de volgende vragen. De CRA in de huidige vorm stelt fabrikanten verplicht om elke actief misbruikte kwetsbaarheid in een product te melden bij ENISA. In hoeverre acht het kabinet dit uitvoerbaar voor ondernemers? Niet elke misbruikte kwetsbaarheid brengt significante veiligheidsrisico’s met zich mee en daarmee zou het melden van elke misbruikte kwetsbaarheid ongeacht zwaarte en risiconiveau een enorme druk leggen op de werkzaamheden van ondernemers en dat achten deze leden onwenselijk zeker gezien de andere verplichtingen die gaan gelden voor ondernemers als gevolg van andere Europese wetgeving zoals de NIS2-richtlijn, de Cybersecurity Act en de AI Act, deelt het kabinet deze zorgen? Zo ja, ziet zij mogelijkheden om de meldplicht te beperken tot significante incidenten waarbij aan een bepaald risiconiveau moet worden voldaan? Zo nee, waarom niet? Zo ja, is het kabinet bereid dit onder de aandacht te brengen in de onderhandelingen?

In het verlengde van het melding doen bij de ENISA, zouden de leden van de VVD-fractie nog willen in gaan op de keuze voor de ENISA als toezichthouder ook in relatie tot de nog aan te wijzen nationale markttoezichthouder. Hoe beoordeelt het kabinet het feit dat aanbieders van slimme apparaten een melding moeten doen bij het Europese ENISA en niet bij de nationale markttoezichthouder, gezien het feit dat de ENISA daarna verplicht is om de melding door te zetten naar de nationale Cyber Security Incident Response Team? Hoe beoordeelt het kabinet deze procedure en rolverdeling? Is zij het met deze leden eens dat het inefficiënt en daarmee onverstandig

is om de meldingen bij de ENISA onder te brengen om ze vervolgens weer naar de nationale autoriteiten door te sturen zoals bij het Nationaal Cyber Security Centrum (NCSC) of de CSIRT-DSP? Zo ja, is het kabinet het met deze leden eens dat het verstandiger is om de procedure te vereenvoudigen en efficiënter te maken door de meldingen eerst aan de nog aan te wijzen nationale markttoezichthouder te doen en vervolgens de Nederlandse nationale cybersecurity incident response teams op de hoogte moeten worden gebracht? Zo ja, is het kabinet bereid om dit voorstel kenbaar te maken in de onderhandelingen? Zo nee, waarom niet?

Ook willen de leden van de VVD-fractie nader ingaan op de bevoegdheid die de CRA aan de Europese Commissie toekent, namelijk dat zij uitzonderlijke gevallen digitale producten uit de Europese markt kan laten terugtrekken. Deze leden maken zich zorgen over deze bevoegdheid gezien de onzekerheid die zich met zich meebrengt voor ondernemers. In hoeverre worden de risico's die ondernemers lopen door deze bevoegdheid adequaat ondervangen door de CRA? Ziet het kabinet aanvullende mogelijkheden om deze risico's te ondervangen? Zo ja, welke?

Vragen en opmerkingen van de leden van de Volt-fractie

De leden van de Volt-fractie hebben met interesse kennisgenomen van het BNC-Fiche met betrekking tot de Verordening Cyber Resilience Act. Daarover zijn deze leden in principe positief gestemd. Zij kunnen zich vinden in een aanzienlijk deel van de posities die het kabinet inneemt. Over de kabinetspositie hebben zij nog wel enkele vragen.

De leden van de Volt-fractie merken op dat een van de voornaamste standpunten die het kabinet inneemt is dat de CRA niet alleen over digitale producten zou moeten gaan maar ook over alle ICT-producten, processen en diensten, ongeacht of zij aan consumenten of bedrijven worden aangeboden. Ziet het kabinet bij de andere lidstaten dezelfde wens? Wat is hier het krachtenveld? Welke inspanningen levert het kabinet om dit doel te bereiken? Kan het kabinet toelichten welke producten onder de reikwijdte van de CRA zouden moeten vallen en welke producten specifiek niet?

De leden van de Volt-fractie merken op dat het kabinet in haar position paper, in samenwerking met Denemarken en Duitsland, schrijft dat zij verheldering wenst te krijgen ten aanzien van de verhouding tussen de CRA en andere (concept)wetgeving op het gebied van cybersecurity. Van welke specifieke vragen en/of onduidelijkheden wenst het kabinet verheldering te krijgen?

De leden van de Volt-fractie hebben ten aanzien van het beoogde toezicht op de CRA en de meldplicht die de concepttekst voorschrijft ook nog enkele vragen. Allereerst merken de leden op dat er een meldplicht komt voor hackincidenten. Daarbij is het niet ondenkbaar dat samenloop ontstaat met de meldplicht voor datalekken in de AVG en de meldplicht voor cyberincidenten in kritieke sectoren onder de NIB2-richtlijn. Het toezicht op de verschillende wet- en regelgeving ligt in Nederland niet bij dezelfde toezichthouder. Dat leidt - zo merkt het kabinet terecht op - tot meer administratieve lasten. Het kabinet gaat de Europese Commissie hierop bevragen. Welke specifieke vragen gaat het kabinet stellen? Voor bedrijven zou het contact met de (Nederlandse) overheid zo simpel mogelijk moeten zijn. Om de meldingsbereidheid te vergroten - en daarmee de risico's van cyberincidenten voor de samenleving te verkleinen - kan het van waarde zijn om het mogelijk te maken om de melding via één loket te doen. Is het kabinet voornemens om het voor bedrijven mogelijk te maken om de verschillende meldingen via één loket te doen? Zo niet, welke andere maatregelen zal zij treffen om de melding zo simpel mogelijk te maken? In aanvulling op het bovenstaande: doordat het toezicht is verdeeld over meerdere toezichthouders, wordt het toezichtslandschap niet overzichtelijker. Deelt het kabinet dit standpunt? Welke inspanningen levert zij om de onoverzichtelijkheid te beperken? Zijn er andere lidstaten in de EU die soortgelijke toezichtsconstructies hebben of lidstaten die het juist anders doen? Wat kan Nederland daarvan leren?

Vragen en opmerkingen van het lid van de BBB-fractie

Algemeen
Het lid van de BBB-fractie heeft met interesse kennisgenomen van de Cyber Resilience Act. Graag hoort het lid wat de stand van zaken in Nederland is van aan de CRA gerelateerde wetgeving op het gebied van cybersecurity? En op welke wijze is of worden deze Europese wetgeving (-svoorstellen) al dan niet omgezet in Nederlandse wetgeving?

Grondrechten
Het doel van de CRA is om de toename van cyberaanvallen in de afgelopen jaren een halt toe te roepen. De CRA moet hiermee de digitale samenleving en de grondrechten, zoals privacy en gegevensbescherming, beter beschermen. Het lid van de BBB-fractie hoort graag in hoeverre de CRA regelt dat ook de bestaande slimme apparaten die al bij consumenten thuis of bij bedrijven staan veilig zijn? Overweegt het kabinet een bewustwordingscampagne voor consumenten en bedrijven gericht op onveilige slimme apparaten, inclusief de apparaten die nu al bij consumenten thuis of bij bedrijven staan? Het lid wil graag weten in hoeverre aanbieders van Europese portemonnees voor digitale identiteit onder de CRA vallen en aan welke eisen moeten zij voldoen.

Administratieve lasten
Het lid van de BBB-fractie vraagt of met de CRA volgens het kabinet voldoende wordt gestimuleerd dat bedrijven meer zullen investeren in veilig ontwerp en ontwikkeling en het leveren van beveiligingsupdates? En hoe vindt het kabinet dat de meldplicht verder kan worden afgebakend?

Toezicht en handhaving
Het lid van de BBB-fractie wil graag weten wie in Nederland toezicht gaat houden op de CRA? En welke middelen deze toezichthouder heeft voor adequaat toezicht en of dat voldoende is? Welke lidstaten vinden net als Nederland dat de versterkte rol van de Europese Commissie op het toezicht verduidelijking behoeft?

Financiële gevolgen
Het lid van de BBB-fractie wil graag van het kabinet weten wanneer meer inzicht gegeven kan worden in de financiële gevolgen van de CRA voor de Rijksbegroting en de budgettaire gevolgen voor medeoverheden? En natuurlijk wil het lid ook weten wat de financiële gevolgen voor producenten, importeurs en distributeurs/detailhandel zijn en welke invloed dit gaat hebben op de verkoopprijzen van de producten.