Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

21 501-33 Raad voor Vervoer, Telecommunicatie en Energie

Nr. 1015

VERSLAG VAN DE RAPPORTEURS

Vastgesteld op 19 april 2023

Inhoudsopgave **blz.**

1. Inleiding

Tijdens de procedurevergadering van 28 september 2022 van de vaste commissie voor Digitale Zaken (DiZa) is besloten om twee rapporteurs aan te stellen voor het EU-voorstel Verordening Cyber Resilience Act (CRA) (COM(2022) 454), te weten Queeny Rajkowski (VVD), Lisa van Ginneken (D66, tot 21 februari 2023) en Hind Dekker-Abdulaziz (D66, vanaf 22 februari 2023). Op 19 oktober 2022 heeft de commissie deze rapporteurs mandaat verleend voor de invulling van het rapporteurschap.

Onderdeel van het mandaat was het organiseren van een technische briefing met ambtenaren van het kabinet van Eurocommissaris Vestager. Tijdens de procedurevergadering van 23 november 2022 is besloten dit om te zetten in een gesprek van de rapporteurs met deze ambtenaren, dat

kst-21501-33-1015
ISSN 0921 - 7371
's-Gravenhage 2023

op 15 maart 2023 heeft plaatsgevonden. De rapporteurs hebben daarnaast met een aantal betrokken Nederlandse stakeholders gesproken.

In dit verslag komen de belangrijkste discussiepunten naar voren uit de gevoerde gesprekken en andere bronnen. Deze punten worden vergeleken met de kabinetspositie en de huidige stand van zaken, zoals blijkt uit de laatst beschikbare (voorlopige) compromistekst van 10 maart 2023 (gepubliceerd door Politico).

Het verslag eindigt met enkele aanbevelingen. De rapporteurs stellen de commissie voor deze aanbevelingen mee te nemen als suggesties voor het commissiedebat van 30 mei 2023 over de Telecomraad van 1–2 juni 2023.

2. EU-voorstel: Verordening Cyberweerbaarheid (CRA)

2.1. Korte inhoud van het EU-voorstel

Op 15 september 2022 heeft de Europese Commissie (EC) een voorstel voor een verordening voor cybersecurity-eisen voor alle producten met digitale elementen (COM(2022) 454) uitgebracht: de verordening Cyberweerbaarheid (CRA).

In dit voorstel wordt meer verantwoordelijkheid toegewezen aan de fabrikanten die digitale producten fabriceren en updaten. De voorschriften voor bedrijven moeten er volgens het voorstel voor zorgen dat alle hardware- of softwareproducten en individuele componenten, waarvan het gebruik en redelijk voorstelbaar gebruik een directe of indirecte verbinding tot een eindapparaat of netwerk bevat (zoals op het internet aangesloten thuiscamera's, koelkasten, tv's, speelgoed en niet-ingebedde software), in de hele toeleveringsketen en gedurende hun hele levenscyclus veilig zijn. Gebruikers kunnen hierdoor bij het selecteren en gebruiken van producten met digitale elementen rekening houden met de mate van cyberbeveiliging.

Het voorstel moet tevens de lacunes opvullen in bestaande Europese wetgeving op het gebied van cyberbeveiliging (zoals de richtlijn netwerk- en informatiesystemen (NIS2-richtlijn) en de cyberbeveiligingsverordening) en overlap voorkomen.

Het voorstel voorziet in:
1. Voorschriften voor het op de Europese interne markt brengen van producten met digitale elementen om de cyberbeveiliging van dergelijke producten te waarborgen;
2. Voorschriften voor het ontwerp, de ontwikkeling en de productie van producten met digitale elementen, en verplichtingen voor marktdeelnemers op het gebied van cyberbeveiliging;
3. Voorschriften voor procedures voor de reactie op kwetsbaarheden om de cyberbeveiliging van producten met digitale elementen gedurende de hele levenscyclus te waarborgen, en verplichtingen voor marktdeelnemers met betrekking tot deze procedures;
4. Voorschriften voor markttoezicht en handhaving van bovengenoemde voorschriften en eisen.

2.2. Status van de Europese besluitvorming

De onderhandelingen over de CRA bevinden zich in een vergevorderd stadium. Vermoedelijk starten eind deze zomer de triloog-onderhandelingen tussen de Raad en het Europees Parlement om te komen tot een finaal akkoord.

Onderhandelingen Raad

Zoals al uit het BNC-fiche (Kamerstuk 22 112, nr. 3552) en het verslag van de Telecomraad van 6 december 2022 (Kamerstuk 21 501-33, nr. 1001) bleek steunen de meeste lidstaten het voorstel. Naar verwachting bereiken de lidstaten in de Telecomraad van 1–2 juni 2023 een Raadsakkoord (algemene oriëntatie). De compromisteksten die op onderdelen al zijn besproken in de Raadswerkgroepen worden betrokken in dit verslag.

Onderhandelingen Europees Parlement

De (eerstverantwoordelijke) industriecommissie (ITRE) in het Europees Parlement stemt naar verwachting op 19 juli 2023 over het conceptverslag en de ingediende amendementen van rapporteur Nicola Danti (Renew, Italië). Een datum voor de plenaire stemming moet nog worden vastgesteld.

Zodra de CRA is aangenomen krijgen lidstaten volgens het voorstel twee jaar de tijd om de wet via nationale wetgeving te implementeren. Een verplichting dat fabrikanten actief misbruikte kwetsbaarheden en incidenten moeten melden wordt naar verwachting al één jaar na de datum van inwerkingtreding van toepassing.

3. Behandeling Tweede Kamer en Eerste Kamer

In de Tweede Kamer heeft de vaste commissie voor Digitale Zaken (DiZa) het voortouw op de behandeling van de CRA. Dit hoofdstuk gaat in op deze behandeling, alsmede op de behandeling van enkele andere dossiers die hieraan raken. Voor de volledigheid betrekt dit hoofdstuk tevens de vragen van de Eerste Kamer over de CRA, vanwege de antwoorden op bepaalde discussiepunten.

De discussiepunten die uit de verschillende debatten naar voren komen worden behandeld in hoofdstuk 4 van dit verslag. Hierbij wordt de kabinetspositie aangehaald, alsmede de huidige stand van zaken in de Raadsonderhandelingen.

Cyber Resilience Act (CRA)

- Op 7 november 2022 heeft de commissie DiZa een schriftelijk overleg gevoerd over het BNC-fiche (Kamerstuk 22 112, nr. 3552) van het kabinet (Kamerstuk 22 112, nr. 3555).
- Op 30 november 2022 heeft de commissie met de Minister van EZK gedebatteerd (Kamerstuk 21 501-33, nr. 997) over de CRA, ter voorbereiding op de Telecomraad van 6 december 2022 (Kamerstuk 21 501-33, nr. 1001).
- De Eerste Kamer heeft op 15 november 2022 een schriftelijk overleg gevoerd over het voorstel voor de CRA en het BNC-fiche (Kamerstuk 36 239, C).
- Op 13 december 2022 heeft de Eerste Kamer een brief met vragen gestuurd aan de Europese Commissie (Kamerstuk 36 239, B). De antwoorden hierop zijn ten tijde van dit schrijven nog niet ontvangen.

Nederlandse Cybersecuritystrategie

- De commissie DiZa heeft op 15 december 2022 het commissiedebat gevoerd over de Nederlandse Cybersecuritystrategie (NLCS) (Kamerstuk 26 643, nr. 925) en het bijbehorende Actieplan (Kamerstuk 26 643, nr. 961). In de NLCS zijn langs vier pijlers doelen geformuleerd om Nederland digitaal veilig te maken en houden. Daarvan richten drie

pijlers zich op het verhogen van de digitale weerbaarheid. In het Actieplan staat onder andere:
  - dat het kabinet zich in de onderhandelingen voor de CRA hard gaat maken voor opname van een zorgplicht voor fabrikanten en leveranciers van alle ICT-producten, -diensten en -processen, inclusief bijbehorende standaarden en toezicht. Deze zorgplicht moet gedurende de hele levenscyclus blijven gelden.
  - dat het kabinet in de onderhandelingen gaat inzetten op goede aansluiting van de CRA op sectorspecifieke cybersecurity-eisen in Europese regelgeving (zoals voor medische hulpmiddelen en auto's) en generieke wetgeving zoals de Richtlijn voor Algemene Productveiligheid en de Richtlijn voor aansprakelijkheid voor producten met gebreken.
  - dat de Rijksinspectie Digitale Infrastructuur (RDI, voorheen Agentschap Telecom) en de Autoriteit Consument en Markt (ACM) intensiever gaan samenwerken om handhaving en toezicht op het gebied van veilige producten en diensten te verbeteren. De ACM houdt toezicht op de verkopers van producten die verplicht zijn informatie te geven aan consumenten over hoe lang (veiligheids-) updates beschikbaar zijn.

Strategie Digitale Economie

- Op 22 maart 2023 heeft de commissie DiZa het debat gevoerd over Digitale Infrastructuur en economie (Kamerstuk 26 643, nr. 1008). Op de agenda stond onder andere:
  - De Strategie Digitale Economie (Kamerstuk 26 643, nr. 941) In de strategie wordt vermeld dat het kabinet in de onderhandelingen over de CRA inzet op horizontale Europese wetgeving die de verantwoordelijkheid primair bij de fabrikant en leverancier van digitale producten en diensten legt door invoering van een zorgplicht om gedurende de hele levenscyclus aan essentiële cybersecurityvereisten te voldoen.
  - De Evaluatie (Kamerstuk 26 643, nr. 867) van de (Voortgang, (Kamerstuk 26 643, nr. 801)) Roadmap Digitaal Veilige Hard- en Software. De aanbevelingen in de evaluatie zijn door het kabinet gebruikt als input voor de Nederlandse Cybersecuritystrategie, waar het beleid ten aanzien van digitaal veilige ICT-producten en -diensten onderdeel van uitmaakt.

4. Stand van zaken op belangrijke discussiepunten

Dit hoofdstuk gaat in op de stand van zaken van een aantal thema's die eerder door de Tweede Kamer en de Eerste Kamer aan de orde zijn gesteld en/of die door het kabinet bij de Europese Commissie en in de Raadsonderhandelingen zijn ingebracht.

Uit diverse vragen van zowel de Tweede (Kamerstuk 22 112, nr. 3555) als de Eerste Kamer (Kamerstuk 36 239, C) bleek ook dat er behoefte is aan meer duidelijkheid in de CRA over de wisselwerking met andere relevante EU-wetgeving op het gebied van cyberbeveiliging, zoals de NIS2-richtlijn en de cyberbeveiligingsverordening, in het bijzonder waar het gaat om de overlap qua verplichtingen die uit deze trajecten voortvloeien, zoals de certificering en de meldplicht. Dit verslag gaat hier nader op in bij de relevante paragrafen.

4.1. Producten met digitale elementen: scope CRA

Onder de reikwijdte van de CRA vallen alle producten met digitale elementen, waarvan het gebruik en redelijk voorstelbaar gebruik een directe of indirecte verbinding tot een eindapparaat of netwerk bevat. Dit omvat alle hardware- of softwareproducten en individuele componenten. Deze paragraaf behandelt de meest gehoorde discussiepunten ten aanzien van de scope.

4.1.1. Open source software en overheidsdiensten

Het kabinet heeft in antwoord op vragen van de Eerste Kamer aangegeven zich tijdens de onderhandelingen in te zetten voor verduidelijking en afbakening van de uitzondering voor open source software en, hiermee samenhangend, wat moet worden verstaan onder een handelsactiviteit. De definitie hiervan bepaalt mede wanneer open source-software al dan niet onder de reikwijdte van de CRA valt. Ook heeft het kabinet aangegeven nog te onderzoeken of en zo ja op welke manier er in de CRA een prikkel zou moeten worden ingevoegd voor commerciële fabrikanten van digitale producten die niet-commerciële open source componenten gebruiken in hun product, om de ontwikkelaars van deze niet-commerciële componenten te ondersteunen in het veilig houden van de componenten.

In een voorlopige compromistekst van 10 maart jl. (gepubliceerd door Politico) staat nu in overweging 10 dat de CRA uitsluitend van toepassing is op producten met digitale elementen die in de EU op de markt worden gebracht en derhalve worden geleverd voor verspreiding of gebruik in het kader van een commerciële activiteit. Open source software (inclusief broncodes en gewijzigde versies die openlijk gedeeld worden en vrij toegankelijk, bruikbaar en aanpasbaar zijn en kan worden verspreid en op de markt gebracht) valt derhalve alleen onder de reikwijdte van de CRA als deze in het kader van een commerciële activiteit wordt geleverd. In de compromistekst staat nu in een extra artikel 11.7 dat als fabrikanten een software aanpassing hebben ontwikkeld om de kwetsbaarheid in een open source onderdeel van hun product te verhelpen, zij geacht worden de relevante code te delen met de persoon of entiteit die het onderdeel onderhoudt.

Ook rapporteur Danti (EP) heeft in zijn conceptverslag opgenomen dat, om de innovatiekracht van open software te behouden, ontwikkelaars niet hoeven te voldoen aan de CRA als ze geen financieel rendement ontvangen voor hun projecten. Open source software die in het kader van commerciële activiteiten wordt geleverd, in het conceptverslag wel onder de CRA.

4.1.2. Software-as-a-Service (SaaS) en gegevensverwerking op afstand

Het kabinet heeft in antwoord op vragen van de Tweede Kamer (Kamerstuk 22 112, nr. 3555) en blijkens het BNC-fiche (Kamerstuk 22 112, nr. 3552) aangegeven dat het de Europese Commissie om verduidelijking wil vragen over de uitzondering voor software-as-a-service-diensten (SaaS; een vorm van clouddienstverlening). In tegenstelling tot SaaS-diensten vallen oplossingen voor gegevensverwerking op afstand wel onder de CRA, terwijl dit ook oplossingen zijn die gebruik maken van SaaS. Het kabinet was net als veel lidstaten van mening dat de teksten over deze uitzonderingen verduidelijking behoeven.

In een voorlopige compromistekst van 10 maart jl. (bron: Politico) wordt in overweging 9 nu verduidelijkt dat SaaS-oplossingen beschouwd mogen worden als oplossingen voor gegevensverwerking op afstand in de zin van de CRA (en dus binnen de scope vallen) als de software of hardware is ontworpen en ontwikkeld door de fabrikant van het betrokken product of onder de verantwoordelijkheid van die fabrikant, en bij gebreke waarvan een dergelijk product met digitale elementen een van zijn functies niet zou kunnen vervullen. Volgens overweging 9 vallen derhalve websites die de functionaliteit van een product met digitale elementen niet ondersteunen, of clouddiensten die zijn ontworpen en ontwikkeld buiten de verantwoordelijkheid van een fabrikant van een product met digitale elementen, buiten het toepassingsgebied van de CRA.

In een nieuwe overweging 9a heeft de Europese Commissie verduidelijkt dat oplossingen voor gegevensverwerking op afstand onder de CRA vallen als deze oplossingen nodig zijn om een product met digitale elementen zijn functies te laten vervullen. Dit kan bijvoorbeeld het geval zijn wanneer een hardware-apparaat toegang nodig heeft tot een door de fabrikant ontwikkelde database.

4.1.3. Europese portemonnees voor digitale identiteit

De Tweede Kamer heeft aan de Minister van EZK extra verduidelijking gevraagd (Kamerstuk 22 112, nr. 3555) in hoeverre aanbieders van Europese portemonnees voor digitale identiteit onder de CRA vallen en aan welke eisen zij moeten voldoen.

Uit een voorlopige compromistekst van 10 maart jl. (bron: Politico), blijkt dat na overweging 18 (die ingaat op de relatie met het voorstel voor de Europese online identiteit) een nieuwe overweging 18a is toegevoegd over het integreren van componenten in bijvoorbeeld een digitale portemonnee. Hierin wordt gesteld dat fabrikanten de nodige zorgvuldigheid moeten betrachten als ze componenten willen integreren, des te meer als deze in belangrijke mate bijdragen aan de functionaliteit van het product en/of toegang hebben tot gegevens die door het product met digitale elementen zijn verwerkt.

Afhankelijk van het risico moeten fabrikanten dan bijvoorbeeld verifiëren dat de fabrikant van een component conform de CRA handelt of dat een component vrij is van kwetsbaarheden (zoals die zijn geregistreerd in openbaar toegankelijke databases met kwetsbaarheden), of verifiëren dat een component regelmatig beveiligingsupdates ontvangt.

4.1.4. Scope in Singapore en Verenigd Koninkrijk

Verschillende bedrijvenorganisaties hebben hun bezorgdheid geuit over de brede reikwijdte van de CRA, te weten alle hardware- of softwareproducten en individuele componenten. Zij wijzen erop dat de scope van de CRA breder is dan vergelijkbare wetgeving in bijvoorbeeld het Verenigd Koninkrijk en Singapore, waar de scope beperkt is tot software gebonden aan apparatuur.

Waar het gaat om dit verschil in relatie tot de concurrentiepositie van ondernemers en de veiligheid van burgers wil de Europese Commissie ENISA de taak geven om samen met de markttoezichtautoriteiten toezicht te houden op digitale producten met een hoog risico die via derde landen in de EU op de markt worden gebracht.

Rapporteur Danti (EP) dringt in zijn conceptverslag daarnaast aan op het sluiten van overeenkomsten inzake wederzijdse erkenning met gelijkgestemde derde landen met vergelijkbare beschermingsniveaus.

4.2. Regeldruk voor bedrijven

Ten aanzien van de regeldruk voor het mkb zijn zowel door de Tweede als de Eerste Kamer veel vragen gesteld in relatie tot de zorgplicht, de conformiteitsbeoordeling en de meldplicht. Deze paragraaf gaat hier nader op in.

4.2.1. Zorgplicht

Nederland heeft, samen met zes andere lidstaten (non-paper (Bijlage bij Kamerstuk 22 112, nr. 3637)), opgeroepen om de zorgplicht voor bedrijven te laten gelden voor de *verwachte* productlevensduur en fabrikanten te verplichten om de garandeerde ondersteuningstermijn duidelijk op de verpakking te vermelden. Dit kan voor fabrikanten een prikkel vormen om zich te onderscheiden met een langere ondersteuningstermijn. Daarnaast kunnen gebruikers er hun aanschaf mede op baseren. Zowel de Eerste (Kamerstuk 36 239, C) als de Tweede Kamer (Kamerstuk 22 112, nr. 3555) hadden hier vragen over gesteld.

Uit een voorlopige compromistekst van 10 maart 2023 (gepubliceerd via Politico) valt uit artikel 10 lid 6 en het nieuwe lid 10a op te maken dat de oproep is overgenomen: de minimumperiode van vijf jaar productlevensduur waarin leveranciers en fabrikanten verplicht zijn om cyberbeveiligingspatches te blijven implementeren is geschrapt. In plaats daarvan wordt nu gesproken over de verwachte levensduur. Fabrikanten moeten duidelijke informatie op hun producten plaatsen over tot wanneer ze van plan zijn om cyberbeveiligingsupdates en -patches uit te brengen (tot op het jaar en de maand). Beveiligingspatches of -updates die al beschikbaar zijn en verspreid onder gebruikers om reeds geïdentificeerde beveiligingsproblemen aan te pakken, moeten tien jaar lang beschikbaar blijven. Daarnaast wordt voorgesteld dat ook verbonden apparaten die al in de handel zijn gebracht voordat de CRA van kracht werd moeten voldoen aan de bepalingen van de CRA zodra er wijzigingen worden aangebracht, zoals functionele updates.

Ook rapporteur Danti (EP) heeft in zijn conceptverslag geen vaste datum voor de verwachte levensduur van producten opgenomen. Ook hij stelt voor om fabrikanten de levensduur van hun respectievelijke producten te laten bepalen, zolang dat in overeenstemming is met de verwachtingen van de consument. Daarnaast heeft Danti ook een verplichting voor fabrikanten opgenomen om consumenten te informeren wanneer de levensduur van hun product bijna afloopt. Tot slot wil Danti fabrikanten verplichten om waar mogelijk *automatische* updates uit te rollen gedurende de verwachte levensduur van het product. Als een fabrikant zijn productlevensduur heeft gedefinieerd als minder dan vijf jaar, moet deze andere bedrijven in staat stellen beveiligingspatches te leveren die die levensduur verlengen. In dat geval moeten fabrikanten de broncode van het product bekend maken.

Het kabinet heeft ook aangegeven om verduidelijking te vragen over mogelijke ondersteunende maatregelen vanuit Brussel. Daarnaast heeft het kabinet aangegeven zelf open te staan voor mogelijkheden om het mkb ondersteuning en voorlichting te bieden over hoe deze bedrijven aan de verplichtingen kunnen voldoen.

4.2.2. Keurmerken en certificering

Zowel de Eerste (Kamerstuk 36 239, C) en Tweede Kamer (Kamerstuk 22 112, nr. 3555) hebben hun zorgen geuit over de verplichte conformiteitsbeoordeling voor bedrijven en in dit kader het ontbreken van standaarden hiervoor. De scope van de CRA brengt met zich mee dat het een flinke uitdaging zal worden om dekkende standaarden voor verschillende type producten beschikbaar te hebben tegen de tijd dat de CRA in werking treedt. De CRA verwijst hiervoor naar de CSA (Cyber Security Act), maar ook daar zijn pas enkele certificeringen in ontwikkeling. Bedrijven die hun conformiteit moeten bewijzen zouden op tijd duidelijkheid moeten hebben over welke standaarden worden geaccepteerd.

Daarnaast zijn vragen gesteld over de klasse 2 in de lijst van kritieke producten (Bijlage III) in relatie tot de kosten voor het mkb. Deze klasse brengt met zich mee dat een bedrijf niet kan volstaan met een zelftoetsing, maar een onafhankelijke conformiteitsbeoordeling moet laten uitvoeren door een externe partij. De gemiddeld geschatte kosten van een conformiteitsbeoordeling door een derde partij zijn 25.000 euro, terwijl die van een zelftoetsing (klasse 1) 18.400 euro zijn. Ook zijn er nog nauwelijks aangewezen «aangemelde instanties» die dergelijke audits kunnen uitvoeren.

Uit de voorlopige compromistekst van 10 maart 2023 (bron: Politico) valt op te maken dat kleine bedrijven en start-ups een lagere vergoeding betalen dan grote bedrijven. De tekst stelt ten aanzien van de conformiteitsbeoordeling nu ook een vereenvoudigde EU-verklaring voor. Op de verklaring moet de naam van het bedrijf staan en de aanduiding van het type product. Deze kan verwijzen naar de volledige tekst op een webadres, in de taal van het land waar het product op de markt is gebracht. De CE-markering hoeft volgens de tekst alleen te worden aangebracht op de begeleidende documenten en indien van toepassing op de verpakking, dus niet meer op de website. Er is echter niets toegevoegd over het beschikbaar stellen van standaarden.

Rapporteur Danti (EP) heeft in zijn conceptverslag de implementatietermijn van de CRA verlengd van twee jaar tot 40 maanden vanaf de inwerkingtreding ervan, zodat het mkb meer tijd heeft om hier aan kan voldoen. Ook staat er dat de Europese Commissie richtsnoeren moet verstreken om bedrijven beter te begeleiden.

Samenhang met andere wetgeving

Het kabinet heeft in het BNC-fiche en in antwoord op vragen van de Tweede en de Eerste Kamer aangegeven meer duidelijkheid te vragen over de mate van afstemming tussen de conformiteitsbeoordeling van de CRA en de cyberbeveiligingsverordening en de certificeringen die hier onderdeel van uitmaken. In het voorstel voor de CRA wordt in overweging 18 wel vermeld dat uitgevers van Europese digitale identiteitsportemonnees hun producten moeten certificeren volgens de cyberbeveiligingsverordening.

Het kabinet geeft in het Actieplan NLCS (Bijlage bij Kamerstuk 26 643, nr. 925) aan in te zetten op de ontwikkeling van Europese certificeringschema's voor (veilige) ICT-producten, diensten en processen, zoals voor clouddiensten, 5G technologie en Common Criteria. In dit kader wil het kabinet ook de bewustwording en implementatie van certificeringsschema's onder de cyberbeveiligingsverordening stimuleren. De CRA wordt in dit kader niet genoemd.

4.2.3. Meldplicht

Zowel de Eerste (Kamerstuk 36 239, C) en Tweede Kamer (Kamerstuk 22 112, nr. 3555) hebben hun zorgen geuit over de verplichting voor bedrijven om een actief misbruikte kwetsbaarheid binnen 24 uur te melden nadat het misbruik is geconstateerd. Het kabinet heeft hierop aangegeven dat de uitzonderingsgronden voor de meldplicht verdere afbakening behoeft en hierover nog in gesprek te gaan met de Europese Commissie. Tot slot zijn zorgen geuit over de vele meldplichten die voortvloeien uit allerlei andere wetgeving en het gebrek aan samenhang hiertussen. Op dit laatste aspect wordt nader ingegaan in 5.1.

In de voorlopige compromistekst van 10 maart jl. (bron: Politico) wordt nu gespecificeerd dat de termijn voor de meldplicht gelijk is aan de bestaande vereisten onder de NIS2-richtlijn. Ook staat in een extra artikel 11.2a de uitzondering dat de fabrikant niet verplicht is een melding te doen bij een incident waar nog geen misbruik van is geconstateerd.

Ook Rapporteur Danti van het EP heeft in zijn conceptverslag de termijnen voor de rapportageverplichtingen voor fabrikanten die zich bewust worden van actief misbruikte kwetsbaarheids- en beveiligingsincidente, afgestemd op die van de NIS2-richtlijn. Ook stelt hij volgens het concept-verslag voor om de meldingsplicht alleen verplicht te stellen voor actief misbruikte kwetsbaarheden en significante incidenten, in plaats van voor alle incidenten.

Samenhang met andere wetgeving

In antwoord op vragen van de Tweede (Kamerstuk 22 112, nr. 3555) en de Eerste Kamer (Kamerstuk 36 239, C) heeft het kabinet aangegeven verduidelijking te vragen over hoe de meldplichten uit de NIS2-richtlijn, de cyberbeveiligingsverordening, de richtlijn betreffende de weerbaarheid van kritieke entiteiten (de CER-richtlijn) en de CRA zich tot elkaar verhouden.

Het beschreven proces van de meldplicht in de CRA (fabrikanten moesten incidenten melden bij ENISA) past niet goed bij het proces van de NIS2-richtlijnen hoe het kabinet de meldplicht volgens het Actieplan NLCS in Nederland wil inregelen. Volgens dit Actieplan (Bijlage bij Kamerstuk 26 643, nr. 925) wil het kabinet het opzetten van één centraal meldloket verkennen. Hiermee kunnen fabrikanten meldingen laagdrempelig en gelijktijdig doen bij zowel het CSIRT als de betreffende toezichthouder. Bij deze verkenning wil het kabinet de verplichte meldingen betrekken die bedrijven vanuit de CRA en de CER-richtlijn moeten doen, alsmede de meldingen vanuit sectorale wetgeving als de Digital Operational Resilience Act (DORA), die geldt voor de financiële sector en de Network Code on cybersecurity (NCCS), die geldt voor de energiesector.

In de voorlopige compromistekst van de CRA van 10 maart 2023 (bron: Politico) is het proces inmiddels aangepast aan de NIS2-richtlijn. Fabrikanten moeten nu de melding doen bij hun nationale CSIRTs in plaats van bij ENISA (zie 4.3). De CSIRTs moeten vervolgens ENISA en hun nationale toezichthouder(s) in kennis stellen.

Paragraaf 4.3 gaat nader in op het proces van de meldplicht en de rol van ENISA en het CSIRTs-netwerk.

4.3. Rol en bevoegdheden Europese Commissie en ENISA

In antwoord op vragen van de Tweede (Kamerstuk 22 112, nr. 3555) en Eerste Kamer (Kamerstuk 36 239, C) heeft het kabinet aangegeven verduidelijking te vragen over de precieze rol en bevoegdheden die aan de Europese Commissie en aan EU-agentschap voor cyberbeveiliging (ENISA) worden toegekend in de CRA, onder meer in relatie tot de verantwoordelijkheden van nationale markttoezichthouders, het Nationaal Cyber Security Centrum (NCSC) en het CSIRTs-netwerk. Daarnaast heeft het kabinet aangegeven de Europese Commissie om verduidelijking te vragen wat wordt bedoeld met «onnodige vertraging» bij het doorzetten van een melding door een fabrikant.

Uit een voorlopige compromistekst van 10 maart 2023 (bron: Politico) valt op te maken dat de rol van nationale computercrisisresponsteams (CSIRTs) en het ENISA nu omgedraaid is. Fabrikanten moeten binnen 24 uur nadat het incident bekend is melding maken van incidenten die impact hebben op de veiligheid van het product bij het betreffende nationale CSIRT (Computer Security Incident Response Team) in plaats van aan ENISA. Van de responsteams wordt vervolgens verwacht dat zij ENISA en de betrokken nationale toezichthouder (in Nederland zou dit de Rijksinspectie Digitale Infrastructuur (RDI; voorheen Agentschap Telecom) zijn) «zonder onnodige vertraging» daarvan in kennis stellen.

Rapporteur Danti van het EP stelt in zijn conceptverslag duidelijke protocollen voor voor de behandeling van dergelijke meldingen, aangezien informatie over niet-gepatchte kwetsbaarheden aanzienlijke schade kan veroorzaken als deze in handen valt van hackers. In tegenstelling tot de Raad (zie boven), wil Danti het centrale meldpunt bij ENISA houden en de middelen van ENISA vergroten.

Hoofdstuk 5 gaat nader in op de meldplicht en de samenhang met andere Europese wetgevingstrajecten.

Europese Commissie

Zoals opgenomen in het BNC-fiche en in antwoord op vragen van de Tweede Kamer heeft het kabinet aangegeven ook aandacht te houden voor de verdere uitwerking van de bevoegdheden van de commissie om, als er mogelijk sprake is van aanzienlijke cyberbeveiligingsrisico's, digitale producten uit de Europese markt te laten terugtrekken door ENISA. Dit kan wellicht op gespannen voet staan met de uitsluitende verantwoordelijkheid van lidstaten op het gebied van bescherming van de nationale veiligheid.

5. Aanbevelingen

U kunt overwegen in te gaan op de volgende punten tijdens het commissiedebat ter voorbereiding op de Telecomraad:

- Het kabinet heeft aangegeven zich in te zetten voor verduidelijking en afbakening van de uitzondering voor open source software. Er is nog niet teruggekoppeld in hoeverre de makers van open source software nu voldoende beschermd zijn als zij dergelijke software gratis beschikbaar stellen en in hoeverre fabrikanten die deze software gebruiken richting de makers ervan een verplichting hebben als zij stuiten op een beveiligingsissue.
- Het kabinet heeft aangegeven open te staan voor mogelijkheden om het mkb te ondersteunen ten aanzien van de wijze waarop zij aan de verplichtingen kunnen voldoen. Hier is nog geen terugkoppeling over gegeven.

- Het kabinet heeft in het Actieplan NLCS aangegeven een centraal meldpunt te willen onderzoeken om het voor bedrijven laagdrempeliger te maken aan de meldplicht te voldoen. Hoe is nog niet bekend hoe het kabinet ervoor gaat zorgen dat dit meldpunt ook voldoende veilig is, zodat het geen doelwit wordt voor hackers. En hoe het kabinet het doorzetten van de melding naar ENISA voldoende veilig kan realiseren. Daarnaast is onduidelijk wat de positie van het kabinet is als toch blijkt dat bedrijven direct moeten melden bij ENISA, bij ENISA een centraal meldpunt komt en mogelijk de middelen van ENISA hiertoe worden opgehoogd.
- Het kabinet heeft in het Actieplan NLCS aangegeven dat het de beschikbaarheid van Europese standaarden en schema's wil bevorderen om bedrijven te ontlasten bij het voldoen aan de conformiteitsbeoordeling. Er is geen informatie over het tijdspad van de beschikbaarheid van deze standaarden. Gezien de brede scope van de CRA, met veel verschillende producttypes, is deze informatie voor bedrijven relevant.
- Zoals opgenomen in het BNC-fiche en in antwoord op vragen van de Kamer heeft het kabinet aangegeven ook aandacht te houden voor de verdere uitwerking van de bevoegdheden van de commissie om in uitzonderlijke gevallen digitale producten uit de Europese markt te laten terugtrekken. Dit kan namelijk op gespannen voet staan met de uitsluitende verantwoordelijkheid van lidstaten op het gebied van bescherming van de nationale veiligheid. Hier is nog geen terugkoppeling over gegeven.
- Vanaf de datum waarop de CRA in het Publicatieblad van de EU wordt gepubliceerd, hebben bedrijven volgens het voorstel 24 maanden om aan de maatregelen te voldoen. De NIS2-richtlijn heeft een deadline van 21 maanden voor implementatie. Het overzicht ontbreekt wanneer de zorgplicht, de meldplicht en de conformiteitsbeoordeling voor fabrikanten van kracht worden krachtens de CRA en in hoeverre deze verplichtingen nu al gelden krachtens andere Europese wetgeving op het gebied van cybersecurity. Ook is niet duidelijk in hoeverre deze verplichtingen nu voldoende op elkaar zijn afgestemd.
- De ontwikkelingen op het gebied van AI gaan razendsnel. Het kabinet heeft niet gedeeld hoe de CRA zich tot deze ontwikkelingen verhoudt en of de CRA qua wetgeving voldoende toekomstbestendig is (en techniekneutraal). In het voorstel voor de CRA wordt ook geen relatie gelegd met de AI-verordening en de conformiteitsbeoordeling die krachtens deze verordening voor hoog-risico-AI-systemen vereist is.

Rajkowski
Dekker-Abdulaziz