36 875 **Uitvoering van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voorproducten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Uitvoeringswet verordening cyberweerbaarheid)**

Nr. 5 **Verslag**

Vastgesteld 13 februari 2026

De vaste commissie voor Digitale Zaken, belast met het voorbereidend onderzoek van bovenstaand wetsvoorstel, heeft de eer als volgt verslag uit te brengen van haar bevindingen.

Onder het voorbehoud dat de regering op de gestelde vragen tijdig en genoegzaam zal hebben geantwoord, acht de commissie de openbare beraadslaging over dit wetsvoorstel voldoende voorbereid.

Inhoudsopgave

I. ALGEMEEN DEEL

1. Inleiding

De leden van de D66-fractie hebben met interesse kennisgenomen van de Uitvoeringswet verordening cyberweerbaarheid. Deze leden steunen de inzet om cyberbeveiligingsvereisten aan te scherpen. Zij achten dit noodzakelijk voor de weerbaarheid van Nederland en Europa, mede gelet op de potentiële kostenbesparingen van €180 tot €290 miljard per jaar als gevolg van minder cyberincidenten. De leden van de D66-fractie hebben enkele vragen over de praktische werking van de wet en de samenhang met andere Europese wetgeving.

De leden van de GroenLinks-PvdA-fractie hebben met interesse kennisgenomen van de uitvoeringswet. Deze leden onderstrepen het belang van het wetsvoorstel: in een steeds verder digitaliserende wereld is het van belang dat de veiligheidseisen die worden gesteld aan digitale producten en diensten worden geharmoniseerd. Zij hebben wel een paar vragen over deze uitvoeringswet.

De leden van de VVD-fractie hebben met interesse kennisgenomen van het wetsvoorstel en hebben hierover enkele vragen.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel en hebben geen verdere vragen.

De leden van de BBB-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel en hebben hierover enkele vragen.

De leden van de ChristenUnie-fractie hebben met interesse kennisgenomen van het onderhavige wetsvoorstel. Deze leden hebben een aantal vragen. Zij zien allereerst dat deze wet gericht is op de veiligheid van producten en daarmee een plek inneemt in het bredere beleid over cyberveiligheid en -weerbaarheid, zoals beleid gericht op het afbouwen of voorkomen van ongewenste strategische afhankelijkheden. De leden van de ChristenUnie-fractie vragen of de regering een overzicht wil geven van (toekomende) EU-wetgeving op het gebied van cyberveiligheid en -weerbaarheid, welke eventuele lacunes de regering nog ziet, en wat de inzet van de regering is (zowel in EU-verband als eventueel op nationaal niveau).

2. De hoofdlijnen van de Verordening cyberweerbaarheid

De leden van de D66-fractie onderschrijven het uitgangspunt dat cyberveiligheid gedurende de gehele levenscyclus van een product moet worden geborgd. Deze leden vragen de regering hoe in de praktijk toezicht wordt gehouden op de naleving van ex-post verplichtingen, zoals het tijdig uitbrengen van beveiligingsupdates en het adequaat omgaan met kwetsbaarheden.

De leden van de GroenLinks-PvdA-fractie lezen dat fabrikanten moeten zorgen dat gedurende de gehele levensduur van een product met digitale elementen het product van veiligheidsupdates wordt voorzien om kwetsbaarheden in het product aan te pakken. Deze leden maken zich echter zorgen dat fabrikanten van dergelijke producten zullen proberen te claimen dat de levenscyclus van een product korter is dan de periode dat een dergelijk product daadwerkelijk functioneert. Zij denken hierbij bijvoorbeeld aan ‘smart’ koelkasten, waarbij deze leden zich kunnen voorstellen dat fabrikanten zullen stellen dat deze een verwachte

levenscyclus van vijf jaar zullen hebben. Dit terwijl een reguliere koelkast, zonder smart functionaliteiten, vaak een levenscyclus van zeker 15 jaar heeft. Kan de regering aangeven hoe zij van plan is om dit probleem te voorkomen, dan wel aan te pakken? De leden van de GroenLinks-PvdA-fractie zijn van mening dat als een reguliere koelkast een levenscyclus van 15 jaar heeft, de smart-versie van een koelkast eveneens een levenscyclus van 15 jaar moet hebben. Deze leden pleiten bij de regering om alles op alles te zetten om zogenoemde 'planned digital obsolescence' (waarmee functionerende apparaten in 'e-waste' kunnen veranderen), nationaal dan wel in Europees verband tegen te gaan.

De leden van de VVD-fractie constateren dat het Adviescollege toetsing regeldruk (ATR) heeft geadviseerd in de memorie van toelichting aandacht te besteden aan de wijze waarop bedrijven ondersteund zullen worden bij het naleven van de verplichtingen die voortvloeien uit voorliggende regelgeving. Hierop is paragraaf 2 in de memorie van toelichting aangevuld. Deze leden lezen daarin het volgende: "De CRA voorziet ook in manieren om bedrijven te ondersteunen bij het naleven van de verplichtingen. Zo zullen lidstaten waar nodig zorgen voor bewustwordingsactiviteiten en trainingen, een speciaal ingericht communicatiekanaal en ondersteuning van test- en conformiteitsbeoordelingsactiviteiten. Daarbij staan de behoeftes van kleine en microbedrijven centraal." Hoe wil de regering deze ondersteuning vormgeven, in het specifiek ook voor start-ups?

Daarnaast lezen zij het volgende: "Lidstaten kunnen ook een testomgeving voor regelgeving opzetten ('regulatory sandbox'), waarin voorafgaand aan het op de markt brengen van een product gekeken kan worden naar ontwikkeling, ontwerp, validering en het testen, met het oog op een goede naleving van de regels." Is de regering voornemens gebruik te maken van de mogelijkheid van een 'regulatory sandbox'? Zo ja, hoe wordt dit concreet vormgegeven? Zo nee, waarom niet?

Tot slot lezen de leden van de VVD-fractie dat onder het Digital Europe-programma subsidie beschikbaar wordt gesteld voor ondersteuning bij naleving. Om welk bedrag gaat het en hoe wordt deze subsidie precies ingezet?

3. Hoofdlijnen van het wetsvoorstel

De leden van de BBB-fractie lezen dat het wetsvoorstel toezichthouders de bevoegdheid geeft om woningen te betreden zonder toestemming (met machtiging), omdat veel digitale handel vanuit huis plaatsvindt. Voor veel mensen is de grens tussen bedrijfsvoering en privéleven flinterdun, bijvoorbeeld bij zzp'ers zonder extern kantoor. Kan de regering concreet aangeven hoe de Rijksinspectie Digitale Infrastructuur (RDI) denkt effectief toezicht te houden op de digitale veiligheid van software door fysiek een woning binnen te stappen? Is de regering van mening dat het binnentreden van een woning voor een softwarecontrole een disproportionele inbreuk is op het huisrecht, terwijl de wet niet duidelijk maakt welk fysiek bewijs daar aangetroffen zou kunnen worden dat niet via digitale weg of op de markt zelf verkregen kan worden?

4. Verhouding tot overig EU-recht

De leden van de D66-fractie vragen hoe de regering de samenhang borgt tussen de cyberweerbaarheidsverordening en andere relevante Europese kaders, zoals de NIS2-richtlijn en de AI-verordening. Op welke wijze wordt in de uitvoering voorkomen dat bedrijven

worden geconfronteerd met overlappende of tegenstrijdige verplichtingen? Daarnaast vragen deze leden hoe de afstemming tussen toezichthouders in de praktijk vorm krijgt bij samenloop van toezicht.

5. Regeldruk

De leden van de fractie van de VVD lezen dat de kosten van deze regelgeving voor de EU als geheel kunnen oplopen tot €29 miljard per jaar. Daartegenover staat een verwachte kostenverlaging van €180 tot €290 miljard per jaar door minder incidenten. Waarop is deze schatting gebaseerd?

De leden van de BBB-fractie lezen dat circa 52.000 fabrikanten gemiddeld €42.700 extra ontwikkelingskosten per product kwijt zijn, bovenop conformiteitskosten. Gezien de brede reikwijdte vrezen deze leden dat kleine ontwikkelaars deze kosten niet kunnen dragen. Heeft de regering in kaart gebracht in hoeverre deze wetgeving leidt tot een verdere marktconcentratie bij enkele grote 'Big Tech'-spelers, omdat kleine, innovatieve familiebedrijven in de techniek de regeldruk simpelweg niet meer kunnen financieren? Dreigt hierdoor niet een situatie waarin innovatieve Nederlandse hardware onbetaalbaar wordt ten opzichte van producten uit derde landen die minder nauwgezet worden gecontroleerd?

6. Advies en consultatie

6.1. Uitvoering- en handhaafbaarheidstoets Rijksinspectie Digitale Infrastructuur en Nationaal Cyber Security Centrum

De leden van de D66-fractie hebben kennisgenomen van de conclusies uit de quick scan van het Nationaal Cyber Security Centrum (NCSC). Deze leden vragen of aan de randvoorwaarden geschetst door het NCSC voldaan gaat worden en of dit naar verwachting ook tijdig lukt, gezien de regering dit niet expliciet benoemd heeft in de memorie van toelchting. Daarnaast vragen zij wanneer inzichtelijk wordt wat de structurele personele en financiële gevolgen zijn voor het NCSC, aangezien deze in de memorie van toelichting nog niet expliciet zijn uitgewerkt.

De leden van de ChristenUnie-fractie lezen in de memorie van toelichting geen expliciete reactie van de regering op de quick scan van het NCSC, bijvoorbeeld over de noodzaak om beleid te formuleren over het moment waarop het publiek moet worden geïnformeerd bij ernstige incidenten. Deze leden vragen de regering hier alsnog een reactie op te geven en uiteen te zetten hoe de regering wil borgen dat de NCSC de toebedeelde taken straks goed kan uitvoeren.

6.2. *Advies van de Raad voor de rechtspraak*

De Raad voor de rechtspraak en de RDI constateren overlap met andere Europese regelgeving. De leden van de VVD-fractie behouden daarom zorgen over dubbele regelgeving en hoge regeldrukkosten. Deze leden verzoeken om een duidelijk, schematisch overzicht van bestaande en te verwachten regelgeving die overlap vertoont, inclusief de verantwoordelijke toezichthouder per kader. Aanvullend verzoeken zij om een toelichting hoe naleving zo eenvoudig mogelijk wordt gemaakt voor ondernemers.

De leden van de ChristenUnie-fractie merken op dat de regering geen expliciete reactie heeft gegeven op het advies van de Raad voor de rechtspraak, waarin aandacht wordt gevraagd voor

een aantal praktische en procedurele punten. Kan de regering alsnog expliciet op deze punten ingaan, en daarbij uiteenzetten welke wel en welke niet zijn overgenomen, en waarom?

II. ARTIKELSGEWIJZE TOELICHTING

Artikel 3.7

De leden van de GroenLinks-PvdA-fractie lezen dat de minister van Economische Zaken de bevoegdheid krijgt tot oplegging van een bestuurlijke boete ter hoogte van het hoogste bedrag, genoemd in artikel 64, tweede tot en met vierde lid, van de Verordening cyberweerbaarheid, ter handhaving van het artikel. Ook wordt de minister bevoegd tot oplegging van een last onder bestuursdwang ter handhaving. Deze leden kennen meerdere voorbeelden van zeer grote multinationals en tech-unicorns die opereren op basis van een ‘move-fast and break stuff’ principe, waarbij de kosten van boetes als onderdeel van de bedrijfslast wordt gezien. Zij zijn van mening dat de opgelegde boetebedragen daarom in principe van een zodanige hoogte moeten zijn dat “ingecalculeerde onveiligheid” en daarmee “ingecalculeerde boetebedragen” nooit winstgevend kunnen zijn voor fabrikanten. Deelt de regering deze mening? Is de regering ervan overtuigd dat het opgenomen sanctiekader voldoende afschrikwekkend is om te voorkomen dat bedrijven incalculeren dat ze veel winst maken en de boete op de koop toe nemen omdat deze niet hoog genoeg is? Zo nee, kan de regering zich voorstellen dat er bedrijven zullen zijn die zich niets van deze regelgeving zullen aantrekken? Welke mogelijkheden ziet de regering in dat geval nog meer om bedrijven te dwingen zich aan de wet te houden?

OVERIG

De leden van de GroenLinks-PvdA-fractie willen nog een opmerking maken over ‘security-by-design’. Volgens de cyberweerbaarheidsverordening (Annex I) moeten producten ‘secure by design’ zijn en beveiliging bieden tegen ongeautoriseerde toegang. Fabrikanten gebruiken deze eis echter regelmatig als voorwendsel om onafhankelijke reparateurs buiten te sluiten (bijvoorbeeld door het versleutelen van ‘bootloaders’). Hoe interpreteert de regering deze eis? Blijven audits en reparaties door derden onder de cyberweerbaarheidsverordening mogelijk? Zo nee, gaat de regering zich ervoor inzetten om dit wel mogelijk te maken? Deze leden zijn van mening dat de eisen uit de cyberweerbaarheidsverordening de gebruiker beschermt tegen zaken als ransomware en staatsactoren. Volgens deze leden is het niet bedoeld om de fabrikant te beschermen tegen reparateurs. Deelt de regering deze mening?

De fungerend voorzitter van de commissie,
Kathmann

De adjunct-griffier van de commissie,
Muller