Advies van het Europees Economisch en Sociaal Comité over het voorstel voor een verordening van het Europees Parlement en de Raad betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020

(COM(2022) 454 final — 2022/0272 (COD))

(2023/C 100/15)

Rapporteur: **Maurizio MENSI**

Corapporteur: **Marinel Dănuț MURESAN**

Raadpleging	Europees Parlement, 9.11.2022
	Raad van de Europese Unie, 28.10.2022
Rechtsgrond	Artikel 114 van het Verdrag betreffende de werking van de Europese Unie
Bevoegde afdeling	Interne Markt, Productie en Consumptie
Goedkeuring door de afdeling	10.11.2022
Goedkeuring door de voltallige vergadering	14/12/2022
Zitting nr.	574
Stemuitslag	
(voor/tegen/onthoudingen)	177/0/0

1. **Conclusies en aanbevelingen**

1.1. Het Europees Economisch en Sociaal Comité (EESC) is ingenomen met het Commissievoorstel voor een cyberweerbaarheidverordening (Cyber Resilience Act, CRA), bedoeld om hogere cyberbeveiligingsnormen vast te stellen en aldus een betrouwbaar systeem voor de marktdeelnemers tot stand te brengen en te garanderen dat de EU-burgers veilig gebruik kunnen maken van producten die op de markt zijn. Dit initiatief maakt deel uit van de Europese datastrategie, waarmee de veiligheid van gegevens, waaronder persoonsgegevens, en de grondrechten — essentiële vereisten voor onze digitale samenleving — kracht wordt bijgezet.

1.2. Het EESC acht het van essentieel belang dat de collectieve reactie op cyberaanvallen wordt versterkt en dat het proces van harmonisatie van de cyberbeveiliging op nationaal niveau waar het gaat om normen en operationele instrumenten wordt geconsolideerd, om te voorkomen dat uiteenlopende nationale benaderingen tot rechtsonzekerheid en juridische belemmeringen leiden.

1.3. Het EESC is ingenomen met het initiatief van de Commissie, dat niet alleen de aanzienlijke kosten van cyberaanvallen voor bedrijven zal helpen terugdringen, maar burgers/consumenten ook een betere bescherming van hun grondrechten (zoals privacy) zal bieden. De Commissie laat met name zien dat zij bij de dienstverlening door certificeringsautoriteiten rekening houdt met de specifieke behoeften van kleine en middelgrote ondernemingen (kmo's). Het EESC wijst er echter op dat de criteria voor de toepassing van de CRA moeten worden verduidelijkt.

1.4. Het EESC vindt het lovenswaardig dat de CRA betrekking heeft op vrijwel alle digitale producten, maar benadrukt wel dat er problemen kunnen optreden bij de praktische toepassing ervan, omdat de CRA een flinke hoeveelheid gecompliceerd verificatie- en controlewerk met zich meebrengt. Daarom moeten de monitoring- en verificatie-instrumenten worden versterkt.

1.5. Het materiële toepassingsgebied van de CRA moet nauwkeurig worden afgebakend, met name wat betreft producten met digitale elementen en software.

1.6. Het EESC wijst erop dat fabrikanten zullen worden verplicht om zowel de kwetsbaarheden van producten als eventuele beveiligingsincidenten te melden aan het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa). In dit verband is het belangrijk dat het Enisa voldoende middelen krijgt om zich nauwkeurig en doeltreffend te kunnen kwijten van de belangrijke en lastige taken waarmee het wordt belast.

1.7. Om twijfels over de interpretatie te voorkomen, stelt het EESC voor dat de Commissie richtsnoeren opstelt om fabrikanten en consumenten wegwijs te maken in de regels en procedures die concreet van toepassing zijn, aangezien verscheidene producten die onder het toepassingsgebied van het voorstel vallen, ook onder andere wettelijke bepalingen inzake cyberbeveiliging vallen. In dit verband is het ook belangrijk dat met name micro-, kleine en middelgrote ondernemingen toegang hebben tot ondersteuning door gekwalificeerde deskundigen die specifieke diensten op beroepsgebied kunnen verlenen.

1.8. Het EESC merkt op dat de relatie tussen de certificeringsautoriteiten in het kader van de CRA en andere instanties die op grond van andere wetgevingsbepalingen cyberbeveiliging mogen certificeren, niet geheel duidelijk is. Hetzelfde probleem inzake operationele coördinatie kan zich ook voordoen tussen de in het verordeningsvoorstel bedoelde toezichthoudende autoriteiten en de autoriteiten die reeds werkzaam zijn op grond van andere wetgeving die op dezelfde producten van toepassing is.

1.9. Met de voorgestelde verordening krijgen de certificeringsautoriteiten een aanzienlijke werklast en verantwoordelijkheid op hun schouders. Gewaarborgd moet worden dat zij in de praktijk volledig operationeel zijn, ook al om te voorkomen dat de CRA de bestaande administratieve rompslomp vergroot en daarmee nadelig uitvalt voor fabrikanten die aan een aantal bijkomende certificeringsvereisten zullen moeten voldoen om op de markt actief te kunnen blijven.

2. **Analyse van het voorstel**

2.1. Met het voorstel voor een CRA wil de Commissie de huidige wetgeving inzake cyberbeveiliging op een alomvattende en horizontale wijze stroomlijnen en herdefiniëren, en deze tegelijkertijd actualiseren in het licht van technologische innovaties.

2.2. Met de CRA worden in wezen vier doelstellingen nagestreefd: ervoor zorgen dat fabrikanten de beveiliging van producten met digitale elementen in de ontwerp- en ontwikkelingsfase en gedurende de gehele levenscyclus ervan verbeteren; zorgen voor een samenhangend kader van voorschriften inzake cyberbeveiliging, zodat de naleving ervan voor fabrikanten gemakkelijker wordt; de transparantie van de beveiligingskenmerken van producten met digitale elementen verbeteren; bedrijven en consumenten in staat stellen deze producten op een veilige manier te gebruiken. Met het voorstel wordt in feite een CE-markering voor cyberbeveiliging geïntroduceerd, die op alle onder de CRA vallende producten moet worden aangebracht.

2.3. Het gaat om een horizontale actie waarmee de Commissie de kwestie als geheel op alomvattende wijze wil reguleren, want ze betreft vrijwel alle producten die digitale componenten bevatten. Alleen producten van medische aard en producten die verband houden met de burgerluchtvaart, voertuigen en producten voor militaire doeleinden zijn van de werkingssfeer uitgesloten. Het voorstel heeft evenmin betrekking op SaaS-diensten (clouddiensten), tenzij deze voor de ontwikkeling van producten met digitale elementen worden gebruikt.

2.4. De definitie van "producten met digitale elementen" is zeer ruim en omvat elk software- of hardwareproduct, alsook software of hardware die niet in het product is ingebouwd maar afzonderlijk op de markt wordt gebracht.

2.5. Met de verordening worden verplichte vereisten inzake cyberbeveiliging ingevoerd voor producten met digitale componenten, die de hele levenscyclus ervan bestrijken, maar ze komt niet in de plaats van de reeds bestaande vereisten. Zo zullen reeds gecertificeerde producten die in overeenstemming zijn met al bestaande EU-normen, ook in het kader van de nieuwe verordening als "goedgekeurd" worden beschouwd.

2.6. Algemeen basisbeginsel is dat in Europa alleen "veilige" producten in de handel worden gebracht en dat de fabrikanten ervoor zorgen dat deze producten gedurende hun hele levenscyclus veilig blijven.

2.7. Een product wordt als "veilig" beschouwd als het zodanig is ontworpen en vervaardigd dat het een beveiligingsniveau heeft dat is afgestemd op de cyberrisico's die aan het gebruik ervan zijn verbonden, op het tijdstip van de verkoop geen bekende kwetsbaarheden vertoont, een standaardconfiguratie voor veilig gebruik heeft, tegen onrechtmatige verbindingen is beschermd, de gegevens die het verzamelt beschermt en alleen gegevens verzamelt die voor de werking ervan noodzakelijk zijn.

2.8. Een fabrikant wordt geschikt geacht om zijn producten in de handel te brengen als hij de lijst van de verschillende softwarecomponenten van zijn producten kenbaar maakt, snel en kosteloos oplossingen aanreikt in geval van nieuwe kwetsbaarheden, de kwetsbaarheden die hij detecteert en verhelpt openbaar maakt en in detail toelicht, en de "degelijkheid" van de door hem in de handel gebrachte producten regelmatig controleert. Deze en andere door de CRA opgelegde activiteiten moeten worden uitgevoerd gedurende de hele levensduur van een product, of gedurende ten minste vijf jaar nadat het in de handel is gebracht. De fabrikant moet ervoor zorgen dat kwetsbaarheden worden verholpen door middel van regelmatige software-updates.

2.9. Overeenkomstig een algemeen beginsel dat in verscheidene sectoren wordt toegepast, gelden deze verplichtingen ook voor importeurs en distributeurs.

2.10. De CRA voorziet in een "standaardcategorie" producten en software waarvoor kan worden vertrouwd op een zelfbeoordeling door de fabrikant, zoals reeds het geval is voor andere soorten CE-markering. Volgens de Commissie valt 90 % van de producten op de markt onder deze categorie.

2.11. De producten in kwestie kunnen in de handel worden gebracht na een zelfbeoordeling van hun cyberveiligheid door de fabrikant, die de in de richtsnoeren voor de toepassing van de regels vermelde passende documentatie indient. De fabrikant moet die beoordeling opnieuw uitvoeren indien er wijzigingen aan het product worden aangebracht.

2.12. De overige 10 % van de producten wordt onderverdeeld in twee andere categorieën (klasse I, lager risico, en klasse II, hoger risico), waarvan het in de handel brengen meer waakzaamheid vereist. Deze staan bekend als "kritieke producten met digitale elementen", waarvan het falen kan leiden tot andere gevaarlijke en bredere inbreuken op de beveiliging.

2.13. Voor producten in deze twee categorieën is de basiszelfbeoordeling alleen toegestaan als de fabrikant aantoont dat hij heeft voldaan aan specifieke marktnormen en beveiligingsspecificaties of aan reeds door de EU vastgestelde certificeringsregelingen voor cyberbeveiliging. Indien dit niet het geval is, kan het product worden gecertificeerd door een geaccrediteerde certificeringsinstantie waarvan het attest verplicht is voor producten van klasse II.

2.14. Het systeem waarbij producten in risicocategorieën worden ingedeeld, is ook opgenomen in het voorstel voor een verordening inzake artificiële intelligentie (AI). Om twijfel over de toepasselijke bepalingen te vermijden, wordt in de CRA rekening gehouden met producten met digitale elementen die in het AI-voorstel tegelijkertijd als "AI-systemen met een hoog risico" zijn ingedeeld. Dergelijke producten zullen in het algemeen moeten voldoen aan de conformiteitsbeoordelingsprocedure van de AI-verordening, behalve voor "kritieke producten met digitale elementen", waarvoor de conformiteitsbeoordelingsregels van de CRA zullen gelden naast de "essentiële vereisten" van de CRA.

2.15. Om de naleving van de CRA te waarborgen, moet elke lidstaat een nationale autoriteit aanwijzen die markttoezicht uitoefent. Indien een nationale autoriteit vaststelt dat de cyberbeveiligingskenmerken van een product niet langer volstaan, dan kan overeenkomstig de wetgeving inzake de veiligheid van andere producten het in de handel brengen ervan in de betrokken staat worden opgeschort. Het Enisa is bevoegd om een gerapporteerd product in detail te beoordelen. Als wordt vastgesteld dat een product onveilig is, kan het in de handel brengen ervan in de EU worden opgeschort.

2.16. De CRA voorziet in een reeks sancties ingeval de essentiële cyberbeveiligingsvereisten voor deze producten worden geschonden. Deze sancties kunnen naargelang de ernst van de inbreuk oplopen tot 15 miljoen EUR of 2,5 % van de omzet van het voorgaande boekjaar.

3. **Opmerkingen**

3.1. Het EESC is ingenomen met het initiatief van de Commissie om, in coördinatie met en in aanvulling op de NIS-richtlijn ([1]) en op de cyberbeveiligingswet ([2]), een belangrijk stuk toe te voegen aan de bredere wetgevingspuzzel op het gebied van cyberbeveiliging. Hoge cyberbeveiligingsnormen spelen immers een sleutelrol bij de totstandbrenging van een robuust EU-cyberbeveiligingssysteem voor alle marktdeelnemers. Dit komt van pas om EU-burgers te garanderen dat alle in de handel gebrachte producten veilig kunnen worden gebruikt en om hun vertrouwen in de digitale wereld te vergroten.

3.2. Met de verordening worden dus twee kwesties aangepakt: het lage cyberbeveiligingsniveau van veel van de producten en vooral het feit dat veel fabrikanten geen updates verstrekken om kwetsbaarheden te verhelpen. Hoewel fabrikanten van producten met digitale elementen soms reputatieschade ondervinden wanneer hun producten onvoldoende beveiligd zijn, worden de kosten van kwetsbaarheden voornamelijk door professionele gebruikers en consumenten gedragen. Dit vermindert de stimulans voor fabrikanten om te investeren in het ontwerp en de ontwikkeling van veilige producten en om veiligheidsupdates te verstrekken. Bovendien zijn bedrijven en consumenten vaak onvoldoende en onnauwkeurig geïnformeerd bij het kiezen van veilige producten en weten zij vaak niet hoe zij ervoor kunnen zorgen dat de

([1]) Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

([2]) Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15).

producten die zij kopen zijn geconfigureerd voor veilig gebruik. In de nieuwe regels worden deze twee aspecten behandeld door de kwesties omtrent de updates en het verstrekken van actuele informatie aan klanten aan te pakken. Het EESC is in dit verband van mening dat de voorgestelde verordening, mits correct toegepast, een internationaal referentiepunt en voorbeeld op het vlak van cyberbeveiliging kan worden.

3.3. Het EESC is ingenomen met het voorstel om voor producten met digitale elementen cyberbeveiligingvereisten in te voeren. Belangrijk is wel dat overlappingen met andere bestaande regelgeving op dit gebied, zoals de nieuwe NIS 2-richtlijn ([3]) en de AI-verordening, worden vermeden.

3.4. Het EESC vindt het lovenswaardig dat de CRA betrekking heeft op vrijwel alle digitale producten, maar benadrukt wel dat er problemen kunnen optreden bij de praktische toepassing ervan, omdat de CRA heel wat verificatie- en controlewerk met zich meebrengt.

3.5. Het materiële toepassingsgebied van de CRA is breed en omvat alle producten met digitale elementen. Volgens de voorgestelde definitie vallen alle software- en hardwareproducten en de daarmee verband houdende gegevensverwerkingsactiviteiten eronder. Het EESC zou graag zien dat de Commissie verduidelijkt of alle software binnen het toepassingsgebied van de voorgestelde verordening valt.

3.6. Fabrikanten zullen worden verplicht om zowel actief uitgebuite kwetsbaarheden als beveiligingsincidenten te melden. Zij zullen het Enisa op de hoogte moeten brengen van alle actief uitgebuite kwetsbaarheden in het product en (afzonderlijk) van elk incident dat gevolgen heeft voor de veiligheid van het product, in beide gevallen binnen 24 uur nadat zij er kennis van hebben genomen. Het EESC wijst er in dit verband op dat het Enisa voldoende middelen moet krijgen (zowel getalsmatig als wat professionele bekwaamheid betreft) om zich doeltreffend te kunnen kwijten van de belangrijke en lastige taken waarmee het krachtens de verordening is belast.

3.7. Het feit dat een aantal producten die onder het toepassingsgebied van het voorstel vallen ook onder andere wettelijke bepalingen inzake cyberbeveiliging vallen, kan leiden tot onzekerheid over welke bepalingen van toepassing zijn. Hoewel wordt verwacht dat de CRA in overeenstemming zal zijn met het huidige EU-regelgevingskader voor producten en met andere voorstellen die momenteel worden ingediend in het kader van de digitale strategie van de EU, overlappen voorschriften zoals die welke bijvoorbeeld worden overwogen voor AI-producten met een hoog risico, met die van de verordening inzake de verwerking van persoonsgegevens. In dit verband stelt het EESC voor dat de Commissie ten behoeve van fabrikanten en consumenten richtsnoeren voor een correcte toepassing van de CRA opstelt.

3.8. Het EESC merkt op dat de relatie tussen de certificeringsautoriteiten in het kader van de CRA en eventuele andere instanties die op grond van andere, eveneens van toepassing zijnde regelingen cyberbeveiliging mogen certificeren, niet geheel duidelijk is.

3.9. Bovendien zullen die certificeringsautoriteiten een aanzienlijke werklast en verantwoordelijkheid krijgen. Er moet geverifieerd en gewaarborgd worden dat zij in de praktijk volledig operationeel zijn om te voorkomen dat de CRA leidt tot een toename van de administratieve lasten waar fabrikanten die op de markt actief zijn al mee te maken hebben. In dit verband is het ook belangrijk dat met name micro-, kleine en middelgrote ondernemingen toegang hebben tot ondersteuning door gekwalificeerde deskundigen die specifieke diensten op beroepsgebied kunnen verlenen.

3.10. Volgens de CRA moeten de certificeringsautoriteiten bij hun dienstverlening rekening houden met de specifieke behoeften van kmo's. Het EESC wijst er echter op dat de criteria voor de toepassing van de CRA moeten worden verduidelijkt.

3.11. Bovendien kan zich een probleem voordoen bij de coördinatie tussen de in deze verordening bedoelde toezichthoudende autoriteiten en de autoriteiten die reeds werkzaam zijn op grond van andere voorschriften die op dezelfde producten van toepassing zijn. Het EESC stelt de Commissie dan ook voor de lidstaten op te roepen waakzaam te zijn en indien nodig maatregelen te nemen om dit te ondervangen.

Brussel, 14 december 2022.

De voorzitter
van het Europees Economisch en Sociaal Comité
Christa SCHWENG

([3]) Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80).