Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2022–2023

# 36 239 Voorstel voor een Verordening betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020

D

## BRIEF VAN VICEVOORZITTER ŠEFČOVIČ VAN DE EUROPESE COMMISSIE EN LID BRETON

Aan de voorzitter van de vaste commissie voor Justitie en Veiligheid

Cc: Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Brussel, 31 maart 2023

De Commissie dankt de Eerste Kamer voor haar advies 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}.

Het voorstel van de Commissie – de verordening cyberweerbaarheid – vormt een belangrijke mijlpaal bij het versterken van de cyberbeveiliging van Europa op alle gebieden. Het beoogt gemeenschappelijke verplichte cyberbeveiligingsvereisten voor producten met digitale elementen vast te stellen, gedurende hun gehele levenscyclus. Met betrekking tot de vragen van de Eerste Kamer wil de Commissie het volgende meedelen.

Vrije en open source software

De Commissie onderkent het belang van opensourcesoftwareproducten en -componenten buiten het kader van handelsactiviteiten. Gezamenlijke projecten, die vaak door vrijwilligers worden geleid, zijn een belangrijke bron van innovatie, en het zou de werkzaamheden aan bestaande en toekomstige projecten kunnen ontmoedigen als ze binnen de reikwijdte van de verordening cyberweerbaarheid zouden vallen. De uitsluiting van opensourcesoftware buiten het kader van handelsactiviteiten volgt de algemene benadering van het nieuw wetgevingskader: Europese productregulering omvat doorgaans enkel producten die gratis of tegen betaling voor distributie, verbruik of gebruik op de markt van de Unie worden aangeboden in het kader van een handelsactiviteit.

kst-36239-D
ISSN 0921 - 7371
's-Gravenhage 2023

De wijze waarop opensourcesoftware buiten handelsactiviteit wordt ontworpen en ontwikkeld, verschilt per project. In het licht van deze diversiteit kan het dictum van de verordening cyberweerbaarheid alleen het algemene uitsluitingsbeginsel bevatten, en niet op elk afzonderlijk geval ingaan. De Commissie is evenwel voornemens om richtsnoeren en een ruime hoeveelheid voorbeelden te verstrekken, zodat ontwikkelaars van opensourcesoftwareproducten en -componenten kunnen bepalen of hun activiteit al dan niet als handelsactiviteit wordt beschouwd.

Inzake de verantwoordelijkheid voor de naleving van door een collectief ontwikkelde producten, is hoofdstuk II van het voorstel alleen van toepassing op de persoon of entiteit die het product met digitale elementen in de handel brengt (d.w.z. die een handelsactiviteit uitoefent). Dat betekent dat vrijwilligers die bijdragen aan een door een andere persoon of entiteit in de handel gebracht project, niet verantwoordelijk zijn voor de nakoming van de verplichtingen die de verordening cyberweerbaarheid stelt ten aanzien van fabrikanten.

Ter ondersteuning van de ontwikkeling van veilige opensourcesoftware buiten handelsactiviteit heeft de Commissie in artikel 11, lid 7, bepaald dat fabrikanten bij de vaststelling van een kwetsbaarheid in een component, met inbegrip van een opensourcecomponent, die in het product met digitale elementen is geïntegreerd, de kwetsbaarheid moeten melden aan de persoon of entiteit die de component onderhoudt.

Handhaving

De verordening cyberweerbaarheid bevat geen aansprakelijkheidsregels. Die regels zijn opgenomen in het algemene EU-kader voor productaansprakelijkheid, waarvoor de Commissie recent een voorstel voor een herziene richtlijn productaansprakelijkheid heeft aangenomen. Het kader voor productaansprakelijkheid bevat aansprakelijkheidsregels voor producten met gebreken, zodat consumenten schadevergoeding kunnen vorderen voor schade ten gevolge van gebrekkige producten. Dit kader regelt het beginsel dat de fabrikant van een product aansprakelijk is voor schade die voortkomt uit een gebrek in zijn product, ongeacht of er sprake is van schuld (risicoaansprakelijkheid). Het voorstel inzake aansprakelijkheid voor gebrekkige producten bepaalt dat rechters bij de vaststelling van de gebrekkigheid van een product, rekening moeten houden met alle elementen, inclusief vereisten zoals de levering van beveiligingsupdates conform het voorstel voor de verordening cyberweerbaarheid. Iedere aansprakelijkheidszaak moet in rechte evenwel op zijn eigen merites worden beoordeeld, met inachtneming van de omstandigheden van het geval.

Inzake de toezichts- en handhavingsaspecten betreffende het voorstel voor de verordening cyberweerbaarheid en de manier waarop de naleving moet worden verzekerd, zij benadrukt dat de nieuwe regels betrekking hebben op het op de interne markt plaatsen van producten met digitale elementen. De verordening cyberweerbaarheid sluit aan bij het bestaande Europese kader voor productwetgeving, dat op nationaal markttoezicht is gebaseerd. De lidstaten moeten (nieuwe of bestaande) autoriteiten aanwijzen als markttoezichtsautoriteiten, die een scala aan toezichts- en handhavingsinstrumenten ter beschikking hebben, waaronder de mogelijkheid om het uit de handel nemen of de terugroeping van non-conforme producten van de interne markt te bevelen. Het voorstel bevat ook afschrikkende boeten, met een bepaald maximum, zoals een percentage van de totale wereldwijde omzet van een onderneming voor het voorafgaande boekjaar (tot 2,5% voor schendingen van de belangrijkste verplichtingen van de verordening cyberweerbaarheid).

In uitzonderlijke omstandigheden die onmiddellijk optreden rechtvaardigen om de goede werking van de interne markt te beschermen, kan de Commissie op grond van het voorstel ook optreden. Na een evaluatie door het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) en na raadpleging van de lidstaten, kan zij, middels een uitvoeringshandeling, besluiten corrigerende of beperkende maatregelen op te leggen. Deze kunnen resulteren in een terugroeping van de markt van non-conforme producten die een significant cyberbeveiligingsrisico inhouden, of van conforme producten met eenzelfde risico, en verder met risico's inzake veiligheids- en gezondheidseisen, de grondrechten, de levering van onder de NIS2-richtlijn vallende essentiële diensten of het algemeen belang.

Bovendien moeten kritieke producten op grond van het voorstel voor de verordening cyberweerbaarheid aan strengere conformiteitsbeoordelingsprocedures worden onderworpen voordat zij in de handel worden gebracht (b.v. geharmoniseerde normen of een conformiteitsbeoordeling door een onafhankelijk derde partij, of zelfs, voor bepaalde categorieën met een verhoogd risico, uitsluitend een conformiteitsbeoordeling door een derde partij).

Levensduur

De termijn van vijf jaar gedurende welke verplichtingen inzake de respons op kwetsbaarheden op fabrikanten rusten, is gekozen na overweging van een aantal factoren. Allereerst wilde de Commissie op een zinvolle manier de lat hoger leggen, door een ambitieuze tijdslijn voor te stellen die moet leiden tot een aanzienlijke verbetering van de cyberbeveiliging voor een breed scala aan producten. Uit de analyse van de Commissie blijkt dat veel hardware- en softwareproducten momenteel korter dan vijf jaar (of helemaal geen) beveiligingsupdates ontvangen. Zo bleek uit een enquête uit 2018 onder smartphonefabrikanten dat 14 van de 19 fabrikanten minder dan drie jaar beveiligingsupdates boden[1].

Langere ondersteuningstermijnen bieden betere beveiligingsresultaten, maar de Commissie is van mening dat het eisen van beveiligingsupdates voor langer dan vijf jaar onevenredig kan zijn, en fabrikanten zou kunnen ontmoedigen om te innoveren, in het bijzonder kleine en middelgrote ondernemingen en startups. Als ze een nieuw product in de handel brengen, weten fabrikanten niet of het een commercieel succes wordt. Door verstrekkende ondersteuningseisen kunnen fabrikanten risicoschuw worden en ervan afzien met nieuwe en innovatieve productiewijzen te experimenteren. Bovendien zou het, in het licht van het brede scala aan producten dat onder het voorstel valt, niet doenbaar zijn om voor iedere productcategorie een specifieke termijn te bepalen gedurende welke verplichtingen inzake de respons op kwetsbaarheden op fabrikanten zouden rusten.

Het is van belang om op te merken dat fabrikanten op grond van het voorstel aan hun gebruikers moeten laten weten hoe lang een product zal worden ondersteund. Hierdoor vergroot de transparantie en kunnen gebruikers kiezen voor producten met de langste ondersteuningstermijn, wat fabrikanten ertoe zal aanzetten om een langere termijn aan te bieden dan de wettelijk verplichte vijf jaar.

---

[1] Europese Commissie (2022): werkdocument van de diensten van de Commissie, effectbeoordeling bij 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, SWD(2022) 282 final, blz. 7.

Startups en innovatie, eerlijke concurrentie en financiële consequenties

De Commissie heeft het voorstel zeer zorgvuldig voorbereid, met het oog op een evenredige benadering die openheid, concurrentie en innovatie bevordert. De verordening cyberweerbaarheid, zoals door de Commissie voorgesteld, beoogt cyberbeveiligingsvereisten vast te leggen voor alle producten met digitale elementen, hardware en software die op de interne markt van de Unie in de handel worden gebracht. Dit geldt voor zowel binnen als buiten de EU gevestigde fabrikanten. Voor hen allen gelden dezelfde regels voor het in de handel brengen van die producten in de EU. De gevolgen van het initiatief voor de verordening cyberweerbaarheid zijn daarom naar verwachting gelijkaardig voor Europese ondernemingen en niet-Europese ondernemingen.

De verordening cyberweerbaarheid wordt waarschijnlijk een internationale referentie. EU-normen op basis van de verordening cyberweerbaarheid vergemakkelijken de uitvoering ervan en vormen een troef voor de cyberbeveiligingssector van de EU op de wereldmarkten.

Na de inwerkingtreding van de verordening cyberweerbaarheid zal de Commissie kleine en middelgrote ondernemingen wijzen op mogelijke steun in de vorm van financiering om hen te helpen de verplichtingen van de verordening na te leven. De Commissie heeft in het verleden een vergelijkbare aanpak toegepast ter ondersteuning van ondernemingen die cyberrisicobeheersmaatregelen moesten treffen in het kader van Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (de NIS-richtlijn). Bovendien is de Commissie voornemens financiële steun beschikbaar te stellen voor markttoezichtsautoriteiten, om hen te ondersteunen bij de opbouw van de nodige capaciteiten om de bij de verordening opgelegde taken te vervullen.

Gijzeling van gegevens en systemen

Uit een recente enquête door het Agentschap van de Europese Unie voor cyberbeveiliging onder aanbieders van essentiële diensten die onder de NIS-richtlijn vielen, bleek dat ongeveer tweederde van de cyberbeveiligingsincidenten voortkomt uit de exploitatie van een kwetsbaarheid in een hardware- of sotfwareproduct[2]. De verordening cyberweerbaarheid beoogt het aantal kwetsbaarheden in die producten aanzienlijk te verminderen, door van fabrikanten te eisen dat ze veiliger producten ontwikkelen en beveiligingsupdates sneller en, waar mogelijk, geautomatiseerd verstrekken. Hierdoor wordt het voor kwaadwillende partijen moeilijker ondernemingen en overheidsinstanties binnen te dringen en hun schadelijke scripts uit te voeren om kostbare data te gijzelen en losgeld te eisen.

Bescherming van klokkenluiders en ethische hackers

Krachtens artikel 2, lid 5, van bijlage I bij het voorstel voor de verordening cyberweerbaarheid moeten fabrikanten een beleid inzake gecoördineerde openbaarmaking van kwetsbaarheden invoeren en handhaven. Dit heeft tot gevolg dat fabrikanten een manier moeten voorzien waarop beveiligingsonderzoekers ontdekte kwetsbaarheden kunnen melden.

Het advies van de Eerste Kamer is aan de vertegenwoordigers van de Commissie ter hand gesteld bij de lopende onderhandelingen van de

[2] Europese Commissie (2022), blz. 51.

medewetgevers – het Europees Parlement en de Raad – en zal als input dienen voor de besprekingen in dat kader.

De Commissie hoopt dat zij met de toelichting in dit antwoord voldoende is ingegaan op de door de Eerste Kamer aan de orde gestelde punten en zij kijkt ernaar uit de politieke dialoog in de toekomst voort te zetten.

Vicevoorzitter,
Maroš Šefčovič

Lid van de Commissie,
Thierry Breton