Raad van de
Europese Unie

Brussel, 16 september 2022
(OR. en)

12429/22
ADD 6

Interinstitutioneel dossier:
2022/0272(COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

BEGELEIDENDE NOTA

van:	de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur
ingekomen:	15 september 2022
aan:	het secretariaat-generaal van de Raad
nr. Comdoc.:	SWD(2022) 283 final
Betreft:	WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE SAMENVATTING VAN HET EFFECTBEOORDELINGSVERSLAG over de verordening cyberweerbaarheid bij 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

Hierbij gaat voor de delegaties document SWD(2022) 283 final.

Bijlage: SWD(2022) 283 final

EUROPESE
COMMISSIE

Brussel, 15.9.2022
SWD(2022) 283 final

WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE

SAMENVATTING VAN HET EFFECTBEOORDELINGSVERSLAG

over de verordening cyberweerbaarheid

bij

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} - {SEC(2022) 321 final} - {SWD(2022) 282 final}

Samenvatting (maximaal twee pagina's)

Effectbeoordeling van de verordening cyberweerbaarheid

A. Behoefte aan actie

Wat is het probleem en waarom is het een probleem op EU-niveau?

Hardware- en softwareproducten hebben vaak te maken met geslaagde cyberaanvallen, waardoor de jaarlijkse kosten van cybercriminaliteit wereldwijd tegen 2021 naar schatting 5,5 biljoen EUR bedragen. Deze producten hebben te kampen met twee grote problemen die voor de gebruikers en de samenleving extra kosten met zich meebrengen: 1) een laag niveau van cyberbeveiliging, dat tot uiting komt in wijdverbreide kwetsbaarheden en de ontoereikende en inconsistente verstrekking van beveiligingsupdates om deze aan te pakken, en 2) onvoldoende inzicht en toegang tot informatie door gebruikers, waardoor zij niet in staat zijn producten met passende cyberbeveiligingskenmerken te kiezen of deze op een veilige manier te gebruiken.

De cyberbeveiliging van producten met digitale elementen heeft een sterke grensoverschrijdende dimensie, aangezien producten die in één land worden vervaardigd vaak op de gehele interne markt worden gebruikt. Daarnaast verspreiden incidenten die aanvankelijk één entiteit of één lidstaat betroffen, zich vaak binnen enkele minuten over de hele interne markt.

Hoewel de bestaande internemarktwetgeving van toepassing is op bepaalde producten met digitale elementen, vallen de meeste hardware- en softwareproducten momenteel niet onder EU-wetgeving inzake cyberbeveiliging. Het huidige rechtskader van de EU heeft met name geen betrekking op de cyberbeveiliging van niet-ingebedde software, ook al zijn cyberaanvallen steeds vaker gericht op kwetsbaarheden in deze producten, wat aanzienlijke maatschappelijke en economische kosten met zich meebrengt. Recente voorbeelden zijn de Pegasus-spyware, die kwetsbaarheden in mobiele telefoons uitbuitte, of de ransomware-worm WannaCry, die gebruikmaakte van een zwakke plek in Windows en computers over de hele wereld trof.

Wat is het doel?

Er werden twee hoofddoelstellingen vastgesteld om de goede werking van de interne markt te waarborgen: 1) de voorwaarden scheppen voor de ontwikkeling van veilige producten met digitale elementen door ervoor te zorgen dat hardware- en softwareproducten met minder kwetsbaarheden in de handel worden gebracht en dat fabrikanten de beveiliging gedurende de hele levenscyclus van een product serieus nemen; en 2) de voorwaarden scheppen die gebruikers in staat stellen rekening te houden met cyberbeveiliging bij het selecteren en gebruiken van producten met digitale elementen. Er werden vier specifieke doelstellingen geformuleerd: i) ervoor zorgen dat fabrikanten de beveiliging van producten met digitale elementen verbeteren vanaf de ontwerp- en ontwikkelingsfase en gedurende de gehele levenscyclus; ii) zorgen voor een samenhangend cyberbeveiligingskader, waardoor naleving voor hardware- en softwarefabrikanten gemakkelijker wordt; iii) de beveiligingskenmerken van producten met digitale elementen transparanter maken, en iv) bedrijven en consumenten in staat stellen producten met digitale elementen veilig te gebruiken.

Wat is de meerwaarde van EU-maatregelen (subsidiariteit)?

De sterk grensoverschrijdende aard van cyberbeveiliging en de toenemende incidenten met spillover-effecten over grenzen, sectoren en producten heen betekenen dat de doelstellingen niet doeltreffend door de lidstaten afzonderlijk kunnen worden verwezenlijkt. Gezien het mondiale karakter van markten voor producten met digitale elementen lopen de lidstaten dezelfde risico's voor hetzelfde product met digitale

elementen op hun grondgebied. Een opkomend versnipperd kader van potentieel uiteenlopende nationale voorschriften dreigt een open en concurrerende eengemaakte markt voor producten met digitale elementen in de weg te staan. Een gezamenlijk optreden op EU-niveau is dan ook noodzakelijk om een hoog niveau van vertrouwen onder de gebruikers tot stand te brengen en de aantrekkelijkheid van in de EU in de handel gebrachte producten met digitale elementen te vergroten. Het zou ook de interne markt ten goede komen door rechtszekerheid te bieden en een gelijk speelveld tot stand te brengen voor fabrikanten van producten met digitale elementen.

B. Oplossingen

Welke opties dienen zich aan? Is er al dan niet een voorkeursoptie? Zo niet, waarom?

Er werden vier beleidsopties en daaraan verbonden subopties geanalyseerd die verder gaan dan de status quo: 1) zachte wetgeving en vrijwillige maatregelen; 2) productspecifieke ad-hocregelgeving voor cyberbeveiliging van materiële producten met digitale elementen en bijbehorende ingebedde software; 3) gemengde aanpak, met inbegrip van horizontale verplichte regels voor cyberbeveiliging van materiële producten met digitale elementen en bijbehorende ingebedde software, en een gespreide aanpak voor niet-ingebedde software, met twee subopties voor conformiteitsbeoordeling; en 4) een horizontale regelgevende interventie waarbij cyberbeveiligingsvereisten worden ingevoerd voor een breed scala aan producten met digitale elementen, waaronder niet-ingebedde software, met subopties betreffende het toepassingsgebied en de conformiteitsbeoordeling.

De conclusie van de effectbeoordeling luidde dat de **voorkeursoptie** optie 4 is, die alle producten met digitale elementen omvat en voorziet in verplichte beoordeling door derden voor kritieke producten, op basis van de beoordeling van de doeltreffendheid ten aanzien van de specifieke doelstellingen, de efficiëntie met betrekking tot kosten en baten, en de samenhang.

Hoe reageren de verschillende belanghebbenden? Wie steunt welke optie?

Met betrekking tot de vraag om de doeltreffendheid van de beleidsmaatregelen te beoordelen, waren de respondenten van de openbare raadpleging het erover eens dat optie 4 de meest doeltreffende maatregel zou zijn (4,08 op een schaal van 1 tot 5). Hiertoe behoorden consumentenorganisaties (5,00), respondenten die zichzelf als gebruikers identificeren (4,22), aangemelde instanties (4,17), markttoezichtautoriteiten (5,00) en fabrikanten van producten met digitale elementen (3,85), waaronder kleine en middelgrote ondernemingen (4,05).

C. Effecten van de voorkeursoptie

Wat zijn de voordelen van de voorkeursoptie (indien er een voorkeur is, anders van de belangrijkste opties)?

De voorkeursoptie zou aanzienlijke voordelen opleveren voor de verschillende belanghebbenden. Voor bedrijven zouden uiteenlopende beveiligingsregels voor producten met digitale elementen worden voorkomen en zouden de nalevingskosten op het gebied van de betrokken cyberbeveiligingswetgeving dalen. Het aantal cyberincidenten, de kosten voor incidentenbehandeling en de reputatieschade zouden worden beperkt. Voor de hele EU kan het initiatief naar schatting leiden tot een vermindering van kosten als gevolg van incidenten die bedrijven treffen, met grofweg 180 tot 290 miljard EUR per jaar. Bovendien zou het initiatief leiden tot een hogere omzet als gevolg van een hogere vraag naar producten met digitale elementen. Ook zou de wereldwijde reputatie van bedrijven door het initiatief verbeteren, waardoor de vraag van buiten de EU zou stijgen. Voor eindgebruikers zou de voorkeursoptie de transparantie van de beveiligingskenmerken vergroten en het gebruik van producten met digitale elementen vergemakkelijken.

Consumenten en burgers zouden ook een betere bescherming genieten van hun grondrechten, zoals privacy en gegevensbescherming.
Wat zijn de kosten van de voorkeursoptie (indien er een voorkeur is, anders van de belangrijkste opties)?
De voorkeursoptie zou aanvullende nalevings- en handhavingskosten met zich meebrengen voor bedrijven, aangemelde instanties en overheidsinstanties, met inbegrip van accreditatie- en markttoezichtautoriteiten. Voor softwareontwikkelaars en hardwarefabrikanten zal zij directe nalevingskosten met zich meebrengen voor nieuwe cyberbeveiligingsvereisten en verplichtingen inzake conformiteitsbeoordeling, documentatie en melding, waardoor de totale nalevingskosten oplopen tot ongeveer 29 miljard EUR bij een geraamde marktwaarde van producten met digitale elementen ten belope van 1 485 miljard EUR aan omzet. Eindgebruikers, met inbegrip van zakelijke eindgebruikers, consumenten en burgers, kunnen te maken krijgen met hogere prijzen van producten met digitale elementen. Deze moeten echter worden gezien tegen de achtergrond van de aanzienlijke voordelen die hierboven zijn beschreven. Voor aangemelde instanties zullen de aanvullende kosten naar verwachting worden gecompenseerd door een stijging van de omzet.
Wat zijn de gevolgen voor kleine en middelgrote ondernemingen (kmo's) en voor het concurrentievermogen?
Kmo's zullen als fabrikant en als eindgebruiker met de nieuwe eisen te maken krijgen. De nalevingskosten zouden in principe een grotere belasting vormen voor kmo's dan voor grote ondernemingen, die doorgaans betere schaalvoordelen hebben en zich meer bewust zijn van cyberbeveiliging. Kmo's zouden echter grote voordelen genieten van het initiatief, aangezien cyberbeveiliging in producten met digitale elementen voor kmo's als gebruikers een aanzienlijke kostenbesparing zou betekenen. Als fabrikanten zouden kmo's profiteren van een groter vertrouwen van eindgebruikers en nieuwe klanten. Een naadloze toegang tot de interne markt en een minder versnipperde markt kunnen zelfs gunstiger zijn voor kmo's, die minder goed zijn toegerust om met verschillende regelgevingsvereisten om te gaan. Hoewel kmo's de noodzaak van een evenredige aanpak en ondersteunende maatregelen benadrukken, waren zij over het algemeen voorstanders van een gelijk speelveld voor alle bedrijven en geloofden zij niet dat zij in een scenario van horizontale dwingende voorschriften benadeeld zouden worden ten opzichte van grotere bedrijven.
Zijn er significante gevolgen voor de nationale begrotingen en overheden?
Het initiatief zal gevolgen hebben voor nationale autoriteiten, zoals nationale aanmeldende autoriteiten, accreditatieautoriteiten en markttoezichtautoriteiten, die verantwoordelijk zijn voor het toezicht op en de handhaving van de voorgestelde maatregelen. Deze autoriteiten zullen extra aanpassingskosten (bv. opleiding en personele middelen) en handhavingskosten moeten dragen om aan de nieuwe eisen te voldoen. De door de accreditatie-instanties bestede middelen worden echter gecompenseerd en grotendeels gedragen door de conformiteitsbeoordelingsinstanties via de aankoop van accreditatiediensten.
Zijn er nog andere significante gevolgen?
Er vallen geen andere significante nadelige gevolgen te verwachten. Het voorkeursbeleid zou het aantal en de ernst van incidenten, waaronder inbreuken op persoonsgegevens, helpen verminderen en zou positieve sociale gevolgen hebben, zoals het terugdringen van cybercriminaliteit. De vraag naar professionals uit de beveiligingssector zal naar verwachting toenemen en de informatieasymmetrie op het gebied van cyberbeveiliging zou afnemen.
Evenredigheid?

De voorkeursoptie gaat niet verder dan wat nodig is om de specifieke doelstellingen op bevredigende wijze te verwezenlijken. De interventie zou ervoor zorgen dat producten met digitale elementen beveiligd worden gedurende hun hele levenscyclus en in verhouding tot de risico's die zij lopen.
D. Evaluatie
Wanneer wordt dit beleid geëvalueerd?
Uiterlijk [36 maanden] na de datum van toepassing van het initiatief en vervolgens om de vier jaar dient de Commissie bij het Europees Parlement en de Raad een verslag in over de evaluatie en herziening van het initiatief.