Staat van de Unie: nieuwe EU-cyberbeveiligingsregels voor beter beveiligde hardware en software

Brussel, 15 september 2022

De Commissie heeft vandaag een voorstel ingediend voor een nieuwe wet inzake cyberweerbaarheid om consumenten en bedrijven te beschermen tegen producten die onvoldoende beveiligd zijn. Het is de eerste EU-brede wetgeving in zijn soort en voert vereisten in op het gebied van cyberbeveiliging gedurende de hele levenscyclus van producten met digitale elementen.

Deze wet werd aangekondigd door voorzitter Ursula **von der Leyen** tijdens haar toespraak over de Staat van de Europese Unie van september 2021, en bouwt voort op de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk van 2020 en de EU-strategie voor de veiligheidsunie van datzelfde jaar. Dankzij de wet zullen digitale producten, zoals al dan niet draadloze producten en software, beter beveiligd worden voor consumenten in de hele EU. De wet zal er niet alleen voor zorgen dat fabrikanten zich verantwoordelijker moeten opstellen door beveiligingsondersteuning en software-updates tegen vastgestelde kwetsbaarheden aan te bieden, maar ook dat consumenten genoeg informatie krijgen over de cyberbeveiliging van de producten die zij kopen.

Margrethe **Vestager**, uitvoerend vicevoorzitter voor een Europa dat klaar is voor het digitale tijdperk: "*Wij moeten ons veilig kunnen voelen met producten die we op de eengemaakte markt kopen. Net zoals een CE-markering ons aantoont dat een stuk speelgoed of een koelkast betrouwbaar is, zal de wet inzake cyberweerbaarheid waarborgen dat geconnecteerde voorwerpen en software aan strenge cyberbeveiligingsvereisten voldoen. De wet zal de verantwoordelijkheid leggen waar zij hoort, namelijk bij degenen die de producten in de handel brengen.*"

Margaritis **Schinas**, vicevoorzitter voor de bevordering van onze Europese levenswijze: *"De wet inzake cyberweerbaarheid is ons antwoord op moderne veiligheidsrisico's, die in onze digitale samenleving alomtegenwoordig zijn. De EU heeft als eerste een ecosysteem voor cyberbeveiliging gecreëerd door middel van regels over kritische infrastructuur, paraatheid voor en reactie op cyberbeveiliging, en de certificering van cyberbeveiligingsproducten. Vandaag komen we met het sluitstuk van dit ecosysteem: een wet die zorgt voor veiligheid in onze huizen, in onze bedrijven en in elk product dat geconnecteerd is. Cyberbeveiliging is een zaak van de samenleving en niet langer een zaak van de industrie."*

Thierry **Breton**, commissaris voor de Interne Markt: "*Wat cyberbeveiliging betreft is Europa slechts zo sterk als zijn zwakste schakel, of dat nu een kwetsbare lidstaat of een onveilig product in de toeleveringsketen is. Computers, telefoons, huishoudelijke apparaten, virtuele assistenten, auto's, speelgoed, … stuk voor stuk vormen miljoenen producten een mogelijke ingang voor een cyberaanval. En toch gelden momenteel voor de meeste hardware en software geen verplichtingen op het gebied van cyberbeveiliging. Door standaard cyberbeveiliging in te voeren, zal de wet inzake cyberweerbaarheid helpen de Europese economie en onze collectieve veiligheid te beschermen.*"

Elke 11 seconden wordt ergens ter wereld wel een organisatie het slachtoffer van een ransomware-aanval. In 2021 werd geraamd dat cybercriminaliteit jaarlijks wereldwijd 5,5 biljoen euro kost (verslag van het Gemeenschappelijk Centrum voor Onderzoek (2020): Cybersecurity – Our Digital Anchor, a European perspective). Het is dus meer dan ooit cruciaal om een hoge mate van cyberbeveiliging te garanderen en digitale producten minder kwetsbaar te maken, omdat geslaagde aanvallen vaak langs die weg verlopen. Een toename van het aantal slimme en geconnecteerde producten leidt ertoe dat een cyberbeveiligingsprobleem bij één product gevolgen kan hebben voor de hele toeleveringsketen, de economie en het sociale leven op de interne markt ernstig kan

verstoren en schadelijk voor de veiligheid of zelfs levensbedreigend kan zijn.

De maatregelen die we vandaag voorstellen zijn gebaseerd op het nieuwe wetgevingskader voor de EU-productwetgeving, en omvatten:

a) regels voor het op de markt brengen van producten met digitale elementen om de cyberbeveiliging ervan te waarborgen;

b) essentiële vereisten voor het ontwerp, de ontwikkeling en de vervaardiging van producten met digitale elementen, en verplichtingen voor marktdeelnemers met betrekking tot deze producten;

c) essentiële vereisten voor de procedures die fabrikanten volgen om kwetsbare punten aan te pakken, om de cyberbeveiliging van producten met digitale elementen gedurende de hele levenscyclus te waarborgen, en verplichtingen voor marktdeelnemers met betrekking tot deze procedures. Fabrikanten zullen ook melding moeten maken van actief misbruikte kwetsbare punten en incidenten;

d) regels inzake markttoezicht en handhaving.

De nieuwe regels leggen de verantwoordelijkheid opnieuw bij de fabrikanten, die ervoor moeten zorgen dat producten met digitale elementen die op de EU-markt worden aangeboden, aan de beveiligingsvereisten beantwoorden. Zo komen de regels ten goede aan consumenten, burgers en ondernemingen die digitale producten gebruiken, doordat de transparantie van de beveiligingskenmerken en het vertrouwen in producten met digitale elementen worden vergroot, en doordat grondrechten zoals privacy en gegevensbescherming beter worden beschermd.

Andere jurisdicties over de hele wereld zijn ook met deze kwesties bezig, en onze wet inzake cyberweerbaarheid zal wellicht een internationaal referentiepunt worden. EU-normen op basis van de wet inzake cyberweerbaarheid zullen de uitvoering ervan vergemakkelijken en zullen een troef zijn voor de Europese cyberbeveiligingsindustrie op de wereldmarkten.

De voorgestelde verordening zal van toepassing zijn op alle producten die direct of indirect met een ander apparaat of netwerk zijn geconnecteerd. Voor sommige producten, waarvoor reeds cyberbeveiligingsvereisten zijn opgenomen in bestaande EU-regels, zijn er een aantal uitzonderingen, bijvoorbeeld voor medische hulpmiddelen, producten voor de luchtvaart en auto's.

Volgende stappen

Het is nu aan het Europees Parlement en de Raad om de ontwerpwet inzake cyberweerbaarheid te bespreken. Zodra de wet wordt aangenomen, krijgen marktdeelnemers en lidstaten twee jaar de tijd om zich aan de nieuwe voorschriften aan te passen. De verplichting dat fabrikanten actief misbruikte kwetsbaarheden en incidenten moeten melden, zal echter al één jaar na de datum van inwerkingtreding van toepassing worden, aangezien daarvoor minder organisatorische aanpassingen nodig zijn dan voor de andere nieuwe verplichtingen. De Commissie zal de wet inzake cyberweerbaarheid periodiek evalueren en verslag uitbrengen over de werking ervan.

Achtergrond

Cyberbeveiliging is een van de topprioriteiten van de Commissie en een hoeksteen van een digitaal en geconnecteerd Europa. De toename van het aantal cyberaanvallen tijdens de coronacrisis heeft aangetoond hoe belangrijk de bescherming is van ziekenhuizen, onderzoekscentra en andere infrastructuur. Er zijn dus krachtige maatregelen nodig om de economie en de samenleving van de EU toekomstbestendig te maken. Gegevensinbreuken kosten jaarlijks naar schatting ten minste 10 miljard euro; kwaadwillige pogingen om het internetverkeer te verstoren naar schatting ten minste 65 miljard euro (effectbeoordeling bij de gedelegeerde verordening van de Commissie tot aanvulling van de gedelegeerde verordening in het kader van de richtlijn radioapparatuur).

De in december 2020 gepresenteerde cyberbeveiligingsstrategie stelde voor om cyberbeveiliging op te nemen in elk onderdeel van de toeleveringsketen, en om de activiteiten en middelen van de EU in de vier cyberbeveiligingsgemeenschappen (interne markt, rechtshandhaving, diplomatie en defensie) verder te bundelen. De strategie is gebaseerd op de Europese digitale strategie en op de EU-strategie voor de veiligheidsunie, en steunt op een aantal wetgevingshandelingen, maatregelen en initiatieven die de EU heeft ingevoerd om de cyberbeveiligingscapaciteit te versterken en te zorgen voor een cyberbestendiger Europa.

De nieuwe wet inzake cyberweerbaarheid vormt een aanvulling op het EU-kader voor cyberbeveiliging: de richtlijn over beveiliging van netwerk- en informatiesystemen in de Unie (NIS-richtlijn), de richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS 2-richtlijn), die onlangs is overeengekomen door het Europees Parlement en de Raad, en de cyberbeveiligingsverordening.

Meer informatie

Vragen en antwoorden: EU-wet inzake cyberweerbaarheid

Factsheet over de wet inzake cyberweerbaarheid

Voorstel voor een wet inzake cyberweerbaarheid

Factsheet over de nieuwe EU-cyberbeveiligingsstrategie

Factsheet over het voorstel voor een richtlijn inzake maatregelen voor een hoog gemeenschappelijk cyberbeveiligingsniveau in de Unie (NIS 2-richtlijn)

Factsheet over cyberbeveiliging: extern optreden van de EU

Vragen en antwoorden: Nieuwe EU-cyberbeveiligingsstrategie en nieuwe regels om fysieke en digitale kritieke entiteiten weerbaarder te maken

Voorstel voor een richtlijn inzake maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie (NIS 2-richtlijn)

Voorstel voor een richtlijn betreffende de veerkracht van kritieke entiteiten

IP/22/5374

Contactpersoon voor de pers:

Johannes BAHRKE (+32 2 295 86 15)
Marietta GRAMMENOU (+32 2 298 35 83)

Voor het publiek: Europe Direct per telefoon 00 800 67 89 10 11 of e-mail

Related media

Cybersecurity