



Raad van de
Europese Unie

Brussel, 2 december 2020
(OR. en)

13629/20

CYBER 263
TELECOM 248
COPEN 362
CODEC 1266
COPS 441
COSI 235
CSC 344
CSCI 86
IND 248
RECH 493
SPACE 77

RESULTAAT BESPREKINGEN

van:	het secretariaat-generaal van de Raad
d.d.:	2 december 2020
aan:	de delegaties

Betreft:	Conclusies van de Raad over de cyberbeveiliging van verbonden apparaten
	- Via de schriftelijke procedure goedgekeurde conclusies van de Raad

Voor de delegaties gaan hierbij de conclusies van de Raad over de cyberbeveiliging van verbonden apparaten, die de Raad op 2 december 2020 via een schriftelijke procedure heeft goedgekeurd.

Conclusies van de Raad over de cyberbeveiliging van verbonden apparaten

De Raad van de Europese Unie,

HERINNEREND AAN

- de conclusies van de Raad over de gezamenlijke mededeling aan het Europees Parlement en de Raad: "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU",
 - de conclusies van de Raad over het opbouwen van capaciteit en vermogens op het gebied van cyberbeveiliging in de EU,
 - de conclusies van de Raad over het belang van 5G voor de Europese economie en de noodzaak om de veiligheidsrisico's in verband met 5G te beperken,
 - de conclusies van de Raad over de toekomst van een sterk gedigitaliseerd Europa na 2020: "Versterking van het digitale en economische concurrentievermogen in de hele Unie en van de digitale cohesie",
 - de conclusies van de Raad over het vormgeven van de digitale toekomst van Europa,
 - de conclusies van de Europese Raad over COVID-19, de eengemaakte markt, het industriebeleid, digitalisering en externe betrekkingen,
 - de mededeling van de Europese Commissie "De digitale toekomst van Europa vormgeven".
1. WIJST EROP dat de Europese Unie en de lidstaten hun digitale soevereiniteit en strategische autonomie zeker moeten stellen, met behoud van een open economie. Dit veronderstelt versterking van het vermogen om autonome technologische keuzes te maken en, als een van de belangrijkste pijlers, veerkrachtige en beveiligde infrastructuren, producten en diensten om vertrouwen in de digitale eengemaakte markt en binnen de Europese samenleving te wekken. Tot de kernwaarden van de Europese Unie behoort de bescherming van met name privacy, veiligheid, gelijkheid, menselijke waardigheid, de rechtsstaat en een open internet als noodzakelijke voorwaarden voor het tot stand brengen van een digitale samenleving, economie en industrie waarin de mens centraal staat.

2. ONDERKENT het toenemende belang van verbonden apparaten en de beveiliging daarvan, onder andere machines, sensoren en netwerken die het internet der dingen (Internet of Things - IoT) vormen. Verbonden apparaten zullen een belangrijke rol spelen bij het verder vormgeven van de digitale toekomst van Europa, vanuit industrieel en zakelijk oogpunt, evenals in het dagelijkse leven van de consumenten van een nieuwe generatie technologie. Naast 5G kunnen artificiële intelligentie, kwantumcomputing, high-performance computing, cloudcomputing, "distributed ledger"-technologieën, met name blockchain, en andere nieuwe toepassingen en kansen voor duurzame economische groei en een hogere mate van digitalisering van onze samenleving alleen door middel van cyberbeveiligde verbonden apparaten worden bereikt.
3. NEEMT ER NOTA VAN dat het toegenomen gebruik van met het internet verbonden consumentenproducten en industriële apparaten ook nieuwe risico's met zich zal brengen op het gebied van privacy en informatie- en cyberbeveiliging, en steeds meer mogelijke gevolgen voor de integriteit en de beschikbaarheid van producten en gegevens, die rechtstreeks van invloed kunnen zijn op de veiligheid. Het is van essentieel belang dat deze risico's tot een minimum worden beperkt om de consumenten te beschermen, de algehele cyberveerkracht van Europa te versterken en het vertrouwen van de burgers in digitale oplossingen en technologieën te vergroten. Dit zal ook het concurrentievermogen en de innovatiecapaciteit van Europese aanbieders van dergelijke apparaten bevorderen. Cyberbeveiliging en privacy moeten bij productinnovatie en in productie- en ontwikkelingsprocessen, met inbegrip van de ontwerpfase (beveiliging door ontwerp), als essentiële vereisten worden erkend en moeten gedurende de hele levenscyclus en in de hele toeleveringsketen van een product worden gewaarborgd.
4. BENADRUKT dat niet alleen een hoog niveau van beveiliging van verbonden apparaten moet worden gewaarborgd, maar consumenten ook bewuster moeten worden gemaakt van de potentiële risico's die zij lopen op het gebied van privacy en beveiliging. Dit zou ertoe bijdragen dat de dreigingen die uitgaan van een toegenomen gebruik van verbonden apparaten zoveel mogelijk worden beperkt, het vertrouwen in de digitale eengemaakte markt wordt vergroot en de economische en sociale voordelen van technologieën voor verbonden apparaten optimaal worden benut.

5. ONDERSTREEPT dat publieke investeringen in onderzoek en innovatie, met name via Horizon Europa en Digitaal Europa, alsook particuliere investeringen, waardevolle stimulansen kunnen zijn om verbonden apparaten veiliger en beter beveiligd - en derhalve slimme communicatienetwerken veerkrachtiger - te maken. De investeringen in de noodzakelijke digitale infrastructuur en technologie voor de uitrol van de meest recente technologieën voor verbonden apparaten moeten ook worden versneld om industrieel en digitaal leiderschap te bewerkstelligen en strategische autonomie te waarborgen, met behoud van een open economie.
6. WIJST OP de noodzaak van een hoog niveau van complementariteit en vergelijkbaarheid van beveiligingsfuncties van ICT-systemen en -componenten, die in veel verschillende sectoren van de digitale eengemaakte markt worden gebruikt.
7. ERKENT de huidige ontwikkelingen op Unieniveau om de cyberbeveiliging van verbonden apparaten te verbeteren, met name met betrekking tot recente initiatieven van de Commissie om op korte termijn cyberbeveiligingsaspecten aan te pakken in relevante rechtshandelingen, bijvoorbeeld handelingen van het nieuwe wetgevingskader (NWK), met name Richtlijn 2014/53/EU (richtlijn radioapparatuur). ONDERSTREEPT dat het belangrijk is na te gaan of er op lange termijn behoefte is aan horizontale wetgeving, onder meer tot nadere bepaling van de noodzakelijke voorwaarden voor marktintroductie, om alle relevante aspecten van cyberbeveiliging van verbonden apparaten, zoals beschikbaarheid, integriteit en vertrouwelijkheid, te regelen. VERWELKOMT in dit verband een bespreking over het toepassingsgebied van dergelijke wetgeving en het verband ervan met het kader voor cyberbeveiligingscertificering, zoals omschreven in de cyberbeveiligingsverordening, met als doel het beveiligingsniveau binnen de digitale eengemaakte markt te verhogen.
8. BENADRUKT dat de vereisten inzake cyberbeveiliging moeten worden omschreven in overeenstemming met de desbetreffende Uniewetgeving, waaronder de cyberbeveiligingsverordening, het nieuwe wetgevingskader, de verordening Europese normalisatie en mogelijke toekomstige horizontale wetgeving, zulks om dubbelzinnigheid en fragmentatie in de wetgeving te voorkomen.

9. ONDERKENT de belangrijke rol van alle belanghebbenden, met name van de fabrikanten, bij het verbeteren van de cyberbeveiliging van verbonden apparaten op de digitale eengemaakte markt, en ROEPT derhalve OP tot coördinatie en nauwe samenwerking met alle betrokken publieke en particuliere belanghebbenden, ook met het oog op mogelijke toekomstige horizontale wetgeving.
- 9 bis IS INGENOMEN MET de lopende werkzaamheden onder leiding van het EU-Agentschap voor netwerk- en informatiebeveiliging (Enisa) voor het opstellen van de eerste EU-regelingen voor cyberbeveiligingscertificering, namelijk de voorgestelde gemeenschappelijke criteria van de Europese Unie en de voorgestelde regelingen voor clouddiensten. Deze regelingen zullen belangrijke grondslagen vormen voor het certificeren van verbonden apparaten.
10. BENADRUKT dat in eventuele aanvullende certificeringsregelingen voor verbonden apparaten en aanverwante diensten die zouden worden opgenomen in het voortschrijdend werkprogramma van de Unie en omschreven in de cyberbeveiligingsverordening, moet worden aangegeven hoe aan de toepasselijke beveiligingseisen op het relevante zekerheidsniveau moet worden voldaan op basis van specifieke Europese en internationaal erkende normen, ongeacht de sector waarin het product zal worden gebruikt, en welke testspecificaties, certificaten, enz. moeten worden gebruikt.
11. ONDERKENT dat de certificering van verbonden apparaten relevante normen, standaarden en technische specificaties zou vereisen voor cyberbeveiligingsevaluaties in het kader van de cyberbeveiligingsverordening. ONDERSTREEPT derhalve dat er normen, standaarden of technische specificaties inzake cyberbeveiliging moeten komen voor verbonden apparaten en BEVEELT AAN dat de inspanningen van de Europese normalisatieorganisaties ter zake worden opgevoerd. WIJST er tevens OP dat de ETSI-norm EN 303 645 voor cyberbeveiliging van IoT-consumentenapparaten een belangrijke stap in deze richting is.

12. VRAAGT de Commissie een verzoek te overwegen inzake [...] kandidaat-regelingen voor cyberbeveiligingscertificering van verbonden apparaten en aanverwante diensten op basis van het voortschrijdend werkprogramma van de Unie dat nu wordt ontwikkeld, waarbij ten volle rekening wordt gehouden met de horizontale Europese regelingen voor cyberbeveiligingscertificering die momenteel worden uitgewerkt. Een dergelijke regeling zal de fabrikanten van die producten in staat stellen om, op vrijwillige basis, producten met het beoordeelde zekerheidsniveau te promoten.
13. VERZOEKT om een bespreking over hoe het doel van cyberbeveiliging kan worden verankerd in toekomstige horizontale wetgeving die cyberbeveiligingsrisico's in verband met verbonden apparaten bestrijkt, en WIJST er tegelijkertijd OP dat, in voorkomend geval, aanpassing moet worden overwogen van essentiële voorschriften van de respectieve NWK-richtlijnen.
14. SPOORT de Commissie AAN om, waar nodig, ook complementaire sectorspecifieke regelgeving te bezien waarin wordt bepaald aan welk niveau van cyberbeveiliging een verbonden apparaat moet voldoen, om ervoor te zorgen dat voor dergelijke apparaten met een hoger beveiligingsrisico specifieke beveiligings- en privacyvereisten worden ingevoerd.
15. ONDERSTREEPT dat de levenskwaliteit en het welzijn van de Europese burgers moeten worden verbeterd en dat het vertrouwen in de digitale eengemaakte markt moet worden vergroot. De beveiliging en de privacy van onze samenlevingen zijn essentieel om de kernwaarden van de Unie te beschermen. BENADRUKT derhalve dat op het kader van de cyberbeveiligingsverordening moet worden voortgebouwd om de beveiligingsvereisten, volgens verschillende zekerheidsniveaus, in alle sectoren van het NWK te harmoniseren, teneinde fragmentatie en meervoudige controles van identieke vereisten te voorkomen en in de hele Europese Unie een gelijk speelveld voor concurrentie en innovatie te bieden.

16. VERZOEKT de Commissie, Enisa, het Comité voor conformiteitsbeoordeling en markttoezicht inzake telecommunicatie en de Europese Groep voor cyberbeveiligingscertificering actief deel te nemen aan dit initiatief ter versterking van de digitale eengemaakte markt en vergroting van het vertrouwen in ICT-producten, -diensten en -processen voor verbonden apparaten door privacy en cyberbeveiliging te garanderen, en een toegenomen wereldwijd concurrentievermogen van de IoT-sector van de Unie te faciliteren door te zorgen voor de hoogst mogelijke normen inzake veerkracht, veiligheid en beveiliging.
17. WIJST ER in dit verband OP dat kleine en middelgrote ondernemingen (kmo's), als essentiële bouwsteen van het Europees cyberbeveiligingsecosysteem, moeten worden ondersteund, en SPOORT de kmo's aan deel te nemen aan alle openbare raadplegingen en aan normalisatieactiviteiten, zodat rekening kan worden gehouden met de waardevolle en belangrijke bijdrage die zij leveren om van cyberbeveiliging een haalbaar doel en een concurrentievoordeel op de Europese markt te maken.
18. NEEMT ER NOTA VAN dat de verplichting om cyberbeveiliging en privacy gedurende de hele levenscyclus en in de hele toeleveringsketen van een product te waarborgen, een positief effect kan hebben op de ecologische voetafdruk van de technologiesector doordat fabrikanten naar slimme en duurzame ontwikkelings- en productieprocessen worden toegeleid en zodoende de hoeveelheid elektronisch afval in verband met de verwijdering van verbonden apparaten wordt verminderd.
