IV

(Informationen)

INFORMATIONEN DER ORGANE, EINRICHTUNGEN UND SONSTIGEN STELLEN DER EUROPÄISCHEN UNION

RAT

Schlussfolgerungen des Rates zur Cybersicherheit vernetzter Geräte

(2020/C 427/04)

DER RAT DER EUROPÄISCHEN UNION —

UNTER HINWEIS AUF

— die Schlussfolgerungen des Rates zur Gemeinsamen Mitteilung an das Europäische Parlament und den Rat: „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“,

— die Schlussfolgerungen des Rates über Cybersicherheitskapazitäten und deren Aufbau in der EU,

— die Schlussfolgerungen des Rates zur Bedeutung von 5G für die europäische Wirtschaft und zur Notwendigkeit der Begrenzung der Sicherheitsrisiken im Zusammenhang mit 5G,

— die Schlussfolgerungen des Rates zur Zukunft eines hoch digitalisierten Europas nach 2020: „Förderung der digitalen und wirtschaftlichen Wettbewerbsfähigkeit in der gesamten Union und des digitalen Zusammenhalts“,

— die Schlussfolgerungen des Rates zur Gestaltung der digitalen Zukunft Europas,

— die Schlussfolgerungen des Europäischen Rates zu den Themen COVID-19, Binnenmarkt, Industriepolitik und Digitalisierung sowie zu den Außenbeziehungen,

— die Mitteilung der Europäischen Kommission zur „Gestaltung der digitalen Zukunft Europas“ —

1. UNTERSTREICHT, dass die Europäische Union und ihre Mitgliedstaaten ihre digitale Souveränität und strategische Autonomie unter Wahrung einer offenen Wirtschaft sicherstellen müssen. Dazu gehören die Stärkung der Fähigkeit, autonome Entscheidungen zu Technologien zu treffen, und — als eine der wichtigsten Säulen — widerstandsfähige und sichere Infrastrukturen, Produkte und Dienste, um Vertrauen in den digitalen Binnenmarkt und innerhalb der europäischen Gesellschaft aufzubauen. Die Grundwerte der Europäischen Union umfassen insbesondere die Privatsphäre, Sicherheit, Gleichberechtigung, die Menschenwürde, Rechtsstaatlichkeit sowie das offene Internet als Voraussetzungen für eine von digitalen Technologien geleitete und auf den Menschen ausgerichtete Gesellschaft, Wirtschaft und Industrie;

2. IST SICH BEWUSST, dass vernetzte Geräte und ihre Sicherheit zunehmend an Bedeutung gewinnen, einschließlich Maschinen, Sensoren und Netze, die das Internet der Dinge (IoT) ausmachen. Vernetzte Geräte werden eine Schlüsselrolle bei der weiteren Gestaltung der digitalen Zukunft Europas spielen, und zwar für Industrie und Unternehmen sowie im Alltag der Verbraucherinnen und Verbraucher einer neuen Technologie-Generation. Neben 5G können künstliche Intelligenz, Quanteninformatik, Hochleistungsrechnen, Cloud-Computing, Distributed-Ledger-Technologie — insbesondere Blockchain — und andere neue Anwendungen, Chancen für ein nachhaltiges Wirtschaftswachstum und ein höheres Maß an Digitalisierung unserer Gesellschaft nur durch cybersichere vernetzte Geräte erreicht werden;

3. STELLT FEST, dass die zunehmende Nutzung von Konsumgütern und industriellen Geräten, die mit dem Internet verbunden sind, auch neue Risiken für die Privatsphäre und die Informations- und Cybersicherheit birgt, einschließlich immer mehr potenzieller Folgen für die Integrität und Verfügbarkeit von Produkten und Daten, die sich direkt auf die Sicherheit auswirken können. Diese Risiken müssen unbedingt minimiert werden, um die Verbraucherinnen und Verbraucher zu schützen, die Abwehrfähigkeit Europas gegenüber Cyberangriffen insgesamt zu verbessern und das Vertrauen der Bürgerinnen und Bürger in digitale Lösungen und Technologien zu stärken. Dies wird auch die Wettbewerbs- und Innovationsfähigkeit von europäischen Anbietern solcher Geräte fördern.

Cybersicherheit und Privatsphäre sollten als wesentliche Anforderungen im Rahmen der Produktinnovation, der Produktions- und Entwicklungsprozesse, einschließlich der Entwurfsphase (eingebaute Sicherheit („security by design")), anerkannt und während des gesamten Lebenszyklus eines Produkts und über seine gesamte Lieferkette hinweg sichergestellt werden;

4. HEBT HERVOR, dass es neben der Gewährleistung eines hohen Sicherheitsniveaus vernetzter Geräte auch wichtig ist, die Verbraucherinnen und Verbraucher für deren potenzielle Datenschutz- und Sicherheitsrisiken zu sensibilisieren. Dies würde dazu beitragen, die Bedrohungen, die sich aus der verstärkten Nutzung vernetzter Geräte ergeben, zu minimieren, das Vertrauen in den digitalen Binnenmarkt zu stärken und die wirtschaftlichen und gesellschaftlichen Vorteile, die die Technologien vernetzter Geräte bieten, optimal zu nutzen;

5. UNTERSTREICHT, dass öffentliche Investitionen in Forschung und Innovation, insbesondere im Rahmen von Horizont Europa und des Programms „Digitales Europa", sowie private Investitionen wertvolle Anreize schaffen könnten, vernetzte Geräte sicherer und damit intelligente Kommunikationsnetze widerstandsfähiger zu machen. Investitionen in die digitale Infrastruktur und Technologie, die für die Einführung der neuesten Technologien vernetzter Geräte erforderlich sind, sollten ebenfalls vorangetrieben werden, um eine industrielle und digitale Führungsrolle zu erreichen sowie die strategische Autonomie zu gewährleisten und gleichzeitig eine offene Wirtschaft zu erhalten;

6. BETONT, dass ein hohes Maß an Komplementarität und Vergleichbarkeit der Sicherheitsfunktionen von IKT-Systemen und IKT-Komponenten, die in verschiedenen Sektoren des digitalen Binnenmarkts verwendet werden, sichergestellt werden muss;

7. WÜRDIGT die laufenden Entwicklungen auf Unionsebene, um das Cybersicherheitsniveau vernetzter Geräte zu erhöhen, insbesondere in Bezug auf die jüngsten Initiativen der Kommission, kurzfristig Aspekte der Cybersicherheit in den einschlägigen Rechtsakten anzugehen, wie beispielsweise Rechtsakten nach dem neuen Rechtsrahmen (NLF), insbesondere der Richtlinie 2014/53/EU (Richtlinie über Funkanlagen); UNTERSTREICHT, wie wichtig es ist zu bewerten, ob langfristig horizontale Rechtsvorschriften, in denen auch die Bedingungen für das Inverkehrbringen festgelegt werden, notwendig sind, um alle einschlägigen Aspekte der Cybersicherheit vernetzter Geräte, wie Verfügbarkeit, Integrität und Vertraulichkeit, anzugehen; BEGRÜßT in diesem Zusammenhang eine Diskussion über den Geltungsbereich solcher Rechtsvorschriften und ihre Verbindungen zum Rahmen für die Cybersicherheitszertifizierung, wie sie im Rechtsakt zur Cybersicherheit festgelegt ist, mit dem Ziel, das Sicherheitsniveau im digitalen Binnenmarkt zu erhöhen;

8. BETONT, dass Anforderungen an die Cybersicherheit im Einklang mit den einschlägigen Unionsvorschriften, einschließlich des Rechtsakts zur Cybersicherheit, des NLF, der Verordnung über die europäische Normung und eines möglichen künftigen horizontalen Rechtsakts, definiert werden sollten, um Zweideutigkeit und Fragmentierung innerhalb der Vorschriften zu vermeiden;

9. WÜRDIGT die wichtige Rolle, die allen Interessenträgern, insbesondere den Herstellern, bei der Erhöhung des Cybersicherheitsniveaus vernetzter Geräte im digitalen Binnenmarkt zukommt, und FORDERT daher die Koordinierung und enge Zusammenarbeit mit allen einschlägigen öffentlichen und privaten Interessenträgern, auch im Hinblick auf mögliche künftige horizontale Rechtsvorschriften;

9a. BEGRÜßT die laufenden Arbeiten unter Federführung der ENISA zu den ersten EU-Schemas für die Cybersicherheitszertifizierung, nämlich die vorgeschlagenen Gemeinsamen Kriterien der Europäischen Union und die vorgeschlagenen Schemas für Cloud-Dienste. Diese Schemas werden maßgebliche Grundlagen für die Zertifizierung vernetzter Geräte bilden;

10. HEBT HERVOR, dass für jedes zusätzliche Zertifizierungsschema für vernetzte Geräte und verbundene Dienstleistungen, das im fortlaufenden Arbeitsprogramm der Union festgelegt und im Rechtsakt zur Cybersicherheit definiert wird, genau beschrieben werden sollte, wie die geltenden Sicherheitsanforderungen auf der entsprechenden Vertrauenswürdigkeitsstufe auf der Grundlage spezifischer europäischer und international anerkannter Normen — unabhängig vom Sektor, in dem das Produkt verwendet wird, — erfüllt werden sollten und welche Prüfspezifikationen, Zertifikate usw. anzuwenden sind;

11. ERKENNT AN, dass die Zertifizierung vernetzter Geräte einschlägige Normen, Standards oder technische Spezifikationen für Cybersicherheitsbewertungen im Rahmen des Rechtsakts zur Cybersicherheit erfordern würde; HEBT daher HERVOR, dass Normen, Standards oder technische Spezifikationen in Bezug auf die Cybersicherheit für vernetzte Geräte festgelegt werden müssen, und EMPFIEHLT, die Bemühungen der europäischen Normungsorganisationen in diesem Bereich zu verstärken; NIMMT gleichzeitig die Cybersicherheitsnorm ETSI EN 303 645 für IoT-Geräte für Verbraucher als wichtigen Schritt in diese Richtung ZUR KENNTNIS;

12. ERSUCHT die Kommission, einen Auftrag für mögliche Schemas für die Cybersicherheitszertifizierung für vernetzte Geräte und verbundene Dienstleistungen auf der Grundlage des derzeit in Ausarbeitung befindlichen fortlaufenden Arbeitsprogramms der Union in Erwägung zu ziehen, wobei die horizontalen europäischen Schemas für die Cybersicherheitszertifizierung, die derzeit erarbeitet werden, weitestgehend zu berücksichtigen sind. Auf freiwilliger Basis wird ein derartiges Schema den Herstellern solcher Produkte ermöglichen, Produkte mit der geprüften Vertrauenswürdigkeitsstufe zu bewerben;

13. REGT eine Diskussion darüber AN, wie das Ziel der Cybersicherheit in künftigen horizontalen Rechtsvorschriften verankert werden könnte, die Risiken für die Cybersicherheit im Zusammenhang mit vernetzten Geräten zum Gegenstand haben, und STELLT gleichzeitig FEST, dass geprüft werden muss, ob gegebenenfalls die Anforderungen der einschlägigen NLF-Richtlinien angepasst werden müssen;

14. ERMUTIGT die Kommission, erforderlichenfalls auch ergänzende sektorspezifische Verordnungen zu prüfen, die das von vernetzten Geräten einzuhaltende Cybersicherheitsniveau festlegen sollten, um sicherzustellen, dass für Geräte mit höheren Sicherheitsrisiken spezifische Anforderungen an die Sicherheit und den Schutz der Privatsphäre eingeführt werden;

15. BETONT, dass die Lebensqualität und das Wohlergehen der europäischen Bürgerinnen und Bürger verbessert und das Vertrauen in den digitalen Binnenmarkt gestärkt werden müssen. Die Sicherheit und der Schutz der Privatsphäre unserer Gesellschaften sind von wesentlicher Bedeutung, um die Grundwerte der Union zu wahren; BETONT daher, dass der durch den Rechtsakt zur Cybersicherheit geschaffene Rahmen als Grundlage dafür dienen muss, die Sicherheitsanforderungen entsprechend den unterschiedlichen Vertrauenswürdigkeitsstufen in allen Sektoren des NLF zu harmonisieren, um eine Fragmentierung und Mehrfachkontrollen identischer Anforderungen zu vermeiden und gleiche Wettbewerbsbedingungen in der gesamten Europäischen Union für Wettbewerb und Innovation zu schaffen;

16. ERSUCHT die Kommission, die Agentur der EU für Cybersicherheit (ENISA), den Ausschuss für Konformitätsbewertung von Telekommunikationsgeräten und Marktüberwachung und die Europäische Gruppe für die Cybersicherheitszertifizierung, sich aktiv an dieser Initiative zur Stärkung des digitalen Binnenmarkts und zur Stärkung des Vertrauens in IKT-Produkte, -Dienstleistungen und -Prozesse für vernetzte Geräte zu beteiligen, indem der Schutz der Privatsphäre und die Cybersicherheit sichergestellt werden und die zunehmende globale Wettbewerbsfähigkeit der IoT-Industrie der Union durch die Gewährleistung der höchsten Standards bei Abwehrfähigkeit und Sicherheit gefördert wird;

17. HEBT in diesem Zusammenhang HERVOR, dass die KMU als wesentliche Elemente des europäischen Cybersicherheitsökosystems unterstützt werden müssen, und ERMUTIGT die KMU, sich an allen eingeleiteten öffentlichen Konsultationen sowie an Normungstätigkeiten zu beteiligen, damit ihr wertvoller und wichtiger Beitrag berücksichtigt werden kann, wenn es darum geht, Cybersicherheit zu einem erreichbaren Ziel und zu einem Wettbewerbsvorteil auf dem europäischen Markt zu machen;

18. STELLT FEST, dass die Verpflichtung, die Cybersicherheit und den Schutz der Privatsphäre während des gesamten Lebenszyklus eines Produkts und über seine gesamte Lieferkette hinweg zu gewährleisten, positive Auswirkungen auf den Umweltfußabdruck des Technologiesektors haben könnte, indem Hersteller zu intelligenten und nachhaltigen Entwicklungs- und Produktionsprozessen geführt würden und dadurch die Menge an Elektronikabfällen im Zusammenhang mit der Entsorgung vernetzter Geräte verringert würde.