IV

(Informacje)

INFORMACJE INSTYTUCJI, ORGANÓW I JEDNOSTEK ORGANIZACYJNYCH UNII EUROPEJSKIEJ

RADA

Konkluzje Rady w sprawie cyberbezpieczeństwa urządzeń podłączonych do internetu

(2020/C 427/04)

RADA UNII EUROPEJSKIEJ,

PRZYPOMINAJĄC:

— konkluzje Rady w sprawie wspólnego komunikatu do Parlamentu Europejskiego i Rady pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej",

— konkluzje Rady w sprawie budowania w UE potencjału i zdolności w zakresie cyberbezpieczeństwa,

— konkluzje Rady w sprawie znaczenia 5G dla gospodarki europejskiej oraz potrzeby ograniczenia zagrożeń dla bezpieczeństwa związanych z 5G,

— konkluzje Rady w sprawie przyszłości wysoce ucyfrowionej Europy po roku 2020: „Stymulowanie cyfrowej i gospodarczej konkurencyjności i spójności cyfrowej w całej Unii",

— konkluzje Rady w sprawie kształtowania cyfrowej przyszłości Europy,

— konkluzje Rady Europejskiej w sprawie COVID-19, jednolitego rynku, polityki przemysłowej oraz stosunków cyfrowych i zewnętrznych,

— komunikat Komisji Europejskiej w sprawie kształtowania cyfrowej przyszłości Europy.

1. PODKREŚLA, że Unia Europejska i jej państwa członkowskie muszą zapewnić swoją suwerenność cyfrową i strategiczną autonomię, jednocześnie zachowując otwartą gospodarkę. Obejmuje to wzmocnienie zdolności do dokonywania autonomicznych wyborów technologicznych oraz – jako jednego z głównych filarów – odpornych i bezpiecznych infrastruktur, produktów i usług mających budować zaufanie na jednolitym rynku cyfrowym i wśród europejskiego społeczeństwa. Podstawowe wartości Unii Europejskiej chronią w szczególności prywatność, bezpieczeństwo, równość, godność ludzką, praworządność i otwarty charakter internetu jako warunki niezbędne do osiągnięcia procyfrowych i ukierunkowanych na człowieka społeczeństwa, gospodarki i przemysłu.

2. UZNAJE rosnące znaczenie urządzeń podłączonych do internetu i ich bezpieczeństwa, w tym maszyn, czujników i sieci, które składają się na internet rzeczy (IoT). Urządzenia podłączone do internetu odegrają kluczową rolę w dalszym kształtowaniu cyfrowej przyszłości Europy, zarówno na płaszczyźnie przemysłowej i biznesowej, jak i w codziennym życiu użytkowników technologii nowej generacji. Oprócz możliwości oferowanych przez sieci 5G, sztuczną inteligencję, obliczenia kwantowe, obliczenia wielkiej skali, przetwarzanie w chmurze, technologie rozproszonego rejestru, w szczególności technologie *blockchain*, i wszelkie inne nowe zastosowania, potencjał w zakresie zrównoważonego wzrostu gospodarczego i wyższego poziomu cyfryzacji naszego społeczeństwa może zostać zrealizowany wyłącznie w oparciu o cyberbezpieczne urządzenia połączone z internetem.

3. STWIERDZA, że rosnące użytkowanie produktów konsumpcyjnych i urządzeń przemysłowych podłączonych do internetu stworzy także nowe zagrożenia dla prywatności, bezpieczeństwa informacji i cyberbezpieczeństwa, w tym coraz częściej może oddziaływać na integralność i dostępność produktów i danych, co z kolei może bezpośrednio wpływać na bezpieczeństwo. Zminimalizowanie takich zagrożeń jest konieczne, tak by chronić konsumentów, wzmocnić ogólną cyberodporność Europy oraz zwiększyć zaufanie obywateli do rozwiązań i technologii cyfrowych.

Działania w tym zakresie zwiększą też konkurencyjność i zdolności innowacyjne europejskich dostawców takich urządzeń. Cyberbezpieczeństwo i prywatność powinny być uznawane za podstawowe wymogi w procesach innowacji, produkcji i rozwoju produktów, w tym w fazie projektowania (uwzględnianie bezpieczeństwa na etapie projektowania) i należy je zapewniać w całym cyklu życia i w całym łańcuchu dostaw produktu.

4. PODKREŚLA, że poza zapewnianiem wysokiego poziomu bezpieczeństwa urządzeń podłączonych do internetu, równie istotne jest zwiększenie świadomości konsumentów na temat wiążących się z tymi urządzeniami potencjalnymi zagrożeniami dla prywatności i bezpieczeństwa. To pomogłoby zminimalizować zagrożenia wynikające z większego użytkowania urządzeń podłączonych do internetu, zwiększyć zaufanie do jednolitego rynku cyfrowego i optymalnie wykorzystać gospodarcze i społeczne korzyści, jakie oferują technologie urządzeń podłączonych do internetu.

5. PODKREŚLA, że publiczne inwestycje w badania naukowe i innowacje, w szczególności za pośrednictwem programów „Horyzont Europa" i „Cyfrowa Europa", a także inwestycje prywatne mogą dostarczać cennych zachęt do zwiększania bezpieczeństwa i ochrony urządzeń podłączonych do internetu, a tym samym wzmacniać odporność inteligentnych sieci komunikacyjnych. Należy również przyspieszyć inwestycje w niezbędną infrastrukturę i technologię cyfrową w celu wdrożenia najnowszych technologii urządzeń podłączonych do internetu, tak by osiągnąć wiodącą pozycję w przemyśle i przywództwo cyfrowe, jednocześnie zachowując otwartą gospodarkę.

6. PODKREŚLA, że należy zapewnić wysoki poziom komplementarności i porównywalności funkcji bezpieczeństwa systemów i komponentów ICT, które są wykorzystywane w wielu różnych sektorach jednolitego rynku cyfrowego.

7. Z ZADOWOLENIEM PRZYJMUJE czynione obecnie na szczeblu unijnym postępy mające na celu podniesienie poziomu cyberbezpieczeństwa urządzeń podłączonych do internetu, w szczególności najnowsze inicjatywy Komisji, których celem jest uwzględnienie w perspektywie krótkoterminowej aspektów cyberbezpieczeństwa w odpowiednich aktach prawnych, na przykład w aktach wchodzących w skład nowych ram prawnych (NLF) w szczególności w dyrektywie 2014/53/UE (dyrektywa w sprawie urządzeń radiowych). PODKREŚLA, że z myślą o uwzględnieniu wszystkich istotnych aspektów cyberbezpieczeństwa urządzeń podłączonych do internetu, takich jak dostępność, integralność i poufność, ważne jest, by ocenić potrzebę wprowadzenia horyzontalnego prawodawstwa w perspektywie długoterminowej, określając także warunki niezbędne do wprowadzenia do obrotu. W tym kontekście Z ZADOWOLENIEM PRZYJMUJE dyskusję na temat zakresu takiego prawodawstwa i jego powiązań z ramami certyfikacji cyberbezpieczeństwa, określonymi na mocy aktu o cyberbezpieczeństwie, z myślą o podniesieniu poziomu bezpieczeństwa na jednolitym rynku cyfrowym.

8. PODKREŚLA, że wymogi w zakresie cyberbezpieczeństwa powinny zostać zdefiniowane zgodnie z odpowiednim prawodawstwem Unii, w tym aktem o cyberbezpieczeństwie, NLF, rozporządzeniem w sprawie normalizacji europejskiej oraz ewentualnym przyszłym prawodawstwem horyzontalnym, tak by uniknąć niejednoznaczności i fragmentacji prawnej.

9. UZNAJE istotną rolę wszystkich interesariuszy, w szczególności producentów w podnoszeniu poziomu cyberbezpieczeństwa urządzeń podłączonych do internetu na jednolitym rynku cyfrowym, w związku z czym APELUJE o koordynację i ścisłą współpracę ze wszystkimi publicznymi i prywatnymi interesariuszami, także z myślą o ewentualnym przyszłym prawodawstwie horyzontalnym.

9a. Z ZADOWOLENIEM PRZYJMUJE prowadzone przez ENISE prace nad opracowaniem pierwszych unijnych programów certyfikacji cyberbezpieczeństwa, w szczególności proponowanych wspólnych kryteriów Unii Europejskiej i proponowanych programów w dziedzinie usług w chmurze. Poprzez te programy zapewnione zostaną odpowiednie podstawy umożliwiające certyfikowanie urządzeń podłączonych do internetu.

10. PODKREŚLA, że wszelkie dodatkowe programy certyfikacji dla urządzeń podłączonych do internetu oraz powiązanych z nimi usług, które to programy mogą zostać ustanowione w unijnym kroczącym programie prac i zdefiniowane w ramach aktu o cyberbezpieczeństwie, powinny określać, w jaki sposób należy spełniać mające zastosowanie wymogi bezpieczeństwa, na odpowiednim poziomie uzasadnienia zaufania, na podstawie konkretnych europejskich i uznanych na szczeblu międzynarodowym norm, bez względu na to, w którym sektorze dany produkt ma być wykorzystywany i jakie specyfikacje testowe, certyfikaty itp. mają być stosowane.

11. STWIERDZA, że certyfikacja urządzeń podłączonych do internetu będzie wymagała odpowiednich norm, standardów lub specyfikacji technicznych na potrzeby prowadzonych w ramach aktu o cyberbezpieczeństwie ocen dotyczących cyberbezpieczeństwa. W związku z tym PODKREŚLA potrzebę opracowania norm, standardów lub specyfikacji technicznych w dziedzinie cyberbezpieczeństwa dla urządzeń podłączonych do internetu i ZALECA nasilenie wysiłków podejmowanych w tej kwestii przez europejskie organizacje normalizacyjne. Jednocześnie ZAUWAŻA, że opracowana przez Europejski Instytut Norm Telekomunikacyjnych (ETSI) norma EN 303 645 w zakresie cyberbezpieczeństwa konsumenckich urządzeń internetu rzeczy stanowi ważny krok w tym kierunku.

12. ZWRACA SIĘ do Komisji, by rozważyła zwrócenie się o [...] propozycję dotyczącą programów certyfikacji cyberbezpieczeństwa dla urządzeń podłączonych do internetu i powiązanych z nimi usług w oparciu o opracowywany obecnie unijny kroczący program prac, w jak największym stopniu uwzględniającą europejskie horyzontalne programy certyfikacji cyberbezpieczeństwa, które są obecnie opracowywane. Taki funkcjonujący na zasadzie dobrowolności program umożliwiałby producentom przedmiotowych urządzeń promowanie swoich produktów posiadających oceniony poziom uzasadnienia zaufania.

13. ZACHĘCA do podjęcia dyskusji na temat tego, w jaki sposób cel polegający na zapewnianiu cyberbezpieczeństwa powinien być zakorzeniony w przyszłym horyzontalnym prawodawstwie obejmującym zagrożenia dla cyberbezpieczeństwa związane z urządzeniami podłączonymi do internetu, a jednocześnie ODNOTOWUJE, że w stosownych przypadkach należy rozważyć dostosowanie podstawowych wymogów odpowiednich dyrektyw NLF.

14. ZACHĘCA Komisję, by w zakresie, w jakim to konieczne oceniła także uzupełniające regulacje sektorowe, które powinny określać, jaki poziom cyberbezpieczeństwa powinno spełniać dane urządzenie podłączone do internetu, tak by zapewnić ustanowienie konkretnych wymogów w zakresie bezpieczeństwa i prywatności dla takich urządzeń, z którymi wiążą się większe zagrożenia dla bezpieczeństwa.

15. PODKREŚLA, że należy poprawiać jakość życia i dobrostan europejskich obywateli i zwiększać zaufanie do jednolitego rynku cyfrowego. Bezpieczeństwo i prywatność naszych społeczeństw mają zasadnicze znaczenie dla ochrony podstawowych unijnych wartości. W związku z tym PODKREŚLA potrzebę wykorzystania ram zapewnionych przez akt o cyberbezpieczeństwie w celu zharmonizowania wymogów bezpieczeństwa, zgodnie z różnymi poziomami uzasadnienia zaufania, we wszystkich sektorach NLF, tak by uniknąć fragmentacji i wielokrotnych kontroli identycznych wymogów, i zapewnić podmiotom w całej Unii Europejskiej równe warunki konkurencji i innowacji.

16. ZACHĘCA Komisję, Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), Komitet ds. Oceny Zgodności Telekomunikacyjnej i Nadzoru Rynku oraz Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa, by aktywnie uczestniczyły w tej inicjatywie wzmacniającej jednolity rynek cyfrowy oraz zwiększającej zaufanie do produktów, usług i procesów ICT z dziedziny urządzeń podłączonych do internetu, poprzez zapewnianie prywatności i cyberbezpieczeństwa, oraz by sprzyjały zwiększonej globalnej konkurencyjności unijnej branży internetu rzeczy poprzez zapewnienie najwyższych standardów, jeśli chodzi o odporność, bezpieczeństwo i ochronę.

17. W tym kontekście PODKREŚLA potrzebę wspierania MŚP jako jednego z istotnych elementów europejskiego ekosystemu cyberbezpieczeństwa i ZACHĘCA MŚP do uczestnictwa we wszystkich rozpoczętych konsultacjach publicznych oraz w działaniach normalizacyjnych, tak by uwzględniony został ich cenny i istotny wkład w uczynienie z cyberbezpieczeństwa osiągalnego celu i konkurencyjnej przewagi na europejskim rynku.

18. STWIERDZA, że obowiązek zapewnienia cyberbezpieczeństwa i prywatności w całym cyklu życia produktu i w całym jego łańcuchu dostaw może mieć pozytywny wpływ na ślad środowiskowy sektora tej technologii poprzez ukierunkowanie producentów ku inteligentnym i zrównoważonym procesom rozwojowym i produkcyjnym, a tym samym może zmniejszyć ilość odpadów urządzeń elektrycznych i elektronicznych w związku ze składowaniem urządzeń podłączonych do internetu.