ZALECENIA

ZALECENIE KOMISJI (UE) 2019/534

z dnia 26 marca 2019 r.

Cyberbezpieczeństwo sieci 5G

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 292,

a także mając na uwadze, co następuje:

(1) Komisja uznała wdrożenie technologii sieciowych 5. generacji (5G) za jeden z najważniejszych czynników sprzyjających rozwojowi przyszłych usług cyfrowych oraz za priorytet strategii jednolitego rynku cyfrowego. Komisja przyjęła plan działania dotyczący sieci 5G, aby zadbać o to, by Unia dysponowała do roku 2020 infrastrukturą telekomunikacyjną niezbędną do przeprowadzenia jej transformacji cyfrowej ([1]).

(2) Sieci 5G będą opierać się na obecnych technologiach sieciowych 4. generacji (4G), zapewniając nowe możliwości pod względem usług oraz stając się centralną infrastrukturą i siłą napędową dla znacznej części unijnej gospodarki. Gdy już zostaną wdrożone, sieci 5G będą stanowić podbudowę szerokiego zakresu usług niezbędnych do funkcjonowania rynku wewnętrznego oraz utrzymania i realizacji podstawowych funkcji społecznych i gospodarczych – takich jak energetyka, transport, bankowość i opieka zdrowotna oraz systemy sterowania produkcją. Od cyfrowej infrastruktury oraz sieci 5G w coraz większym stopniu zależna również będzie organizacja procesów demokratycznych, takich jak wybory.

(3) Z powodu uzależnienia wielu usług o krytycznym znaczeniu od sieci 5G konsekwencje systemowych i rozległych zakłóceń byłyby szczególnie poważne. W rezultacie zapewnienie cyberbezpieczeństwa sieci 5G jest kwestią o strategicznym znaczeniu dla Unii w czasie, gdy cyberataki przybierają na sile i są coraz bardziej wyrafinowane.

(4) Ponadnarodowy charakter infrastruktury stanowiącej podstawę ekosystemu cyfrowego, która charakteryzuje się siecią wzajemnych powiązań, jak również transgraniczny charakter zagrożeń oznaczają, że wszelkie istotne luki bezpieczeństwa lub cyberincydenty dotyczące sieci 5G występujące w jednym państwie członkowskim miałyby wpływ na całą Unię. Dlatego też należy przewidzieć środki w celu zapewnienia wysokiego wspólnego poziomu cyberbezpieczeństwa sieci 5G.

(5) Państwa członkowskie potwierdziły konieczność podjęcia działań na szczeblu Unii. W swoich konkluzjach z dnia 21 marca 2019 r. Rada Europejska wyraziła pragnienie, by Komisja przyjęła zalecenie w sprawie skoordynowanego podejścia do bezpieczeństwa sieci 5G ([2]).

(6) Głównym celem powinno być zapewnienie suwerenności Europy, przy pełnym poszanowaniu europejskich wartości: otwartości i tolerancji ([3]). Inwestycje zagraniczne w sektorach strategicznych, nabywanie aktywów, technologii i infrastruktury o krytycznym znaczeniu w Unii oraz dostawy urządzeń mających krytyczne znaczenie mogą również stanowić zagrożenie dla bezpieczeństwa Unii.

(7) Cyberbezpieczeństwo sieci 5G ma kluczowe znaczenie dla zapewnienia strategicznej autonomii Unii, co znalazło odzwierciedlenie we wspólnym komunikacie „UE-Chiny – perspektywa strategiczna" ([4]).

(8) W rezolucji Parlamentu Europejskiego w sprawie zagrożeń dla bezpieczeństwa wynikających z rosnącej obecności technologicznej Chin w Unii również wezwano Komisję i państwa członkowskie do podjęcia działań na szczeblu Unii ([5]).

(9) W niniejszym zaleceniu odniesiono się do zagrożeń dla cyberbezpieczeństwa w sieciach 5G poprzez określenie wytycznych dotyczących odpowiednich środków w zakresie analizy ryzyka i zarządzania nim na szczeblu krajowym, opracowania skoordynowanej europejskiej oceny ryzyka oraz ustanowienia procesu mającego na celu opracowanie wspólnego zbioru najlepszych środków zarządzania ryzykiem.

(10) Istnieją już solidne unijne ramy prawne służące ochronie sieci łączności elektronicznej.

([1]) COM(2016) 588 final.
([2]) Konkluzje Rady Europejskiej z dnia 21 i 22 marca 2019 r.
([3]) Orędzie o stanie Unii 2018 – Godzina suwerenności Europy, 12 września 2018 r.
([4]) JOIN(2019) 5 final.
([5]) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//PL.

(11) Obowiązujące w Unii ramy z zakresu łączności elektronicznej ([6]) wspierają konkurencję, rynek wewnętrzny i interesy użytkowników końcowych oraz – wraz z Europejskim kodeksem łączności elektronicznej ([7]) – służą realizacji dodatkowego celu w zakresie łączności, którego osiągnięcie powinno przynieść oczekiwane rezultaty, a mianowicie: powszechny dostęp do łączności stacjonarnej i ruchomej o wysokiej przepustowości dla wszystkich obywateli Unii i unijnych przedsiębiorstw przy zagwarantowaniu interesów obywateli oraz upowszechnienie tego rodzaju łączności na szeroką skalę. W dyrektywie 2002/21/WE zobowiązano państwa członkowskie do zapewnienia integralności i bezpieczeństwa publicznych sieci łączności, powierzając im obowiązek dbania o to, by przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej stosowały środki techniczne i organizacyjne w celu odpowiedniego zarządzania zagrożeniami dla bezpieczeństwa sieci i usług. Przewidziano w niej również uprawnienia dla właściwych krajowych organów regulacyjnych, w tym uprawnienia do wydawania wiążących instrukcji, w celu zapewnienia wypełniania tych obowiązków.

(12) Ponadto w dyrektywie 2002/20/WE Parlamentu Europejskiego i Rady ([8]) zezwolono państwom członkowskim na obwarowanie ogólnych zezwoleń warunkami dotyczącymi zabezpieczenia sieci publicznych przed nieuprawnionym dostępem z myślą o ochronie poufności komunikacji zgodnie z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady ([9]).

(13) W celu wsparcia realizacji tych obowiązków Unia utworzyła szereg organów ds. współpracy. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), Komisja, państwa członkowskie oraz krajowe organy regulacyjne opracowały skierowane do krajowych organów regulacyjnych wytyczne techniczne w sprawie zgłaszania incydentów, środków bezpieczeństwa oraz zagrożeń i aktywów ([10]). Grupa współpracy utworzona na mocy dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 ([11]) („grupa współpracy") skupia właściwe organy z myślą o wspieraniu i ułatwianiu współpracy, w szczególności poprzez wydawanie strategicznych wytycznych dotyczących działalności sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego, co na poziomie technicznym ułatwia współpracę operacyjną.

(14) Przyszłe ramy europejskiego systemu certyfikacji cyberbezpieczeństwa ([12]) powinny stanowić istotne narzędzie wsparcia służące propagowaniu spójnego poziomu bezpieczeństwa. Powinny one umożliwiać opracowywanie systemów certyfikacji cyberbezpieczeństwa w odpowiedzi na potrzeby użytkowników sprzętu i oprogramowania 5G. Ze względu na krytyczne znaczenie tej infrastruktury opracowanie odpowiednich europejskich systemów certyfikacji cyberbezpieczeństwa na potrzeby produktów, usług i procesów z zakresu technologii informacyjno-komunikacyjnych stosowanych w ramach sieci 5G powinno stać się pilnym priorytetem. Państwa członkowskie i uczestnicy rynku powinni aktywnie uczestniczyć w opracowywaniu takich systemów certyfikacji, w tym udzielać wsparcia przy formułowaniu definicji szczegółowych profilów ochrony dla sieci 5G.

(15) Wobec braku zharmonizowanych przepisów unijnego prawa państwa członkowskie mogą przewidzieć – w drodze krajowych przepisów technicznych przyjętych zgodnie z prawem Unii – że europejski system certyfikacji cyberbezpieczeństwa powinien być obowiązkowy. Państwa członkowskie mają również możliwość odwoływania się do europejskich systemów certyfikacji cyberbezpieczeństwa w kontekście zamówień publicznych oraz dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE ([13]), a także mogłyby wspierać opracowywanie mechanizmów pomocy – takich jak centrum wsparcia – na potrzeby zakupów rozwiązań z zakresu cyberbezpieczeństwa przez nabywców z sektora publicznego.

(16) W zapewnieniu bezpieczeństwa sieci 5G istotną rolę odgrywa wysoki poziom ochrony danych i prywatności. Na poziomie Unii określono również przepisy gwarantujące bezpieczeństwo przetwarzania danych osobowych, w tym w łączności elektronicznej. W ogólnym rozporządzeniu o ochronie danych ([14]) przewidziano wymóg przetwarzania danych osobowych w sposób, który zapewnia ich bezpieczeństwo, w tym w celu zapobiegania nieuprawnionemu dostępowi do danych osobowych i sprzętu służącego do ich przetwarzania oraz nieuprawnionemu wykorzystywaniu tych danych i tego sprzętu. W dyrektywie o prywatności i łączności elektronicznej

([6]) Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) (Dz.U. L 108 z 24.4.2002, s. 33) oraz dyrektywy szczególne.

([7]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (Dz.U. L 321 z 17.12.2018, s. 36).

([8]) Dyrektywa 2002/20/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej (dyrektywa o zezwoleniach) (Dz.U. L 108 z 24.4.2002, s. 21).

([9]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz.U. L 201 z 31.7.2002, s. 37).

([10]) https://resilience.enisa.europa.eu/article-13.

([11]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

([12]) Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie „Agencji UE ds. Cyberbezpieczeństwa" ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt w sprawie cyberbezpieczeństwa"), (COM(2017) 477 final – 2017/0225 (COD)).

([13]) Dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (Dz.U. L 94 z 28.3.2014, s. 65).

([14]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

określono szczegółowe przepisy dotyczące ochrony poufności komunikacji oraz ochrony urządzeń końcowych stosowanych przez użytkowników końcowych. Nałożono w niej również na dostawców usług obowiązek stosowania odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa świadczonych przez nich usług.

(17) Unia przyjęła również instrument, który zapewni ochronę infrastruktury krytycznej oraz technologii o krytycznym znaczeniu, m.in. wykorzystywanych w komunikacji, umożliwiając państwom członkowskim monitorowanie bezpośrednich inwestycji zagranicznych pod kątem zagrożeń dla bezpieczeństwa lub porządku publicznego oraz tworząc mechanizm współpracy, w ramach którego państwa członkowskie i Komisja będą mogły wymieniać się informacjami oraz zgłaszać zastrzeżenia do konkretnych inwestycji ([15]).

(18) Państwa członkowskie i operatorzy podejmują obecnie istotne działania przygotowawcze, które mają umożliwić wprowadzenie na szeroką skalę sieci 5G. Kilka państw członkowskich wyraziło obawy dotyczące potencjalnych zagrożeń dla bezpieczeństwa związanych z sieciami 5G w kontekście postępowań o przyznanie praw do użytkowania pasm widma radiowego wyznaczonych na potrzeby sieci 5G ([16]) oraz analizuje środki, które pozwoliłyby zaradzić tym zagrożeniom.

(19) Działania mające na celu wyeliminowanie zagrożeń dla cyberbezpieczeństwa w sieciach 5G powinny uwzględniać czynniki techniczne oraz czynniki innego rodzaju. Czynniki techniczne mogą obejmować luki cyberbezpieczeństwa, które mogą być wykorzystane w celu uzyskania nieuprawnionego dostępu do informacji (cyberszpiegostwo motywowane gospodarczo lub politycznie) lub do innych złośliwych celów (cyberataki mające na celu zakłócanie lub niszczenie systemów i danych). Ważne aspekty, które należy wziąć pod uwagę, obejmują konieczność ochrony sieci przez cały cykl ich życia oraz potrzebę objęcia działaniami wszystkich odpowiednich urządzeń, w tym na etapie projektowania, rozwoju, zakupu, wdrażania, eksploatacji i utrzymania sieci 5G.

(20) Inne czynniki mogą obejmować wymogi regulacyjne lub innego rodzaju wymogi, którym podlegają dostawcy sprzętu informacyjno-komunikacyjnego. Przy ocenie istotności tych czynników należałoby brać pod uwagę m.in. ogólne ryzyko wywierania wpływu przez państwo trzecie, zwłaszcza w świetle funkcjonującego w nim modelu sprawowania rządów, brak porozumień między Unią a danym państwem trzecim o współpracy w zakresie bezpieczeństwa lub podobnych ustaleń – takich jak decyzje stwierdzające odpowiedni stopień ochrony – dotyczących ochrony danych bądź to, czy państwo to jest stroną międzynarodowych, wielostronnych lub dwustronnych umów w sprawie cyberbezpieczeństwa, zwalczania cyberprzestępczości lub ochrony danych.

(21) Ocena ryzyka – jako istotny krok w kierunku opracowania unijnego podejścia do cyberbezpieczeństwa sieci 5G – powinna zostać przeprowadzona na szczeblu krajowym. Pomogłoby to państwom członkowskim dostosować krajowe środki w zakresie wymogów bezpieczeństwa i zarządzania ryzykiem z uwzględnieniem wyników tej oceny.

(22) Należy opracować mechanizmy koordynacji, aby zapewnić skuteczność środków mających na celu eliminowanie zagrożeń dla cyberbezpieczeństwa oraz środków istotnych do zapewnienia sprawnego funkcjonowania rynku wewnętrznego i ochrony danych osobowych i prywatności.

(23) Krajowe oceny ryzyka powinny stanowić podstawę skoordynowanej unijnej oceny ryzyka, obejmującej analizę krajobrazu zagrożeń oraz wspólny przegląd prowadzony przez państwa członkowskie przy wsparciu Komisji oraz wraz z Agencją Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA).

(24) Uwzględniając krajowe oceny ryzyka i unijną ocenę ryzyka, grupa współpracy powinna opracować zestaw instrumentów służący identyfikacji różnego rodzaju zagrożeń dla cyberbezpieczeństwa oraz zbiór możliwych środków mających na celu ograniczenie zagrożeń w obszarach takich jak certyfikacja, testy i kontrole dostępu. Grupa ta powinna również wskazać możliwe szczególne środki, które byłyby właściwe w celu wyeliminowania zagrożeń zidentyfikowanych przez państwo lub państwa członkowskie. Grupa współpracy powinna korzystać ze wsparcia Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), Europolu, Organu Europejskich Regulatorów Łączności Elektronicznej (BEREC) oraz Centrum Analiz Wywiadowczych Unii Europejskiej. Wspomniane instrumenty powinny służyć Komisji pomocą przy opracowywaniu minimalnych wspólnych wymogów, aby w jeszcze większym stopniu zagwarantować wysoki poziom cyberbezpieczeństwa sieci 5G w całej Unii.

(25) Przy stosowaniu środków mających na celu zaradzenie zagrożeniom dla cyberbezpieczeństwa należy rozważyć wspieranie cyberbezpieczeństwa poprzez zróżnicowanie grona dostawców w przypadku budowy każdej pojedynczej sieci.

([15]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/452 z dnia 19 marca 2019 r. ustanawiające ramy monitorowania bezpośrednich inwestycji zagranicznych w Unii (DzU L 79 I z 21.3.2019, s. 1.).

([16]) Aukcję częstotliwości w przynajmniej jednym paśmie widma zaplanowano na 2019 r. w 11 państwach członkowskich: w Austrii, Belgii, Czechach, Francji, Grecji, Irlandii, na Litwie, w Niderlandach, Niemczech, Portugalii, i na Węgrzech. Na 2020 r. zaplanowano kolejnych sześć aukcji: w Hiszpanii, na Litwie (różne częstotliwości), Malcie, w Polsce, na Słowacji i w Zjednoczonym Królestwie. Źródło: http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) Niniejsze zalecenie powinno pozostawać bez uszczerbku dla kompetencji państw członkowskich w odniesieniu do działalności z zakresu bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego oraz działalności państwa w obszarach prawa karnego, w tym dla prawa państw członkowskich do wykluczenia usługodawców lub dostawców z ich rynków ze względów bezpieczeństwa narodowego,

PRZYJMUJE NINIEJSZE ZALECENIE:

I. **CELE**

1. W celu wsparcia opracowania unijnego podejścia do zapewnienia cyberbezpieczeństwa sieci 5G w niniejszym zaleceniu wskazano działania, które należy podjąć, aby umożliwić:

   a) państwom członkowskim ocenę zagrożeń dla cyberbezpieczeństwa mających wpływ na sieci 5G na poziomie krajowym i zastosowanie niezbędnych środków bezpieczeństwa;

   b) państwom członkowskim i odpowiednim unijnym instytucjom, agencjom i innym organom wspólne opracowanie skoordynowanej unijnej oceny ryzyka, która opiera się na krajowej ocenie ryzyka;

   c) grupie współpracy utworzonej na podstawie dyrektywy (UE) 2016/1148 („grupa współpracy") wskazanie możliwego wspólnego zestawu środków, które należy stosować w celu ograniczenia zagrożeń dla cyberbezpieczeństwa związanych z infrastrukturą stanowiącą podstawę ekosystemu cyfrowego, w szczególności sieci 5G.

II. **DEFINICJE**

2. Do celów niniejszego zalecenia:

   a) „sieci 5G" oznaczają zbiór wszystkich istotnych elementów infrastruktury sieciowej z zakresu technologii łączności ruchomej i bezprzewodowej, wykorzystywanej na potrzeby łączności i usług o wartości dodanej, o zaawansowanych parametrach eksploatacyjnych, takich jak bardzo wysoka prędkość przesyłu danych i przepustowość łączy, łączność charakteryzująca się niskim opóźnieniem, ekstremalnie wysoka niezawodność bądź zdolność obsługi dużej liczby podłączonych urządzeń. Mogą one obejmować elementy dotychczasowych sieci wykorzystujących technologię łączności ruchomej i bezprzewodowej poprzednich generacji, takich jak 4G lub 3G. Sieci 5G należy rozumieć jako obejmujące wszystkie istotne części sieci;

   b) „infrastruktura stanowiąca podstawę ekosystemu cyfrowego" oznacza infrastrukturę stosowaną, aby umożliwić cyfryzację szerokiej gamy rozwiązań o krytycznym znaczeniu znajdujących zastosowanie w gospodarce i społeczeństwie.

III. **DZIAŁANIA NA POZIOMIE KRAJOWYM**

3. Do dnia 30 czerwca 2019 r. państwa członkowskie powinny przeprowadzić ocenę infrastruktury sieci 5G pod kątem ryzyka, w tym zidentyfikować najbardziej wrażliwe elementy, w przypadku których naruszenia bezpieczeństwa miałyby znaczny negatywny wpływ. W tym samym terminie państwa członkowskie powinny również dokonać przeglądu wymogów w zakresie bezpieczeństwa oraz metod zarządzania ryzykiem mających zastosowanie na szczeblu krajowym, aby uwzględnić zagrożenia dla cyberbezpieczeństwa, które mogą powstać w związku z (i) czynnikami technicznymi, takimi jak szczególne parametry techniczne sieci 5G, oraz (ii) innymi czynnikami, takimi jak ramy prawne i ramy polityki, którym mogą podlegać dostawcy sprzętu informacyjno-komunikacyjnego w państwach trzecich.

4. W oparciu o wyniki wspomnianej krajowej oceny ryzyka oraz wspomnianego przeglądu oraz przy uwzględnieniu działań koordynacyjnych prowadzonych na szczeblu Unii państwa członkowskie powinny:

   a) zaktualizować wymogi w zakresie bezpieczeństwa oraz metody zarządzania ryzykiem stosowane w odniesieniu do sieci 5G;

   b) zaktualizować odpowiednie obowiązki nakładane na przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej zgodnie z art. 13a i 13b dyrektywy 2002/21/WE;

   c) obwarować ogólne zezwolenia warunkami dotyczącymi zabezpieczenia sieci publicznych przed nieuprawnionym dostępem oraz uzyskać od przedsiębiorstw uczestniczących w przyszłych postępowaniach o udzielenie praw użytkowania częstotliwości radiowych w pasmach 5G zobowiązanie do przestrzegania wymogów w zakresie bezpieczeństwa sieci na podstawie dyrektywy 2002/20/WE;

   d) stosować inne środki zapobiegawcze mające na celu ograniczenie potencjalnych zagrożeń dla cyberbezpieczeństwa.

5. nakładane na dostawców i operatorów mające zapewnić bezpieczeństwo wrażliwych części sieci, jak również, w stosownych przypadkach, inne obowiązki, takie jak obowiązek przekazywania właściwym organom krajowym istotnych informacji na temat planowanych zmian w sieciach łączności elektronicznej, oraz wymogi, zgodnie z którymi określone komponenty i systemy informatyczne muszą być testowane z wyprzedzeniem pod kątem bezpieczeństwa i integralności przez krajowe laboratoria audytowe/certyfikacyjne.

6. Wspólne przeglądy bezpieczeństwa powinny być przeprowadzane przez dwa państwa członkowskie lub większą ich liczbę, z wykorzystaniem i współdzieleniem odpowiedniej wiedzy technicznej i zaplecza technicznego, w odniesieniu do infrastruktury stanowiącej podstawę ekosystemu cyfrowego oraz sieci 5G, na przykład w przypadku gdy to samo przedsiębiorstwo eksploatuje lub buduje infrastrukturę sieciową w więcej niż jednym państwie członkowskim lub w przypadku gdy występują znaczne podobieństwa w konfiguracjach sieci. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), Europol oraz Organ Europejskich Regulatorów Łączności Elektronicznej (BEREC) powinni priorytetowo traktować wnioski ze strony państw członkowskich o wsparcie w tej dziedzinie. Wyniki wspomnianych przeglądów należy przekazywać grupie współpracy i sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego.

IV. SKOORDYNOWANE DZIAŁANIA NA SZCZEBLU UNII

7. W celu sformułowania wspólnego podejścia do eliminacji zagrożeń dla cyberbezpieczeństwa w sieciach 5G państwa członkowskie powinny rozpocząć do dnia 30 kwietnia 2019 r. działania w ramach specjalnego toku prac na forum grupy współpracy. W stosownych przypadkach państwa członkowskie powinny zapraszać odpowiednie organy do uczestnictwa w pracach grupy współpracy.

Skoordynowana europejska ocena ryzyka

8. Państwa członkowskie powinny wymieniać się informacjami ze sobą nawzajem oraz z innymi odpowiednimi organami Unii w celu uzyskania wspólnego obrazu istniejących i potencjalnych zagrożeń dla cyberbezpieczeństwa związanych z sieciami 5G.

9. Państwa członkowskie powinny przekazać swoje krajowe oceny ryzyka Komisji i Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) do dnia 15 lipca 2019 r.

10. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) powinna przeprowadzić szczegółową analizę krajobrazu zagrożeń związanych z sieciami 5G. Grupa współpracy oraz sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego utworzone na mocy dyrektywy (UE) 2016/1148 powinny wspierać ten proces.

11. Uwzględniając wszystkie te elementy, państwa członkowskie, przy wsparciu Komisji oraz wraz z Agencją Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), powinny do dnia 1 października 2019 r. ukończyć wspólny przegląd ekspozycji – w skali całej Unii – na ryzyko związane z infrastrukturą stanowiącą podstawę ekosystemu cyfrowego, a w szczególności z sieciami 5G.

12. W ramach tego wspólnego przeglądu należy nadać priorytet analizie ryzyka, na jakie narażone są szczególnie wrażliwe lub szczególnie podatne na zagrożenia elementy wchodzące w skład podstawowych komponentów sieci 5G, centrum operacji i utrzymania, jak również elementy sieci dostępowej 5G wykorzystywane do zastosowań przemysłowych.

13. Na drugim etapie zakresem tego wspólnego przeglądu należy objąć inne strategiczne elementy cyfrowego łańcucha wartości.

Wspólny unijny zestaw instrumentów służących eliminowaniu zagrożeń

14. Prace grupy współpracy powinny prowadzić do wskazania środków odzwierciedlających najlepsze praktyki stosowane na szczeblu krajowym w rodzaju tych, które przewidziano w pkt 4. W oparciu o te krajowe najlepsze praktyki do dnia 31 grudnia 2019 r. należy uzgodnić zestaw odpowiednich, skutecznych i proporcjonalnych środków zarządzania ryzykiem służących minimalizacji zidentyfikowanych zagrożeń dla cyberbezpieczeństwa na szczeblu krajowym i unijnym celem zapewnienia Komisji doradztwa przy opracowywaniu minimalnych wspólnych wymogów mających w jeszcze większym stopniu zagwarantować wysoki poziom cyberbezpieczeństwa sieci 5G w całej Unii.

15. Zestaw ten powinien obejmować:

    a) wykaz rodzajów zagrożeń dla bezpieczeństwa, które mogą mieć wpływ na cyberbezpieczeństwo sieci 5G (np. zagrożenia w łańcuchu dostaw, zagrożenia związane z lukami w oprogramowaniu, zagrożenia w kontroli dostępu, zagrożenia wynikające z ram prawnych i ram polityki, którym dostawcy sprzętu informacyjno-komunikacyjnego mogą podlegać w państwach trzecich); oraz

    b) zbiór możliwych środków ograniczających ryzyko (np. prowadzona przez stronę trzecią certyfikacja sprzętu, oprogramowania lub usług, formalne testy lub weryfikacja zgodności sprzętu i oprogramowania, procesy zapewniające istnienie i egzekwowanie kontroli dostępu, wskazanie produktów, usług lub dostawców uznanych za potencjalnie niebezpiecznych itp.). Środki te powinny uwzględniać każdy rodzaj zagrożenia dla bezpieczeństwa, które zidentyfikowano w jednym państwie członkowskim lub większej liczbie państw członkowskich w wyniku oceny ryzyka.

16. Gdy europejskie systemy certyfikacji cyberbezpieczeństwa dotyczące sieci 5G zostaną już opracowane, państwa członkowskie powinny przyjąć – zgodnie z prawem Unii – krajowe przepisy techniczne przewidujące obowiązkową certyfikację produktów, usług lub systemów informacyjno-komunikacyjnych objętych tymi systemami.

17. Państwa członkowskie wraz z Komisją powinny określić warunki dotyczące zabezpieczenia sieci publicznych przed nieuprawnionym dostępem, którymi należy obwarować zezwolenie ogólne, jak również wymogi w zakresie bezpieczeństwa sieci na potrzeby uzyskania od przedsiębiorstw uczestniczących w postępowaniach o udzielenie praw użytkowania widma w pasmach 5G na mocy dyrektywy 2002/20/WE zobowiązania do ich przestrzegania. W miarę możliwości powinny one znaleźć odzwierciedlenie w środkach stosowanych zgodnie z pkt 4 lit. c).

18. Państwa członkowskie powinny współpracować z Komisją w celu opracowania szczególnych wymogów w zakresie bezpieczeństwa, które mogłyby mieć zastosowanie w kontekście zamówień publicznych związanych z sieciami 5G. Powinny one obejmować m.in. bezwzględny wymóg wdrażania systemów certyfikacji cyberbezpieczeństwa w zamówieniach publicznych tam, gdzie systemy te nie są jeszcze wiążące dla wszystkich dostawców i operatorów.

V. **PRZEGLĄD**

19. Państwa członkowskie powinny współpracować z Komisją w celu przeprowadzenia oceny skutków niniejszego zalecenia do dnia 1 października 2020 r., aby określić odpowiednie dalsze kroki. W ocenie tej należy uwzględnić wyniki skoordynowanej unijnej oceny ryzyka oraz unijny zestaw instrumentów.

Sporządzono w Strasburgu dnia 26 marca 2019 r.

W imieniu Komisji

Julian KING

Członek Komisji