ODPOWIEDZI KOMISJI EUROPEJSKIEJ NA SPRAWOZDANIE SPECJALNE EUROPEJSKIEGO TRYBUNAŁU OBRACHUNKOWEGO: „WPROWADZENIE SIECI 5G W UE: OPÓŹNIENIA WE WDRAŻANIU I NIEROZWIĄZANE KWESTIE ZWIĄZANE Z BEZPIECZEŃSTWEM”

STRESZCZENIE

Uwagi wstępne Komisji:

I. Wprowadzenie sieci 5G w szybki i bezpieczny sposób jest jednym z głównych priorytetów Komisji Europejskiej. Ochrona sieci 5G przed zagrożeniami cybernetycznymi wiąże się z oceną oraz ograniczaniem zagrożeń i różnych rodzajów ryzyka. Te zagrożenia i rodzaje ryzyka zostały zidentyfikowane i ocenione wspólnie przez państwa członkowskie przy wsparciu Komisji oraz ENISA i na tej podstawie określono zestaw kompleksowych środków ograniczania ryzyka. Chociaż w niektórych państwach członkowskich nadal trwają prace, zdecydowana większość państw członkowskich już zaostrzyła lub jest w trakcie zaostrzania wymogów bezpieczeństwa dotyczących sieci 5G, korzystając przy tym z unijnego zestawu narzędzi.

Unijny zestaw narzędzi został uznany za kompleksowe ramy przeciwdziałania ryzyku związanemu z bezpieczeństwem sieci 5G.

Skoordynowane działanie w zakresie cyberbezpieczeństwa sieci 5G na poziomie UE oraz unijny zestaw narzędzi wpisują się w szersze europejskie ramy ochrony sieci łączności elektronicznej i innych infrastruktur krytycznych oraz uzupełniają obowiązujące środki, takie jak Europejski kodeks łączności elektronicznej, ramy prawne w zakresie telekomunikacji, akt o cyberbezpieczeństwie oraz dyrektywa w sprawie bezpieczeństwa sieci i systemów informatycznych (dyrektywa NIS), a także, w stosownych przypadkach, przepisy dotyczące swobodnego przepływu określone w Traktacie i Karcie praw podstawowych UE.

III. W nadchodzących latach technologia 5G będzie odgrywać kluczową rolę w naszej gospodarce cyfrowej i społeczeństwie cyfrowym. Musimy zadbać o cyberbezpieczeństwo sieci 5G i ich odporność na cyberzagrożenie i cyberincydenty, których liczba stale rośnie. Dlatego też Komisja i państwa członkowskie zainicjowały proces koordynacji mający na celu określenie i wdrożenie kompleksowych ram bezpieczeństwa sieci 5G, w formie zestawu narzędzi obejmującego środki ograniczania ryzyka uzgodnione w styczniu 2020 r., aby w skuteczny i skoordynowany sposób przeciwdziałać poważnym zagrożeniom dla sieci 5G, takim jak ataki hakerskie, szpiegostwo i sabotaż. Chociaż w niektórych państwach członkowskich nadal trwają prace, zdecydowana większość państw członkowskich już zaostrzyła lub jest w trakcie zaostrzania wymogów bezpieczeństwa dotyczących sieci 5G, korzystając przy tym z unijnego zestawu narzędzi.

VII. Unijny zestaw narzędzi zapewnia ramy sprzyjające zachowaniu spójności na rynku wewnętrznym, przy jednoczesnym poszanowaniu krajowych kompetencji w zakresie bezpieczeństwa w tej dziedzinie.

Jeżeli chodzi o podejście państw członkowskich do dostawców stwarzających wysokie ryzyko, Komisja uważa, że dokonanie ostatecznej oceny będzie możliwe dopiero wtedy, kiedy dostępnych będzie więcej informacji.

W trakcie wdrażania Komisja współpracuje z państwami członkowskimi w ramach grupy współpracy ds. bezpieczeństwa sieci i informacji na rzecz zapewnienia dostosowania i zbieżności podejść krajowych.

IX. Tiret pierwsze – Komisja przyjmuje zalecenie.

Tiret drugie – Komisja przyjmuje zalecenie.

Tiret trzecie – Komisja przyjmuje zalecenie.

Komisja przeprowadzi ocenę z uwzględnieniem kompetencji krajowych.

WPROWADZENIE

04. Komisja przyznaje, że istnieją różne rodzaje ryzyka w zakresie bezpieczeństwa sieci 5G, zwraca jednak uwagę, że technologia i standardy sieci 5G mogą również przynieść poprawę bezpieczeństwa w porównaniu z sieciami poprzednich generacji.

UWAGI

30. Wprawdzie technologia 4G jest już w stanie obsłużyć szeroką gamę usług, ale technologia 5G powinna stanowić duży przeskok – istotną zmianę w porównaniu z 4G, a zatem głównym wyzwaniem jest przejście z 4G na 5G, czyli wprowadzenie sieci 5G w całej UE. Ryzyko powstania przepaści cyfrowej zawsze istnieje, ale planuje się jego wyeliminowanie, co zostało uznane za jeden z priorytetów politycznych w programie polityki „Droga ku cyfrowej dekadzie" w ramach dążeń do osiągnięcia celu, jakim jest objęcie zasięgiem sieci 5G wszystkich zaludnionych obszarów do 2030 r., i wspieranie w związku z tym państw członkowskich w podejmowaniu działań w tym obszarze, zwłaszcza w odniesieniu do dostępu na obszarach wiejskich.

32. Mimo pewnych niedociągnięć obserwatorium 5G jest wiarygodnym źródłem umożliwiającym monitorowanie wprowadzania sieci 5G w UE i poza nią. Służby Komisji liczą, że nowy wykonawca zapewni bardziej aktualne informacje.

Wspólna odpowiedź Komisji do pkt 48 i 49:

Komisja uważa wybór instrumentu (zalecenie) i podejście oparte na współpracy z państwami członkowskimi, jakie przyjęto w celu określenia ryzyka i środków ograniczania ryzyka w zakresie bezpieczeństwa, za najodpowiedniejszy sposób przeciwdziałania ryzyku w zakresie bezpieczeństwa sieci 5G w szybki, skuteczny i skoordynowany sposób.

Komisja zdecydowała się na wydanie zalecenia i współpracę z państwami członkowskimi w celu określenia ryzyka i środków jego ograniczania z uwagi na złożoność i przekrojowy charakter przedmiotu, który wykracza poza kompetencje krajowe i kompetencje UE, a także istotny aspekt związany z bezpieczeństwem narodowym. Ponadto Komisja wzięła również pod uwagę fakt, że sytuacja w poszczególnych państwach członkowskich jest bardzo zróżnicowana (struktura rynku, zdolności w zakresie cyberbezpieczeństwa, analiza zagrożeń itp.).

Unijny zestaw narzędzi stanowi elastyczny instrument oparty na analizie ryzyka, który pomaga sprostać wyzwaniom w zakresie bezpieczeństwa i który umożliwił terminowe i efektywne rozwiązywanie kwestii związanych z cyberbezpieczeństwem sieci 5G.

W komunikacie „Bezpieczne wprowadzanie sieci 5G w UE – wdrażanie unijnego zestawu narzędzi" ze stycznia 2020 r. Komisja zapowiedziała, że zapewni wsparcie we wdrażaniu środków przewidzianych w zestawie narzędzi, dotyczących wymogów w zakresie bezpieczeństwa, w szczególności w odniesieniu do odpowiednich reguł w ramach europejskich przepisów dotyczących łączności elektronicznej, oraz rozważy wartość dodaną ewentualnych aktów wykonawczych określających szczegółowo techniczne i organizacyjne środki bezpieczeństwa w celu uzupełnienia przepisów krajowych oraz zwiększenia skuteczności i spójności środków bezpieczeństwa nakładanych na operatorów.

Wspólna odpowiedź Komisji do pkt 51 i 52:

W związku z przeglądem zalecenia Komisji, który miał miejsce w grudniu 2020 r., Komisja przeprowadziła wywiady z właściwymi organami wszystkich państw członkowskich. Określiły one skoordynowane europejskie działania w zakresie cyberbezpieczeństwa sieci 5G jako terminowe, efektywne i proporcjonalne. Uznano, że podejście oparte na współpracy między organami krajowymi,

Komisją, ENISA i innymi odpowiednimi zainteresowanymi stronami jest odpowiednie do tego, aby można było rozwiązać tę złożoną kwestię. Umożliwiło ono terminowe określenie wspólnych celów i metod, a jednocześnie pozwoliło państwom członkowskim dostosować środki do ich sytuacji krajowej.

W unijnym zestawie narzędzi i sprawozdaniu z postępu prac opublikowanym przez grupę współpracy ds. bezpieczeństwa sieci i informacji w lipcu 2020 r. zalecono określenie planów wdrażania lub okresów przejściowych dla tych operatorów, którzy obecnie korzystają ze sprzętu dostawców stwarzających wysokie ryzyko lub którzy przed przyjęciem unijnego zestawu narzędzi już zawarli umowy z dostawcami stwarzającymi wysokie ryzyko (np. poprzez uwzględnienie cykli modernizacji sprzętu, w szczególności przejścia z „niesamodzielnych" na „samodzielne" sieci 5G).

55. Komisja przyjmuje do wiadomości uwagi przedstawione przez Europejski Trybunał Obrachunkowy.

Aby dalej wspierać wdrażanie kryteriów, które wchodzą w zakres zestawu narzędzi i są stosowane do oceny dostawców stwarzających wysokie ryzyko, od czasu uzgodnienia unijnego zestawu narzędzi kryteria te były przedmiotem licznych wymian opinii między właściwymi organami krajowymi w ramach grupy współpracy ds. bezpieczeństwa sieci i informacji.

56. W unijnym zestawie narzędzi zaleca się, aby przy ocenie profilu ryzyka dostawców uwzględniać czynniki ryzyka przedstawione w unijnej skoordynowanej ocenie ryzyka, a także informacje dotyczące poszczególnych krajów (np. ocenę zagrożeń przekazaną przez krajowe służby bezpieczeństwa itp.).

61. Jednym z kryteriów zalecanych w unijnym zestawie narzędzi do oceny profilu ryzyka dostawców jest zdolność dostawcy do zapewnienia dostaw. Jak wspomniano w scenariuszu ryzyka dotyczącym „uzależnienia", o którym mowa w unijnej skoordynowanej ocenie ryzyka, na zdolność do zapewnienia dostaw mogą mieć również wpływ ewentualne sankcje handlowe, na które narażony jest konkretny sprzedawca.

Wspólna odpowiedź Komisji do pkt 70 i 73:

Komisja i państwa członkowskie dzielą się szczegółowymi informacjami na temat wdrażania zestawu narzędzi na poziomie krajowym w ramach grupy współpracy ds. bezpieczeństwa sieci i informacji. W odniesieniu do publicznego ujawniania informacji niepublicznych obowiązek ten spoczywa na państwach członkowskich.

Wspólna odpowiedź Komisji do pkt 74–76 oraz ramki 5:

Unijny zestaw narzędzi zapewnia ramy sprzyjające zachowaniu spójności na rynku wewnętrznym, przy jednoczesnym poszanowaniu krajowych kompetencji w zakresie bezpieczeństwa w tej dziedzinie.

Jeżeli chodzi o podejście państw członkowskich do dostawców stwarzających wysokie ryzyko, Komisja uważa, że dokonanie ostatecznej oceny będzie możliwe dopiero wtedy, kiedy dostępnych będzie więcej informacji.

W trakcie wdrażania Komisja współpracuje z państwami członkowskimi w ramach grupy współpracy ds. bezpieczeństwa sieci i informacji na rzecz zapewnienia dostosowania i zbieżności podejść krajowych.

WNIOSKI I ZALECENIA

81. Wprowadzenie sieci 5G w szybki i bezpieczny sposób jest jednym z głównych priorytetów Komisji. Ochrona sieci 5G przed zagrożeniami cybernetycznymi wiąże się z oceną oraz ograniczaniem zagrożeń i różnych rodzajów ryzyka. Te zagrożenia i rodzaje ryzyka zostały zidentyfikowane i ocenione wspólnie przez państwa członkowskie przy wsparciu Komisji oraz ENISA i na tej podstawie określono zestaw kompleksowych środków ograniczania ryzyka. Chociaż

w niektórych państwach członkowskich nadal trwają prace, zdecydowana większość państw członkowskich już zaostrzyła lub jest w trakcie zaostrzania wymogów bezpieczeństwa dotyczących sieci 5G, korzystając przy tym z unijnego zestawu narzędzi.

Unijny zestaw narzędzi zapewnia kompleksowe ramy przeciwdziałania ryzyku związanemu z bezpieczeństwem sieci 5G.

83. 5G stanowi duży przeskok – istotną zmianę w porównaniu z 4G, tak więc głównym wyzwaniem, jakiemu trzeba sprostać, aby uniknąć przepaści cyfrowej, jest przejście z 4G na 5G w całej UE.

Specyfikacje w odniesieniu do 5G obejmują szeroki zakres wskaźników skuteczności działania, w szczególności związanych z przypadkami pionowego wykorzystania. Może to obejmować m.in. wymogi dotyczące niezawodności, szybkość konkretyzacji usługi, elastyczność wdrażania, poziomy bezpieczeństwa.

Zalecenie 1 – Promowanie równomiernego i terminowego wdrażania sieci 5G w UE

a) Komisja przyjmuje zalecenie.

Komisja będzie współpracować z państwami członkowskimi w celu opracowania wspólnej definicji oczekiwanej jakości usług w sieciach 5G. W kontekście cyfrowej dekady i proponowanej decyzji w sprawie programu polityki cyfrowej do 2030 r. Komisja zamierza współpracować z państwami członkowskimi nad wspólnym podejściem do jakości usług 5G w UE, w tym w zakresie porównywalności pomiarów i danych z monitorowania.

Jakość usług obejmuje nie tylko szybkość i opóźnienie, ale cały zakres wskaźników skuteczności działania, w szczególności związanych z przypadkami pionowego wykorzystania.

Komisja zamierza współpracować z państwami członkowskimi w celu określenia takich pomiarów, a także przeprowadzać coroczne przeglądy prac w punktach kontrolnych oraz przekazywać zalecenia w zakresie polityki, środków i działań w celu osiągnięcie pełnego zasięgu sieci 5G do 2030 r.

W ramach programu polityki cyfrowej powstanie solidny model zarządzania za pomocą mechanizmu monitorowania i współpracy, aby zapewnić postępy w realizacji celów programu polityki, w tym wprowadzenia sieci 5G, a państwom członkowskim zalecane będą działania naprawcze w tym zakresie.

b) Komisja przyjmuje zalecenie.

c) Komisja przyjmuje zalecenie.

Zalecenie 2 – Promowanie skoordynowanego podejścia państw członkowskich do bezpieczeństwa sieci 5G

a) Komisja przyjmuje zalecenie.

Komisja wraz z państwami członkowskimi oceni potrzebę dalszych działań lub wsparcia, na przykład w formie wskazówek związanych z niektórymi aspektami unijnego zestawu narzędzi.

b) Komisja przyjmuje zalecenie.

Komisja zajmie się monitorowaniem i sprawozdawczością, współpracując przy tym w pełni z państwami członkowskimi i ENISA.

c) Komisja przyjmuje zalecenie.

Zalecenie 3 – Monitorowanie podejść państw członkowskich do kwestii bezpieczeństwa sieci 5G i ocena wpływu rozbieżności na skuteczne funkcjonowanie jednolitego rynku

a) Komisja przyjmuje zalecenie.

b) Komisja przyjmuje zalecenie.

Komisja przeprowadzi ocenę z uwzględnieniem kompetencji krajowych.

W ramach unijnego zestawu narzędzi do państw członkowskich należy podjęcie decyzji co do dokładnego zakresu odpowiednich ograniczeń lub koniecznych wykluczeń w odniesieniu do kluczowych aktywów określonych w unijnej skoordynowanej ocenie ryzyka jako krytyczne i wrażliwe (np. funkcje sieci szkieletowej, funkcje zarządzania siecią i organizacji sieci czy funkcje sieci dostępowej), aby skutecznie ograniczyć zidentyfikowane ryzyko, z uwzględnieniem także oceny zagrożeń przeprowadzonej przez krajowe służby wywiadowcze. Państwa członkowskie mają prawo do stosowania środków związanych z bezpieczeństwem narodowym, w tym potencjalnych ograniczeń lub wykluczeń dostawców stwarzających wysokie ryzyko.