KOMISJA
EUROPEJSKA

Bruksela, dnia 15.6.2023 r.
C(2023) 4049 final

KOMUNIKAT KOMISJI

Wdrożenie zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G

KOMUNIKAT KOMISJI

Wdrożenie zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G

Bezpieczeństwo sieci 5G jest jednym z głównych priorytetów Komisji Europejskiej. Sieci te są kluczową infrastrukturą, która stanowi podstawę szerokiego zakresu usług niezbędnych do funkcjonowania rynku wewnętrznego oraz utrzymania i funkcjonowania podstawowych funkcji społecznych i gospodarczych. Aby chronić sieci 5G, państwa członkowskie wspólnie zidentyfikowały i oceniły[1] zagrożenia i ryzyko związane z cyberbezpieczeństwem, przy wsparciu Komisji i Agencji UE ds. Cyberbezpieczeństwa (ENISA), i na tej podstawie określono zestaw kompleksowych środków mających na celu ograniczenie tego ryzyka, w formie unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G[2] przyjętego w 2020 r. przez grupę współpracy NIS i zatwierdzonego przez Radę Europejską i Komisję.

W marcu 2022 r. w Wersalu szefowie państw lub rządów postanowili wziąć na siebie większą odpowiedzialność za nasze bezpieczeństwo i przedsięwziąć dalsze zdecydowane kroki w kierunku budowania naszej europejskiej suwerenności i zmniejszenia naszych zależności, w tym poprzez wzmocnienie naszej cyberodporności i ochronę infrastruktury, zwłaszcza infrastruktury krytycznej[3]. Wdrożenie unijnego zestawu narzędzi jest podstawowym elementem strategii w zakresie unii bezpieczeństwa[4] i wspiera szersze ramy europejskiej polityki strategicznej autonomii i zwiększonej odporności, a także szczególne ramy ochrony sieci łączności elektronicznej i innych infrastruktur krytycznych[5], sprzyjając zwłaszcza wdrożeniu art. 40 Europejskiego kodeksu łączności elektronicznej, zgodnie z którym „operatorzy podejmują właściwe i proporcjonalne środki techniczne i organizacyjne w razie wystąpienia zagrożenia dla bezpieczeństwa sieci lub usług”[6].

W ramach unijnego zestawu narzędzi, biorąc pod uwagę ostateczny cel, jakim jest zapewnienie bezpieczeństwa i odporności sieci 5G oraz ich zrównoważonego charakteru, państwa członkowskie zgodziły się co do konieczności oceny profilu ryzyka poszczególnych dostawców i w konsekwencji stosowania odpowiednich ograniczeń wobec dostawców uznanych za stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń, aby skutecznie łagodzić ryzyko w odniesieniu do kluczowych aktywów, jak wskazano w zestawie narzędzi.

Zgodnie z unijną skoordynowaną oceną ryzyka profil ryzyka poszczególnych dostawców można ocenić na podstawie kilku czynników. Prawdopodobieństwo, że dostawca zostanie poddany ingerencjom ze strony państwa niebędącego członkiem UE, jest przedstawione jako jeden z kluczowych aspektów oceny zagrożeń o charakterze nietechnicznym związanych z sieciami 5G i może być spotęgowane

[1] Sprawozdanie w sprawie unijnej skoordynowanej oceny ryzyka związanego z sieciami 5G, grupa współpracy NIS.

[2] Unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, grupa współpracy NIS, 29 stycznia 2020 r. Unijny zestaw narzędzi został przyjęty przez krajowe organy ds. cyberbezpieczeństwa państw członkowskich i zatwierdzony przez Radę Europejską i Komisję.

[3] Nieformalne posiedzenie szefów państw lub rządów, Deklaracja wersalska, 10–11 marca 2022 r.

[4] Strategia UE w zakresie unii bezpieczeństwa, COM(2020) 605 final.

[5] Unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, grupa współpracy NIS, 29 stycznia 2020 r. Unijny zestaw narzędzi został przyjęty przez krajowe organy ds. cyberbezpieczeństwa państw członkowskich i zatwierdzony przez Radę Europejską i Komisję.

[6] Przepis ten zostaje zastąpiony przez art. 21 ust. 1 dyrektywy NIS 2 od października 2024 r.

przez szereg czynników, w szczególności powiązanie między dostawcą a rządem danego państwa trzeciego, przepisy państwa trzeciego oraz charakterystykę struktury własnościowej przedsiębiorstwa dostawcy.

Komisja przyjmuje do wiadomości i z zadowoleniem wita przyjęcie przez grupę współpracy NIS drugiego sprawozdania z postępów we wdrażaniu unijnego zestawu narzędzi.

W świetle tego sprawozdania Komisja jest głęboko zaniepokojona zagrożeniami, jakie niektórzy dostawcy urządzeń łączności ruchomej stwarzają dla bezpieczeństwa Unii, co znajduje również odzwierciedlenie w decyzjach podejmowanych przez niektóre państwa członkowskie. W sprawozdaniu grupy współpracy NIS podkreślono „wyraźne ryzyko utrzymywania się zależności od dostawców wysokiego ryzyka na rynku wewnętrznym, co może mieć potencjalnie poważny negatywny wpływ na bezpieczeństwo użytkowników i przedsiębiorstw w całej UE oraz na infrastrukturę krytyczną UE".

Jak wspomniano w sprawozdaniu z postępu prac przedstawionym przez grupę współpracy NIS oraz we wcześniejszym sprawozdaniu Europejskiego Trybunału Obrachunkowego[7], oczywiste jest, że dostawcy sieci 5G wykazują wyraźne różnice w zakresie swojej charakterystyki, w szczególności jeśli chodzi o prawdopodobieństwo, że wpływ na nich będą miały określone państwa trzecie, w których obowiązują przepisy dotyczące bezpieczeństwa i ład korporacyjny stanowiące potencjalne zagrożenie dla bezpieczeństwa Unii. Jak wskazano również w sprawozdaniu NIS, Huawei i ZTE podlegają publicznym decyzjom i doradztwu w niektórych państwach członkowskich[8] w oparciu o obawy dotyczące bezpieczeństwa narodowego, w tym ocenom dokonywanym przez służby wywiadowcze tych państw członkowskich. W innych państwach członkowskich decyzje o ograniczeniu lub wykluczeniu niektórych dostawców z sieci 5G tych państw zostały podjęte w sposób poufny na podstawie ich oceny. Ustalenia tych państw członkowskich są podobne do analizy przeprowadzonej przez właściwe organy niektórych państw trzecich[9].

Ze względu na to wysokie ryzyko oraz na podstawie oceny kryteriów określonych w zestawie narzędzi służących identyfikacji „dostawców wysokiego ryzyka" Komisja uważa, że decyzje przyjęte przez państwa członkowskie w celu ograniczenia lub wykluczenia Huawei i ZTE są uzasadnione i zgodne z zestawem narzędzi na potrzeby sieci 5G. Bez uszczerbku dla kompetencji państw członkowskich w zakresie bezpieczeństwa narodowego Komisja zastosowała również kryteria zestawu narzędzi w celu oceny potrzeb i słabych punktów jej własnych systemów komunikacji instytucjonalnej oraz podobnych systemów innych instytucji, organów i agencji europejskich, a także wdrażania unijnych programów finansowania w świetle ogólnych celów polityki Unii.

W tym kontekście, zgodnie ze stosowaniem przez niektóre państwa członkowskie zestawu narzędzi na potrzeby sieci 5G, Komisja uważa, że Huawei i ZTE stwarzają w rzeczywistości znacznie wyższe ryzyko niż inni dostawcy 5G. Ta ocena przeprowadzona przez Komisję w świetle kryteriów zestawu narzędzi opiera się na dostępnych informacjach dotyczących:

[7] Sprawozdanie specjalne: bezpieczeństwo sieci 5G (europa.eu)
[8] Drugie sprawozdanie z postępów we wdrażaniu unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, 15 czerwca 2023 r.
[9] Huawei Designated Vendor Direction (publishing.service.gov.uk)

1) krajowych ocen przeprowadzonych przez państwa członkowskie UE i państwa trzecie w odniesieniu do ryzyka stwarzanego przez dostawców;
2) odpowiednich aktów prawnych i regulacyjnych państw członkowskich UE i państw trzecich związanych ze środkami przeciwdziałającymi ryzyku ze strony dostawców;
3) stosownych sprawozdań Europejskiego Trybunału Obrachunkowego;
4) prawdopodobieństwa ingerencji rządu państwa niebędącego członkiem UE bez odpowiednich ograniczeń prawnych lub sądowych;
5) poziomu szkodliwych działań mających wpływ na cyberbezpieczeństwo instytucji UE;
6) ryzyka potencjalnych zakłóceń w łańcuchu dostaw sprzętu 5G w obecnym kontekście geopolitycznym;
7) znaczącej obecności tych dostawców w unijnych sieciach 5G.

Dziesięć państw członkowskich wykorzystało swoje uprawnienia do nakładania obowiązków w celu ograniczenia lub wykluczenia dostawców wysokiego ryzyka ze swoich sieci 5G. Ze względu na wzajemne powiązania sieci Komisja wzywa państwa członkowskie, które nie wdrożyły jeszcze zestawu narzędzi, do pilnego przyjęcia odpowiednich środków, zgodnie z zaleceniami zawartymi w unijnym zestawie narzędzi, w celu skutecznego i szybkiego przeciwdziałania zagrożeniom, z uwzględnieniem tego, co inne państwa członkowskie już zrobiły zgodnie z zestawem narzędzi, a także z niniejszą oceną.

Państwa te powinny również podjąć działania, biorąc pod uwagę ryzyko związane z potencjalnymi zakłóceniami mającymi wpływ na łańcuch dostaw urządzeń na potrzeby sieci 5G, w obecnym kontekście geopolitycznym, oraz znaczącą obecność tych dostawców w unijnych sieciach 5G, co prowadzi do poważnych słabości i zależności dla Unii jako całości.

Jeśli chodzi o wdrażanie tych środków, Komisja wzywa państwa członkowskie, by w jak największym stopniu uwzględniły również zalecenia zawarte w sprawozdaniu NIS, w szczególności dotyczące zakresu ograniczeń, które powinny obejmować krytyczne i wysoce wrażliwe aktywa określone w skoordynowanej unijnej ocenie ryzyka, w tym sieci dostępu radiowego, oraz dotyczące stosowania okresów przejściowych, które należy określić w celu zapewnienia usunięcia istniejącego sprzętu w jak najkrótszym czasie,

Komisja może podjąć dalsze inicjatywy w celu wsparcia kompleksowego wdrożenia zestawu narzędzi na potrzeby sieci 5G.

Ponadto, jak wspomniano powyżej, Komisja jest również zaniepokojona bezpieczeństwem i poufnością komunikacji instytucjonalnej Komisji oraz innych instytucji, organów i agencji UE. W ramach swojej instytucjonalnej polityki cyberbezpieczeństwa oraz w ramach stosowania zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G Komisja wprowadzi środki w celu uniknięcia narażenia swojej komunikacji instytucjonalnej wobec sieci mobilnych wykorzystujących Huawei i ZTE jako dostawców. Środki te będą obejmować niezamawianie nowych usług łączności, które opierają się na sprzęcie od tych dostawców, przy zastosowaniu odpowiednich warunków bezpieczeństwa. Komisja będzie współpracować z państwami członkowskimi i operatorami telekomunikacyjnymi, aby zapewnić stopniowe wycofywanie tych dostawców z istniejących usług łączności w siedzibach Komisji.

Dotyczy to wszystkich siedzib Komisji, w tym jej siedzib głównych, przedstawicielstw i biur we wszystkich państwach członkowskich[10]. Komisja będzie zachęcać inne instytucje, organy i agencje UE do podejmowania podobnych działań. Komisja poczyni niezbędne kroki w celu szybkiego wdrożenia tych decyzji.

Komisja zamierza również uwzględnić tę decyzję, zgodnie ze swoimi kompetencjami wynikającymi z odpowiednich zasad zarządzania, we wszystkich odpowiednich unijnych programach i instrumentach finansowania.

ODPIS UWIERZYTELNIONY
W imieniu Sekretarza Generalnego

Martine DEPREZ
Dyrektor
Proces Decyzyjny i Kolegialność
KOMISJA EUROPEJSKA

[10] W tym agencji wykonawczych Komisji.