Komisja Europejska

UNIJNY ZESTAW NARZĘDZI NA POTRZEBY CYBERBEZPIECZEŃSTWA SIECI 5G

Zestaw solidnych i kompleksowych środków do celów skoordynowanego unijnego podejścia do bezpieczeństwa sieci 5G

Styczeń 2020
#Cybersecurity

5G: nowa technologia

Podczas gdy sieć 3G przyniosła mobilny internet, a sieć 4G umożliwiła łączność szerokopasmową, oczekuje się, że sieć 5G ma stać się infrastrukturą łączności, która utoruje drogę dla nowych produktów i usług oraz wpłynie na wszystkie grupy społeczeństwa. Korzyści z nowej technologii są następujące:

E-ZDROWIE

- Zdalne monitorowanie zdrowia, rejestry pacjentów i inteligentna diagnostyka
- Wykorzystywanie robotów jako pomocy dla chirurgów i do poprawy wyników medycznych.

INTELIGENTNE SIECI ENERGETYCZNE

- Wysoko wydajne linie energetyczne oraz mniejsza liczba przerw w dostawie prądu na mniejszą skalę
- Łatwiejsza budowa sieci, mająca mniejszy wpływ na środowisko

FABRYKI JUTRA

- Lepsza kontrola procesów wewnętrznych, w których istotnym czynnikiem jest czas
- Zdalne sterowanie urządzeniami magazynowymi

MEDIA I ROZRYWKA

- Lepsze doznania wizualne, np. rzeczywistość wirtualna
- Zastosowania ultraszybkich łączy szerokopasmowych, takie jak streaming wideo

MOBILNOŚĆ

- Wprowadzenie opartej na sieci i zautomatyzowanej mobilności celem zmniejszenia liczby wypadków do zera
- Umożliwienie konektywności we wszystkich rodzajach transportu

Europa jest jednym z najbardziej zaawansowanych na świecie regionów, jeśli chodzi o komercyjne uruchomienie usług 5G, przy czym inwestycje związane z sieciami 5G pochłonęły 1 mld euro, w tym 300 mln euro pochodzących ze środków unijnych. Oczekuje się, że do końca bieżącego roku pierwsze usługi 5G będą dostępne w 138 europejskich miastach.

Cyberbezpieczeństwo sieci 5G: konieczny warunek wstępny

Sieci 5G stanowią przyszły trzon naszych coraz bardziej ucyfrowionych gospodarek i społeczeństw. Dotyczy to miliardów połączonych przedmiotów i systemów, także tych stosowanych w kluczowych sektorach, takich jak energetyka, transport, bankowość i opieka zdrowotna, a także w systemach kontroli przemysłowej, które przetwarzają wrażliwe informacje oraz wspierają systemy bezpieczeństwa. Kluczowe znaczenie ma zatem zapewnienie cyberbezpieczeństwa i odporności sieci 5G.

Jednocześnie ze względu na mniej scentralizowaną architekturę, inteligentną moc obliczeniową w architekturze rozproszonej, konieczność zapewnienia większej liczby anten i większą zależność od oprogramowania sieci 5G są bardziej podatne na ataki.

Kalendarium

12 marca 2019 r.
Sprawozdanie Parlamentu Europejskiego.

22 marca 2019 r.
Konkluzje Rady Europejskiej.

26 marca 2019 r.
Komisja opublikowała zalecenie, aby państwa członkowskie podjęły konkretne działania w celu oceny zagrożeń dla cyberbezpieczeństwa w sieciach 5G oraz wzmocnienia środków zmniejszających ryzyko.

9 października 2019 r.
Państwa członkowskie zakończyły unijną skoordynowaną ocenę ryzyka w zakresie bezpieczeństwa sieci 5G.

21 listopada 2019 r.
ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa – opublikowała obszerne sprawozdanie na temat zagrożeń związanych z sieciami 5G.

29 stycznia 2020 r.
Publikacja przez państwa członkowskie zestawu narzędzi ograniczających ryzyko. Komunikat Komisji w sprawie wdrażania unijnego zestawu narzędzi.

30 kwietnia 2020 r.
Komisja wzywa państwa członkowskie do podjęcia konkretnych i wymiernych działań w celu wprowadzenia zestawu kluczowych środków.

30 czerwca 2020 r.
Komisja wzywa państwa członkowskie do przygotowania sprawozdania na temat wdrażania przez nie kluczowych środków

Do października 2020 r.
Przegląd realizacji zalecenia Komisji przyjętego dnia 26 marca 2019 r.

Unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G

W oparciu o skoordynowaną unijną ocenę ryzyka związanego z bezpieczeństwem sieci 5G zestaw narzędzi określa szereg środków bezpieczeństwa, które umożliwiają skuteczne ograniczenie ryzyka i zapewniają bezpieczne wdrożenie sieci 5G w całej Europie. Określono w nim szczegółowe **plany ograniczenia ryzyka** dla każdego ze zidentyfikowanych zagrożeń i zalecono **kluczowe środki strategiczne i techniczne**, które powinny zostać zastosowane przez wszystkie państwa członkowskie lub Komisję.

ŚRODKI STRATEGICZNE

- Uprawnienia regulacyjne
- Dostawcy będący osobami trzecimi
- Dywersyfikacja dostawców
- Zrównoważony charakter i różnorodność łańcucha dostaw i łańcucha wartości 5G

ŚRODKI TECHNICZNE

- Bezpieczeństwo sieci – środki podstawowe
- Bezpieczeństwo sieci – środki szczególne dotyczące 5G
- Wymogi związane z procesami i wyposażeniem dostawców
- Odporność i ciągłość działania

Plany ograniczania ryzyka

W odniesieniu do każdego z dziewięciu obszarów ryzyka określonych w sprawozdaniu z unijnej skoordynowanej oceny ryzyka zestaw narzędzi określa i przedstawia plany ograniczania ryzyka. Polegają one na ewentualnym połączeniu środków w oparciu o ich skuteczność.

Konkluzje dotyczące unijnego zestawu narzędzi: kluczowe środki

Państwa członkowskie: powinny dysponować środkami i uprawnieniami w zakresie ograniczania ryzyka. W szczególności powinny uwzględniać następujące aspekty:

- zaostrzenie **wymogów w zakresie bezpieczeństwa** wobec **operatorów sieci komórkowych**;
- ocena profili ryzyka dostawców; zastosowanie odpowiednich ograniczeń dla dostawców uznanych za stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń w odniesieniu do kluczowych zasobów;
- zapewnienie, aby każdy operator posiadał odpowiednią **strategię obejmującą wielu dostawców** w celu **uniknięcia** lub **ograniczenia wszelkiej poważnej zależności** od jednego dostawcy oraz uniknięcia uzależnienia od dostawców uznanych za stwarzających wysokie ryzyko;

Komisja Europejska wraz z państwami członkowskimi powinny podjąć działania w celu:

- utrzymywania **zróżnicowanego** i **zrównoważonego łańcucha dostaw 5G** w celu uniknięcia długotrwałej zależności, w tym poprzez:
  - pełne wykorzystanie istniejących narzędzi i instrumentów UE (kontrola bezpośrednich inwestycji zagranicznych, instrumenty ochrony handlu, konkurencja);
  - dalsze zwiększanie zdolności UE w zakresie technologii 5G i następnych poprzez wykorzystanie odpowiednich programów i środków finansowych UE;
- ułatwienie koordynacji między państwami członkowskimi w zakresie **normalizacji**, tak aby osiągnąć określone cele w zakresie bezpieczeństwa, oraz opracowanie odpowiednich ogólnounijnych **systemów certyfikacji**.

Ponadto należy rozszerzyć kompetencje **grupy roboczej w ramach grupy współpracy NIS** na wsparcie, monitorowanie i ocenę wdrożenia zestawu narzędzi.

Print ISBN 978-92-76-15584-3 doi:10.2775/73052 NA-03-20-052-PL-C
PDF ISBN 978-92-76-15572-0 doi:10.2775/507907 NA-03-20-052-PL-N