Cyberdefence 24

aut. Andrzej Kozłowski 13.05.2020

SIEĆ 5G KRĘGOSŁUPEM WSPÓŁCZESNEGO PAŃSTWA. JAK JĄ ZABEZPIECZYĆ?

„Toolbox Komisji Europejskiej będzie fundamentem budowy bezpiecznego ekosystemu cyberbezpieczeństwa sieci 5G" to jeden ze wniosków debaty zatytułowanej: „Czy sieć 5G w UE będzie bezpieczna. Państwa członkowskie przed ważną decyzją?", w której wzięli udział Izabela Albrycht - prezes Instytutu Kościuszki, Dr Jacek Falkiewicz – Ericsson Polska oraz Michał Kanownik - Prezes Zarządu, ZIPSEE „Cyfrowa Polska".

5G to nie jest tylko kolejna ewolucja czy generacja sieci, to rewolucja. Będzie ona miała zastosowanie w krytycznych systemach i sektorach państwa oraz gospodarki – rozpoczęła dyskusję Izabela Albrycht. Logistyka, medycyna, rolnictwo to tylko niektóre z sektorów, które zostaną zrewolucjonizowane przez sieć 5G. Czeka nas rozwój przemysłu 4.0, autonomicznego transportu i smart home – zapowiedziała ekspertka. Nie można jednak zapominać o zastosowaniu sieci 5G dla wojska. To sprawia, że 5G ma znaczenie geopolityczne. Może zadecydować o potędze danego regionu – dodała prezes Instytut Kościuszki.

Albrycht dodała, że jednym z kryteriów siły we współczesnym świecie stał się arsenał technologiczny, którym dysponują kraje, ale również, ten który mają zdolność wyprodukować. Zaawansowane sieci 5G to narzędzia projekcji siły, obecnie soft power, a w przyszłości także hard power. Sieć 5G stworzy fundamenty pod rozwój, z którego będzie można czerpać korzyści - co będzie kluczowe dla gospodarek państw. Geopolityczne i geoekonomiczne znaczenie sieci nowej generacji, powoduje, że niezwykle istotne jest zapewnienie ochrony zarówno w warstwie software ja i hardware. Powoduje to również, że konieczne jest wsparcie dla europejskich producentów, ponieważ sieć 5G będzie kluczem dla osiągnięcia strategicznej cyfrowej autonomii przez Unię Europejską, co umożliwi zagwarantowanie długoterminowego rozwoju gospodarczego – dodała Albrycht.

Unia Europejska dostrzega ten problem i w jednym ze swoich dokumentów stwierdziła, że podmioty, które kontrolują cyfrowe technologie będą miały większy wpływ na gospodarkę i politykę. Mimo wielu autów, które posiada UE istnieje realne zagrożenie dla dobrobytu gospodarczego wspólnoty. Tym samym otwiera się cała gama wyzwań związanych z rywalizacją. Komisja Europejska zdaje się dostrzegać ten problem i naciska na suwerenność cyfrową oraz osiągnięcie pozycji lidera w wyścigu technologicznym. Budowa sieci 5G będzie testem i papierkiem lakmusowym jak idea suwerenności cyfrowej zmaterializuje się w działaniach UE – podkreśliła Albrycht.

W dalszej części prezentacji prezes Instytutu Kościuszki przedstawiła zagrożenia dla sieci 5G mówiąc np. o potencjale zablokowania sieci 5G, problemach związanych z aktualizacją oprogramowania oraz tylnymi furtkami, które wynikają z niskiego poziomu bezpieczeństwa hardware'u. Problem bezpieczeństwa sieci 5G został nie tylko poruszony na agendzie Unii Europejskiej, ale również NATO, które zwróciło uwagę na potrzebę zagwarantowania ochrony infrastruktury krytycznej. Sieć 5G będzie miało kluczowe znaczenie dla sił wojskowych – dodała Albrycht.

Michał Kanownik Prezes Zarządu, ZIPSEE podkreślił, że toolbox KE jest wynikiem analizy ryzyka dokonanej i przedstawionej przez państwa członkowskie. „Mówiąc o toolboxsie należy odpowiedzieć na dwa kluczowe pytania: co toolbox rekomenduje dla państw członkowskich oraz dlaczego został stworzony" – podkreślał.

Powodem utworzenia tego rozwiązania, jest fakt, że sieć 5G musi być odpowiednio zabezpieczona, żeby podmioty miały pewność i zaufanie, że są bezpieczne. Przechodząc do szczegółów, KE namawia państwa członkowskie do wzmocnienia bezpieczeństwa operatorów sieci mobilnych poprzez wprowadzenie m.in. monitoringu czy ograniczenie outsourcingu w ramach sieci mobilnych. W drugiej kolejności KE podkreśla również ocenę profilu ryzyka sieci 5G i każde państwo członkowskie powinno taką ocenę przeprowadzić, potem ją wdrożyć oraz przygotować wynikające z niej odpowiednie rozwiązania prawne. To również etap, w którym państwa powinny wdrożyć odpowiednie rozwiązania ograniczające udział dostawców wysokiego ryzyka, w szczególnie w kluczowych zasobach sieci – powiedział prezes Zarządu ZIPSEE.

Kanownik podkreślił, że toolbox wymaga, aby każdy operator telekomunikacyjny posiadał strategię obejmującą dywersyfikację elementów sieci 5G. Pozwoli to na ograniczenie ryzyka uzależnienia od jednego wiodącego dostawcy, w szczególności, jeśli został on zakwalifikowany jako podmiot wysokiego ryzyka. Nie chodzi tylko o wyeliminowanie uzależnienia, ale też, żeby była pewna równowaga na rynku dostawców usług telekomunikacyjnych – podkreślił ekspert. Wskazał również na role Komisji Europejskiej, która stara się podjąć działania ukierunkowane na zabezpieczenie ochrony łańcucha dostaw zdając sobie sprawę z tego, że od jego utrzymania może zależeć bezpieczeństwo całej gospodarki Unii Europejskiej.

W tym zakresie, jak podkreślił ekspert, Komisja Europejska zamierza stosować trzy rozwiązania:

- Wprowadzenie narzędzi kontroli inwestycji zagranicznych do ochrony handlu, aby unikać uzależnienia od jednego dostawcy;
- Zwiększenie inwestycji w rodzime technologie 5G;
- Wprowadzenia systemu certyfikacji tak aby domknąć proces zamykania drzwi dla dostawców, którzy mogą stawiać zagrożenie;

Jest to ogólnounijny, kompleksowy system, który musi zostać wdrożony przez poszczególne kraje członkowskie. W Polsce ciałem odpowiedzialnym za ten proces jest Ministerstwo Cyfryzacji, które przygotowało projekt rozporządzenia w sprawie minimalnych środków technicznych i organizacyjnych dla przedsiębiorców telekomunikacyjnych. Dokument ten nie jest jeszcze gotowy i nie wiadomo czy będzie spełniał rekomendacje KE – dodał Kanownik.

Podsumowując, ekspert powiedział, że toolbox wynika ze słusznej idei Komisji Europejskiej, która dąży do stworzenia skoordynowanego systemu bezpieczeństwa na poziomie UE. Konieczna jest minimalizacja ryzyka oraz występowania dziur, które mogą naruszyć systemy bezpieczeństwa. Dlatego tak ważne jest, aby toolbox był efektywnie wdrożony. Będzie to fundament budowy bezpiecznego ekosystemu cyberbezpieczeństwa sieci 5G – zakończył ekspert.

Jako trzeci, w debacie zabrał głos dr Jacek Falkiewicz – ekspert Ericsson Polska, który podkreślił, że Ericsson jako pierwszy uruchomił komercyjne sieci 5G na 4 kontynentach. „Obecnie mamy 90 publicznie ogłoszonych kontraktów, z czego 33 to komercyjne sieci" – stwierdził. Wczoraj uruchomiliśmy sieć 5G z firmą Polkomtel – podkreślił Falkiewicz. Przedstawił również prognozy dotyczące przewidywanej liczby użytkowników sieci nowej generacji, których na koniec 2019 roku było na świecie 13 milionów. Jak podkreślił ekspert, przewiduje się, że w 2025 roku będzie ich już 2,8 miliarda osób.

Ekspert Ericsson Polska w dalszej części wypowiedzi zarysował rozwój sieci 5G w Polsce, w którym to przewiduje aktywny udział szwedzkiej firmy. Po raz pierwszy zademonstrowano działanie sieci 5G w listopadzie 2017 roku w Krakowie podczas RadioTechDay. Kolejne lata to m.in. testy w Zakopanem czy uruchomienie sieci testowej w Warszawie w 2019 roku. W 2020 roku odbyły się testy Ericsson Sharing w którym doszło do dzielenia się widmem. Falkiewicz podkreślił, że szwedzka firma współpracuje z wszystkimi operatorami sieci 5G. Duże znaczenie dla rozwoju ma również projekt badawczy realizowany na kampusie Politechniki Łódzkiej od 2018 roku. Zapowiedział również otwarcie Centrum Kompetencyjnego w tym miejscu w maju br. Podkreślił tym samym, że ze z technologicznego punktu widzenia Ericsson jest gotowy do wdrożenia sieci nowej generacji.

Jego zdaniem bezpieczeństwo 5G wymaga holistycznego podejścia zamiast skupiania się na pojedynczych elementach. „Musimy te wyzwania rozpatrywać łącznie, korzystając z infrastruktury krytycznej. Ericsson opiera swoją filozofię na czymś co nazywa się „stosem zaufania", w którym bierze się pod uwagę proces standaryzacji, produkcji elementów oprogramowania, budowy sieci i jej eksploatacji" – podkreślił ekspert.

Standaryzacja polega na stworzeniu odpowiednich zasad ochrony sieci oraz bezpieczeństwa produktów. Następnie te standardy są przekładane na procesy oraz oprogramowanie. W następnym etapie następuje proces planowania i budowy sieci z uwzględnieniem standardów bezpieczeństwa. Wykorzystywanie sieci również musi być robione z myślą o bezpieczeństwie – podkreślił przedstawiciel Ericssona.

Skrytykował również pomysł oparcia bezpieczeństwa jedynie o certyfikację. Podkreślił, że praktycznie co dwa miesiące wgrywana jest nowa aktualizacja oprogramowania. Nie oznacza to jednak, że konieczne jest robienie certyfikacji tego samego urządzenia co 2 miesiące. Dlatego Ericsson stosuje zasadę security by design a nie security by test. Musi istnieć zaufanie do produktu, co jest najważniejsze, jeżeli chodzi o bezpieczeństwo sieci 5G – zakończył.

Debata „Czy sieć 5G w UE będzie bezpieczna. Państwa członkowskie przed ważną decyzją? Odbywała się we 12 maja 2020 roku.