Opinia Polskiej Izby Informatyki i Telekomunikacji (PIIT)
w sprawie Rekomendacji Komisji Europejskiej dot. Cyberbezpieczeństwa w sieci 5G Strasbourg, 26.3.2019 C(2019) 2335 final

Jesteśmy gorącymi zwolennikami rozwoju sieci 5G widząc w nich narzędzie do zwielokrotnienia kilkadziesiąt razy przepustowości sieci i konieczny warunek dalszego rozwoju tzw. Przemysłu 4.0, a w szerszym aspekcie - demokratycznego społeczeństwa opartego o nowoczesne technologie.
W związku z przygotowywaną przez Rząd RP, jako kraj członkowski Unii Europejskiej, analizą ryzyk, zgodnie z procedurami przyjętymi przez Komisję Europejską pragniemy zwrócić uwagę Polskiego Rządu na najistotniejsze zagrożenia związane z cyberbezpieczeństwem w budowie sieci 5G w Polsce.

I. Zagrożenia natury ogólnej

1. Opowiadamy się za zgodną współpracą z wszystkimi krajami na świecie - w tym z ChRL, ponieważ pracujemy dla firm ICT i nie zajmujemy się polityką. Jako Polacy wspieramy jednak przynależność RP do wspólnoty transatlantyckiej - NATO - jako gwaranta naszego bezpieczeństwa i ducha tego przymierza. Nie możemy bowiem pozostawać obojętni na liczne sygnały dot. zagrożeń związanych z budowa sieci 5G zwłaszcza przez dostawców dalekowschodnich.

Komisja Europejska w rekomendacjach zwraca uwagę, że oprócz zagrożeń technologicznych państwa członkowskie powinny zwrócić uwagę także na inne zagrożenia (pkt. 20 rekomendacji).

II. Ryzyka związane wytwarzaniem oprogramowania

Nasze zaniepokojenie budzą następujące ryzyka sygnalizowane przez poważne instytucje publiczne związane z potencjalnym udziałem chińskich firm w budowie sieci 5G:
1.Ryzyka związane z niskim poziomem wytwarzania oprogramowania.
2. W naszej ocenie, ani Polska ani UE nie dysponuje obecnie potencjałem organizacyjnym czy eksperckim, który pozwoliłby w sposób ciągły i przewidywalny badać oprogramowanie nawet z pełnym kodem źródłowym w skali systemów operacyjnych dostarczane przez strony trzecie.
3. Co więcej, oprogramowanie w sieciach telekomunikacyjnych jest złożone z dużej ilości (dziesiątek, czasami setek) modułów, które są często aktualizowane. Certyfikacja jednej konkretnej jego wersji jest nie tylko czasochłonna, ale również ograniczona tylko do tej konkretnej, certyfikowanej wersji. Z uwagi na fakt, że w sieciach operatorskich wydzielona sieć przeznaczona do zarządzania umożliwia zwykle dostęp autoryzowanym użytkownikom zdalnie, kolejnym ryzykiem mogłoby być dogrywanie już po okresie certyfikacji dodatkowych modułów.
Samo odłączenie możliwości zarządzania zdalnego również nie rozwiązuje problemu, ponieważ jest niemożliwością nawet dla wysokiej klasy specjalisty bezpieczeństwa czy też inżyniera sieciowego zbadania poprawki systemowej w wersji binarnej, lub porównanie kodu źródłowego z jego binarną wersją.
Oznacza to, że z uwagi na historycznie doświadczenia, procesy certyfikacyjne urządzeń i oprogramowania przestają mieć znaczenie jako gwarancja bezpieczeństwa.

III. Niektóre ryzyka technologiczne związane z wdrażaniem prawie każdej nowej technologii

Każda nowa technologia rodzi pewne ryzyka. Technologia 5G pozostaje w ścisłym związku z rozwojem sieci i współczesnych systemów IT, co przejawia się w nowych zagrożeniach, koniecznych do uwzględnienia - na przykład:

1. W związku z rozwojem internetu rzeczy - IoT & M2M - praktycznie brak wbudowanych mechanizmów bezpieczeństwa i autocertyfikacji rozwiązań IoT. Obecna tendencja w badaniu

tych systemów pozwala założyć, że nie da się efektywnie zabezpieczyć każdego z nich, a zatem jeszcze większy nacisk kładziony jest na bezpieczeństwo infrastruktury tak, aby zapewniała segmentację tych rozwiązań od siebie. Wzrasta zagrożenie atakami horyzontalnymi pomiędzy takimi urządzeniami.

2. Wraz z wszechobecną wirtualizacją, kolejnym poważnym wyzwaniem bezpieczeństwa staje się konwergencja wielu technologii - bez stabilnej, bezpiecznej platformy, wydaje się niemożliwe zabezpieczenie całości rozwiązania (czyli np. sieci 5G).
3. Wymóg na minimalne opóźnienia sygnału (w sieciach 5G) uniemożliwia w praktyce wbudowanie silnych mechanizmów ochronnych jak w tradycyjnych sieciach a może powodować fałszywe poczucie bezpieczeństwa przez szyfrowanie w warstwie użytkownika - bez możliwości inspekcji przez operatora, lub uprawnione służby czy transmisja faktycznie zawiera tylko i wyłącznie dane nadawane i odbierane przez uprawnionych członków dyskusji/transmisji.

Te rodzaje zagrożeń może być jednak skutecznie niwelowane w ramach współpracy pomiędzy państwami wewnątrz UE w oparciu o Cybersecurity Act, procesy certyfikacji i współpracę z ENISA.

Te ryzyka minimalizuje też zaufanie do sprawdzonych dostawców technologii w tym zrzeszonych w PIIT.

Wnioski

W związku z powyższymi ryzykami powinny zostać przyjęte przez rząd i parlament adekwatne do nich środki zabezpieczające, zgodnie z postulatem Komisji Europejskiej: http://europa.eu/rapid/press-release_IP-19-1832_pl.htm w którym czytamy m.in., że:

„Każde państwo członkowskie powinno do końca czerwca 2019 r. przeprowadzić krajową ocenę ryzyka związanego z infrastrukturą sieci 5G. Na tej podstawie państwa członkowskie powinny zaktualizować dotychczasowe wymogi w zakresie bezpieczeństwa, którym podlegają dostawcy usług sieciowych, oraz wprowadzić warunki gwarantujące bezpieczeństwo sieci publicznych, zwłaszcza przy przyznawaniu praw użytkowania częstotliwości radiowych w pasmach 5G. Środki te powinny obejmować nałożenie na dostawców i operatorów zaostrzonych wymogów, zobowiązujących ich do zapewnienia bezpieczeństwa sieci. Krajowe oceny ryzyka oraz środki powinny uwzględniać różne czynniki ryzyka, takie jak ryzyko techniczne oraz ryzyko związane z zachowaniem dostawców lub operatorów, w tym dostawców i operatorów z państw trzecich. Krajowe oceny ryzyka będą stanowić centralny element w procesie opracowywania skoordynowanej unijnej oceny ryzyka.
Państwa członkowskie UE mają prawo wykluczyć przedsiębiorstwa ze swoich rynków ze względów bezpieczeństwa narodowego, jeżeli przedsiębiorstwa te nie przestrzegają norm i przepisów obowiązujących w danym państwie.”

Zdanie odrębne:

Huawei Polska sp. z o.o. zgłasza zdanie odrębne do przedmiotowej opinii wskazując, że:

1. zidentyfikowane w niej ryzyka, można odnieść w całej rozciągłości do wszelkich dostawców bez względu na kraj pochodzenia;
2. dokument niniejszy naszym zdaniem nie stanowi istotnego wkładu w dyskusję o cyberbezpieczeństwie sieci 5G.