aut. Andrzej Kozłowski 18.08.2020

CERTYFIKACJA NESAS – HISTORYCZNY PRZEŁOM W BEZPIECZEŃSTWIE SIECI 5G?

„Oceniajcie nas po tym co robimy, jakie produkty przynosimy, jak je wytwarzamy - a nie po tym skąd pochodzimy. To jest właśnie sens NESAS" – mówi Rafał Jaczyński, Regional Cyber Security Officer CEE&Nordics, Huawei. „Pierwszy raz w historii telekomunikacji będzie dostępna jednolita certyfikacja dla wszystkich producentów i operatorów, bez konieczności ponoszenia dodatkowych kosztów" - podkreśla ekspert. Czym jest i jak działa NESAS? Jak wpłynie na bezpieczeństwo sieci 5G i postrzeganie producentów sprzętu?

NESAS (Network Equipment Security Assurance Scheme). Czym jest?

NESAS jest to schemat certyfikacji produktów i urządzeń dla sieci 4 i 5 generacji, wspólny dla wszystkich producentów, którzy by chcieli swoje rozwiązania wstawić do sieci. W tym tych producentów, którzy opierają te produkty na ORAN (Open Ran). „Pierwszy raz w historii telekomunikacji będzie dostępna jednolita certyfikacja dla wszystkich producentów i operatorów, bez konieczności ponoszenia dodatkowych kosztów" – wyjaśnia Rafał Jaczyński z Huawei. „Wcześniej niewiele rządów oraz operatorów miało możliwości, czas i zasoby, aby rozwiązania, które instalują w sieci testować dogłębnie pod względem bezpieczeństwa" – przypomina ekspert.

„NESAS jest inicjatywą branży, mającą na celu położenie kresu bezprzedmiotowym dyskusjom odwracającym uwagę od rzeczywistych wyzwań w bezpieczeństwie sieci – wyjaśnia Rafal Jaczyński. „Branża liczy na to, że po pierwsze będzie można w sposób przejrzysty udowodnić, że dany producent spełnia wymagania bezpieczeństwa, a po drugie operator będzie mógł porównać między sobą produkty różnych dostawców pod kątem bezpieczeństwa. Ponadto będzie to platforma, dzięki której każdy nowy gracz przychodzący do sieci, np. w ramach ORAN, będzie musiał spełnić określony poziom bezpieczeństwa. To skok milowy. Jest to absolutnie pierwszy raz w historii telekomunikacji mobilnej, kiedy coś takiego będzie możliwe" – podkreśla ekspert.

„Raporty z audytów będą dostępne dla operatorów bez żadnych dodatkowych kosztów. Nawet mniejsi operatorzy, którzy nie posiadają wystarczających zasobów, będą mogli z tego programu skorzystać. Informacja o tym, kto został poddany procesowi certyfikacji będzie dostępna publicznie – co gwarantuje, że podmiot, który nie będzie miał certyfikatu, nie będzie w stanie tego ukryć" – podkreśla Regional Cyber Security Officer w Huawei.

Rola 3GPP i GSMA

3GPP (międzynarodowa organizacja normalizacyjna mająca na celu rozwój systemów telefonii komórkowej) tworzy i określa wymagania techniczne, które muszą być spełnione przez poszczególne elementy sieci, czyli jakie funkcjonalności mają być dostępne, jakie mechanizmy bezpieczeństwa mają być obsługiwane, jaki poziom konfiguracyjny bezpieczeństwa musi zostać zapewniony. GSMA, organizacja reprezentująca główne operatorów sieci komórkowych, uzupełnia schemat oczekiwaniami

dotyczącymi kontroli, jaką producenci mają nad wytwarzaniem i aktualizacją swoich rozwiązań. „Weryfikuje nie tylko na samą technologię, ale również procesy, które są wykorzystywane przez dostawców do tego, żeby technologie wytworzyć i w sposób bezpieczny utrzymać. Z jednej strony patrzy czy i jak tworzony jest projekt systemu i czy wymagania bezpieczeństwa są w nim uwzględniane - czyli tzw. security by design. Potem przechodzimy przez kontrolę zmiany i kontrolę wersji, analizę kodu i testy bezpieczeństwa oraz procesy tworzenia binariów oraz sposób zarządzania służącym do tego środowiskiem.Następnie weryfikuje zarządzanie podatnościami i kwestie czy producent jest w stanie sprawnie zareagować na problemy związane z bezpieczeństwem oraz dostarczyć odpowiednie poprawki. Na koniec sprawdza, czy te wszystkie procesy i działania odnajdują odzwierciedlenie w dokumentacji bezpieczeństwa. W sumie ocenia 20 zagadnień istotnych dla bezpieczeństwa i wiarygodności finalnego produktu" – podkreśla ekspert. Jednocześnie przypomina, że NESAS nie służy do weryfikacji w jaki sposób operator zarządza siecią.

Jak dokładnie działa NESAS?

„Prace nad tym projektem rozpoczęły w 2012 roku. Pod koniec 2019 roku został on oficjalnie przyjęty przez dwie organizacje, czyli GSMA i 3GPP. Obecnie toczą się pracę nad kolejną wersją tego systemu certyfikacji i jest to związane z tym, że NESAS stał się naturalnym kandydatem pod europejski system certyfikacji wprowadzony w ramach unijnego Cybersecurity Act" – przypomina Rafał Jaczyński. „NESAS uzupełnia się tutaj m.in. z normą Common Criteria, która również ma bardzo dobre zastosowanie, w szczególności pod kątem całego ekosystemu sieci 5. generacji". Jaczyński podkreśla, że GSMA nie może być właścicielem schematu NESAS ze względu na wymagania wynikające właśnie z Cybersecurity Act. Zgodnie z dokumentem, kontrola nad schematem certyfikacji nie powinna być w rękach organizacji ani stowarzyszenia komercyjnego. Jednocześnie musi on być nadzorowany przez Komisję Europejską i organy takie jak Europejska Grupa Certyfikacji Cyberbezpieczeństwa czy ENISA przy współpracy ze stowarzyszeniem GSMA.

Audytorzy bezpieczeństwa w ramach NESAS

„W ramach CyberSecurity Act mamy trzy poziomy wymagań: podstawowy, istotny i wysoki. Różnią się one zarówno głębokością, zakresem koniecznych testów oraz tym kto będzie wykonywał ewaluację i certyfikację. Aby NESAS spełnił te wymagania, w szczególności na wyższym poziomie musi zostać rozszerzony" – zaznacza Rafał Jaczyński.

Jak podkreśla ekspert Huawei, niezależnych audytorów obecnie wybiera GSMA, która również następnie kontraktuje firmy i nimi zarządza. „W kontekście europejskiego systemu certyfikacji będą też dodatkowe warianty, bo poziom wysoki jest zarezerwowany dla krajowych jednostek certyfikacyjnych i taka możliwość musi być w NESAS przewidziana" – mówi ekspert.

Regional Cyber Security Officer przybliżył również potencjalne zastosowanie NESAS do najnowszego unijnego narzędzia zabezpieczenia sieci 5G, czyli „EU toolbox". W jego opinii NESAS odpowiada na kilka postulatów, oczekiwań i mechanizmów z toolboxa, głównie technicznych. Nie adresuje jednak tego, co leży po stronie operatorów, czyli projektowania, utrzymywania sieci i kontroli dostępu do niej. Nie obejmuje też zachowania ciągłości działania i innych operacyjnych aspektów.

Jeżeli chodzi o środki strategiczno-polityczne, to zdaniem Jaczyńskiego nie ma żadnego schematu certyfikacji, który mógłby rozstrzygnąć, czy dany kraj pochodzenia dostawcy jest właściwy czy nie. „Moim zdaniem tego problemu certyfikacją nie da się rozwiązać - natomiast stanowisko operatorów i producentów idzie w kierunku, że dla bezpieczeństwa sieci 5G nie ma to podstawowego znaczenia, bardziej istotne jest bezpieczeństwo samych produktów i sposób, w jaki operator zarządza siecią. Dlatego też nie za bardzo interesują się kwestiami czy siedziba producenta znajduje się w Szwecji, Chinach, czy Finlandii, zdając sobie zresztą doskonale sprawę z tego, że wszystkie rozwiązania 5G i

tak są rozwijane i produkowane głównie w Chinach”. Można to streścić słowami: „oceniajcie nas po tym co robimy, jakie produkty przynosimy, jak je wytwarzamy - a nie po tym skąd pochodzimy. To jest właśnie sens NESAS. Dlatego też nie pokrywa on całego toolboxa, bo po prostu nie może. Nie wyobrażam sobie takiego mechanizmu niezależnego certyfikowania, który mógłby nam odpowiedzieć na pytanie, które państwo aktualnie bardziej lubimy” – podkreślił ekspert.

Przyszłość NESAS

Jaczyński zapowiada również, że w przyszłości będą zmiany w samym zakresie NESAS. „Standaryzacja jest dużym wyzwaniem, bo trzeba pogodzić ze sobą oczekiwania dostawców i operatorów. I to wszystko zapisać w standard, który jest jednoznaczny i tak samo interpretowany przez wszystkich” – dodaje. „Pierwsza wersja NESAS ustępowała Common Criteria pod względem zakresu i głębokości weryfikacji wymaganej do wyższych poziomów zaufania. W drugiej wersji, która powinna być już gotowa w tym roku, te brakujące elementy będą już uwzględnione. Spowodują one na przykład, że rozwiązania będą testowane szerzej, czyli będą obejmowały nie tylko skanowanie i poszukiwanie podatności, ale również testy penetracyjne oraz analizę kodu. Być może w przyszłości na bazie NESAS i Common Criteria powstanie jeden, ujednolicony schemat certyfikacji, w tej chwili oba oba te podejścia się uzupełniają. Common Criteria jest dojrzałą i sprawdzoną metodyką pozwalającą na weryfikację rozwiązań o najwyższym oczekiwanym poziomie zaufania, nie dysponuje jednak wspólnym zestawem wymagań bezpieczeństwa dedykowanym do elementów sieci 5G, które zapewniałyby pełną obiektywność i porównywalność testów. NESAS odwrotnie – zdefiniował, jakie wymagania produkty i producenci muszą spełniać, ale wymaga rozwoju w zakresie samej metodyki testów. Jak to mówi się często w biznesie – potencjał synergii jest ewidentny – podkreśla ekspert.