digitalpoland
Fundacja DigitalPoland

KIGEIT

KRÓTKA OPOWIEŚĆ O SPOŁECZEŃSTWIE 5.0 CZYLI JAK ŻYĆ I FUNKCJONOWAĆ W DOBIE GOSPODARKI 4.0 I SIECI 5G

ZAŁĄCZNIK 3

BEZPIECZEŃSTWO W EKOSYSTEMIE SIECI 5G

Bezpieczeństwo każdej sieci telekomunikacyjnej – sieć 5G nie jest pod tym względem wyjątkiem – wymaga efektywnej współpracy operatorów, dostawców rozwiązań i regulatorów rynku. Wymaga również zaadresowania ryzyk pojawiających się podczas całego cyklu życia sieci telekomunikacyjnej.

Rola operatora w zapewnieniu bezpieczeństwa sieci 5G jest kluczowa – operator telekomunikacyjny odpowiada za bezpieczeństwo sieci i świadczonych usług. Rolą operatora jest w szczególności:

1. Określenie wymagań bezpieczeństwa dla dostawców rozwiązań 5G.
2. Zaprojektowanie mechanizmów kontrolnych sieci, w oparciu zarówno o rozwiązania dostawców rozwiązań 5G, jak i własne procesy i rozwiązania firm trzecich.
3. Kontrola nad dostępem do urządzeń sieciowych i danych przesyłanych w sieci 5G.
4. Monitorowanie bezpieczeństwa sieci i obsługa incydentów.
5. Zapewnienie wymaganych parametrów jakościowych i ciągłości działania usług.

Rolą dostawców rozwiązań jest wsparcie operatorów sieci w zapewnieniu jej bezpieczeństwa, a przede wszystkim:

- kompletna implementacja mechanizmów bezpieczeństwa przewidzianych standardami 3GPP w fizycznych rozwiązaniach sprzętowych i oprogramowaniu,
- zaprojektowanie produktów z uwzględnieniem najlepszych praktyk, standardów i wymogów regulacyjnych dotyczących bezpieczeństwa,
- budowa produktów w sposób zgodny z najlepszymi praktykami – w tym analiza oprogramowania pod względem bezpieczeństwa w procesie ciągłym, jeszcze na etapie rozwoju produktu oraz zarządzanie bezpieczeństwem w łańcuchu dostaw,
- weryfikacja bezpieczeństwa rozwiązań zgodnie z wymaganiami rynkowymi – z uwzględnieniem adekwatnej certyfikacji, jeśli jest wymagana,
- wdrożenie rozwiązań w sieci operatora i przekazanie sieci do utrzymania zgodnie z zasadami bezpieczeństwa,
- obsługa podatności zidentyfikowanych w produktach i udostępnianie aktualizacji bezpieczeństwa,
- w przypadku świadczenia usług wsparcia lub monitorowania – zachowanie zgodności z wymaganiami bezpieczeństwa operatora, w szczególności dbałość o przetwarzanie danych zgodnie z umową i wymaganiami prawa obowiązującego w naszym kraju.

Niezmiernie istotna rola w zapewnieniu bezpieczeństwa sieci 5G w Polsce przypada również regulatorowi rynku. Jako podstawowe zadania administracji publicznej warto wskazać:

1. Określenie wymagań bezpieczeństwa, które powinny spełniać sieci 5G budowane w Polsce
2. Zdefiniowanie zasad weryfikacji bezpieczeństwa sieci i urządzeń sieciowych, obejmujących wszystkich uczestników rynku
3. Zapewnienie działania systemu weryfikacji bezpieczeństwa i – w przypadku podjęcia takiej decyzji – zastosowanie adekwatnego programu certyfikacji

1.1 ZAGROŻENIA ZWIĄZANE Z ŁAŃCUCHEM DOSTAW

Łańcuch dostaw wszystkich dostawców rozwiązań sieci 5G jest podatny na takie same zagrożenia związane z międzynarodową siecią dostawców, a wynikające z eksterytorialnych przepisów prawa, polityki realizowanej przez kraje nie będące członkami Unii Europejskiej, wojny handlowe o zasięgu globalnym i katastrofy naturalne mogące zaburzyć ciągłość dostaw.

Poziom ryzyka obecny w zglobalizowanym łańcuchu dostaw producentów sprzętu 5G wymaga szczególnej staranności w zarządzaniu bezpieczeństwem – operatorzy telekomunikacyjni powinni wymagać od producentów rozwiązań zgodności z najlepszymi praktykami, w tym certyfikacji według odpowiednich norm międzynarodowych (np. ISO 28001).

1.2 CYBERBEZPIECZEŃSTWO SIECI 5G

Sieci 5G – dzięki radykalnie lepszym parametrom technicznym – niosą ze sobą obietnicę otwarcia na nowe zastosowania, dotychczas niemożliwe do realizacji przy zastosowaniu wcześniejszych generacji mobilnych technologii komunikacyjnych. Jest wysoce prawdopodobne, że liczba różnych zastosowań sieci 5G będzie znacząco większa, niż dla sieci 3G i 4G – oznacza to również, że liczba i zróżnicowanie urządzeń korzystających z sieci również znacząco się zwiększy. Te dwa czynniki skutkują zwiększoną „powierzchnią ataku" w przypadku sieci 5G.

Ten efekt został bardzo wcześnie zidentyfikowany przez 3GPP – dlatego normy techniczne bezpieczeństwa dla sieci 5G począwszy do wydania R15 zawierają znaczące ulepszenia względem sieci 4G, adresując niektóre kluczowe ryzyka już na poziomie standaryzacji. Dodatkowo, dzięki współpracy w ramach ekosystemu operatorów, dostawców rozwiązań i niezależnych usługodawców, stosunkowo wcześnie pojawiają się rozwiązania rynkowe uzupełniające mechanizmy przewidziane w normach technicznych 5G.

Warto podkreślić cztery kluczowe udoskonalenia mechanizmów bezpieczeństwa w porównaniu do standardu czwartej generacji:

1. Zunifikowane uwierzytelnienie – w porównaniu do mechanizmów specyficznych dla technologii dostępowej w standardzie 4G.
2. Elastyczną politykę bezpieczeństwa sieci, pozwalającą na dostosowanie do różnych zastosowań sieci – przy braku takiej elastyczności w sieciach 4G.
3. Lepszą ochronę prywatności użytkownika sieci – dzięki szyfrowaniu jego numeru identyfikacyjnego zapewniającego wyższy poziom bezpieczeństwa, niż mechanism pseudoanonimizacji stosowany w poprzedniej generacji.
4. Wprowadzenie dodatkowego elementu architektury pozwalającego na filtrowanie wiadomości sygnalizacyjnych i „ukrywanie" topologii sieci operatora przed światem zewnętrznym – w sieciach 4G te funkcje nie były wymagane standardami.

Już te udoskonalenia powodują, że standard piątej generacji zapewnia najwyższy poziom bezpieczeństwa spośród dotychczasowych publicznych systemów komunikacji mobilnej. Oczywiście, same mechanizmy bezpieczeństwa przewidziane standardami 3GPP nie są wystarczającą odpowiedzią na zagrożenia, które mogą wystąpić w sieciach 5G – dlatego zarówno operatorzy, jak i dostawcy stosują rozwiązania wykraczające poza zabezpieczenia przewidziane standardami.

Należy również podkreślić, że dostawca aplikacji korzystających z sieci 5G nie powinien polegać wyłącznie na sieciowych mechanizmach bezpieczeństwa, jeżeli nie spełniają one wymagań jego klientów (np. nie zapewniają poufności *end-to-end*). Mechanizmy warstwy aplikacji powinny w takiej sytuacji zapewnić wymagany w danej usłudze poziom ochrony.

1.2.1 WRAŻLIWE ELEMENTY SIECI 5G

Podstawowym założeniem przyjętym podczas projektowania mechanizmów bezpieczeństwa 5G był podział elementów sieci na domeny zaufania, przy czym im dalej od rdzenia sieci, tym poziom zaufania może być niższy. Tę koncepcję wyjaśnia poniższy diagram – funkcje sieciowe takie, jak UDM czy ARPF wymagają najwyższego poziomu zaufania, a gNB (przedstawiona pod postacią DU/CU) jest uważana za zdecydowanie mniej wrażliwy element architektury sieci. Warto w tym miejscu podkreślić, że ze względu na ewolucyjne podejście do wdrożenia sieci 5G, elementy sieci rdzeniowej piątej generacji nie pojawią się w naszym kraju wcześniej, niż za kilka lat – w pierwszej fazie budowy 5G operatorzy rozszerzą po prostu istniejące sieci 4G o nowe nadajniki zgodne ze standardem 5G (gNodeB). Oznacza to również, że omawiane w dalszej części zagrożenia związane z siecią rdzeniową 5G mają w chwili obecnej charakter teoretycznej analizy ryzyka.

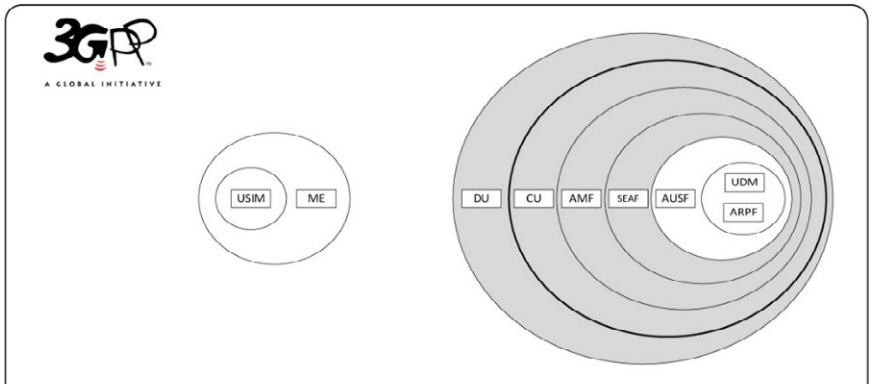


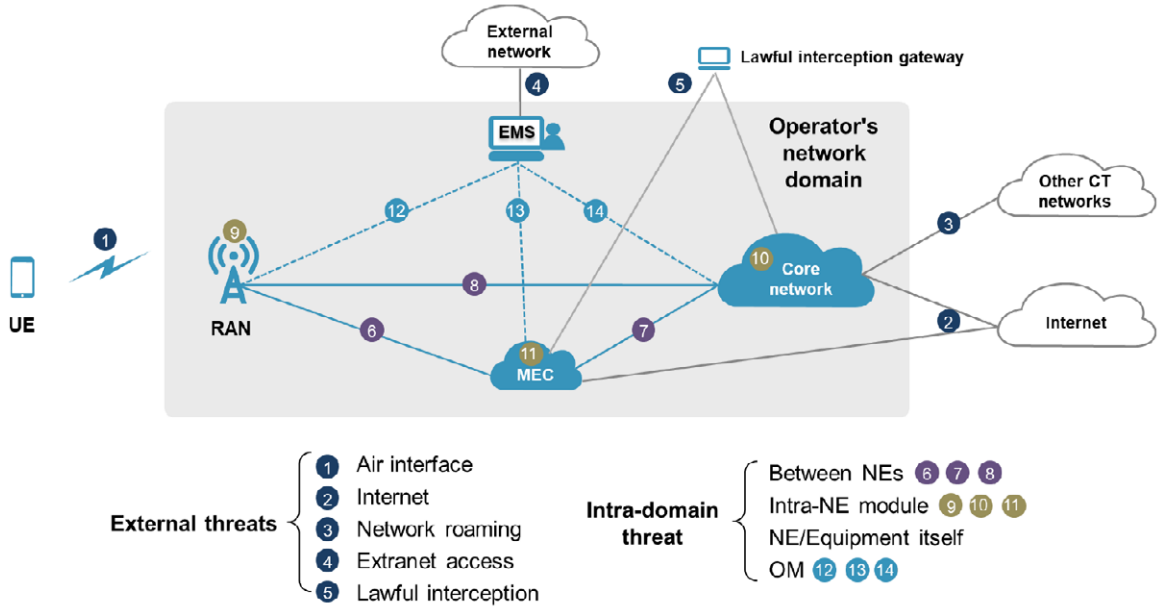
Figure 1 Trust model of non-roaming scenario

Zarówno architektura, jak i ekosystem biznesowy 5G zawiera elementy istotne dla bezpieczeństwa, a nie ujęte w powyższym modelu zaufania – przykładowo, aplikacje działające w Multi-access Edge Computing (MEC), dostarczane mogą być przez partnerów lub klientów operatorów, co wymaga od operatora dodatkowej analizy pod względem bezpieczeństwa.

1.2.2 ZAGROŻENIA TECHNOLOGICZNE

Co do zasady, główne zagrożenia technologiczne dla bezpieczeństwa sieci piątej generacji nie różnią się od zagrożeń już aktualnie obecnych w sieci 4G i od zagrożeń znanych z innych zastosowań kluczowych dla realizacji 5G technologii (wirtualizacja, Software Defined Networking, mikrousługi itp.). Można z dużą dozą prawdopodobieństwa stwierdzić, że **wraz z pojawieniem się w Polsce sieci 5G nie pojawią się u nas żadne nowe, nieznane dotychczas rodzaje zagrożeń dla cyberbezpieczeństwa.** Co więcej, wbrew pojawiającym się w przestrzeni publicznej informacjom, nawet technologie specyficzne dla sieci rdzeniowej (*Core*) piątej generacji są już aktualnie wykorzystywane przez polskich operatorów – przykładowo, technologia wirtualizacji funkcji sieciowych (NFV) jest już wykorzystywana w zwirtualizowanych sieciach rdzeniowych 4G.

Poniższy diagram przedstawia główne kategorie zagrożeń technicznych, które mogą wystąpić w sieciach 5G. Scenariusze zagrożeń co do zasady dzielą się na dwie grupy: związane z interfejsami sieci 5G ze światem zewnętrznym (*extra-domain threats*), i związane z samą wewnętrzną architekturą 5G, bądź jej niewłaściwą implementacją (*intra-domain threats)*.



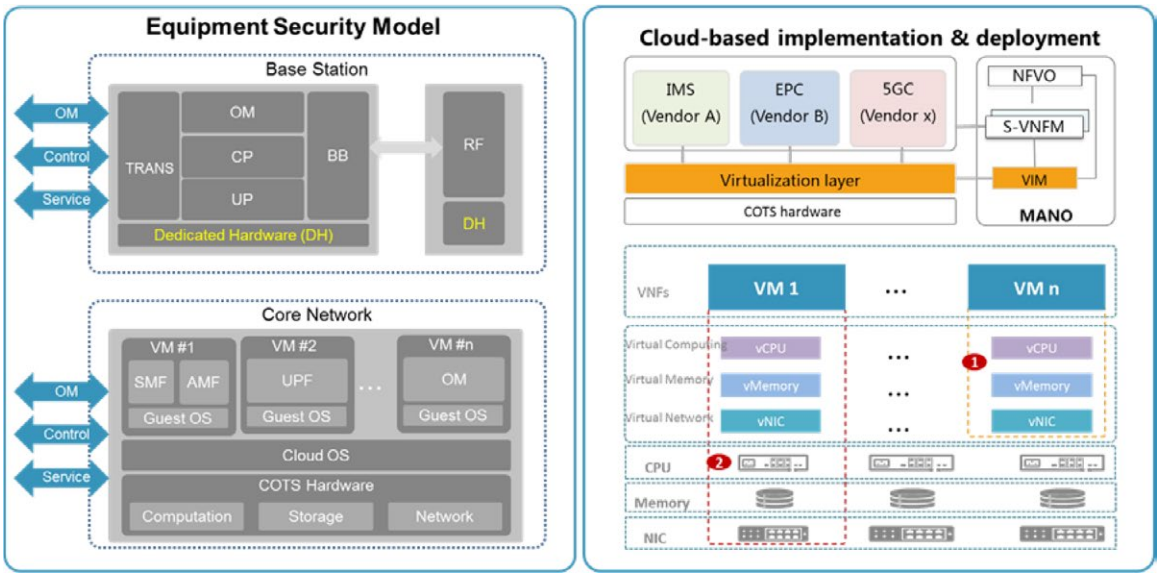
Zagrożenia zewnętrzne dla sieci 5G są identyczne, jak w sieciach poprzednich generacji – zostały one zestawione w poniższej tabeli. Mechanizmy bezpieczeństwa wprowadzone w standardach 5G adresują zagrożenia zewnętrzne lepiej, niż w sieciach 4G – co powoduje, że poziom związanego z nimi ryzyka jest mniejszy.

Typ scenariusza zagrożeń	Główne scenariusze zagrożeń	Opis
Extra-domain	**Air Interface** Zagrożenia związane z interfejsem radiowym – podsłuch, ataki DoS pochodzące od urządzeń Internetu Rzeczy	– Mechanizmy bezpieczeństwa 5G lepiej chronią prywatność i dane użytkownika przesyłane w interfejsie radiowym – podsłuch i pozyskanie metadanych (np. informacji o lokalizacji) jest znacząco utrudniony. – Mechanizmy ograniczające ryzyka związane z atakami Denial of Service pochodzącymi od urządzeń Internetu Rzeczy nie są związane bezpośrednio z 5G, nie są więc standaryzowane – niektórzy dostawcy rozwiązań 5G wprowadzają jednak w gNB własne rozwiązania pozwalające na wykrycie i ograniczenie nadmiarowego ruchu.
	Internet Zagrożenia związane z połączeniem z sieciami pakietowymi, w szczególności Internetem	Zagrożenia tego rodzaju są znane i obecne w aktualnych sieciach mobilnych
	Network roaming Zagrożenia związane z połączeniem z sieciami innych operatorów	Zagrożenia związane z atakami za pośrednictwem sygnalizacji, oraz zagrożenia związane z uwierzytelnieniem użytkowników w sieciach “wizytowanych” występują w sieciach każdej poprzedniej generacji – standard 5G wprowadza w tym przypadku dodatkowe mechanizmy bezpieczeństwa powodujące, że ryzyko jest ograniczone

	External Access to EMS Zagrożenia związane z dostępem do system zarządzania siecią	Zagrożenie polega na zdalnym dostępie do system zarządzania siecią – w przypadku, jeśli operator udostępnia taką możliwość. Mitygacja tego ryzyka wymaga odpowiedniej infrastruktury zdalnego dostępu po stronie operatora, zarządzania uprawnieniami i spełnienia standardu bezpieczeństwa stacji roboczych uzyskujących dostęp do serwera zarządzającego. Powyższe zagrożenie występuje w istniejących sieciach
	Lawful Interception Security Threats Zagrożenia związane z dostępem do funkcjonalności uprawnionego monitorowania	Zagrożenie jest związane z nieautoryzowanym dostępem do funkcji uprawnionego monitorowania, wykorzystywanego pod odpowiednią kontrolą przez uprawnione służby państwowe. Tego rodzaju zagrożenie istnieje i jest ograniczane również w aktualnych sieciach.

Zagrożenia wewnątrz sieci są związane z komunikacją pomiędzy elementami sieci – realizowanej zasadniczo w oparciu o protokół IP, technologiami wykorzystywanymi do realizacji wymagań funkcjonalnych sieci 5G (np. NFV, SDN, SBA) lub lokalizacją poszczególnych elementów (odgrywającą rolę np. w przypadku *Multi-access Edge Computing*).

Rdzeń sieci realizowany w technologii chmury obliczeniowej może być oparty na ogólnodostępnej platformie sprzętowej (*Commercial-Off-The-Shelf* – COTS) lub wykorzystywać dedykowaną platformę wykorzystującą specjalizowane układy elektroniczne (FPGA, ASIC). Oba rozwiązania mają swoje wady i zalety, w przypadku sprzętu COTS należy uwzględnić ryzyko związane z większą heterogenicznością całego rozwiązania, w tym prawdopodobnym wykorzystaniem rozwiązań klasy open-source.



Warto zwrócić uwagę, że 5G wprowadzając w szerszym stopniu do świata telekomunikacji mobilnej zagrożenia typowe dla Internetu i środowisk informatycznych w przedsiębiorstwach, umożliwia też zastosowanie najlepszych praktyk i sprawdzonych zabezpieczeń organizacyjno-technicznych wypracowanych w branży IT.

Podsumowanie głównych kategorii zagrożeń 5G występujących wewnątrz sieci zawiera poniższa tabela:

Typ scenariusza zagrożeń	Główne scenariusze zagrożeń	Opis
Intra-domain	**Between NEs** Zagrożenia lokalizujące się pomiędzy elementami sieci (w tym komunikacja pomiędzy mikrousługami), zagrożenia pomiędzy 5GC/MEC/gNodeB	– Sieć rdzeniowa 5G (5GC) wprowadza architecture opartą o mikrousługi (SBA), co powoduje zagrożenia w przypadku złego zabezpieczenia komunikacji pomiędzy usługami – gNodeB i 5GC/MEC znajdują się w innych domenach (poziomach zaufania) bezpieczeństwa – zagrożenia dotyczą przesyłu sygnalizacji i danych użytkowych pomiędzy gNodeB i 5GC/MEC – Występują zagrożenia interfejsu zegarowego: spoofing serwera czasu, modyfikacja informacji zegarowych, manipulacja sygnału GPS – Zagrożenia związane z transmisją – spoofing, podsłuch, modyfikacja informacji, ataki DoS
	Intra-NE module Zagrożenia występujące wewnątrz elementów sieciowych i wewnątrz MEC, zagrożenia związane z chmurą obliczeniową, zagrożenia warstwowania sieci (*slicing*)	– Mobile Edge Computing nie jest zdefiniowane w normach 3GPP's Release 15, ale zastosowanie tego podsystemu w przyszłości jest bardzo prawdopodobne. Lokalizacje MEC będą znajdowały się bliżej brzegu sieci, więc nie będą tak dobrze chronione, jak centralne serwerownie – dodatkowo środowiska te będą obejmowały aplikacje stron trzecich. – Wirtualizacja funkcji sieciowych (NFV) jest już wykorzystywana w sieciach 4G, ale dopiero w 5G rdzeń sieci będzie w pełni realizowany w chmurze prywatnej. Oznacza to, że wszystkie znane zagrożenia dotyczące chmury obliczeniowej będą dotyczyły również 5G. – 5G wprowadza warstwowanie sieci *end-to-end*, co powoduje zagrożenia w przypadku niewystarczającej separacji pomiędzy warstwami o różnych właściwościach I udostępnianych różnym odbiorcom oraz złego zarządzania dostępem do usług.
	NE/equipment Zagrożenia związane z oprogramowaniem, sprzętem, przetwarzaniem danych	Rodzaje zagrożeń związanych z oprogramowaniem i sprzętem są identyczne, jak w sieciach poprzednich generacji i w rozwiązaniach klasy Enterprise.
	O&M Security Zagrożenia związane z interfejsem zarządzania	Niewystarczająco zabezpieczone interfejsy zarządzania mogą spowodować utratę kontroli nad siecią telekomunikacyjną

REKOMENDACJE DOTYCZĄCE BEZPIECZEŃSTWA 5G

Praktyka budowy bezpiecznych sieci 5G w Polsce – a co za tym idzie ewentualne regulacje – powinny uwzględniać następujące zasady:

1. Wsparcie dla rozwiążań opartych na standardach (GSMA/3GPP)
   - Z punktu widzenia bezpieczeństwa, sieć 5G stosuje warstwowy i oparty na separacji domen model zgodny z normą ISO 19249. Zgodnie z tym modelem, wszyscy interesariusze – dostawcy aplikacji/usług, dostawcy urządzeń końcowych, dostawcy i operatorzy sieci – powinni realizować odpowiedzialność za zabezpieczenie sieci we właściwym sobie zakresie.
   - Bezpieczeństwo sieci musi opierać się na otwartych standardach, definiowanych przez organizacje takie, jak 3GPP, czy IETF. Otwarte podejście powinno być również stosowane podczas współpracy publiczno-prywatnej na rzecz podniesienia bezpieczeństwa polskich sieci 5G, w tym analizy ryzyka czy definiowania wymagań bezpieczeństwa.
   - Standardy bezpieczeństwa sieci obowiązujące w Polsce powinny zapewniać, że sieci 5G będą zaprojektowane, zbudowane i utrzymywane w sposób w maksymalnym stopniu uniezależniający poziom ich bezpieczeństwa od wyboru konkretnego dostawcy (-ów) elementów sieci 5G
2. Niezależna weryfikacja/certyfikacja rozwiązań sieci 5G
   - Weryfikacja i certyfikacja bezpieczeństwa sprzętu sieciowego jest kluczowym narzędziem do zapewnienia, że rozwiązania spełniają określone normy w zakresie cyberbezpieczeństwa. Weryfikacja lub certyfikacja powinna być realizowana przez niezależne laboratoria.
   - Przykładowym podejściem zapewniającym efektywność kosztową i spójność wymagań bezpieczeństwa są zdefiniowany przez 3GPP i GSMA schemat weryfikacji obejmujący wymagania bezpieczeństwa dla urządzeń sieciowych SCAS (Security Assurance Specification) i schemat akredytacji procesów oraz rozwiązań NESAS (Network Equipment Security Assurance Scheme). W chwili obecnej zakończone zostały testy pilotażowe, oczekuje się, że NESAS zostanie udostępniony jeszcze w tym roku.
   - Wymagania SCAS są definiowane przez 3GPP dla każdej funkcji sieciowej (np. gNB) of the system. NESAS definiuje proces testów i akredytacji procesów związanych z bezpiecznym cyklem życia produktów 5G – ich projektowania, rozwoju, testowania i utrzymania. Takie podejście umożliwia operatorom uzyskanie informacji nie tylko na temat bezpieczeństwa sprzętu i oprogramowania, ale również na temat kompetencji dostawcy w zakresie zarządzania zmianą, konfiguracją, aktualizacjami i podatnościami.
   - NESAS i SCAS są przygotowywane przez organizacje nie związane z żadnym z dostawców, a testy będą przeprowadzane przez niezależne laboratoria.
   - Aktualnie zgodnie z planem nakreślonym przez Cybersecurity Act, w Unii Europejskiej toczą się prace nad schematami i programami certyfikacji, uwzględniającymi również podejścia oparte o Common Criteria. Prowadzone są również analizy weryfikujące możliwość dostosowania NESAS do wymagań postawionym programom certyfikacyjnym zgodnym z Cybersecurity Act.
3. Wykorzystywanie najlepszych praktyk, również spoza branży telekomunikacyjnej
   - Mechanizm Coordinated Vulnerability Disclosure (CVD) powinien zostać zastosowany w celu wymiany informacji o zidentyfikowanych podatnościach, ich weryfikacji przez dostawców, GSMA i 3GPP i zapewnieniu odpowiednich aktualizacji.
   - Obsługa podatności i incydentów wymaga istnienia specjalizowanych zespołów po stronie dostawców, afiliowanych przy odpowiednich branżowych organizacjach (np. FIRST). Wymagania dotyczące istnienia i kompetencji zespołów szybkiego reagowania powinny być elementem składowym oczekiwań stawianych przez operatorów producentom rozwiązań

digitalpoland

Fundacja DigitalPoland

KIGEiT

Krajowa Izba Gospodarcza
Elektroniki i Telekomunikacji