NASK Cyber POLICY

Unijna skoordynowana ocena ryzyka związanego z cyberbezpieczeństwem w sieciach piątej generacji (5G)

Sieć 5G[1] będzie miała kluczowe znaczenie dla cyfrowej transformacji gospodarki i społeczeństwa Unii Europejskiej. Połączy miliardów urządzeń i systemów, w tym w kluczowych sektorach, takich jak energetyka, transport, bankowość czy zdrowie. Szacuje się, że przychody związane z 5G osiągną w 2025 roku 225 miliardy euro[2], dlatego Europa musi podjąć kroki, aby być w stanie konkurować na globalnym rynku. Według Planu Działania 5G dla Europy z 2016 roku, państwa członkowskie powinny rozpocząć wdrażanie usług 5G najpóźniej do końca 2020 roku.

W ocenie Komisji Europejskiej niezbędne jest zapewnienie cyberbezpieczeństwa sieci nowej generacji, tak aby można było w pełni korzystać z jej możliwości. Dlatego państwa członkowskie zostały zobowiązane do przygotowania krajowych ocen ryzyka sieci 5G. Przekazane w lipcu 2019 roku do KE oraz ENISA dokumenty były podstawą do przygotowania unijnej skoordynowanej ocena ryzyka związanego z cyberbezpieczeństwem sieci 5G.

Raport, opublikowany w październiku 2019 roku przez Grupę Współpracy NIS, skupia się na najważniejszych zagrożeniach dotyczących sieci 5G, opisuje szczególnie wrażliwe aktywa i zasoby sieci, wskazuje na jej możliwe podatności i słabe punkty, a także przedstawia przykładowe scenariusze ryzyka.

Nowe rozwiązania technologiczne – nowe wyzwania

Autorzy raportu zwracają uwagę, że wykorzystanie sieci 5G będzie oznaczało odejście od tradycyjnej architektury sieci. Przede wszystkim środek ciężkości przeniesiony zostanie na oprogramowanie. Może to spowodować zarówno korzyści (łatwiejsza aktualizacja i łatanie luk), jak i zagrożenia (większa rola zewnętrznych dostawców, wymóg przemyślanych i skutecznych procedur zarządzania poprawkami).

Wprowadzenie nowych funkcjonalności będzie odbywać się etapowo.

- Perspektywa krótkoterminowa: **sieci niesamodzielne** (non-standalone) opierające się na istniejącej infrastrukturze 4G. Uaktualniona do technologii 5G zostaje tylko sieć dostępu radiowego. Zwiększy to wydajność mobilnego Internetu dla użytkowników.

[1] Komisja Europejska zdefiniowała sieć 5G jako zbiór elementów infrastruktury sieciowej służący do mobilnej oraz bezprzewodowej komunikacji. Będzie ona wykorzystywana w połączeniach i usługach, które wymagają zaawanasowanej wydajności. Charakteryzuje się bardzo dużą szybkością transmisji danych i przepustowością, komunikacją o niskich opóźnieniach, wysoką niezawodnością oraz możliwością obsługi dużej liczby podłączonych urządzeń.

[2] ABI Research projection: https://www.abiresearch.com/press/abi-research-projects-5g-worldwide-servicerevenue

- Perspektywa średnio i długoterminowa: **sieci samodzielne** (standalone) umożliwią wdrożenie funkcji sieci bazowej 5G oraz wprowadzenie nowych funkcjonalności[3]. Wymagana będzie znacznie szersza zmiana w architekturze sieci.

Nowe funkcje przyniosą wiele nowych wyzwań bezpieczeństwa. Jeśli więc sieć 5G nie będzie właściwie zarządzana, zastosowane rozwiązania mogą zwiększyć ogólną powierzchnię ataku oraz liczbę potencjalnych punktów wejścia dla atakujących.

Odpowiedzialność za bezpieczeństwo sieci 5G

W ocenie autorów raportu wszyscy interesariusze mają do odegrania dużą rolę w zapewnieniu cyberbezpieczeństwa sieci 5G. Największe znaczenie przypisywane jest jednak dwóm typom podmiotów[4]:

- **operatorom sieci komórkowych**, którzy są decyzyjni, jeśli chodzi o bezpieczeństwo swoich sieci. To od nich w dużej mierze zależeć będzie wdrożenie standardów 5G.
- **producentom sprzętu telekomunikacyjnego**, którzy są odpowiedzialni za dostarczanie oprogramowania i sprzętu wymaganego do obsługi sieci.

Operatorzy sieci komórkowych, którzy świadczą usługi w UE, podlegają przepisom unijnym i krajowym, które właściwe organy mogą egzekwować. Jednak różnią się np. w kwestiach dotyczących strategii wyboru dostawców sprzętu, systemów i usług. Jest to niezwykle istotne, jako że na rynku jest **zaledwie kilka firm, które mogą dostarczyć technologię niezbędną do wdrożenia sieci 5G**. Są to głównie Ericsson, Nokia i Huawei, ale także ZTE, Samsung i Cisco.

Autorzy raportu podkreślają, że poszczególni dostawcy mają różne modele biznesowe czy strategie zarządzania. Co więcej, mogą korzystać z usług podwykonawców. Jest to o tyle istotne, że w sieci 5G niektóre funkcje sieciowe trafią do podwykonawców. Tymczasem niektórzy z nich mogą znajdować się w innym państwie członkowskim niż operator sieci komórkowej lub w państwie poza Unią Europejską[5].

[3] Oprogramowanie i wirtualizacja sieci (Programowalna sieć komputerowa (SDN), Wirtualizacja funkcji sieciowych (NFV); Segmentacja sieci (Network slicing); Mniej scentralizowana architektura - wsparcie tzw. *mobile Edge computing* , czyli kierowania ruchu sieciowego do zasobów obliczeniowych i usług w pobliżu użytkownika, dzięki czemu skraca się czas reakcji.

[4] Jako główni interesariusze wymieniani są: operatorzy sieci komórkowych; dostawcy operatorów sieci komórkowych; producenci podłączonych urządzeń i dostawcy usług; inni interesariusze, np. użytkownicy.

[5] Główną siedzibę w UE mają jedynie Ericsson i Nokia.

NASK Cyber POLICY

Krajowe oceny ryzyka

Zagrożenia

Sieć 5G będzie podstawą, na której oprze się wiele aspektów gospodarki oraz życia społecznego. W związku z tym **integralność** i **dostępność** sieci stanie się kluczowa. Cały czas wyzwaniem będzie również **poufność**. Główne zagrożenia dotyczyć będą np.:

- Zakłócenia lokalnej lub globalnej sieci 5G (dostępność);
- Szpiegowania ruchu lub kradzieży danych (poufność);
- Przekierowania ruchu/danych w sieci 5G (integralność/poufność);
- Zniszczenia lub modyfikacji innej infrastruktury cyfrowej lub systemów informatycznych za pośrednictwem sieci 5G (integralność/dostępność).

Rozpatrując scenariusze zagrożeń dla sieci 5G, autorzy raportu wskazują czynniki takie jak: liczba i rodzaj użytkowników, których dotyczy zagrożenie; czas trwania, objęte usługi, a także zakres szkód lub strat ekonomicznych.

Kto zagraża sieci 5G

Rodzaje zagrożeń	Opis zagrożenia
Przypadkowe Nie wrogie	Błędy ludzkie, naturalne zjawiska, awarie systemów.
Haker	Cyberprzestępca motywowany finansowo lub chęcią rozgłosu.
Grupa haktywistów	Grupa posiadająca agendę polityczną. Poprzez publiczny atak zwraca uwagę na swoje racje lub szkodzi danym organizacjom.
Zorganizowana grupa przestępcza	Motywowana finansowo zorganizowana działalność przestępcza.
Insider	Osoba pracująca np. dla operatora sieci komórkowej lub jego dostawcy.
Państwo Podmiot wspierany przez państwo	Motywacje głównie natury politycznej.
Inni: cyberterroryści przedsiębiorstwa	Cyberterroryści - cele polityczne. Możliwość zbliżone do zorganizowanej grupy przestępczej. Przedsiębiorstwa - przewaga konkurencyjna poprzez kradzież własności intelektualnej, wrażliwych danych lub poprzez cyberatak, mający zaszkodzić np. reputacji konkurencji.

Podmioty zagrażające sieciom 5G oceniono, biorąc pod uwagę dwa aspekty: możliwości (zasoby) oraz intencje (motywacje). Jako najbardziej znaczące wskazano zagrożenia ze strony **państw lub podmiotów wspieranych przez państwo**. Co ważne, w przesłanych krajowych ocenach ryzyka, kilka państw członkowskich stwierdziło, że jest celem ofensywnych działań w cyberprzestrzeni prowadzonych przez określone kraje spoza UE.

Zasoby/Aktywa

W raporcie oceniono wrażliwość na atak głównych aktywów sieciowych. Podzielono je na:

- **Funkcje zdefiniowane w normie 3GPP**[6]
  - Funkcje bazowe, zapewniające abonentom szereg usług;
  - Dostęp do funkcji, łączących abonentów z dostawcą sieci.
- **Funkcje podstawowe nie zdefiniowane w normie 3GPP**
  - Transportu i transmisji - utrzymanie połączenia sieci dostępowej z rdzeniem;
  - Wymiany wewnątrz sieci (*internetwork exchanges*);
  - Systemy zarządzania i usługi pomocnicze (np. orkiestracja sieci).

Raport przedstawia podział na główne kategorie aktywów, wraz z ich poziomem wrażliwości oraz wykazem kluczowych elementów.

Kategorie elementów i funkcji	**Ogólny poziom wrażliwości**	**Kluczowe elementy**
Bazowe funkcje sieciowe Zarządzanie NFV (wirtualizacja funkcji sieciowych) i organizacja sieci (MANO)	Krytyczny	• Uwierzytelnianie, roaming i zarządzanie sesjami urządzeń użytkownika • Przesyłanie danych urządzeń użytkownika • Zarządzanie zasadami dostępu • Rejestracja i autoryzacja usług sieciowych • Przechowywanie danych użytkowników • Połączenie z zewnętrznymi sieciami mobilnymi • Ekspozycja podstawowych funkcji sieciowych na aplikacje zewnętrzne • Przypisywanie urządzeń końcowych użytkowników do segmentów/warstw sieci
Systemy zarządzania i usługi wspierające (inne niż MANO)	Umiarkowany/ wysoki	• Systemy zarządzania bezpieczeństwem • Rozliczanie i inne systemy wsparcia (np. wydajności sieci)
Sieć dostępu radiowego	Wysoki	• Stacje bazowe
Funkcje transportu i transmisji	Umiarkowany/ wysoki	• Sprzęt sieciowy niskiego poziomu (np. router) • Sprzęt filtrujący (firewall)
Funkcje wymiany wewnątrz sieci	Umiarkowany /wysoki	• Zewnętrzne sieci operatorów sieci mobilnych • Zewnętrzne usługi sieciowe

Funkcje bazowe sieci 5G są uważane za krytycznie wrażliwe. Wpływ na sieć bazową może zagrozić poufności, dostępności i integralności wszystkich usług sieciowych. Również **systemy**

[6] Kwestie bezpieczeństwa 5G są coraz częściej rozwiązywane w pracach organów normalizacyjnych, w szczególności w grupie roboczej „Service and System Aspects 3" (SA3) w ramach 3rd Generation Partnership (3GPP). Zajmuje się ona opracowaniem standardów dotyczących bezpieczeństwa i prywatności w sieciach 5G i zamierza opracować specyfikacje niezbędne do spełnienia tych wymagań.

zarządzania i usługi wspierające są bardzo wrażliwe, ponieważ kontrolują istotne elementy sieci. Mogą być wykorzystywane np. do sabotażu czy szpiegostwa. Za **szczególnie ważne uznano** m.in. zarządzanie NFV oraz siecią (MANO)[7]. Warto zwrócić uwagę na **sieć dostępu radiowego,** której również przypisano wysoki poziom wrażliwości. Jej rola wzrośnie w przyszłości, wraz z położeniem akcentu na *edge computing*[8].

Aktywa inne niż techniczne

Raport wymienia podmioty oraz typy użytkowników, którzy wymagają szczególnej uwagi:

- Operatorzy usług kluczowych (Dyrektywa NIS) oraz infrastruktury krytycznej;
- Podmioty rządowe, organy ścigania, wojsko;
- Kluczowe sektory i podmioty nieobjęte przepisami dotyczącymi cyberbezpieczeństwa.

Aktywem o dużym znaczeniu mogą być również obszary geograficzne (np. inteligentne miasta, obszary ze szczególnie wrażliwymi podmiotami).

Podatności i luki w zabezpieczeniach

Autorzy raportu wskazują na trzy rodzaje możliwych podatności:

1. **Podatności związane ze sprzętem, oprogramowaniem i procedurami**

Poważne wady bezpieczeństwa, wynikające np. ze złych procesów tworzenia oprogramowania w sprzęcie dostarczonym przez dostawcę, mogą ułatwić złośliwe działania. Prawdopodobnie pojawią się również nowe rodzaje luk technicznych, wpływające m.in. na systemy chmurowe oraz ich konfigurację. Podatności mogą dotyczyć też wycieków danych między środowiskami wirtualnymi lub segmentami sieci. Raport wskazuje **luki bezpieczeństwa, które mogą mieć szczególne znaczenie** w przyszłym środowisku 5G:

Dla wszystkich zainteresowanych stron	Dla operatorów sieci komórkowych
Brak wyspecjalizowanego personelu do zabezpieczenia i utrzymania sieci 5G.	Niewłaściwy projekt lub architektura sieci (brak mechanizmów awaryjnych i zapewnienia ciągłości, błędna konfiguracja, brak izolacji systemów niskiego zaufania).
Brak odpowiedniej wewnętrznej kontroli; błędy w zarządzaniu ryzykiem; brak systemów zarządzania bezpieczeństwem.	Słabe bezpieczeństwo fizyczne sieci i infrastruktury IT (niewystarczające zabezpieczenie personelu, sprzętu czy danych).
Brak lub nieodpowiednie procedury bezpieczeństwa oraz utrzymania sieci (aktualizacje i poprawki).	Słaba polityka lokalnego i zdalnego dostępu do komponentów sieci (wiele wirtualnych urządzeń ze zdalnym dostępem).

[7] NFV, czyli wirtualizacja funkcji sieciowych (Network Function Virtualization). Polega na odseparowaniu usług od wykorzystywanego sprzętu. Dotychczas oprogramowanie było zasadniczo ściśle związane ze sprzętem. MANO (Management and Orchestration), odpowiada za orkiestrację usług - orkiestracja może być zdefiniowana jako proces łączenia i koordynowania różnych elementów w spójną całość.

[8] Przetwarzanie, a także przechowywanie danych, będzie miało miejsce na urządzeniach końcowych, w kontrolerach lub mikrocentrach danych, które działają w pobliżu tych urządzeń, czyli na brzegu sieci.

Brak zgodności ze standardami 3GPP lub nieprawidłowe wdrożenie standardów.	Brak nacisku na wymogi bezpieczeństwa przy udzielaniu zamówień (np. wybór dostawców).

2. **Podatności specyficzne dla dostawców**

Większa rola dostawców zewnętrznych w sieciach 5G, sprawia, że konieczna jest **ocena profilu ryzyka poszczególnych dostawców**. Można ją przygotować na podstawie czynników:

- Prawdopodobieństwo, że dostawca będzie podlegać ingerencji ze strony państwa spoza UE (silny związek między dostawcą a rządem danego kraju trzeciego; brak umów o bezpieczeństwie lub ochronie danych między UE a danym krajem trzecim).
- Zdolność dostawcy do zapewnienia dostaw.
- Ogólna jakość produktów i dbałość dostawcy o cyberbezpieczeństwo.

3. **Podatności wynikające z zależności od poszczególnych dostawców**

Zależność od jednego dostawcy wpływa na brak różnorodności używanych urządzeń i rozwiązań. Na poziomie krajowym i europejskim może to doprowadzić do zwiększenia ogólnej wrażliwości infrastruktury 5G, zwłaszcza jeśli wielu operatorów będzie korzystać z usług dostawcy o wysokim poziomie ryzyka. Taki dostawca może znaleźć się pod presją handlową, ponieść komercyjną porażkę lub zostać objęty sankcjami. Ponadto ograniczona liczba dostawców może obniżyć ich motywację do opracowywania bezpieczniejszych produktów.

Scenariusze ryzyka

W raporcie zidentyfikowano ryzyka o znaczeniu strategicznym z perspektywy UE. Zostały one zilustrowane konkretnymi scenariuszami:

Ryzyko	Czynniki ryzyka	Scenariusz
Środki bezpieczeństwa	• źle zaprojektowane lub skonfigurowane systemy • słabe środki bezpieczeństwa i procedury • wysoki stopień złożoności sieci • brak specjalistów • decentralizacja sieci 5G • ryzyko nieautoryzowanego dostępu do ważnych systemów	• **Błędna konfiguracja sieci:** przeniknięcie do sieci i skompromitowanie jej bazowych funkcji. • **Brak kontroli dostępu:** podwykonawca z uprawnieniami administratora wykonuje działania niepożądane, prowadząc do naruszenia poufności, integralności lub dostępności.
Łańcuch dostaw 5G	○ **Sprzęt niskiej jakości** ○ stary sprzęt ○ słabe procesy inżynierii oprogramowania	○ **Niska jakość produktu:** podmioty państwowe lub wspierane przez państwo, wykorzystują do szpiegostwa

	○ słabe zarządzanie podatnościami ○ brak zgodności ze standardami 5G ○ brak standardowych funkcji bezpieczeństwa ○ **Zależność** ○ jeden dostawca ○ większe ryzyko wpływu awarii na systemy ○ kompatybilność wsteczna	złośliwe oprogramowanie, słabej jakości elementy sieci lub podatności. ○ **Zależność:** operator sieci mobilnej zamawia wrażliwe elementy sieci lub usługi od jednego dostawcy. Następnie dostawca zostaje obłożony sankcjami handlowymi. Spadek dostępności oferowanego sprzętu lub aktualizacji.
Sposób działania głównych aktorów zagrożeń	• kraje trzecie, które mogą wywierać presję na dostawców 5G • brak wystarczających zabezpieczeń i kontroli dostępu • niezamierzone luki w zabezpieczeniach lub celowo wprowadzone podatności • złośliwa działalność zorganizowanej przestępczości dla zysku	• **Ingerencja państwa w łańcuch dostaw 5G**: podmiot państwowy wywiera presję na dostawcę, aby zapewnić dostęp do wrażliwych zasobów sieci. • **Wykorzystywanie sieci 5G przez przestępczość zorganizowaną**: ○ zakłócenie różnych usług w sieci 5G, żeby wymusić okup. ○ phishing, oszustwa online, uzyskanie wrażliwych danych.
Zależności między sieciami 5G a innymi krytycznymi systemami	• współzależność systemów w obszarach krytycznych • podatności w infrastrukturze krytycznej, od której zależą sieci 5G (np. energetycznej) • brak mechanizmów awaryjnych i ciągłości działania • awaria dostawcy usługi (np. zasilanie) lub cyberatak na krytyczną infrastrukturę	**Znaczące zakłócenie infrastruktury krytycznej lub usług**: hakerzy przejmują kontrolę nad segmentem sieci wydzielonym dla służb ratunkowych. **Awaria sieci z powodu przerwy w dostawie energii elektrycznej lub innych systemów wsparcia**: klęska żywiołowa lub cyberatak na sieć energetyczną.
Urządzenia użytkowników końcowych	• wzrost liczby i różnorodności urządzeń IoT • zróżnicowany wymagany poziom bezpieczeństwa dla poszczególnych urządzeń • przeciążenie sieci	**Wykorzystanie IoT:** przejęcie kontroli nad urządzeniami o niskim poziomie bezpieczeństwa, takimi jak IoT (czujniki, urządzenia domowe itp.), aby zaatakować i przeciążyć sieć.

Podsumowanie

1. Sieć 5G będzie podstawą, na której oprze się wiele aspektów gospodarki oraz życia społecznego. Kluczowe będą jej **integralność**, **dostępność** oraz **poufność**.
2. **Unijna skoordynowana ocena ryzyka związanego z cyberbezpieczeństwem sieci 5G** powstała w październiku 2019 roku. Grupa Współpracy NIS przygotowała raport w oparciu o krajowe oceny ryzyka.
3. Raport opisuje szczególnie wrażliwe aktywa i zasoby sieci, wskazuje na jej możliwe podatności i słabe punkty, a także przedstawia przykładowe scenariusze ryzyka.
4. W sieci 5G szczególnie istotną rolę odgrywać będą operatorzy sieci komórkowych oraz producenci sprzętu telekomunikacyjnego. Sprawia to, że konieczna jest **ocena profilu ryzyka poszczególnych dostawców**.
5. Źródła zagrożenia: jako najbardziej znaczące wskazano zagrożenia ze strony **państw lub podmiotów wspieranych przez państwo**.
6. Zasoby i aktywa: za krytycznie wrażliwe uznano **funkcje bazowe sieci 5G** oraz **zarządzanie NFV** (wirtualizacja funkcji sieciowych) i **organizację sieci** (MANO).