aut. Andrzej Kozłowski 19.05.2020

CERTYFIKACJA JEST NIEWYSTARCZAJĄCA. POTRZEBUJEMY KOMPLEKSOWEGO PODEJŚCIA DO BEZPIECZEŃSTWA SIECI 5G [WYWIAD]

Konsekwencje przełamania sieci 5G będą o wiele groźniejsze niż miało to miejsce w przypadku poprzednich generacji sieci. Mówimy tutaj choćby o wypadkach samochodów autonomicznych – mówi Rene Summer dyrektor Government and Industry Relations w Ericsson Group. Ekspert w wywiadzie przedstawił również, podejście szwedzkiej firmy do bezpieczeństwa oraz przekonywał, dlaczego sama certyfikacja czy testowanie kodu to za mało, żeby zapewnić bezpieczeństwo sieci 5G.

Andrzej Kozłowski: Jakie czynniki decydują o tym, że cyberbezpieczeństwo stało się jednym z priorytetów przy wdrażaniu sieci 5G? Przy poprzednich generacjach, problem ten nie był aż tak istotny.

Rene Summer: Sieć 5G jest pierwszą generacją komunikacji mobilnej, która jest zaprojektowana z myślą o maszynach. Cofnijmy się w przeszłość. Przed nadejściem ery 2G ludzie używali telefonów stacjonarnych dzwoniąc do miejsc z nadzieją, że ktoś odbierze. Sieć 2G to zmieniła oferując możliwość dzwonienia do „ludzi" a nie do konkretnych „miejsc". Głównym wyzwaniem w obszarze bezpieczeństwa była tutaj ochrona prywatności osób uczestniczących w komunikacji i zabezpieczenie ich rozmów głosowych. 3G generacja sieci pozwoliła urządzeniom mobilnym na podłączenie się do Internetu w celu wykonywania prostych czynności takich jak przeglądanie stron internetowych czy komunikacji. Potem ewoluowało to do 4G, gdzie wykorzystywano telefony już do pełnego korzystania z zasobów globalnej sieci.

Sieć 5G od samego początku opracowywana była z myślą o maszynach i internecie rzeczy. Sieć nowej generacji zapewnia niskie opóźnienia, co pozwala maszynom na reakcję niemalże w czasie rzeczywistym i dostosowanie pracy do zmieniających się warunków.

Mówimy również o tym, że już niedługo do sieci masowo będą podłączane urządzenia IoT, które będą wykorzystywane w codziennych czynnościach. Wprowadzenie sieci 5G dla użytkowników prywatnych oraz masowe podłączanie urządzeń IoT do niej spowoduje, że sieć ta będzie odpowiedzialna za obsługę komunikacji interpersonalnej jak i funkcjonowanie usług i infrastruktury krytycznej w tym samym czasie.

Konsekwencją takiego stanu rzeczy będzie wzrost ryzyka i konieczność mitygowania go zarówno przez użytkowników, operatorów jak i regulatorów. Przykładowo, jeżeli mamy do czynienia z autonomicznymi samochodami to implikacje potencjalnego opóźnienia zobaczymy w świecie rzeczywistym, w postaci wypadku.

Ciągle obserwujemy zwiększająca się liczbę cyberataków. Są one coraz bardziej zaawansowane. Ta tendencja wzrostowa oraz poziom ich zaangażowania są elementami, które również muszą zostać

wzięte pod uwagę.

Z drugiej jednak strony złamanie zabezpieczeń sieci 5G będzie trudniejsze niż 4G czy 3G. Na czym trzeba się skupić przy zabezpieczeniu sieci 5G?

Każda sieć, niezależnie od tego czy mówimy o bezpieczeństwie 3G, 4G czy 5G składa się z czterech warstw. Pierwszą z nich, znajdującą się na samym dole są standardy, które określają cechy i wymogi bezpieczeństwa, które muszą być spełnione przez wszystkich. Druga warstwa to produkty, które są rozwinięte i dostarczone przez dostawców dla operatorów i muszą wykazywać się odpowiednim poziomem bezpieczeństwa. Mówimy tutaj o produktach dostarczonych przez jakiegokolwiek dostawcę - nie obejmujące tylko rdzeń sieci lub jego krawędzi, ale o każdym sprzęcie telekomunikacyjnym. Ich bezpieczeństwo musi być zgodne z opracowanymi, ogólnym standardami. Trzecia warstwa, czyli bezpieczeństwo konfiguracji sieci 5G jest osiągane m.in. poprzez odpowiednią konfigurację i wzmocnienie komponentów sieci. Gdy operator wybierze rozwiązanie innego dostawcy niż dotychczas, będzie musiał je wdrożyć i zintegrować z elementami starej infrastruktury lub nowej infrastruktury innego dostawcy.

Jest to związane z projektowaniem sieci oraz jej utwardzaniem. Kiedy te trzy warstwy sprawnie połączymy ze sobą, przechodzimy do czwartej, ostatniej czyli codziennych operacji w sieciach. Polega to na zarządzaniu na co dzień sieciami oraz wykonywaniem odpowiednich operacji bezpieczeństwa. Musimy pamiętać, że bezpieczeństwo nie jest statyczne i nie stoi w bezruchu. Te cztery warstwy są od siebie zależne i razem definiują bezpieczeństwo sieci.

Sieć i jej bezpieczeństwo powiązane jest z urządzeniami, które są do niej przyłączone. Z punktu widzenia sieci RAN (Radio Access Network), będą to smartfony czy urządzenia IoT. Bezpieczeństwo Internetu Rzeczy ma również konsekwencje dla bezpieczeństwa samej sieci. Dlatego na pewno możemy mówić o pewnej zależności. Patrząc na produkty IoT widzimy różnice w chipsecie, systemach operacyjnych i przede wszystkim poświadczeniach bezpieczeństwa danego urządzenia co również ma duże znaczenie.

Istnieje jednak znacząca różnica, jeśli chodzi o bezpieczeństwo smartfonu i urządzenia IoT. Użytkownik końcowy smartfona dba o bezpieczeństwo operacyjne każdego dnia i będzie w stanie zauważyć, że ten dziwnie się zachowuje. W przypadku IoT nie będzie to takie proste, żeby stwierdzić, że zabezpieczenia urządzenia zostały przełamane czy nie, w szczególności, jeśli są one częścią innych procesów.

Ustanowienie standardu w 3GPP jest procesem wielostronnym, do którego może przyłączyć się każdy, zazwyczaj uczestniczą w nim operatorzy, dostawcy sprzętu, telefonów i chipsetów oraz regionalne organy normalizacyjne. Ericsson podobnie jak inni dostawy jest odpowiedzialny za swoje produkty. Jako dostawca kontrolujemy rozwój naszych produktów – od zastosowanego hardware po software. Jeśli chodzi o projektowanie sieci i ich konfigurację to główne zadanie spoczywa na barkach operatorów, którzy je kontrolują oraz podejmują decyzję o inwestycjach. W ich gestii leży stworzenie odpowiednich zasad i wymagań bezpieczeństwa, zgodnych z przyjętym prawem krajowym, do których jako dostawcy sprzętu musimy się dopasować. Bezpieczeństwo operacyjne jest również pod kontrolą operatorów i jako dostawcy musimy sprostać określonym wymaganiom.

Jakie mogą byś konsekwencje przełamania zabezpieczenia sieci 5G?

Mamy trzy główne elementy bezpieczeństwa, które są najczęściej określane jako tzw. trójkąt CIA (dostępność, integralność i poufność – przyp. red. Nie możemy jednak też zapominać o kwestiach prywatności, które w pewnym zakresie pokrywają się z bezpieczeństwem. Prywatność jest jednak traktowana jako dodatek do tych trzech elementów.

Skupmy się jednak na trzech aspektach bezpieczeństwa. Z punktu widzenia bezpieczeństwa sieci oraz regulatorów, najważniejsza była zawsze dostępność oraz integralność sieci. Stale dostępna musi być możliwość komunikacji choćby dla funkcjonowania numerów alarmowych - sieć musi być dostępna. To była fundamentalna kwestia dla większości operatorów przez długi okres czas.

Drugi aspekt bezpieczeństwa, który od zawsze był bardzo istotny dla przemysłu to integralność, która polega na tym, że sieć funkcjonuje tak jak została do tego zaprojektowana. Patrząc na przykłady to ja nie widzę konkretnego powodu, dla którego atakujący miałby ją wyłączać (tzw. availability attack). Prędzej będzie chciał dokonać pewnych zmian w funkcjach, które potrzebują np. odpowiedź uzyskiwana w przeciągu 5 milisekund, zostanie intencjonalnie zmieniona na 1 sekundę. Przykładowo, w przypadku samochodów autonomicznych taka modyfikacja może doprowadzić do kraksy. Stanowiłoby to atak na integralność.

Integralność 5G będzie miała o wiele większe znaczenie niż w sieciach poprzedniej generacji. 10 - 15 lat temu jak używaliśmy telefonów komórkowych i nie mieliśmy zasięgu, szukaliśmy go, żeby zadzwonić. W tym sensie, doświadczaliśmy braku dostępności usługi, ale konsekwencje były takie, że po prostu czekaliśmy aż będziemy mieli zasięg, co umożliwi wykonanie połączenia lub surfowanie w Internecie. Czy taka sytuacja jest możliwe, kiedy mamy różne typy maszyn i aplikacji, których funkcjonowanie zależy na ciągłym podłączeniu do sieci?

Sieć 5G ma zapewnić korzyści w zakresie bezpieczeństwa, takie jak np. szyfrowanie interfejsu radiowego w celu ochrony poufności komunikacji

Atak na poufność polega na naruszeniu komunikacji pomiędzy użytkownikami końcowymi i w tym przypadku np. 5G oferuje szyfrowanie przez interfejs radiowy (słuchawka - radiowa stacja bazowa), co oznacza znaczną poprawę w stosunku do wcześniejszych generacji urządzeń mobilnych.

Jeśli zobaczymy jak obecnie zbudowane są sieci to sytuacja kompletnego ich załamania jest bardzo rzadko spotykana. Nie można wykluczyć sytuacji, że część sieci przestaje czasowo pracować albo jej integralność jest zmieniona. Nie można też zapomnieć o atakach na poufność komunikacji. Z perspektywy historycznej ataki na poufność w sieciach 3G i 4G były często utożsamiane z naruszeniem prywatności. Większość treści, która przechodziła przez sieci telekomunikacyjne to były rozmowy telefoniczne i wiadomości wymieniane między użytkownikami. W przypadku 5G mówimy o kradzieży informacji o znaczeniu strategicznym dla konkretnego sektora gospodarczego. Ryzyko dla poufności również się zmienia, dlatego 5G będzie musiało zmierzyć się z większą ilością problemów bezpieczeństwa. To szersze spektrum problemów bezpieczeństwa jest w wielu miejscach krytyczne, ponieważ bezpieczeństwo wielu sektorów będzie zależało od odpowiedniej ochrony przed cyberatakami.

Ericsson jest częścią ekosystemu cyberbezpieczeństwa sieci 5G. Jaka jest jego odpowiedzialność w tym obszarze?

Patrząc na cztery warstwy, które wymieniłem, Ericsson jako dostawca jest przede wszystkim odpowiedzialny za drugą z nich, czyli bezpieczeństwo produktów, które projektuje i rozwija. Musimy być pewni, że spełniamy konkretne standardy, posiadamy odpowiednie zdolności oraz rozwiązania z obszaru cyberbezpieczeństwa, które zapewniają odpowiedni poziom ochrony. Normy te rozwijane są w środowisku złożonym z wielu podmiotów, głównie w ramach organizacji 3rd Generation Partnership Project (3GPP). Na rzecz poprawy bezpieczeństwa pracują tam operatorzy oraz dostawcy. Rządy też są mile widziane, jeśli tylko uważają, że poziom bezpieczeństwa standardów musi zostać podniesiony, to ich reprezentanci powinni wziąć udział w dyskusjach oraz zaproponować konkretne rozwiązania.

Pewne wymagania bezpieczeństwa nie muszą być oficjalnie standaryzowane. Musimy zadać sobie

pytanie, które z nich muszą zostać ustanawiane jako obowiązkowe normy do wprowadzenia w sieciach operatorów oraz ustanowić te obszary, które są dobrowolne. Ustanowienie odpowiedniego balansu powinno być przedmiotem dyskusji.

Mamy również dyskusje wśród dostawców, że nie będziemy certyfikować tylko produktów, ale również proces rozwojowy. Przykładowo, Ericsson wdrożył w ścieżkę implementacji swoich produktów koncepcję security by design oraz privacy by design. Chcemy umożliwić niezależnym podmioty możliwość weryfikacji.

Wspomniał Pan o 5G toolbox UE. Jakie jest podejście Ericssona do tego nowego rozwiązania Komisji Europejskiej?

ToolBox proponuje około 20 różnych sposób zmniejszania ryzyka, które zostały uzgodnione przez państwa członkowskie. Jest to odpowiedź na analizę ryzyka przeprowadzoną przez państwa członkowskie dla ekosystemu bezpieczeństwa sieci 5G. Jeżeli na nią spojrzymy to widzimy na co zgodziły się państwa członkowskie, czyli jakie są główne zagrożenia. W tym kontekście, operatorzy i dostawcy muszą się dostosować do standardów, które zostały implementowane.

Największym pozytywem tego procesu jest, że toolbox podchodzi kompleksowo do bezpieczeństwa sieci 5G z perspektywy rozmieszczonej sieci. Mówimy o odpowiednich standardach, bezpieczeństwie produktów, projekcie sieci oraz operacjach. Jest to bardziej ważne dla ochrony użytkowników końcowych 5G, ponieważ bezpieczeństwo musi zacząć od ochrony wdrożonych sieci. Ostatecznie użytkownicy końcowi doświadczają bezpieczeństwa sieci w taki sam sposób, w jaki doświadczają zasięgu lub prędkości sieci, to właśnie wdrożona sieć określa ich wrażenia.

Początkowo problemem było, że oferowane rozwiązania w zakresie polityki bezpieczeństwa były sfragmentyzowane, w żaden sposób nie połączone ze sobą w jeden system. Jednym z takich elementów było bezpieczeństwo kodu źródłowego. Uznawano, że skoro go sprawdzono i wszystko jest ok, to na pewno nie ma żadnych problemów. Podejście Ericssona jest inne. Jeżeli chcemy chronić użytkownika końcowego to musimy zacząć od bezpieczeństwa wdrożonych sieci i musimy zrozumieć istotne dla bezpieczeństwa zależności wdrożonej sieci i urządzeń do niej podłączonych. Podobnie jak w ruchu drogowym nie powinniśmy myśleć o pojedynczych elementach jak np. niesprawnych elementach w samochodzie, ale patrzeć na problem kompleksowo - biorąc pod uwagę jakości dróg, sygnalizację świetlną, wdrożone przepisy, pracę policji, umiejętności kierowcy i stan jego trzeźwości.

Dzięki tej współzależności i stopniu skomplikowania mamy szansa na efektywne minimalizowanie ryzyka. Toolbox UE mówi, że wszechstronne podejście, rekomendowane krajom członkowskim, oznacza pełną implementację wszystkich środków, ponieważ to są elementy, które razem wzmacniają siebie nawzajem. Musimy też pamiętać, że proponowane narzędzia w ramach toolboxu 5G, zostały zaakceptowane przez wszystkie kraje członkowskie UE w celu ochrony użytkownika końcowego, ale nie wiemy jeszcze jak będzie wyglądało ich wdrożenie. To zadanie leży teraz w rękach władz krajów UE.

Rene Summer, dyrektor Government and Industry Relations w Ericsson Group