aut. Andrzej Kozłowski 27.01.2020

PROJEKT WYMOGÓW BEZPIECZEŃSTWA SIECI 5G OPUBLIKOWANY. NIE WYKLUCZONO ŻADNEGO PODMIOTU

Ministerstwo Cyfryzacji opublikowało długo wyczekiwany projekt rozporządzania dotyczącego bezpieczeństwa sieci i systemów telekomunikacyjnych, odnoszących się m.in. do budowy sieci 5G. Nie znajdziemy w nim informacji na temat wykluczenia jakiegokolwiek producenta, jednak resort rekomenduje stosowanie sprzętu od wielu producentów, tak żeby unikać uzależnia od jednego podmiotu.

Resort cyfryzacji opublikował projekt rozporządzanie ministra "w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewniania bezpieczeństwa lub integralności sieci lub usług". Przepisy te będą określały minimalne środki techniczne i organizacyjne oraz metody, które obejmą swoim zakresem ogólną działalność telekomunikacyjną.

Na mocy projektu rozporządzenia przedsiębiorstwa telekomunikacyjne będą musiały opracować i aktualizować dokumentację dotyczącą bezpieczeństwa i integralności sieci i usług. Będzie ona obejmować opis wszystkich przedsięwzięć podjętych w celu realizacji pozostałych środków. Ponadto będą zobowiązane do opracowania i aktualizacji wykazów infrastruktury telekomunikacyjnej i oprogramowania służącego do świadczenia usług telekomunikacyjnych, obejmujących ich rodzaj i konfigurację. Taki wykaz jest konieczny, jako punkt wyjścia do oceny, czy sieć jest podatna oraz czy wykorzystywany w niej sprzęt spełnia wymogi bezpieczeństwa.

Projekt dokumentu określa, że do obowiązków przedsiębiorstw ma należeć również identyfikacja zagrożeń, uwzględniając w szczególności długoterminowe analizy strategiczne cyberzagrożeń i incydentów w celu rozpoznania pojawiających się tendencji i w celu pomocy w zapobieganiu incydentom. Do identyfikacji ryzyka powinna zostać wykorzystana publikowana corocznie ENISA Threat Landspace. Przedsiębiorca musi również zapewnić monitorowanie i dokumentowanie funkcjonowania sieci i usług telekomunikacyjnych, których celem jest wykrywanie naruszeń bezpieczeństwa i ustalanie przyczyn takiego naruszenia.

Projekt rozporządzania nałoży również na przedsiębiorców telekomunikacyjnych obowiązek oceny prawdopodobieństwa wystąpienia oddziaływania zagrożeń oraz zapewni minimalne środki bezpieczeństwa. Zobowiązani będą również do ustanowienia zasad i procedur dostępu do kluczowych zasobów systemowych i przetwarzania danych oraz zabezpieczenia dostępu do kluczowych zasobów infrastruktury telekomunikacyjnej i będą musieli ten dostęp monitorować oraz wskazywać na środki reagowania na nieuprawniony dostęp lub jego próbę. Środki bezpieczeństwa muszą również dotyczyć zabezpieczenia danych poprzez ustanowienie zasad gwarantujących ich zdalne przetwarzanie oraz zastosowanie środków, które mają zmniejszyć ryzyko ich nieuprawnionego przetwarzania.

Środki bezpieczeństwa dotyczą również zawieranych umów. Dokument sugeruje, że w trakcie ich zawierania należy zidentyfikować zagrożenia z nimi związane. Jest to element tzw. bezpieczeństwa prawnego i rozszerzeniem potencjalnego ryzyka również na ten obszar.

Przedsiębiorcy muszą również sformułować procedury umożliwiające zgłaszanie naruszeń bezpieczeństwa lub integralności sieci lub usług. Stanowi to uzupełnienie obowiązku ustawowego z art. 175a prawa telekomunikacyjnego dotyczącego zgłaszania naruszeń.

Ostatni punkt dotyczy przeprowadzania okresowej oceny bezpieczeństwa sieci i usług telekomunikacyjnych, co najmniej raz na rok lub po każdym incydencie naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych o istotnym wpływie na ich funkcjonowanie. Nie musi to być pełen audyt i uwzględnia się możliwość przeprowadzania tego własnymi środkami przedsiębiorcy.

Z tego też powodu przedsiębiorstwa, które dostarczą sieć 5G będą musiały identyfikować zagrożenie, oceniać prawdopodobieństwo jego wystąpienia, zapewniać i stosować środki minimalizujące skutki wystąpienia zagrożeń. Rozporządzanie wskazuje na konieczność dostosowania się do rekomendacji Pełnomocnika Rządu ds. Cyberbezpiezpieczeństwa dotyczącego stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Nie oznaczają jednak one konieczności pozbycia się sprzętu z sieci.

Projekt rozporządzenia rekomenduje również unikanie uzależnienia od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług. Jest to zgodne z promowanym i sugerowanym przez Unię Europejską podejściem multi-vendor, którego celem jest uniknięcie uzależnienia od pojedynczego dostawcy. Rozporządzanie nie wskazuje jednak rekomendowanego procentowego udziału konkretnego sprzętu. Przedsiębiorcy telekomunikacyjni muszą również działać na rzecz podwyższenia odporności na zakłócenia sieci i usług. Projekt zamiast wskazywać na szczegółowe metody i redundancję sprzętu, podchodzi do tego kompleksowo i wskazuje konieczność podwyższenia odporności całej sieci.

Przedłożony projekt rozporządzenia w sprawie minimalnych środków technicznych i organizacyjnych dla przedsiębiorców telekomunikacyjnych stanowi wykonanie upoważnienia zawartego w art. 175d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. W uzasadnieniu decyzji czytamy, że upoważnienie to ma charakter fakultatywny i rozporządzenie takie dotychczas nie zostało wydane, jednakże rozwój w telekomunikacji nowych technologii wrażliwych na naruszenia bezpieczeństwa wskazuje na potrzebę wskazania minimalnych środków technicznych i organizacyjnych zapewniającą bezpieczeństwo sieci, świadczonych usług oraz przetwarzania danych. Wprowadzone rozwiązania mają na celu zmniejszenie poziomu ryzyka oraz zagwarantowanie ciągłości działania. Wraz z rozwojem technologii zwiększa się także liczba zagrożeń, które mogą wpłynąć na bezpieczeństwo i integralność sieci i usług telekomunikacyjnych, utrudniać życie obywatelom oraz niekorzystnie wpływać na sprawne funkcjonowanie państwa – czytamy w rozporządzaniu. W dokumencie podkreślono również, że projektowane przepisy rozporządzenia powinny być neutralne technologicznie, a zatem nie mogą podawać konkretnych rozwiązań, a jedynie wskazywać na cel zastosowania środków technicznych.

W obecnej sytuacji przedsiębiorcy telekomunikacyjni sami decydują, jakie rodzaje środków technicznych i organizacyjnych chcą zastosować, aby zapewnić bezpieczeństwo sieci i usług telekomunikacyjnych. Brakuje jednolitych standardów prawnych, które działając w interesie obywateli, obligowałyby przedsiębiorców telekomunikacyjnych do stosowania konkretnych rodzajów rozwiązań w zakresie bezpieczeństwa.