Cyberdefence 24

aut. Andrzej Kozłowski 16.09.2020

ROBERT KOŚLA: „NIE MOŻNA WYKLUCZYĆ, ŻE DOSTAWCY WYSOKIEGO RYZYKA BĘDĄ W POLSKICH SIECIACH"

„Kwestia dostawców wysokiego ryzyka była omawiana już od dłuższego czasu i dotyczy dostawców oprogramowania i sprzętu, ale również usług, które są wykorzystywane przede wszystkim przez podmioty KSC" - stwierdził Robert Kośla, dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji. Przedstawiciel resortu wyjaśnił dlaczego nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa koncentruje się na sektorze telekomunikacji oraz przedstawił w jaki sposób powinno się zwiększyć cyberbezpieczeństwo samorządów.

„Do tej pory ten sektor był poza krajowym systemem cyberbezpieczeństwa czyli informacje dotyczące dostępności chociażby usług telekomunikacyjnych czy incydentów w tym sektorze nie trafiały do CSIRTów poziomu krajowego, które odpowiadały za budowanie i analizę ryzyka na poziomie krajowym – stwierdził dyrektor Departamentu Cyberbezpieczeństwa objaśniając dlaczego nowelizacja ustawy o KSC koncentruje się w tak dużym stopniu na sektorze telekomunikacyjnym. „Operatorzy usług kluczowych, którzy w dużej części korzystają z usług telekomunikacyjnych do wymiany informacji nie dysponowali informacjami np. o incydentach" - dodał.

„Na operatorach usług kluczowych spoczywa obowiązek utrzymania usługi, która została zdefiniowana jako kluczowa. Do jej utrzymania niezbędne są elementy, które wspomagają system teleinformatyczny, czyli urządzenia, oprogramowanie i usługi. W związku z czym, żeby utrzymać usługę kluczową musimy dysponować rozwiązaniami technicznymi, które nie stwarzają dodatkowego ryzyka dla jej utrzymania" – podkreślił Kośla. „Kwestia dostawców wysokiego ryzyka była omawiana już od dłuższego czasu i dotyczy dostawców oprogramowania i sprzętu, ale również usług, które są wykorzystywane przede wszystkim przez podmioty KSC" - tłumaczy Dyrektor Departamentu Cyberbezpieczeństwa.

Kryteria techniczne - testy, badania i certyfikacja

Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa wprowadza kryteria techniczne, które muszą spełnić dostawcy. „Dostawcy wysokiego ryzyka będą definiowani na podstawie zarówno oceny aspektów technicznych, gdzie będziemy brali pod uwagę testy, badania i certyfikację. – podkreśla Kośla. „Polska wspólnie z Niemcami pracuje nad europejskim programem certyfikacji komponentów dla sieci 5G."

„Do tej porty na podstawie aktu o cyberbezpieczeństwie Unii Europejskiej rozpoczęły się prace na forum unijnym nad programem certyfikacji zgodnym z kryteriami Common Criteria. Jest to schemat, który umożliwia ocenę produktów teleinformatycznych, ale jest zdecydowanie mniej użyteczny przy ocenie komponentów telekomunikacyjnych, które są uwzględniane przy budowie sieci 5G. Takim uzupełnieniem jest program certyfikacji opracowany przez GSMA (stowarzyszenie branżowe firm

technologicznych - przyp. red.) system certyfikacji NESAS” – mówi Kośla. Dodaje jednak, „że ani sam NESAS ani Common Critera nie są wystarczające, dlatego pomysł jest taki, żeby połączyć te dwa schematy i uzupełnić je tymi elementami, która są istotne z punktu widzenia bezpiecznego wdrożenia sieci 5G. Nad tym pracujemy wspólnie z Niemcami” – podkreślił.

Kryteria polityczne - bezpieczeństwo łańcucha dostaw

Obok kryteriów technicznych, projekt nowelizacji ustawy o KSC wprowadził również tzw. kryteria polityczne. „Kwestie nietechniczne obejmują rzeczy związane z bezpieczeństwa łańcucha dostaw. Jeżeli mamy dostawcę, który nie jest w stanie zagwarantować ciągłości wykorzystania komponentów bezpiecznych tak jak mieliśmy to w ocenie brytyjskiej wobec jednego z chińskich podmiotów, który został uznany za dostawcę wysokiego ryzyka” – wyjaśnia Kośla. Tłumaczy, że „stało się to dlatego, że w związku z ograniczeniem możliwości dostępności procesów, które wykorzystywały amerykańskie licencje, ten dostawca nie był w stanie zagwarantować, że będzie w stanie dostarczać swoje produkty oparte i wykorzystujące komponenty, które dotychczas były badane i certyfikowane przez dedykowane centrum w Wielkiej Brytanii”.

Zapytany o to, które środki będą ważniejsze - technicznie czy nietechniczne, Kośla odpowiedział, że „będziemy oceniali najgorszy wariant". Kiedy mamy do czynienia z podmiotem, który jest uzależniony od rządu innego państwa, które prowadzi agresywne działania w stosunku do państw europejskich, to trudno nad takim faktem przejść do porządku dziennego” – dodaje. Dyrektor Departamentu Cyberbezpieczeństwa podkreślił, że „wszystkie te elementy będą brane pod uwagę - również informacje ze źródeł operacyjnych oraz analiza dotychczasowych zamiarów i działań, w które zaangażowany był dany podmiot, jak również państwo z którego pochodzi”. Kośla przypomniał, „że w NATO mówiliśmy już od dawna skąd mogą pochodzić komponenty, które są wykorzystywane w systemach niejawnych. Były ograniczenia w stosunku do podmiotów, które miały swoją siedzibę poza państwami NATO”.

Kośla komentując medialne doniesienia, że projekt nowelizacji doprowadzi do wykluczenia producentów sprzętu podkreślił, że „w ustawie o KSC nie ma mowy o wykluczaniu podmiotów, mowa jest o ocenie ryzyka ze strony dostawcy sprzętu lub oprogramowania. Nie można wykluczyć sytuacji, że dostawcy wysokiego ryzyka wciąż będą w polskich sieciach funkcjonować” - mówi Robert Kośla.

Dyrektor Departamentu Cyberbezpieczeństwa odniósł się również do tego jak z zabezpieczeniem sieci 5G poradzono sobie z Wielkiej Brytanii i Niemczech. „Nie możemy wykluczyć zastosowania pierwszego modelu brytyjskiego i tego że np. dostawca wysokiego ryzyka będzie mógł znaleźć się w sieciach w ograniczonym stopniu. Niemcy skonstruowały swoje przepisy w ten sposób, że wskazano krytyczne komponenty z punktu widzenia sieci 5G. Tamta ocena dotyczyła dostawców do budowy sieci 5G.” Kośla podkreśla, że ustawa o KSC dotyczy dowolnych dostawców i systemów z których korzystają podmioty KSC, czyli może to dotyczyć np. komputerów czy komputerów przenośnych, bądź serwerów wykorzystywanych w sektorze energii przez dostawców usług zasilania.” – wyjaśnia Kośla. Dodaje, że taka ocena będzie też prowadzona wobec dostawców tych komponentów od których zależy funkcjonowanie usług kluczowych.

„Cyberbezpieczny samorząd”

Robert Kośla mówił również o problemie zabezpieczenia samorządów w cyberprzestrzeni. Wskazał, że „cyberbezpieczeństwo jest grą zespołową i wszyscy muszą chcieć, żeby rzeczywiście podnieść poziom odporności na ataki, poziom ochrony informacji w systemach.” Dodaje, że „ministerstwo wychodzi z inicjatywami wykorzystania nowych technologii takich jak modele przetwarzania w chmurach obliczeniowych”. „W tej chwili mamy przygotowane rozwiązanie techniczne, które jednostkom samorządu terytorialnego, które nie chcą we własnym zakresie zabezpieczać usług informacyjnych dla

obywateli, umożliwia skorzystanie z platformy zabezpieczonej i skalowalnej przez administrację rządową”- kontynuował.

Dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji wyjaśnił również, skąd będą brane fundusze na podniesienie poziomu cyberbezpieczeństwa. Finansowanie dla zwiększenia bezpieczeństwa samorządów przewidujemy w ramach interwencji zarówno z funduszu odbudowy jak i Programu Operacyjnego Polska Cyfrowa z dedykowanej osi Cyberbezpieczeństwo, gdzie środki mają pójść na zakupy, wymianę infrastruktury i szkolenia” – wyjaśnia Kośla. Rozpoczęliśmy już kampanię „Cyberbezpieczny samorząd”, bo podnoszenie świadomości dotyczy nie tylko użytkowników, ale również decydentów w jednostkach samorządu terytorialnego. Muszą oni w odpowiedni sposób chronić dane, które przetwarzają w swoich systemach, bo od tych danych zależy funkcjonowanie obywateli” - zakończył Kośla.