aut. Andrzej Kozłowski 08.03.2021

KOŚLA O KSC: ZMIANY DOTYCZĄ IDENTYFIKACJI DOSTAWCÓW WYSOKIEGO RYZYKA

„Polecenie zabezpieczające w żadnym stopniu nie dotyczy blokowania treści w Internecie. To skrajnie nieprawidłowa interpretacja” - mówi Robert Kośla, dyrektor departamentu cyberbezpieczeństwa w Kancelarii Premiera Rady Ministrów. W rozmowie z ekspertem omówiliśmy kontrowersje związane z nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa (KSC).

Porównując obecną nowelizację ustawy o KSC z poprzednim projektem jakie są najważniejsze zmiany?

Najważniejsze zmiany dotyczą identyfikacji dostawców wysokiego ryzyka. Wcześniejsza propozycja dotyczyła kilkupoziomowego procesu oceny ryzyka dostawców sprzętu i oprogramowania. W nowej wersji projektu zaproponowana została procedura uznawania dostawców za dostawców wysokiego ryzyka w zakresie opiniowanych typów produktów, rodzajów usług i konkretnych procesów ICT wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa.

Ponadto, w pierwotnej wersji projektu postępowanie oceny ryzyka dostawców miało być prowadzone przez Kolegium ds. Cyberbezpieczeństwa. Związku z tym, że Kolegium jest organem opiniodawczo-doradczym i nie może wydawać decyzji zmieniony został tryb uznawania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. W aktualnej wersji projektu do postępowania będą stosowane przepisy Kodeksu postępowania administracyjnego, a organem prowadzącym postępowanie będzie minister właściwy do spraw informatyzacji. Poprzez zastosowanie trybu postępowania administracyjnego wprowadzamy większą jego transparentność.

Minister właściwy do spraw informatyzacji prowadzący postępowanie o uznanie dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka będzie zasięgał opinii Kolegium ds. Cyberbezpieczeństwa. Decyzja o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka będzie wydawana w przypadku, gdy z przeprowadzonego postępowania wyniknie, że dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi. Decyzja wraz z uzasadnieniem będzie mogła być zaskarżona do sądu administracyjnego. To jest główna różnica, jeżeli chodzi o proces uznawania dostawców sprzętu lub oprogramowania za dostawców wysokiego ryzyka dla Krajowego Systemu Cyberbezpieczeństwa.

Wniosek Przewodniczącego Kolegium ds. Cyberbezpieczeństwa o wszczęcie postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka będzie musiał zawierać nie tylko dane identyfikujące tego dostawcę, ale również wskazanie zakresu typów produktów, rodzajów usług lub konkretnych procesów ICT pochodzących od tego dostawcy. Do wniosku będzie musiała być dołączona opinia Kolegium w zakresie uznania tego dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka dla Krajowego Systemu Cyberbezpieczeństwa.

Procedura sporządzania opinii przez Kolegium ds. Cyberbezpieczeństwa będzie odgrywała bardzo ważną rolę. Będzie się ona składała, podobnie jak w pierwotnej wersji projektu, z kilku kroków. W pierwszym z nich Przewodniczący Kolegium powoła zespół w celu opracowania projektu opinii w sprawie uznania dostawcy za dostawcę wysokiego ryzyka. W skład tego zespołu wejdą przedstawiciele członków Kolegium wskazanych przez Przewodniczącego Kolegium. Następnie każdy członek Kolegium przygotuje stanowisko w obszarze swojej właściwości w oparciu o zakres analizy uwzgledniającej zarówno ryzyka o charakterze technicznym jak i pozatechnicznym. Opinia Kolegium będzie zawierała analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania, z uwzględnieniem informacji o zagrożeniach uzyskanych od państw członkowskich lub organów Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego. Analiza będzie dotyczyła przepisów prawa regulujących stosunki pomiędzy dostawcą a państwem spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego oraz praktyki stosowania prawa w tym zakresie, a także struktury własnościowej dostawcy sprzętu lub oprogramowania oraz zdolności ingerencji tego państwa w swobodę działalności gospodarczej tego dostawcy. Bardzo istotna będzie również analiza trybu, zakresu i rodzaju powiązań dostawcy sprzętu lub oprogramowania z podmiotami objętymi sankcjami unijnymi w związku ze zwalczaniem cyberataków zagrażających Unii lub jej państwom członkowskim. Z kolei w zakresie aspektów technicznych analiza obejmie zdolności dostawcy reagowania na incydenty oraz wykrywania i usuwania podatności w dostarczanym przez niego sprzęcie lub oprogramowaniu oraz rekomendacje wydane przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa na postawie badań podatności w urządzeniach i oprogramowaniu tego dostawcy. Pod uwagę przy sporządzaniu opinii będzie brane również bezpieczeństwo łańcucha dostaw urządzeń i oprogramowania tego dostawcy.

Nowym elementem przy formułowaniu opinii Kolegium będzie uwzględnienie certyfikatów w zakresie cyberbezpieczeństwa wydawanych lub uznawanych w państwach Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego.

Postępowanie o uznanie dostawcy urządzeń lub oprogramowania za dostawcę wysokiego ryzyka będzie mogło być prowadzone - tak jak już mówiłem - na wniosek Kolegium, albo z urzędu przez ministra właściwego ds. informatyzacji. Minister będzie mógł wszcząć postępowanie z urzędu jeżeli uzyska informacje od innego państwa członkowskiego NATO, bądź w ramach współpracy z państwami Unii Europejskiej , że dostawca stwarza wysokie ryzyko dla operatorów usług kluczowych np. w sektorze energii czy infrastruktury cyfrowej. Po wszczęciu postępowania z urzędu minister właściwy do spraw informatyzacji zwróci się do Kolegium o przygotowanie opinii – Kolegium przekaże opinię w terminie 3 miesięcy.

Decyzja o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka będzie publikowana w formie ogłoszenia w Dzienniku Urzędowym Monitor Polski, na stronie podmiotowej ministra w Biuletynie Informacji Publicznej, a także na stronie internetowej urzędu obsługującego ministra.

Jakie są konsekwencje tego, że jakiś podmiot zostanie uznany za dostawcę wysokiego ryzyka?

Decyzja podlega natychmiastowej wykonalności i jest wiążąca dla podmiotów krajowego systemu cyberbezpieczeństwa, przedsiębiorców telekomunikacyjnych obowiązanych posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej oraz przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym.

Natychmiastowa wykonalność decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka będzie uniemożliwiała tym podmiotom wprowadzanie przez nie do użytkowania produktów, usług i procesów objętych decyzją. Ponadto, podmioty te będą zobowiązane do wycofania z użytkowania nie później niż w ciągu 7 lat od wydania decyzji produktów, usług procesów nią objętych. W przypadku produktów, usług i procesów wskazanych w decyzji i określonych w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług, przedsiębiorcy telekomunikacyjni obowiązani posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń będą je wycofywać z użytkowania w terminie do 5 lat od wydania decyzji. Są to okresy, które mają umożliwić ewolucyjną wymianę w Krajowym Systemie Cyberbezpieczeństwa produktów, usług i procesów pochodzących od dostawcy, który został uznany za dostawcę wysokiego ryzyka.

A jeżeli producent sprzętu uznanego za dostawcę wysokiego ryzyka nie zgodzi się z tą decyzją. Jakie działania może podjąć?

Może zaskarżyć decyzję do sądu administracyjnego i wtedy, tak jak każdą inną decyzję administracyjną skargę rozpatruje sąd, który może decyzję ministra właściwego ds. informatyzacji potrzymać albo ją uchylić.

Czy te posiedzenia są jawne?

Sąd administracyjny rozpatruje skargę na decyzje o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka na posiedzeniu niejawnym. Odpis sentencji wyroku z uzasadnieniem doręczany będzie wyłącznie ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręczany będzie odpis wyroku z tą częścią uzasadnienia, która nie zawiera informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych.

Załóżmy, że mamy posiedzenie niejawne, to co ze stroną reprezentującą producenta, on jest obecny na tej rozprawie czy nie?

Zastosowanie mają przepisy ustawy o ochronie informacji niejawnych.

Jeżeli nie ma jednak dostępu do informacji niejawnej, to wtedy dostaje tylko decyzję sądu?

Jeżeli nie ma informacji niejawnych, to mamy normalne postępowanie administracyjne, także strona skarżąca wnieść zażalenie, zaskarżyć decyzję sądu w pierwszej instancji do Naczelnego Sądu Administracyjnego, potem przysługuje jej tryb odwoławczy od decyzji Naczelnego Sądu Administracyjnego, włącznie z Europejskim Trybunałem Sprawiedliwości i arbitrażem międzynarodowym.

Załóżmy, że sąd w Polsce zadecydował, że producent A jest dostawcą wysokiego ryzyka i odwołuje się on od tej decyzji do sądu w UE. W związku z tym powstaje pytanie czy wspomniane 5 lub 7 lat mierzy się od decyzji polskiego organu? A może UE?

Aktualna wersja projektu zawiera przepis mówiący o tym, że decyzja ma tryb natychmiastowej wykonalności, czyli termin 7 lub 5 lat liczy się od dnia opublikowania informacji o decyzji.

Jeżeli jednak sąd w Polsce stwierdza, że podmiot jest dostawcą wysokiego ryzyka i przestaje się sprzęt kupować, wdrażać, a sąd UE stwierdza inaczej? Czy planowane jest odszkodowanie dla tych podmiotów?

W kwestiach odszkodowań decyzje będą podejmowały sądy oraz arbitraż międzynarodowy.

Szwecja jest jedynym krajem, który wykluczyło dane podmioty z budowy sieci 5G. Czy

bierzecie przykład z tego państwa?

Szwecja zrobiła to inaczej - wykluczając dostawców w wymaganiach aukcyjnych, czyli szwedzki regulator PTS przygotowując wymagania aukcyjne wpisał wprost, że ze względu na bezpieczeństwo narodowe nie może być to sprzęt Huawei i ZTE. Urządzenia radiowe tych firm zostały uznane przez Szwedzkie Siły Zbrojne i Szwedzką Służbę Bezpieczeństwa jako zagrażające bezpieczeństwu. Ocena ofert aukcyjnych uwzględniająca proces konsultacji ze Szwedzkimi Siłami Zbrojnymi i Szwedzką Służbą Bezpieczeństwa była zgodna z przepisami, które weszły w życie 1 stycznia 2020 r. Decyzja regulatora została zaskarżona przez Huawei do sądu, ale ostatecznie sąd nie uchylił decyzji PTS.

Druga kontrowersyjna kwestia, która pojawiła się wokół nowelizacji ustawy o KSC to sprawa polecenia zabezpieczającego. W mediach krążą spekulacje, że w ten sposób KPRM będziecie wyłączać Internet w Polsce.

Polecenie zabezpieczające to kolejny przepis, który został zmieniony w stosunku do wrześniowej wersji projektu. Pierwotnie zakładano, że będzie ono wydawane przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa. Jednakże ze względu na większą transparentność został wprowadzony tryb postepowania administracyjnego, które z definicji musi być prowadzone przez organ, a Pełnomocnik ds. Cyberbezpieczeństwa nie jest organem. Dlatego też, podobnie jak w przypadku decyzji o uznaniu dostawcy urządzeń i oprogramowania za dostawcę wysokiego ryzyka, decyzję o poleceniu zabezpieczającym ma wydawać minister właściwy do spraw informatyzacji na wniosek Zespołu ds. Incydentów Krytycznych, którego pracom przewodniczy Dyrektor Rządowego Centrum Bezpieczeństwa. O ile ostrzeżenie może wydawać Pełnomocnik Rządu ds. Cyberbezpieczeństwa, to polecenie zabezpieczające w formie decyzji administracyjnej musi jako organ wydawać minister właściwy ds. informatyzacji.

Wracając do kontrowersji wokół ostrzeżeń i poleceń zabezpieczających to chciałbym zaznaczyć, że te nowe instrumenty stosowane są tylko wyłącznie w sytuacji incydentu krytycznego. Jego definicja znajduje się w aktualnie obowiązujących przepisach ustawy. Przypomnę, że incydent krytyczny to incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV.

Żeby minister do spraw informatyzacji mógł wydać decyzję o poleceniu zabezpieczającym niezbędne jest najpierw sklasyfikowanie aktualnie trwającego incydentu jako incydentu krytycznego przez któryś z zespołów CSIRT poziomu krajowego. Wyobraźmy sobie sytuację, w której trwa równoległy atak na sektor energii, transportu i ochrony zdrowia. Najpierw właściwy zespół CSIRT GOV, CSIRT MON lub CSIRT NASK dokona analizy czy rzeczywiście atak ten można uznać za incydent krytyczny i zawnioskuje o zwołanie Zespołu ds. Incydentów Krytycznych. Ponadto wydanie polecenia zabezpieczającego musi uzasadniać wynik analizy przeprowadzonej przez ministra do spraw informatyzacji we współpracy z Zespołem ds. Incydentów Krytycznych. Analiza ta musi uwzględniać istotność cyberzagrożenia, przewidywane skutki incydentu krytycznego, rodzaje ryzyk oraz, co bardzo istotne, skutki finansowe, społeczne i prawne wydania polecenia zabezpieczającego. Ta analiza będzie musiała być włączana do akt sprawy.

Minister do spraw informatyzacji będzie wydawał polecenie zabezpieczające drodze decyzji administracyjnej na czas koordynacji obsługi incydentu krytycznego, nie dłużej niż na dwa lata, a informację o wydaniu i treści polecenia zabezpieczającego będzie publikował w Dzienniku Urzędowym ministra właściwego do spraw informatyzacji, na stronie podmiotowej ministra w Biuletynie Informacji Publicznej, a także na stronie internetowej urzędu obsługującego ministra.

Polecenie zabezpieczające będzie podlegało natychmiastowej wykonalności. Będzie ono zawierało wskazanie rodzajów podmiotów Krajowego Systemu Cyberbezpieczeństwa których dotyczy, wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu się, datę wejścia w życie oraz uzasadnienie zawierające wyniki analizy przeprowadzonej przez ministra właściwego do spraw informatyzacji we współpracy z Zespołem ds. Incydentów Krytycznych.

To co budziło niezrozumiałe kontrowersje to katalog określonych zachowań, które mogą być nakazane podmiotom Krajowego Systemu Cyberbezpieczeństwa w decyzji o poleceniu zabezpieczającym. Katalog zawiera 10 zachowań takich jak nakaz przeprowadzenia szacowania ryzyka; przegląd planów ciągłości działania i planów odtworzenia działalności; polecenie zastosowania określonej poprawki bezpieczeństwa; nakaz szczególnej konfiguracji sprzętu lub oprogramowania , zabezpieczającej przed wykorzystaniem określonej podatności; polecenie wzmożonego monitorowania zachowania systemu; zakaz korzystania z określonego sprzętu lub oprogramowania; nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania; zabezpieczenie określonych informacji, w tym dzienników systemowych czy wytworzenie obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem.

W przestrzeni medialnej pojawiła się całkowicie błędna interpretacja pkt. 7) który sformułowany był jako „nakaz wprowadzenia reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL". Interpretowano ten punkt niezależnie od zakresu podmiotowego i przedmiotowego ustawy o krajowym systemie cyberbezpieczeństwa, którego głównym celem jest zapewnienie bezpieczeństwa usługom kluczowym i usługom publicznym. Przypominam, że bezpieczeństwo to nie tylko poufność czy integralność, ale również dostępność. Punkt ten odnosił się do konieczności ograniczenia złośliwego ruchu sieciowego, który wchodząc do infrastruktury podmiotu krajowego systemu cyberbezpieczeństwa powoduje incydent krytyczny, zakłócając usługi kluczowe i publiczne – nie ma tu mowy o jakimkolwiek blokowaniu funkcjonowania sieci Internet lub ograniczaniu dostępu do treści publicznie dostępnych.

Po dodatkowych konsultacjach zaproponowaliśmy inne brzmienie tego punktu bardziej precyzyjnie określające zakres niezbędnych działań ograniczających skutki trwającego incydentu krytycznego. Nowe brzmienie tego punktu to „nakaz wprowadzenia ograniczenia ruchu sieciowego z adresów IP lub adresów URL wchodzącego do infrastruktury podmiotu *(krajowego systemu cyberbezpieczeństwa)*, który skutkując zakłóceniem usług świadczonych przez ten podmiot został sklasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV jako przyczyna trwającego incydentu krytycznego".

Chciałbym podkreślić, że polecenie zabezpieczające jest wprowadzane jako środek wymuszający pilne i skuteczne działania w sytuacji najpoważniejszych incydentów – incydentów krytycznych. Mówiąc o incydentach krytycznych należy zauważyć, że żaden z incydentów zaobserwowanych i zgłoszonych do zespołów CSIRT GOV, CSIRT MON i CSIRT NASK od chwili obowiązywania ustawy o krajowym systemie cyberbezpieczeństwa – czyli od sierpnia 2018 roku – nie został sklasyfikowany jako incydent krytyczny. To, że takich incydentów nie odnotowaliśmy nie znaczy, że nigdy nie będą miały miejsca i musimy się przygotować na szybkie i skuteczne reagowanie, aby ograniczyć ich krytyczne skutki.

Przykładowo, w sytuacji wystąpienia incydentu na skalę SolarWinds w Polsce mogłaby zaistnieć przesłanka (oczywiście jeżeli wskazywałaby to analiza przeprowadzona przez zespoły CSIRT w ramach Zespołu ds. Incydentów Krytycznych) do wydania polecenia zabezpieczającego. W takim przypadku polecenie zabezpieczające mogłoby zawierać zakaz korzystania z zainfekowanej wersji biblioteki Orion i polecenie zastosowania określonej poprawki bezpieczeństwa w sprzęcie lub oprogramowaniu.
wskazywałoby, że z tej biblioteki nie można korzystać i trzeba ją wyłączyć z eksploatacji.

Wracając do praktyki funkcjonowania Krajowego Systemu Cyberbezpieczeństwa chciałbym przypomnieć, że rekomendacje wprowadzania dodatkowych reguł monitorowania ruchu oraz

ograniczania ruchu wchodzącego z adresów sieciowych zidentyfikowanych jako źródła ataków są rutynowo przekazywane do podmiotów krajowego systemu cyberbezpieczeństwa od chwili wejścia w życie ustawy ponad 2 i pół roku temu. W szczególności dotyczy to sytuacji kiedy podnoszony jest stopień alarmowy CRP. Przykładowo CSIRT GOV ma informacje, że z określonych adresów sieciowych przygotowywane są ataki typu DDoS, wówczas rekomendowane jest skonfigurowanie zabezpieczeń brzegowych z siecią Internet tak, aby zapewnić filtrowanie i nieprowadzenie komunikacji z tym adresami. To jest rutynowe działanie, które nigdy nie powodowało blokowania Internetu lub ograniczania dostępu do publicznych treści dla indywidualnych użytkowników. W uproszczeniu, to tak jakby zamknąć drzwi i nie wpuścić kogoś niepożądanego, co nie znaczy, że blokujemy jego ruch na zewnątrz czy ograniczamy jego wolność poza naszym domem, który przecież mamy prawo chronić przez intruzami...