Cyberdefence 24

aut. Ireneusz Piecuch 17.09.2020

PROJEKT NOWELIZACJI USTAWY O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA: LEKARSTWO GORSZE OD CHOROBY? [OPINIA]

Projekt nowelizacji spowoduje, że ciało polityczne jakim jest Kolegium ds. Cyberbezpieczeństwa otrzyma uprawnienia do nakładania embarga (bez jakiejkolwiek kontroli sądowej) na konkretne firmy uznane za „ryzykowne" - przestrzega Ireneusz Piecuch przed negatywnymi skutkami projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa.

Od przyjęcia dyrektywy 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii minęło już ponad 4 lata. Od jej włączenia do polskiego porządku prawnego poprzez uchwalenie ustawy o Krajowym Systemie Cyberbezpieczeństwa ponad 2 lata. Od samego początku wydawało się, że ta implementacja nie będzie prosta. Trzy osobne CSIRT-y, zespoły sektorowe, Pełnomocnik Rządu i Kolegium o nie zawsze klarownych kompetencjach, nie do końca jasne kryteria kwalifikacji na operatorów usług kluczowych. A najgorsze w tym wszystkim było to, że zarówno ustawa jak i jej uzasadnienie bardzo lakonicznie potraktowała dwa kluczowe warunki sukcesu: budżet i dostęp do wysoko wykwalifikowanych specjalistów. Ale, jak głosił konsensus, pod którym i ja się podpisywałem, największą wartością tej ustawy było to, że w końcu się pojawiła nadając cyberbezpieczeństwu legislacyjne obywatelstwo. I faktycznie wydaje się, że z punktu widzenia jakości procesu wdrożenia KSC, przez ostatnie dwa lata nie osiągnęliśmy oszałamiającego sukcesu. Proces decyzji wyznaczających operatorów usług kluczowych nie został zakończony. Sektorowe zespoły cyberbezpieczeństwa nie były powoływane. Zabrakło wykwalifikowanych specjalistów oraz szerszej współpracy sektora publicznego i prywatnego. Tyle przynajmniej można wyczytać z uzasadnienia dużej nowelizacji ustawy o KSC skierowanej właśnie do tak jakby konsultacji, bo 14 dni trudno uznać za poważny termin przy takim zakresie proponowanych zmian.

Niestety kierunek proponowanych zmian może doprowadzić do tego, że za kolejne dwa lata czekać nas będzie kolejna duża zmiana. Powołanie CSIRT Telco odpowiedzialnego za wsparcie sektora komunikacji elektronicznej, CISRT-ów sektorowych, SOC-ów przypomina trochę sytuację leczenia „klina klinem". Brak ekspertów, zespoły nie są powoływane? To zamiast 3 CESIRT-ów zrobimy kilkanaście a do tego jeszcze dodamy obowiązkowe SOC-i. Nie wydaliśmy wszystkich decyzji wyznaczających operatorów usługi kluczowej to do podmiotów objętych ustawa dorzucimy jeszcze przedsiębiorców komunikacji elektronicznej. To nic, że Dyrektywa NIS wyłącza tę grupę podmiotów (oczywiście, są też argumenty za i sam je wielokrotnie wskazywałem, ale wtedy warto byłoby to zsynchronizować ze zmianami w projekcie Prawa Komunikacji Elektronicznej tak, żeby nie tworzyć w tej mierze legislacyjnych dysonansów). A kto za to wszystko zapłaci? Zgodnie z uzasadnieniem projektu – jeśli dobrze odczytałem intencję autorów projektu - najpierw uchwalamy zmiany - budżetem zajmiemy się później. Ustawa przewiduje co prawda zwiększenie wydatków na

informatyzację, ale dopiero od 2022 roku.

Punktem kulminacyjnym proponowanych zmian jest jednak art.66a. Otóż Kolegium ds. cyberbezpieczeństwa może sporządzić ocenę „ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa". Skutek? Zakaz „wprowadzania do użytkowania" (cokolwiek to nie oznacza) i obowiązek wycofania produktów i usług określonych w ocenie w ciągu 5 lat. Od oceny Kolegium można się odwołać do … Kolegium. I to jedyne prawo, które ma dostawca sprzętu lub oprogramowania uznany za „wysoce ryzykownego". Warto przypomnieć, że Kolegium to w istocie taki mini-rząd. Premier jako przewodniczący, Pełnomocnik Rządu ds. Cyberbezpieczeństwa, kilku ministrów. Innymi słowy ciało jak najbardziej polityczne otrzyma uprawnienia do nakładania embarga (bez jakiejkolwiek kontroli sądowej) na konkretne firmy uznane za „ryzykowne".

Ktoś powie – tak trzeba, bo cyberbezpieczeństwo jest wartością nadrzędną. Cóż mam nadzieję, że taki argument padnie. Bo będzie to ten moment, kiedy będziemy mogli podyskutować co tak naprawdę zostało zrobione przez ostatnie lata aby teza ta okazała się prawdziwa. W jaki sposób kształcimy rzesze specjalistów w nowych dziedzinach związanych z cyberbezpieczeństwem? Jakie zalecenia wprowadziliśmy dla sektora publicznego, aby upewnić się, że w ramach przeprowadzanych zamówień publicznych budujemy łańcuch cyberbezpieczeństwa obejmujący wszystkie elementy wymagane dla zapewnienia najwyższego stopnia odporności budowanych systemów informatycznych? Jak wygląda system finansowania przez Państwo wszystkich tych działań? Jak wykorzystujemy zasoby sektora prywatnego i jak wygląda współpraca w tej mierze?

Niezależnie od odpowiedzi na te pytania, pojawia się też kolejna wątpliwość. Jeżeli ryzyko jest tak duże, że wymaga nałożenia embargo na danego dostawcę, to przykładowo, jak maja sobie radzić operatorzy telekomunikacyjni którzy muszą w ciągu 5 lat wymienić część swojej sieci? Czy abonenci nie przejdą do innej sieci – bezpieczniejszej zdaniem Kolegium? A kto pokryje koszty takiej operacji? Państwo (czytaj my)? Projekt na to nie wskazuje. Operatorzy? Ale mówimy przecież o setkach milionów a niekiedy o miliardach złotych?

Cyberbezpieczeństwo jest wyzwaniem nie tylko dla nas – użytkowników, przedsiębiorców narażonych na paraliż ich działalności i kradzież danych, ale także dla rządów, które muszą dbać o bezpieczeństwo wszystkich elementów krytycznych z punktu widzenia funkcjonowania państwa. To zrozumiałe. Dobrze zatem, że powstają ustawy i rozporządzenia tworzące narzędzia niezbędne dla zapewnienia właściwego poziomu ochrony. Dobrze, że staramy się włączyć Polskę, w system cyberbezpieczeństwa UE. Mam jednak poważne wątpliwości czy aby skupianie się niemal wyłącznie na legislacji i wytyczaniu różnego rodzaju „ścieżek na skróty" nie okaże się lekarstwem gorszym niż sama choroba.