Prawda o Krajowym Systemie Cyberbezpieczeństwa: jak nowelizacja ustawy wzmocni polskie bezpieczeństwo cyfrowe

CYFROWA POLSKA

Autorzy:
eksperci Związku Cyfrowa Polska

Projekt nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) oraz niektórych innych ustaw stał się przedmiotem szerokiej debaty publicznej. To naturalne, biorąc pod uwagę jego kluczowe znaczenie dla bezpieczeństwa narodowego Polski – jednego z najczęściej atakowanych cyfrowo państw w Europie – oraz fakt, że planowane przepisy będą miały bezpośredni wpływ na szerokie grono podmiotów z sektora publicznego i prywatnego.

Złożoność i waga tego projektu sprawiają jednak, że w przestrzeni publicznej pojawia się wiele nieporozumień, uproszczeń i mitów, które mogą prowadzić do błędnych ocen proponowanych rozwiązań. Celem niniejszego opracowania jest rzeczowe wyjaśnienie najczęściej powielanych w debacie publicznej nieprawdziwych narracji dotyczących nowelizacji KSC oraz przedstawienie faktów i realnych skutków proponowanych zmian dla polskiego systemu cyberbezpieczeństwa.

MIT 1

„Projektowane przepisy dotyczące Dostawców Wysokiego Ryzyka (DWR) wykraczają poza ramy prawa unijnego i stanowią przejaw przeregulowania, niespotykany w innych państwach. Projekt przewiduje rozwiązania zupełnie nowe, niespotykane wcześniej w państwach UE".

W rzeczywistości w większości państw Unii Europejskiej wprowadzone zostały przepisy umożliwiające wyłączenie z budowy sieci 5G dostawcy uznanego za potencjalne zagrożenie dla bezpieczeństwa narodowego. Przepisy dotyczące DWR obowiązują też w wielu państwach spoza UE. Inne kraje, które podjęły działania w obszarze DWR to m.in. Estonia, Rumunia, Portugalia, Francja, Szwecja, Norwegia, Dania, Litwa, ale także Wielka Brytania. Co ważne, Projektodawca dokonał analizy porównawczej rozwiązań prawno-organizacyjnych i mechanizmów zaimplementowanych lub zaproponowanych w innych państwach, a wyniki tej analizy zostały zaprezentowane w aneksie do Oceny Skutków Regulacji. Minęło pięć lat odkąd unijny zestaw narzędzi na rzecz bezpieczeństwa sieci 5G, tzw. 5G Toolbox obowiązuje w UE. Polska jest jednym z ostatnich krajów pod względem implementacji jego założeń. Projektowane przepisy stanowić będą zatem także element harmonizacji z istniejącym w pozostałych państwach członkowskich prawem.

MIT 2

"Decyzja o uznaniu podmiotu za DWR będzie zapadać arbitralnie i podejmowana będzie w oparciu o motywy polityczne, a kryteria identyfikacji DWR wydają się dyskryminujące, niejasne i mogą nieproporcjonalnie dotknąć podmioty spoza UE lub NATO, niezależnie od ich dotychczasowego dorobku lub zaangażowania w bezpieczeństwo".

W myśl projektu o statusie DWR nie będą decydować "decyzje polityczne". Tzw. "przesłanki nietechniczne" z zakresu uznania podmiotu za DWR wynikają wprost właśnie z unijnego 5G Toolbox i są obecnie standardem w państwach członkowskich UE. Co więcej, procedura uznania podmiotu za DWR jest szczegółowo i transparentnie opisana w projekcie. Przejrzystość tego procesu w polskim projekcie jest wysoka na tle standardu innych państw UE. Postępowanie w tej sprawie nie ma nic wspólnego z arbitralną decyzją Ministra Cyfryzacji. Ta podejmowana będzie w oparciu o opinię całego kolegium podmiotów, w skład którego wchodzą m.in. służby i UOKIK, a o pracach którego informowany jest prokurator generalny. Proces dotyczy bardzo konkretnych procedur i powstaje, by uporządkować kwestie związane z cyberbezpieczeństwem i ma na celu wyłącznie nadanie techniczno-formalnego porządku tak istotnemu obszarowi. Co ważne, wszystkie podmioty podlegać będą tej samej transparentnej procedurze, bez względu na ich pochodzenie, a od decyzji przysługiwać ma możliwość skargi do sądu administracyjnego.

MIT 3

“Sprzęt niezbędny do wymiany infrastruktury jest trudno lub zupełnie niedostępny”.

Twierdzenie takie nie znajduje pokrycia w doświadczeniach dostawców oraz przebiegu takiego procesu w innych państwach. Z doświadczenia dostawców wynika, że prowadzone w innych państwach UE procedury wymiany infrastruktury na szeroką skalę trwają mniej niż 4 lata. Sama produkcja niezbędnych elementów infrastruktury sieciowej w Polsce pozwoliłaby na wymianę sprzętu w kraju w ciągu 4 lat.

MIT 4

“Czas na wymianę sprzętu jest zbyt krótki. Wymiana jest też dodatkowym kosztem”.

Oczywiście wycofanie sprzętu, szczególnie jeśli odbywa się na dużą skalę, to skomplikowany proces. Wymiana sprzętu (infrastruktury IT) nie jest jednak zjawiskiem nadzwyczajnym. Urządzenia sieciowe regularnie podlegają modernizacji i wymianom, co wynika z cyklu życia produktów, zmian technologicznych i oczekiwań klientów. Pamiętać należy również, że w tym przypadku mówimy o kwestiach bezpieczeństwa narodowego i gospodarczego kraju. Sieci 5G stają się podstawą cyfrowej gospodarki, której bezpieczeństwo zależeć będzie od najsłabszego ogniwa sieci. Z tej perspektywy to najsłabsze ogniwo może stać się elementem krytycznym, niezależnie gdzie jest zlokalizowane. W przypadku uznania, że dostawca infrastruktury nie jest godny zaufania, podjąć należy możliwie najszybsze działania na rzecz wymiany dostarczanych przez niego elementów i produktów. Cyberbezpieczeństwo nie może czekać, szczególnie, gdy na szali są procesy o znaczeniu krytycznym.

MIT 5

“Wymiana infrastruktury podchodzącej od potencjalnych DWR spowoduje wzrost kosztów dla konsumentów korzystających z sieci”.

Nic nie wskazuje na wzrost kosztów dla konsumentów na rynku telefonii komórkowej, czy pogorszenie jakości usług telekomunikacyjnych w związku z procesem wymiany infrastruktury (ponownie, będącej normalną, cykliczną praktyką rynkową). Przeciwnie, wymiana infrastruktury prowadzi na ogół do poprawy jakości świadczonych konsumentom usług sieciowych.

MIT 6

“Małe i średnie przedsiębiorstwa poniosą znaczne koszty w związku z nowymi przepisami”.

Trudno jednoznacznie oszacować koszty, które miałyby ponieść podmioty objęte zapisami nowej UKSC. Zależeć będą one oczywiście od rozmiaru przedsiębiorstwa i rozległości stosowanej infrastruktury sieciowej. Z punktu widzenia bezpieczeństwa narodowego, oraz bezpieczeństwa zainteresowanych podmiotów, należy mówić jednak o istotnej inwestycji, a nie wymuszonym wydatku.

MIT 7

“Zmiana prawa dotycząca Krajowego Systemu Cyberbezpieczeństwa (KSC), która ma dostosować je do wymogów unijnej dyrektywy NIS2, może oznaczać dla szpitali publicznych poważne wyzwanie, a nawet zagrozić ciągłości ich działania”.

Ochrona zdrowia należy do sektorów najbardziej narażonych na ataki cyfrowe. Sektor ten jest bardzo chętnie obierany za cel przez grupy przestępcze właśnie m.in. ze względu na braki i niedociągnięcia w infrastrukturze i cyberbezpieczeństwie. Adaptacja do obecnych realiów i nowych wymogów prawnych jest konieczna dla zagwarantowania bezpieczeństwa pacjentów i kadr placówek, a w efekcie naszego zdrowia publicznego. Cyberatak na szpital może realnie zagrażać życiu pacjentów – przypadki z Niemiec, Francji i Czech pokazują, że ataki ransomware doprowadzały do paraliżu placówek i opóźnień w leczeniu. Wdrażanie NIS2 – i szerzej nowelizacja ustawy o KSC – nie jest więc biurokratycznym wymysłem, ale elementem ochrony życia i zdrowia. Co ważne koszty incydentu (utrata danych medycznych, wstrzymanie zabiegów, odszkodowania) bywają znacznie wyższe niż koszty prewencji takich wypadków. Prace nad nowelizacją ustawy o KSC trwają od dawna. Nie jest i nie było sekretem, że szpitale również będą objęte nowymi obowiązkami. Nie można mówić zatem o “zaskoczeniu” osób zarządzających placówkami medycznymi. Fakt, że według szacunków 78% dyrektorów szpitali w Polsce nie wie o wpływie projektowanych przepisów na ich placówki pokazuje lukę w zarządzaniu ryzykiem IT w kadrach zarządzających w ochronie zdrowia, a nie problem z samą regulacją. Nowe przepisy mają m.in. skutkować w instytucjach krytycznych właśnie podniesieniem kompetencji zarządczych. Brak wiedzy nie może być powodem, by odkładać przepisy chroniące system ochrony zdrowia. Co więcej, modernizacja systemów IT i sprzętu może przynieść szpitalom korzyści długoterminowe: niższe ryzyko awarii, lepszą interoperacyjność danych, możliwość wykorzystania AI i telemedycyny. Nowe wymogi mogą być zatem bodźcem do poprawy zarządzania, efektywności kosztowej i jakości usług, a wiele z obecnych systemów i urządzeń w szpitalach i tak wymaga wymiany z powodów technicznych (koniec wsparcia, niezgodność z RODO lub innymi standardami technicznymi).

MIT 8

“Koszty i nakład pracy związany z obowiązkowymi audytami dla niektórych podmiotów (zwłaszcza mniejszych lub tych, które dopiero będą zakwalifikowane jako „ważne/kluczowe”) mogą oznaczać znaczne obciążenie. Ryzykujemy stworzeniem sytuacji, w której podmiot będzie musiał spełniać dwa zestawy obowiązków, a audyt przez organ lub nakaz audytu może być postrzegany jako bardzo mocne działanie nadzorcze”.

Audyt bezpieczeństwa jest uznawany za kluczowe narzędzie w identyfikacji luk i niedociągnięć w systemach IT, które podmioty kluczowe i ważne muszą wdrożyć, zwłaszcza w kontekście rosnących zagrożeń cybernetycznych. Wdrożenie audytów i raportowania wspiera podejście oparte na ryzyku, które jest coraz częściej wymagane w regulacjach unijnych (np. Dyrektywa NIS2). Audyt umożliwia ocenę stanu przygotowania podmiotu do obowiązków prawnych i stanowi rutynową praktykę.