Stanowisko ZPP w sprawie projektu nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa

- Związek Przedsiębiorców i Pracodawców z zadowoleniem przyjmuje rozpoczęcie konsultacji dotyczących długo wyczekiwanego projektu nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa.
- Wiele badań i analiz wskazuje, że w obszarze cyberbezpieczeństwa Polska zajmuje stosunkowo wysoką pozycję. W rankingu NCSI, który wymienia kraje mające najlepsze na świecie rozwiązania gwarantujące systemom IT bezpieczeństwo, zajmujemy 11 miejsce. Choć nie zaliczamy się do grona światowych liderów, to nasz kraj postrzegany jest jako relatywnie bezpieczny cyfrowo. Nie oznacza to jednak, że brakuje nam w tym obszarze wyzwań. W ostatnich latach doświadczyliśmy wielu cybernetycznych incydentów, uderzających nie tylko w instytucje publiczne, ale również firmy obsługujące krytyczną infrastrukturę. Co więcej, napięcia geopolityczne, a zwłaszcza konflikt na Ukrainie, zwiększają ryzyko ataków hakerskich na Polskę.
- W dobie rosnącej liczby cyberataków i zagrożeń w sieci aktualizacja przepisów jest niezbędna do skutecznego reagowania na nowe formy ataków. W tym kontekście, jedną z priorytetowych kwestii będzie uchwalenie nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa. Zapewni ona lepszą zgodność polskiego systemu cyberbezpieczeństwa z unijnymi standardami oraz dyrektywami (m.in. NIS2 oraz CER), istotną dla międzynarodowej współpracy i wymiany informacji o występujących zagrożeniach. Dodatkowo udoskonalenie ustawy pozwoli na lepszą ochronę krytycznej infrastruktury narodowej, która coraz częściej staje się celem zaawansowanych ataków.
- Cieszymy się z decyzji o przeprowadzeniu szerokich konsultacji projektu nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa i popieramy jej jak najszybsze przeprocedowanie. Pragniemy zwrócić jednak uwagę na m.in. na potrzebę doprecyzowania niektórych przepisów w kontekście dyrektywy NIS2, kwestię dostawców sprzętu wysokiego ryzyka oraz Oceny Skutków Regulacji.

TERMIN NA WYCOFANIE SPRZĘTU WYSOKIEGO RYZYKA PRZEDSIĘBIORCÓW ICT

Zachęcamy, żeby podmioty infrastruktury krytycznej w Polsce otrzymały obowiązek do wycofania sprzętu w ciągu 1 roku. Natomiast przewidziany w art. 67c ust. 2 projektu KSC dla przedsiębiorców telekomunikacyjnych termin 4-letni na wycofanie typów produktów ICT, rodzajów usług ICT oraz konkretnych procesów ICT, wskazanych w decyzji uznającej dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, w naszej opinii jest zbyt krótki i nie uwzględnia praktycznych możliwości realizacji takiego procesu. Zarówno uzasadnienie do Projektu KSC, jak i OSR, nie wskazują na podstawowy problem związany z Procedurą DWR dla podmiotów objętych Załącznikiem nr 3 do projektu. Niezauważono, że

wymiana sprzętu dla sieci 5G wymaga również wymiany sprzętu dla sieci 4G (ze względu na obecnie wykorzystywaną konfigurację 5G non-standalone), i to nie tylko w tych samych lokalizacjach, ale w całej sieci. W konsekwencji jest to znacznie bardziej złożony projekt niż budowa sieci 5G, obejmujący wielokrotnie więcej lokalizacji fizycznych. Skala inżynieryjna projektu jest tak duża, że próba jego realizacji w ciągu 4 lat będzie ograniczona z powodu braku dostępności wyspecjalizowanych ekip instalacyjnych, które będą dokonywały wymian, równolegle dla kilku przedsiębiorców telekomunikacyjnych. Wymiana sprzętu oznacza uruchomienie dużego programu obejmującego wiele projektów, dotyczących równoczesnej zmiany kilku systemów oraz dostosowania pozostałych systemów do współpracy z nowym rozwiązaniem. Ryzyko niedotrzymania terminu z art. 67c może być całkowicie niezależne od przedsiębiorcy telekomunikacyjnego, ponieważ pozostali dostawcy oferujący dany typ rozwiązania (ich liczba również jest ograniczona) mogą nie być w stanie wywiązać się z zamówień od nowych klientów w określonym czasie.

ODPOWIEDZIALNOŚĆ ZARZĄDZAJĄCYCH

Zgodnie z dyrektywą NIS2, państwa członkowskie muszą zapewnić, że zarządy kluczowych i ważnych podmiotów zatwierdzają i nadzorują wdrażanie środków zarządzania ryzykiem cyberbezpieczeństwa, zgodnie z artykułem 21. Odpowiedzialność za naruszenia tego artykułu może spoczywać na tych organach. Polski projekt implementacji określa obowiązki zarządów oraz zasady dotyczące kar finansowych (artykuł 8c do 8e i artykuł 73a). Kara może być nałożona, jeśli zarząd nie spełni swoich obowiązków lub jeśli podmiot nie wypełni swoich obowiązków wynikających z implementacji NIS2. Kara nie może przekroczyć 600% wynagrodzenia ukaranej osoby.

Te przepisy różnią się od zasad określonych w dyrektywie, ponieważ nie uwzględniają zdolności finansowej osoby karanej. Ponadto, artykuł 53 ust. 1 projektu daje władzom szersze uprawnienia egzekucyjne, w tym możliwość zawieszenia lub cofnięcia licencji, usunięcia z rejestru działalności, czasowego zakazu pełnienia funkcji przez zarząd oraz nakazu przeprowadzania audytów bezpieczeństwa.

Rozszerzenie tych uprawnień może prowadzić do nadmiernej ingerencji w działalność podmiotów, co może destabilizować ich funkcjonowanie. Zalecamy ponowną analizę przepisów w celu znalezienia bardziej zrównoważonego rozwiązania, które zapewni bezpieczeństwo, minimalizując jednocześnie ryzyko nadmiernych obciążeń i zakłóceń.

PRZEPISY DOTYCZĄCE KAR

Dyrektywa NIS2 (art. 36) wymaga, aby państwa członkowskie ustanowiły skuteczne, proporcjonalne i odstraszające kary za naruszenia. Polski projekt implementacji (art. 73 ust.

1) określa kary finansowe dla kluczowych i ważnych podmiotów, podobnie jak dyrektywa, z wyjątkiem dwóch przypadków, gdzie możliwe są wyższe kary: do 100 000 000 PLN oraz od 500 PLN do 100 000 PLN za każdy dzień opóźnienia.

W naszej opinii wysokie kary mogą być nieproporcjonalne do naruszeń, co może prowadzić do nadmiernej represji wobec podmiotów. Surowe kary za drobne uchybienia mogą nadmiernie obciążyć kluczowe i ważne podmioty. Dodatkowo, pragniemy podkreślić, że przyznanie organom prawa do nakładania wysokich kar oraz decydowania o zawieszeniu lub cofnięciu licencji stwarza ryzyko arbitralności i nadużycia władzy. Sugerujemy ponowne rozważenie wysokości kar oraz wprowadzenie mechanizmów zapewniających proporcjonalność i sprawiedliwość w egzekwowaniu przepisów.

OCENA SKUTKÓW REGULACJI

Zwracamy uwagę na fakt, że, przy braku wątpliwości co do celu regulacji, przewidziane w projekcie rozwiązania będą wiązały się z koniecznością poniesienia nakładów przez konkretne grupy firm. Ocena Skutków Regulacji w obecnym brzmieniu nie uwzględnia tego faktu i nie wskazuje choćby przewidywanych “widełek”, w których mogłyby się mieścić rzeczywiście poniesione koszty.

Mając powyższe na uwadze, warto rozważyć uzupełnienie OSR o choćby szacunkowe dane, tak aby przedsiębiorcy mieli świadomość, jakie koszty będą musieli ponieść w związku z koniecznością dostosowania się do projektowanej nowelizacji.

ZGŁASZANIE ISTOTNYCH INCYDENTÓW

Polski projekt implementacji NIS2 rozszerza zasady zgłaszania incydentów. Elektroniczni operatorzy muszą zgłaszać poważne incydenty w ciągu 12 godzin od ich wykrycia (art. 11 ust. 1a). Projekt definiuje poważny incydent jako taki, który powoduje szkodę materialną lub niematerialną, wpływając na inne podmioty (art. 2 pkt 7). W przeciwieństwie do dyrektywy NIS2, nie odnosi się do "znacznej" szkody ani możliwości wpływu incydentu na osoby. Poważne zagrożenie cybernetyczne to takie, które może poważnie wpłynąć na bezpieczeństwo systemów informatycznych, powodując szkodę (art. 2 pkt 20).

Dodatkowo przepisy różnicują termin na zgłoszenie wczesnego ostrzeżenia o incydencie poważnym – dla podmiotów ważnych i kluczowych 24 godziny zgodnie z przepisami NIS2, a dla przedsiębiorcy komunikacji elektronicznej – 12 godzin od momentu jego wykrycia. Sugerujemy, żeby zgodnie z przepisami dyrektywy NIS2, ustawodawca trzymał się terminu 24 godziny na zgłaszanie takich incydentów. Termin 12 godzin jest zbyt krótki, przy uwzględnieniu warunków pracy przedsiębiorcy.

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Propozycja art. 8 zawiera przepis dotyczący systemu zarządzania bezpieczeństwem informacji oraz dokładne określenie funkcji, które ten system ma spełniać. Ze względu na oczywiste przyczyny, przepisy ustawy są sformułowane ogólnie, a jednocześnie obejmują dużą liczbę podmiotów z różnych sektorów. Problem polega na narzuceniu konkretnych wymogów przedsiębiorcom bez jednoznacznego wskazania, czy ich działania i wprowadzane zmiany są zgodne z oczekiwaniami i przepisami właściwych organów. Ma to szczególne znaczenie w kontekście ust. 4 omawianego przepisu, który wymaga od podmiotów uwzględnienia podatności danego dostawcy oraz „ogólnej jakości produktów ICT (…)".

Ustawa proponuje dwa rozwiązania

- Przede wszystkim, art. 67a przewiduje możliwość wydania przez Pełnomocnika ds. cyberbezpieczeństwa stosownych rekomendacji dla podmiotów krajowego systemu cyberbezpieczeństwa. Jest to formuła prawa miękkiego, jednak warto rozważyć, czy przepis nie powinien nakładać obowiązku działania Pełnomocnika ds. cyberbezpieczeństwa, który uzupełniałby przepisy konkretnymi rekomendacjami i przewodnikami dla przedsiębiorców.
- Art. 8a wskazuje na możliwość działania Rady Ministrów w drodze rozporządzenia. Choć takie działanie miałoby charakter wiążący dla przedsiębiorców, wyznaczenie Rady Ministrów jako organu właściwego może okazać się nieefektywne. Jeżeli forma rozporządzenia jest konieczna, naszym zdaniem lepszym rozwiązaniem byłoby powierzenie tej funkcji Ministrowi.

Podsumowując Związek Przedsiębiorców i Pracodawców z zadowoleniem przyjmuje rozpoczęcie konsultacji nad projektem nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa. Popieramy szybkie wprowadzenie zmian, które zwiększą zgodność polskiego systemu z unijnymi standardami oraz zapewnią skuteczną ochronę infrastruktury krytycznej. Jednocześnie zwracamy uwagę na konieczność doprecyzowania przepisów dotyczących kar, odpowiedzialności zarządzających oraz terminów wycofania sprzętu wysokiego ryzyka. Sugerujemy również uwzględnienie rzeczywistych kosztów implementacji oraz dostosowanie wymogów do praktycznych możliwości przedsiębiorców.