Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.49.2024
Warszawa, 04 lipca 2024 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 10 czerwca br. Posła na Sejm RP Pana Grzegorza Matusiaka w sprawie projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa obejmującej przepisami przedsiębiorstwa z woj. śląskiego (interpelacja nr 2865)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Jakie jest uzasadnienie dla zaostrzenia wymogów klasyfikowania podmiotów z ważnych na kluczowe w sektorze produkcji, wytwarzania i dystrybucji chemikaliów, sektorze produkcji, przetwarzania i dystrybucji żywności oraz sektorze produkcji?

Sektor produkcji spożywczej ma bardzo istotne znaczenie dla zapewnienia żywnościowego wszystkim obywatelom Polski. Przy produkcji żywności wykorzystywana jest szeroko technologia operacyjna (OT). W związku z tym wystąpienie incydentu w tych systemach mogłoby wpłynąć na produkcję żywności, a w szczególnie niebezpiecznym przypadku, prowadzić do zagrożeń dla życia i zdrowia ludzi wynikających np. z zanieczyszczenia żywności w procesie produkcji. Dlatego też sektor ten wymaga szczególnej ochrony. Podobna sytuacja, zwłaszcza w zakresie wykorzystania technologii operacyjnych, występuje w sektorze produkcji oraz produkcji, wytwarzania i dystrybucji chemikaliów.

Ponadto, objęcie średnich i dużych przedsiębiorców w tej branży m.in. obowiązkami w zakresie stworzenia systemu zarządzania bezpieczeństwem informacji czy zgłaszania incydentów poważnych wynika wprost z przepisów dyrektywy NIS2[1]. Dlatego też z samego prawa europejskiego wynika konieczność objęcia ich tymi obowiązkami. Także dyrektywa o odporności podmiotów krytycznych[2], dotycząca infrastruktury krytycznej wskazuje ten sektor jako jeden z sektorów krytycznych. Również wiele podmiotów z sektorów produkcji oraz chemikaliów może stanowić podmioty krytyczne.

Średni i duzi przedsiębiorcy w sektorze żywności mają istotne znaczenie z punktu widzenia społeczeństwa i gospodarki i jest to kolejny powód, dla którego powinni być objęci określonymi obowiązkami z zakresu cyberbezpieczeństwa. Branża ta jest coraz częstszym celem cyberataków. Dla przykładu, zaatakowany z wykorzystaniem ransomware został największy na świecie producent wołowiny i drobiu, brazylijski JBS Food. Koncern zmuszony został na ponad tydzień wstrzymać działalność swoich zakładów w Stanach Zjednoczonych, Kanadzie i Australii, a także zapłacić okup w wysokości 11 mln dolarów,

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)
[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (dyrektywa CER)

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

aby odzyskać dostęp do danych. Zmiany te są więc konieczne dla zapewnienia bezpieczeństwa żywności i dostępu do niej.

Również w branży chemicznej zdarzały się już ataki na szczególnie istotne podmioty. Brenntag, firma zajmująca się dystrybucją chemikaliów z siedzibą w Niemczech, doświadczyła w maju 2021 r. ataku ransomware. Incydent ten doprowadził do utraty poufnych danych i pociągnął za sobą zapłacenie okupu w wysokości 4,4 miliona dolarów. W branży produkcyjnej istotne incydenty dotknęły w ostatnich latach m.in. producenta sprzętu komputerowego ACER oraz KIA Motors w branży motoryzacyjnej. W związku z tym również w tych sektorach zagrożenie jest realne. Ponadto, projekt ustawy wciąż jest przedmiotem prac w ramach rządowego procesu legislacyjnego i jego ostateczna treść nadal może ulec zmianom w toku prac na poziomie rządowym i parlamentarnym.

Ad 2) Jakie koszty dla sektora górniczego i spożywczego ze Śląska wiążą się z dostosowaniem do nowych regulacji?

Koszty dostosowania się do nowych regulacji są bardzo trudne do oszacowania ze względu na to, że obejmuje ona podmioty o zróżnicowanej wielkości, sposobie i zakresie wykorzystania technologii ICT oraz zróżnicowanym zaawansowaniu w sprawach cyberbezpieczeństwa.

W zakresie sektora górniczego należy zwrócić uwagę, że zgodnie z obecnie obowiązującymi przepisami wydobycie kopalin jest jednym z podsektorów w sektorze energii. W związku z tym podmioty będące obecnie operatorami usług kluczowych będą miały już wdrożone wiele z rozwiązań wymaganych przez NIS2 co znacząco obniży koszt dostosowania.

Koszty te rosną proporcjonalnie do wielkości danego przedsiębiorstwa, w związku z czym mniejsze podmioty poniosą odpowiednio mniejsze koszty. Dla podmiotów, które dotychczas nie były objęte krajowym systemem cyberbezpieczeństwa, dostosowanie się do nowych regulacji będzie oznaczało konieczność zwiększenia ich budżetów przeznaczonych na systemy teleinformatyczne.

Niemniej należy podkreślić, że koszty dostosowania się podmiotów do wymogów wynikających z projektu ustawy będą znacznie niższe niż ewentualne koszty wynikające ze skutków cyberataków, np. ransomware, które często wiążą się z zapłatą wielomilionowych okupów lub koniecznością odbudowy całych segmentów systemu informatycznego.

Ad 3) Jakie koszty dla tych sektorów ze Śląska wiążą się z procedurą uznania dostawcy za dostawcę wysokiego ryzyka?

Uznanie dostawcy za dostawcę wysokiego ryzyka to szczególny środek mający zapewnić bezpieczeństwo w przypadku gdy zmitygowanie ryzyka związane z danym podmiotem nie byłoby możliwe w inny sposób. Jest to środek szczególny, który może być wykorzystany tylko w ostateczności. Istnieje również możliwość, że nigdy nie zostanie on zastosowany.

Oszacowanie kosztów uznania dostawcy za dostawcę wysokiego byłoby możliwe tylko wówczas gdyby przyjąć na etapie projektowania przepisów jaki podmiot potencjalnie jest takim dostawcą. Ministerstwo Cyfryzacji nie identyfikuje takiego podmiotu w Polsce, w związku z czym nie jest możliwe oszacowanie kosztów związanych ze skutkami decyzji w tej sprawie.

Istotne jest też, że w samej decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka zostaną wskazane typy produktów ICT, usług ICT lub procesów ICT, które mają być usunięte z tych systemów. Nie będzie to więc oznaczało konieczności usunięcia

wszystkich produktów takiego dostawcy. To kolejny aspekt tych przepisów, który uniemożliwia precyzyjne określenie kosztu takiej decyzji.

Należy również dodatkowo podkreślić, że na wycofanie sprzętu pochodzącego od takiego dostawcy podmioty kluczowe i ważne będą miały, co do zasady 7 lat. Do czasu upływu terminu sprzęt ten będzie mógł być dalej użytkowany, a także naprawiany i aktualizowany, tak aby zapewnić pełną ciągłość działania. 7 lat to termin, w którym w wielu wypadkach cykl życia danego sprzętu i tak uległby zakończeniu, a więc i tak często musiałby on zostać wymieniony.

Ad 4) Dlaczego Ministerstwo Cyfryzacji zaniechało oszacowania tych koszt ów w Ocenie Skutków Regulacji?

Jak w odpowiedzi na pytanie nr 3.

Ad 5) Jakie powody stanęły za objęciem postępowaniem w sprawie uznania dostawcy za dostawcę wysokiego ryzyka wszystkich osiemnastu sektor ów? Czy dokonano oszacowania ryzyka i analizy zagrożeń w tym zakresie? Dlaczego inne kraje (jak Francja, Hiszpania, Portugalia), wskazane w załączniku nr 1 do OSR, zastosowały tą procedurą tylko dla telekomunikacji, a nawet tylko do sieci 5G?

Uznanie dostawcy za dostawcę wysokiego ryzyka jest szczególnym środkiem, który będzie zastosowany tylko w przypadku gdy ten dostawca stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi. Jest to więc szczególny środek, który będzie wykorzystany tylko w przypadku poważnego zagrożenia, którego nie można inaczej zmitygować. W przypadku tak szczególnego ryzyka, sprzęt powinien zostać wycofany ze wszystkich systemów należących do podmiotów kluczowych i ważnych, gdyż wpływają one na aspekty istotne dla funkcjonowania państwa i społeczeństwa. Należy też podkreślić, że decyzja w tej sprawie wydawana jest w szczególnie długiej i skomplikowanej procedurze, w której biorą udział podmioty takie jak Prokurator Generalny czy Prezes Urzędu Ochrony Konkurencji i Konsumentów, których rolą jest zagwarantowanie prawidłowego przebiegu postępowania. Jeśli taka zostanie już wydana to konieczne jest podjęcie wszelkich działań, aby zapewnić bezpieczeństwo wszystkich systemów informacyjnych, które mają istotny wpływ na funkcjonowanie państwa i społeczeństwa. Takimi systemami są systemy wykorzystywane przez podmioty kluczowe i ważne. W związku z tym konieczne jest zmitygowanie już wykrytego ryzyka. W celu zapewnienia, że te działania nie będą nadmiernym obciążeniem dla przedsiębiorców zdecydowano się na przyjęcie 4–letniego terminu na wycofanie sprzętu i oprogramowania dotyczącego funkcji krytycznych i 7–letniego dla pozostałego sprzętu i oprogramowania.

Ad 6) Kto zwróci koszty wycofania sprzętu, oprogramowania lub proces ów ICT podmiotom ze Śląska? Czy planowane jest wprowadzenie odszkodowania albo funduszu mającego na celu zwrot koszt ów poniesionych na wymianę?

Należy podkreślić, że uznanie dostawcy za dostawcę wysokiego ryzyka jest szczególnym środkiem, który będzie zastosowany tylko w przypadku, gdy ten dostawca stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi. Dlatego też, ze względów bezpieczeństwa, najlepszym rozwiązaniem byłoby jak najszybsze wycofanie całego tego rodzaju sprzętu. Aby jednak zagwarantować, że nie będzie to nadmierny obowiązek dla podmiotów dotkniętych tą decyzją zdecydowano się na przyjęcie 4–letniego terminu na wycofanie sprzętu i oprogramowania dotyczącego funkcji krytycznych i 7-letniego dla pozostałego sprzętu i oprogramowania. W czasie trwania tego terminu podmioty objęte tym obowiązkiem będą mogły dalej korzystać z tego sprzętu a także naprawiać go i aktualizować. Termin ten gwarantuje, że objęci obowiązkiem przedsiębiorcy będą mogli

rozplanować wymiany i zminimalizować ponoszone w związku z tym koszty. Rozwiązanie to jest więc kompromisem między potrzebami bezpieczeństwa, a bieżącymi wydatkami podmiotów.

Ad 7) Dlaczego hurtownie wina, jaj lub olejów stanowią podmioty kluczowe, objęte najsurowszym nadzorem, który powinien być zarezerwowany dla podmiotów krytycznych dla gospodarki?

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) nie przewiduje nałożenia obowiązków na wszystkie podmioty w sektorze produkcja, przetwarzanie i dystrybucja żywności. Zgodnie z treścią projektu ustawy i załącznika do niej, obowiązki w zakresie cyberbezpieczeństwa obejmują przedsiębiorstwa spożywcze zajmujące się dystrybucją hurtową oraz przemysłową produkcją i przetwarzaniem żywności, które są co najmniej średnimi przedsiębiorstwami. Oznacza to, że aby ustawa miała do takiego przedsiębiorstwa zastosowanie musi ono zatrudniać co najmniej 50 pracowników, a jego roczna suma bilansowa musi wynosić co najmniej 10 milionów EUR. W związku z tym mali przedsiębiorcy działający w tym obszarze nie będą objęci obowiązkami.

W pozostałym zakresie należy ponownie odnieść się do argumentacji przywołanej w odpowiedzi na pytanie nr 1 w zakresie w jakim konieczne jest zapewnienie bezpieczeństwa żywności oraz zapewnienie spójności z regulacjami dotyczącymi infrastruktury krytycznej.

Ad 8) Dlaczego hurtownie wina, jaj lub olej ów stanowi ą podmioty, objęte postępowaniem w sprawie dostawcy uznanego za dostawcę wysokiego ryzyka?

Jak wskazano w odpowiedzi na pytanie nr 1, sektor żywności jest sektorem istotnym z punktu widzenia bezpieczeństwa państwa, a istotne podmioty z tego sektora w innych krajach były już celami zaawansowanych cyberataków.

Należy tu ponownie podkreślić, że uznanie dostawcy za dostawcę wysokiego ryzyka jest szczególnym środkiem, który będzie zastosowany tylko w przypadku gdy ten dostawca stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi. Jest to więc szczególny środek, który będzie stosowany tylko w przypadku poważnego zagrożenia, którego nie można inaczej zmitygować. W przypadku tak szczególnego ryzyka taki sprzęt powinien zostać wycofany ze wszystkich systemów należących do wszystkich podmiotów kluczowych i ważnych, gdyż wpływają one na aspekty istotne dla funkcjonowania państwa i społeczeństwa. Dlatego średnie i większe przedsiębiorstwa w branży spożywczej zostały objęte tymi przepisami.

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
w Ministerstwie Cyfryzacji
/dokument podpisany elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa