Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.53.2024
Warszawa, 04 lipca 2024 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 10 czerwca br. Posła na Sejm RP Pana Jarosława Sachajko w sprawie wpływu przepisów nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa na polski sektor rolnospożywczy (interpelacja nr 2974)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Z jakiego powodu podmioty kluczowe i ważne z sektora produkcji, przetwarzanie i dystrybucji żywności zostały objęte regulacjami zawartymi w projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw? Kto i kiedy podjął decyzje o takim rozszerzeniu materii tej regulacji?

Objęcie sektora produkcji, przetwarzania i dystrybucji żywności regulacją projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) wynika wprost z dyrektywy NIS2[1]. Sektor ten został ujęty w załączniku nr 2 do dyrektywy NIS2. Ponadto, sektor ten uznawany jest jako jeden z sektorów krytycznych w świetle dyrektywy o odporności podmiotów krytycznych[2].

Średni i duzi przedsiębiorcy w sektorze żywności mają istotne znaczenie z punktu widzenia społeczeństwa i gospodarki i jest to więc 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, aby odzyskać dostęp do danych. Zmiany te są więc konieczne dla zapewnienia bezpieczeństwa żywności i dostępu do niej.

Ad 2) Z jakiego powodu do konsultacji publicznych projektu ustawy nie zostali zaproszeni przedstawiciele zrzeszeń rolników i producentów rolno-spożywczych?

Konsultacje publiczne były otwarte i szerokie. Projekt ustawy został umieszczony na stronie Rządowego Procesu Legislacyjnego oraz na BIP Ministerstwa Cyfryzacji. Każdy więc mógł zapoznać się projektem i zgłosić do niego uwagi. Z takiej możliwości skorzystało dużo podmiotów i osób fizycznych.

[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

Ad 3) Jakie działania podjęło Ministerstwo w celu zakomunikowania przedstawicielom tej branży nowych obowiązków, które będą wynikały z regulacji zawartych w rzeczonym projekcie ustawy?

W dniu skierowania projektu ustawy do uzgodnień międzyresortowych, konsultacji publicznych oraz opiniowania w Ministerstwie Cyfryzacji została zorganizowana konferencji, której celem było upublicznienie informacji o projekcie ustawy. Na stronie internetowej Ministerstwa Cyfryzacji została zamieszczona informacja o skierowaniu projektu ustawy do uzgodnień międzyresortowych[3]. W informacji tej omówiono proponowane rozwiązania oraz wskazano na możliwość zgłoszenia uwag do projektu. Przedstawiciele Ministerstwa Cyfryzacji uczestniczyli w konferencjach, na których omawiano projekt ustawy.

Ad 4) Gdzie konkretnie podmioty działające w tej branży mogą uzyskać informację o tym czy będą objęte obowiązkami określonymi w tych przepisach, jaki będzie zakres tych obowiązków i jakie konkretnie sprzęty bądź oprogramowanie przez nich wykorzystywane może zostać uznane za dostarczane przez dostawcę wysokiego ryzyka?

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw 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.

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. Nie jest możliwe stwierdzenie, czy dany dostawca jest dostawcą wysokiego ryzyka, ponieważ taka procedura nie została do tej pory ustanowiona w polskim porządku prawnym.

Ad 5) Czy Ministerstwo analizowało jaki może być szacunkowy koszt wymiany sprzętu i oprogramowania, który może ponieść branża rolno-spożywcza w przypadku wejścia w życie tej ustawy? Jeśli tak, to proszę o przekazanie wniosków z tych analiz. Jeśli nie, to proszę o ich przeprowadzenie.

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

Koszty te rosną proporcjonalnie do wielkości danego przedsiębiorstwa, w związku z czym mniejsze podmioty poniosą odpowiednio mniejsze koszty. Niemniej należy zauważyć, że koszty dostosowania się podmiotów do wymogów wynikających z projektu ustawy będą znacznie niższe niż ewentualne koszty wynikające ze skutków cyberataków, np.

[3] https://www.gov.pl/web/cyfryzacja/walka-z-cyberzagrozeniami-wchodzi-w-nowy-wymiar

ransomware, które często wiążą się z zapłatą wielomilionowych okupów lub koniecznością odbudowy całych segmentów systemu informatycznego.

Ad 6) Z jakiego powodu w Ocenie Skutków Regulacji ww. projektu ustawy nie znalazły się dane dotyczące tych kosztów? Proszę o uzupełnienie OSR w tym zakresie.

Jak w odpowiedzi na pytanie nr 5.

Ad 7) Czy ww. nowelizacja była konsultowana przed zaprezentowanie projektu ustawy z Ministerstwem Rolnictwa i Rozwoju Wsi? Jakie było stanowisko tego resortu w zakresie włączenia branży rolno-spożywczej w zakres tej regulacji?

Projekt ustawy został przekazany do Ministerstwa Rolnictwa i Rozwoju Wsi w ramach uzgodnień międzyresortowych.

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