KONFEDERACJA LEWIATAN

STANOWISKO KONFEDERACJI LEWIATAN W SPRAWIE FINANSOWANIA CYBERBEZPIECZEŃSTWA PRZEDSIĘBIORSTW

Konfederacja Lewiatan postuluje uruchomienie w programie Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 dedykowanego instrumentu wsparcia cyberbezpieczeństwa przedsiębiorstw bądź uwzględnienie takiego instrumentu w pracach nad programowaniem wsparcia w nowej perspektywie finansowej na lata 2028-2034.

Instrument powinien umożliwiać finansowanie całego procesu podnoszenia cyberodporności firmy: od diagnozy potrzeb, przez przygotowanie procedur i realizację inwestycji, po rozwój kompetencji zarządów oraz pracowników.

Regulacje w zakresie cyberbezpieczeństwa

Cyberbezpieczeństwo nie może być traktowane wyłącznie jako zagadnienie techniczne lub element infrastruktury informatycznej. Jest ono bezpośrednio związane z zarządzaniem ryzykiem, ciągłością działania przedsiębiorstwa, bezpieczeństwem łańcuchów dostaw, ochroną danych oraz zaufaniem klientów i kontrahentów.

Rosnąca skala zagrożeń cyfrowych wymaga od przedsiębiorstw systematycznych inwestycji w technologie, organizację procesów oraz kompetencje pracowników. Potrzeby te są dodatkowo wzmacniane przez regulacje unijne, w szczególności dyrektywę NIS2, rozporządzenie DORA oraz akt w sprawie cyberodporności – CRA. Nakładają one na przedsiębiorstwa nowe obowiązki organizacyjne, techniczne, inwestycyjne i sprawozdawcze, obejmujące m.in. zarządzanie ryzykiem, reagowanie na incydenty, bezpieczeństwo dostawców i odpowiedzialność organów zarządzających.

Obowiązki wynikające z nowych regulacji dotyczą nie tylko największych przedsiębiorstw. Pośrednio obejmują także firmy działające w łańcuchach dostaw podmiotów kluczowych i ważnych. Oznacza to, że zapewnienie odpowiedniego poziomu cyberbezpieczeństwa staje się warunkiem utrzymania relacji handlowych i możliwości uczestniczenia w coraz bardziej zintegrowanych łańcuchach wartości.

Obecny system finansowania

Wsparcie cyberbezpieczeństwa przedsiębiorstw jest obecnie dostępne w ramach różnych programów i instrumentów, jednak ma charakter fragmentaryczny. Poszczególne źródła koncentrują się m.in. na inwestycjach infrastrukturalnych, badaniach i rozwoju, transformacji cyfrowej albo projektach konsorcjalnych. Brakuje natomiast prostego i bezpośrednio dostępnego dla firm instrumentu, który łączyłby wsparcie technologiczne, organizacyjne, kompetencyjne oraz regulacyjne.

Dotychczasowe rozwiązania w ograniczonym stopniu odpowiadają na potrzeby przedsiębiorstw jako bezpośrednich odbiorców pomocy. W szczególności FERC koncentruje się przede wszystkim na

systemach publicznych i infrastrukturze państwa, a przedsiębiorstwa nie mają w nim dostępu do dedykowanego mechanizmu finansowania własnych inwestycji w cyberbezpieczeństwo.

Istniejące instrumenty nie zapewniają również ciągłości wsparcia od identyfikacji problemu do jego rozwiązania. Firmy mogą uzyskać pomoc w wybranym obszarze, ale często nie są w stanie sfinansować pełnego procesu obejmującego audyt, przygotowanie procedur, zakup i wdrożenie technologii, szkolenia oraz utrzymanie rezultatów. System finansowania pozostaje w rezultacie rozproszony, a przedsiębiorcy muszą samodzielnie łączyć różne źródła pomocy lub rezygnować z części niezbędnych działań.

Problemem jest również niedostateczne uwzględnienie potrzeb dużych przedsiębiorstw. Część instrumentów jest dostępna wyłącznie dla MŚP albo dla firm z określonych sektorów, mimo że duże podmioty ponoszą wysokie koszty dostosowania do regulacji i odgrywają kluczową rolę w bezpieczeństwie całych łańcuchów dostaw.

Postulat uruchomienia dedykowanego instrumentu dla przedsiębiorstw

Konfederacja Lewiatan rekomenduje utworzenie w FERC instrumentu skierowanego zarówno do mikro-, małych i średnich przedsiębiorstw, jak i do dużych firm. Wsparcie powinno być dostępne dla przedsiębiorstw objętych bezpośrednio regulacjami z zakresu cyberbezpieczeństwa, a także dla podmiotów, które muszą spełnić określone wymagania ze względu na udział w łańcuchach dostaw.

Postulujemy, aby instrument opierał się na modelu mieszanym i obejmował trzy wzajemnie powiązane komponenty:

1. Komponent doradczy i diagnostyczny

Punktem wyjścia projektu powinien być wystandaryzowany audyt cyberbezpieczeństwa, obejmujący m.in.:

- analizę ryzyka i podatności,
- ocenę stosowanych technologii i zabezpieczeń,
- analizę polityk, procedur oraz sposobu reagowania na incydenty,
- ocenę planów ciągłości działania i odtwarzania po awarii,
- analizę bezpieczeństwa łańcucha dostaw,
- ocenę zgodności z obowiązującymi regulacjami,
- przygotowanie planu wdrożenia rekomendowanych działań.

Standaryzacja diagnozy, np. przez zastosowanie jednolitej „checklisty cyberodporności", pozwoli zapewnić odpowiednią jakość usług, porównywalność projektów oraz racjonalne powiązanie finansowanych inwestycji z rzeczywistymi potrzebami przedsiębiorstwa. Postulat ten został również podniesiony podczas dyskusji członków Komitetu Monitorującego FERC.

2. Komponent inwestycyjny

Wsparcie powinno obejmować zakup oraz wdrożenie technologii wskazanych jako niezbędne w wyniku audytu. Finansowane powinny być zarówno środki trwałe, jak i wartości niematerialne i prawne, w tym sprzęt, oprogramowanie, licencje, rozwiązania chmurowe oraz specjalistyczne usługi wdrożeniowe.

Zakres inwestycji powinien wynikać z potrzeb danego przedsiębiorstwa, a nie z zamkniętego katalogu produktów. Możliwe działania mogą obejmować m.in. systemy zarządzania tożsamością i dostępem, uwierzytelnianie wieloskładnikowe, systemy monitorowania i reagowania na incydenty, zabezpieczenia środowisk IT i OT, rozwiązania do tworzenia odpornych kopii zapasowych, ochronę danych oraz zarządzanie bezpieczeństwem dostawców.

Instrument nie powinien finansować pojedynczych, niepowiązanych zakupów. Każda inwestycja powinna wynikać z diagnozy oraz stanowić część spójnego planu podnoszenia cyberodporności organizacji.

3. Komponent szkoleniowy i kompetencyjny

Projekty powinny obejmować rozwój kompetencji osób odpowiedzialnych za zarządzanie przedsiębiorstwem oraz pracowników wykorzystujących wdrożone rozwiązania. Finansowane powinny być w szczególności:

- szkolenia dla członków zarządów dotyczące odpowiedzialności i zarządzania ryzykiem,
- szkolenia dla zespołów technicznych i osób odpowiedzialnych za cyberbezpieczeństwo,
- praktyczne szkolenia z obsługi wdrożonych technologii,
- ćwiczenia reagowania na incydenty i sytuacje kryzysowe,
- działania podnoszące świadomość pracowników w zakresie phishingu, ransomware oraz ochrony danych.

Komponent szkoleniowy powinien być integralną częścią projektu, a nie fakultatywnym dodatkiem do zakupu technologii. Bez odpowiednich kompetencji nawet zaawansowane rozwiązania techniczne nie zapewnią trwałego wzrostu bezpieczeństwa.

Dostępność instrumentu

Potrzeby przedsiębiorstw różnią się w zależności od ich wielkości, poziomu dojrzałości cyfrowej oraz charakteru prowadzonej działalności. MŚP potrzebują przede wszystkim prostych, dostępnych cenowo rozwiązań, podstawowych procedur, skutecznego backupu, uwierzytelniania wieloskładnikowego oraz szkoleń. Duże przedsiębiorstwa częściej mierzą się ze złożonością infrastruktury, integracją systemów IT i OT, zagrożeniami dla łańcuchów dostaw oraz koniecznością prowadzenia zaawansowanego monitoringu.

Kryteria wyboru projektów nie powinny zatem narzucać identycznego zakresu rzeczowego wszystkim wnioskodawcom. Instrument musi umożliwiać dostosowanie zakresu i wartości projektu do wyników diagnozy oraz skali działalności przedsiębiorstwa.

Jednocześnie wsparcie powinno być dostępne dla szerokiego grona przedsiębiorców, a nie wyłącznie dla firm działających w wybranych branżach. Podejście takie znalazło poparcie również podczas spotkania roboczego Komitetu Monitorującego FERC, podczas którego wskazano, że pomoc powinna mieć charakter kompleksowy i docierać do możliwie szerokiej grupy przedsiębiorstw.

Elastyczne podstawy udzielania pomocy

Ze względu na zróżnicowanie zakresu projektów oraz sytuacji przedsiębiorców instrument powinien umożliwiać łączenie różnych podstaw udzielania pomocy publicznej.

W zależności od rodzaju wydatku zasadne jest wykorzystanie:

- pomocy de minimis, przede wszystkim w odniesieniu do diagnozy, usług doradczych i szkoleń;
- pomocy na usługi doradcze dla MŚP;
- regionalnej pomocy inwestycyjnej w odniesieniu do wydatków technologicznych i inwestycyjnych;
- innych dostępnych podstaw pomocy, jeżeli pozwolą one na bardziej adekwatne finansowanie usług lub inwestycji związanych z cyberbezpieczeństwem.

Model mieszany umożliwi objęcie wsparciem zarówno MŚP, jak i dużych przedsiębiorstw oraz pozwoli uniknąć sytuacji, w której cały projekt jest ograniczony niskim limitem pomocy de minimis. Rekomendowany model zakłada odrębne traktowanie komponentu doradczego, inwestycyjnego i szkoleniowego, z zastosowaniem odpowiedniej podstawy pomocy do każdego z nich.

W przypadku zastosowania regionalnej pomocy inwestycyjnej należy jednak uwzględnić jej ograniczenia, w szczególności zróżnicowanie intensywności wsparcia ze względu na lokalizację i wielkość przedsiębiorstwa, wyłączenia sektorowe oraz wymóg wykazania efektu zachęty. Instrument powinien być zaprojektowany tak, aby formalne warunki pomocy nie uniemożliwiały finansowania uzasadnionych i pilnych inwestycji w cyberbezpieczeństwo.

Uproszczenie procedur

Warunkiem skuteczności instrumentu jest ograniczenie obciążeń administracyjnych, zwłaszcza po stronie MŚP. Nabory powinny mieć charakter ciągły lub być organizowane w regularnych, odpowiednio częstych rundach. W przypadku przedsiębiorstw bezpośrednio objętych obowiązkami regulacyjnymi warto rozważyć uruchomienie szybkiej ścieżki oceny projektów.

Konfederacja Lewiatan rekomenduje w szczególności:

- uproszczony formularz wniosku,
- ograniczenie liczby wymaganych załączników,
- stosowanie kosztów uproszczonych tam, gdzie jest to możliwe,
- jasne i mierzalne kryteria oceny,
- krótkie terminy oceny wniosków,
- możliwość etapowego składania i realizowania projektu,
- zapewnienie przedsiębiorcom dostępu do informacji i doradztwa przed złożeniem wniosku,
- powiązanie instrumentu z działalnością europejskich hubów innowacji cyfrowych, CSIRT-ów oraz sektorowych centrów kompetencji.

Obowiązkowy audyt nie powinien prowadzić do tworzenia nadmiernych barier ani mechanizmu wspierającego przede wszystkim dostawców usług doradczych. Głównym odbiorcą i beneficjentem interwencji musi pozostać przedsiębiorstwo, a koszt oraz zakres diagnozy powinny być proporcjonalne do skali działalności i ryzyka.

Trwałość efektów projektów

Instrument powinien premiować projekty prowadzące do rzeczywistego wzrostu cyberodporności przedsiębiorstwa, a nie wyłącznie do zakupu wyposażenia lub oprogramowania.

Rezultaty projektu mogą być mierzone m.in. poprzez:

- wdrożenie procedur zarządzania ryzykiem i reagowania na incydenty,
- skrócenie czasu wykrywania incydentów i podejmowania reakcji,
- objęcie kluczowych systemów monitoringiem,
- wdrożenie planu ciągłości działania i odtwarzania po awarii,
- zwiększenie liczby pracowników objętych szkoleniami,
- przeprowadzenie testów bezpieczeństwa lub ćwiczeń kryzysowych,
- wdrożenie zaleceń wynikających z audytu,
- zapewnienie utrzymania i aktualizacji wdrożonych rozwiązań.

Wymogi dotyczące trwałości nie mogą jednak prowadzić do nakładania na przedsiębiorstwa nieproporcjonalnych obowiązków. Cyberbezpieczeństwo jest procesem ciągłym, a stosowane technologie oraz rodzaje zagrożeń szybko się zmieniają. Beneficjent powinien mieć możliwość aktualizowania i zastępowania wdrożonych rozwiązań, o ile nadal realizuje cel projektu i utrzymuje osiągnięty poziom cyberodporności.

Otwarcie FERC i jego następcy na udział przedsiębiorstw

Program Fundusze Europejskie na Rozwój Cyfrowy odgrywa kluczową rolę w budowaniu bezpieczeństwa cyfrowego państwa. Cyberodporność administracji publicznej, infrastruktury oraz systemów państwowych nie może być jednak budowana w oderwaniu od bezpieczeństwa przedsiębiorstw.

Firmy są operatorami infrastruktury, dostawcami technologii, uczestnikami łańcuchów dostaw oraz podmiotami świadczącymi usługi o kluczowym znaczeniu dla obywateli i gospodarki. Dlatego w projektowaniu oraz realizacji działań FERC należy zwiększyć udział sektora prywatnego – zarówno jako odbiorcy wsparcia, jak i partnera w projektach systemowych.

Podczas prac Komitetu Monitorującego FERC przedstawiciele Konfederacji Lewiatan zwracali uwagę na potrzebę angażowania przedsiębiorstw i organizacji pozarządowych w projekty dotyczące cyberbezpieczeństwa. Obecnie udział firm w części planowanych przedsięwzięć pozostaje ograniczony lub nie został przewidziany.

Podsumowanie

W ocenie Konfederacji Lewiatan istnieje pilna potrzeba uzupełnienia obecnego systemu o instrument, który będzie bezpośrednio dostępny dla przedsiębiorstw i umożliwi im systemowe, a nie punktowe podnoszenie poziomu cyberbezpieczeństwa. Wyniki przygotowanej ekspertyzy zostały już wskazane jako materiał, który ma zostać wykorzystany w pracach nad zakresem wsparcia na lata 2028-2034. Nie powinno to jednak wykluczać przeanalizowania możliwości uruchomienia odpowiedniego mechanizmu jeszcze w ramach dostępnych środków FERC 2021-2027.