KPO w praktyce

Jak organizacje publiczne mogą skutecznie wdrożyć
i utrzymać projekty cyberbezpieczeństwa

Wprowadzenie

Wdrażanie projektów cyberbezpieczeństwa finansowanych w ramach Krajowego Planu Odbudowy wkroczyło w decydującą fazę. Dla wielu organizacji etap analizy potrzeb i definiowania priorytetów jest już zamknięty. Oznacza to, że w centrum uwagi znajdują się teraz decyzje operacyjne i wdrożeniowe, które będą miały realne konsekwencje nie tylko dla powodzenia projektu, ale dla długoterminowego bezpieczeństwa całej organizacji.

Dobrze opracowana koncepcja to dopiero połowa sukcesu. Teraz, gdy priorytety zostały jasno określone, kluczowe staje się to, jak zostaną przełożone na konkretne rozwiązania technologiczne, jak zostanie zaplanowana ich realizacja i – co równie ważne – jak zapewnić ich trwałość po zakończeniu finansowania. Z perspektywy organizacji to moment, w którym cyberbezpieczeństwo przestaje być tylko strategią na papierze, a staje się codzienną praktyką, wymagającą konkretnych decyzji, konsekwencji i zaufanych partnerów rozumiejących specyfikę działania w środowisku regulowanym i publicznym.

Poniżej przedstawiamy trzy kolejne kroki, które powinny zostać podjęte, aby projekt miał rzeczywisty, długoterminowy wpływ na odporność cyfrową.

Krok 1
Wybór rozwiązań dopasowanych do organizacji

Wnioski o dofinansowanie złożone, faza definiowania potrzeb zakończona, więc teraz naturalnym krokiem jest wybór konkretnych rozwiązań technologicznych. Niezależnie od tego, czy chodzi o systemy klasy EDR, platformy SIEM, budowę zespołu SOC czy rozwój kompetencji zespołu, kluczowe jest, aby wybrane narzędzia nie tylko spełniały bieżące wymagania projektowe, ale w przyszłości były możliwe do utrzymania i rozwijania - również po zakończeniu wsparcia finansowego.

Technologia powinna być traktowana jako element większej całości: razem z procesami, ludźmi i kulturą organizacyjną. Dlatego równie istotna, jak sam wybór rozwiązań, jest także jakość współpracy z partnerem wdrożeniowym. Firmy, które znają realia projektów finansowanych ze środków publicznych i potrafią dostosować się do specyfiki sektora, są w stanie nie tylko dostarczyć odpowiednie narzędzia, ale też zapewnić ich optymalne dopasowanie do struktury organizacyjnej i operacyjnej.

Dobrze zaprojektowane środowisko bezpieczeństwa musi być elastyczne, skalowalne i gotowe na przyszłe zmiany, zarówno regulacyjne, jak i technologiczne.

Krok 2
Realistyczny harmonogram i skuteczna realizacja

Właściwe zaplanowanie działań to warunek sprawnej realizacji każdego projektu, także tego realizowanego w ramach KPO. Program ten działa w konkretnych ramach czasowych i proceduralnych, dlatego harmonogram musi być zarówno ambitny, jak i wykonalny. Kluczowe znaczenie mają tu nie tylko same daty wdrożeń, ale też kamienie milowe, terminy odbiorów, testów oraz przestrzeń na ewentualne korekty.

Na tym etapie jeszcze wyraźniej ujawnia się wartość dobrze dobranego partnera. Współpraca z zespołem, który ma doświadczenie w podobnych projektach, może w praktyce zadecydować o tym, czy harmonogram zostanie dotrzymany. Ważna jest nie tylko wiedza technologiczna, ale też umiejętność zarządzania ryzykiem, komunikacji między zespołami i przewidywania potencjalnych przeszkód. Prawidłowo zaplanowany i zrealizowany projekt nie tylko zwiększa szansę na pełne wykorzystanie środków i ich późniejsze poprawne rozliczenie, ale minimalizuje ryzyko opóźnień i nieporozumień, które mogą zagrozić powodzeniu całego przedsięwzięcia.

Krok 3
Trwałość efektów po zakończeniu projektu

Jednym z kluczowych kryteriów oceny projektów finansowanych z KPO jest ich trwałość. Organizacja, która wdrożyła nowe rozwiązania, musi wykazać, że będą one utrzymywane i rozwijane również po zakończeniu finansowania. W praktyce oznacza to konieczność jasnego określenia, kto będzie odpowiedzialny za zarządzanie środowiskiem bezpieczeństwa, w jaki sposób będzie ono aktualizowane, monitorowane i rozwijane, a także jak zostanie zabezpieczona ciągłość kompetencji w zespole.

Z tych powodów już na etapie wdrożenia warto uwzględnić fakt, że każde rozwiązanie bezpieczeństwa będzie wymagać bieżącej opieki – zarówno technicznej, jak i organizacyjnej. Cyberbezpieczeństwo to nie projekt „raz na zawsze". Skuteczna ochrona oznacza ciągłe działanie: aktualizacje, dostosowania do nowych ryzyk, regularne przeglądy. Brak zaplanowanego modelu utrzymania może szybko obniżyć efektywność nawet najlepszego rozwiązania. Zbyt często zakłada się, że po zakończeniu wdrożenia system będzie działał bezobsługowo, a to prosta droga do utraty kontroli nad bezpieczeństwem. Świadomość, że to proces, a nie jednorazowe zadanie, jest kluczowa dla realnej odporności organizacji.

KPO to szansa – pomożemy Ci ją dobrze wykorzystać

Jeśli jesteś na etapie wyboru partnera lub chcesz skonsultować swoje plany dotyczące wdrożenia i utrzymania rozwiązań z obszaru cyberbezpieczeństwa – zapraszamy do kontaktu.

Chętnie podzielimy się naszym doświadczeniem i wspólnie poszukamy optymalnych rozwiązań, które będą działać nie tylko na papierze, ale przede wszystkim w praktyce – skutecznie, bezpiecznie i długofalowo.

Szukasz wsparcia w zakresie cyberbezpieczeństwa?

Skontaktuj się z ekspertem

Malwina Pobłocka
Business Development Manager
Centrum Kompetencyjne
Cybersecurity

Zatrudniając ponad 7 300 specjalistów, Sii jest liderem usług IT, biznesowych i inżynieryjnych w Polsce.

www.sii.pl