Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Wnioski i Rekomendacje

Executive summary

Państwo powinno pełnić rolę integratora i katalizatora rynku cyberbezpieczeństwa, budując interoperacyjność, zaufanie, mechanizmy jakości oraz bodźce inwestycyjne dla sektora prywatnego, zamiast konkurować z rynkiem jako dominujący dostawca usług. W projekcie Strategii widać zarówno elementy zgodne z tym podejściem, jak i zapisy tworzące realne ryzyko wypierania rynku, zwłaszcza w obszarze platform usługowych, narzędzi operacyjnych oraz aspiracji do zastępowania rozwiązań komercyjnych rozwiązaniami państwowymi.

Pięć kluczowych dowodów liczbowych wskazujących na wagę korekty kursu i wykonalność w segmencie MŚP:

1. Rząd deklaruje rekordowe wydatki na cyberbezpieczeństwo w 2025 roku na poziomie 3,1 mld zł, co istotnie zwiększa wpływ instrumentów państwowych na strukturę rynku i architekturę usług. [1]
2. Jeden program grantowy dla samorządów ma całkowitą wartość ponad 1,507 mld zł, przy dofinansowaniu unijnym ponad 1,251 mld zł, co pokazuje skalę kanału inwestycji publicznych. [2]
3. Uruchomiono nabór dla cyberbezpieczeństwa administracji rządowej z alokacją 350 mln zł, co wzmacnia popyt publiczny, ale nie rozwiązuje automatycznie bariery wdrożeń w MŚP. [3]
4. Dedykowany instrument grantowy dla MŚP w cyber w ramach Digital Europe ma budżet 1,8 mln EUR, a pojedynczy grant 30 do 60 tys. EUR, przy jednoczesnym formalnym wykluczeniu JDG oraz spółek cywilnych,

co ogranicza inkluzywność i zdolność do budowania podaży usług u mikro dostawców. [4]

5. Udział osób w wieku 16 do 74 posiadających podstawowe lub ponadpodstawowe umiejętności cyfrowe wyniósł 48,8 procent, co ogranicza tempo wdrożeń w MŚP i podnosi koszty wsparcia użytkowników, a jednocześnie wskazuje na konieczność skalowalnych mechanizmów rynku szkoleń, nie wyłącznie rozwiązań centralnych. [5]

Wnioski wykonawcze

Strategia powinna precyzyjnie rozdzielić funkcje państwa jako regulatora, integratora, operatora zaufania i koordynatora odporności, od funkcji dostawcy usług komercyjnych. Kluczowe korekty dotyczą: zakresu portalu cyber.gov.pl i Krajowego Cyber Hub, modelu centralnej instytucji typu jedno okienko, polityki komunikatorów i platform państwowych, a także modelu certyfikacji oraz rozwoju potencjału testowania i oceny zgodności.

Analiza treści Strategii

Poniższe mapowanie obejmuje fragmenty projektu Strategii, interpretację skutków rynkowych, ryzyko wypierania rynku oraz rekomendowaną korektę w logice integracji i katalizowania rynku.

Mapa treści Strategii a rynek cyberbezpieczeństwa

1. **Wizja i zaufanie:** „budowę zaufania między administracją rządową a poszczególnymi sektorami rynkowymi”
   Interpretacja skutków rynkowych: państwo deklaruje model oparty o współpracę i zaufanie jako warunek działań systemowych
   Ryzyko wypierania rynku: niskie, o ile kolejne instrumenty będą wspierać kierowanie do rynku, a nie zastępowanie usług rynkowych
   Rekomendowana korekta: dopisać doprecyzowanie, że zaufanie budowane jest przez standardy, interoperacyjność i mechanizmy jakości, a nie przez monopol usług
2. **Centralna instytucja:** „PCOC zostanie przekształcone w centralną instytucję”
   Interpretacja skutków rynkowych: tworzy silny ośrodek koordynacji, potencjalnie także operacyjnego świadczenia usług
   Ryzyko wypierania rynku: średnie, gdy instytucja zacznie pełnić rolę dostawcy usług dla rynku zamiast roli koordynatora i brokera
   Rekomendowana korekta: dopisać, że instytucja centralna pełni funkcję integratora, a usługi wdrożeniowe realizuje rynek w modelu akredytacji i zamówień wynikowych
3. **Jedno okienko:** „jedno okienko dla podmiotów KSC i obywateli”
   Interpretacja skutków rynkowych: asymetria informacyjna może zostać zmniejszona, jeśli państwo zbuduje kanał zgłoszeń, poradnik i kierowanie do dostawców
   Ryzyko wypierania rynku: wysokie, jeśli jedno okienko będzie zapewniać pełne doradztwo i narzędzia zastępujące usługi rynkowe dla firm
   Rekomendowana korekta: wprost ograniczyć zakres: triage, informacja o obowiązkach, katalog akredytowanych dostawców, uruchamianie instrumentów popytowych

4. **Platforma usługowa:** „cyber.gov.pl wszystkie kluczowe usługi i narzędzia”
   Interpretacja skutków rynkowych: państwo buduje jednolitą bramę usług, co może poprawić dostęp, ale łatwo rozszerza się w stronę świadczenia usług
   Ryzyko wypierania rynku: wysokie, bo opis obejmuje narzędzia operacyjne i szkolenia jako usługi państwowe konkurujące z rynkiem
   Rekomendowana korekta: zmienić model na warstwę interoperacyjności, standardów i dystrybucji informacji z integracją usług rynku i mechanizmem kierowania do dostawców
5. **Krajowy Cyber Hub:** „krajowa platforma wykrywanie zagrożeń dla sektora publicznego i prywatnego”
   Interpretacja skutków rynkowych: wspólne zdolności detekcji mogą zwiększyć odporność, jeśli mają otwarte interfejsy integracyjne
   Ryzyko wypierania rynku: średnie do wysokiego, jeśli platforma stanie się substytutem komercyjnych usług SOC i MDR dla firm MŚP
   Rekomendowana korekta: dopisać obowiązek integracji przez otwarte API i model partnerski, w którym dostawcy prywatni są warstwą usługową
6. **Zastępowanie rozwiązań komercyjnych:** „komercyjne rozwiązania będą zastępowane rozwiązaniami państwowymi”
   Interpretacja skutków rynkowych: deklaruje kierunek budowy państwowych odpowiedników usług, co zmienia rynek w stronę monopsonu i monopolu podaży
   Ryzyko wypierania rynku: bardzo wysokie, bo zapis wprost mówi o zastępowaniu rozwiązań rynkowych usługami instytucji państwowych
   Rekomendowana korekta: zastąpić zasadą neutralności dostawcy, preferencja ma dotyczyć zgodności, interoperacyjności i audytowalności, nie własności rozwiązania
7. **Partnerstwo z rynkiem:** „Partnerstwo dla Cyberbezpieczeństwa otwarty dla wszystkich”
   Interpretacja skutków rynkowych: dobre ramy współpracy nie finansowej, budujące kanał dialogu i wymianę informacji
   Ryzyko wypierania rynku: niskie, jeśli partnerstwo pozostanie platformą współpracy, a nie kanałem preferencyjnego dostępu

Rekomendowana korekta: wzmocnić o mierniki, governance, zasady publikacji standardów oraz sposób włączania MŚP i mikro firm

8. **Certyfikacja:** „Krajowy system certyfikacji będzie nadzorowany przez ministra”
   Interpretacja skutków rynkowych: nadzór państwa jest zgodny z rolą operatora zaufania, o ile wykonawstwo jest rynkowe i otwarte
   Ryzyko wypierania rynku: średnie, jeśli państwo będzie jednocześnie nadzorcą i dominującym wykonawcą badań, audytów i certyfikacji
   Rekomendowana korekta: doprecyzować rozdział ról: nadzór i uznawalność po stronie państwa, ocena zgodności i certyfikacja po stronie rynku, w tym jednostek oceny zgodności i laboratoriów
9. **Potencjał badawczy w państwowych instytutach:** „rozwijanie potencjału państwowych instytutów badawczych”
   Interpretacja skutków rynkowych: rozwój laboratoriów może zwiększyć zdolności kraju, ale wymaga uważnego modelu konkurencji i dostępu
   Ryzyko wypierania rynku: wysokie, jeśli finansowanie preferuje sektor państwowy kosztem prywatnych laboratoriów i jednostek oceny zgodności
   Rekomendowana korekta: dodać zasadę otwartego dostępu, nie wyłączności oraz mechanizm współpracy laboratoriów publicznych z prywatnymi
10. **Wykonalność kompetencyjna:** „zależy w znacznym stopniu od dostępności kadr”
    Interpretacja skutków rynkowych: Strategia trafnie identyfikuje ograniczenie podażowe kadr jako warunek powodzenia
    Ryzyko wypierania rynku: pośrednie, bez instrumentów rynkowych deficyt kadr skanalizuje popyt do kilku dużych dostawców i podniesie ceny dla MŚP
    Rekomendowana korekta: wprowadzić instrumenty popytowe dla MŚP mapowane do ECSF i mierników jakości
11. **Standard dla MŚP:** „Firma Bezpieczna Cyfrowo”
    Interpretacja skutków rynkowych: standaryzacja może obniżyć koszty wdrożeń, o ile standard jest rynkowo mapowalny do ofert i dobrowolnej walidacji

Ryzyko wypierania rynku: średnie, ryzyko powstania quasi obowiązkowego programu państwowego konkurującego z rynkowymi modelami dojrzałości
Rekomendowana korekta: dopisać, że standard ma charakter neutralny i może być realizowany przez rynek, w tym przez oddolne inicjatywy ekosystemowe dedykowane MŚP, które przekładają wymagania na kontrole i oferują dobrowolne potwierdzanie dojrzałości.

Finansowanie państwowe vs. rynek

Projekt Strategii wskazuje, że finansowanie ma pochodzić z istniejących źródeł, w tym budżetu państwa, Funduszu Cyberbezpieczeństwa, NCBR oraz funduszy UE, w tym Digital Europe, Horizon Europe oraz KPO. W praktyce skala instrumentów publicznych adresowanych do administracji i infrastruktury publicznej jest wielokrotnie większa niż skala instrumentów bezpośrednio wzmacniających popyt w MŚP i budujących podaż usług prywatnych. Poniższa tabela zestawia publicznie zadeklarowane kwoty dla kluczowych instrumentów. [6]

Finansowanie i instrumenty wsparcia

1. **Rekordowe wydatki na cyberbezpieczeństwo 2025**, 3,1 mld zł,
   beneficjenci: państwo, system krajowy, instytucje,
   typ wsparcia: budżet publiczny i inwestycje,
   wnioski: zależy od konstrukcji wydatkowania, bez preferencji rynkowej może wzmacniać państwową podaż usług zamiast katalizować rynek
2. **Cyberbezpieczny Samorząd**, 1 507 219 343 zł w tym UE 1 251 504 388 zł,
   beneficjenci: JST,
   typ wsparcia: grant inwestycyjny na modernizacje,
   wnioski: buduje popyt publiczny, dla rynku kluczowy jest model zakupów, dostęp MŚP do zamówień oraz katalog interoperacyjnych wymagań
3. **Cyberbezpieczny Rząd**, 350 000 000 zł,
   beneficjenci: administracja rządowa,
   typ wsparcia: grant inwestycyjny,
   wnioski: wzmacnia odporność administracji, ważne by nie budować państwowego monopolisty usług operacyjnych
4. **Cyberbezpieczne Wodociągi**, 759 projektów, wartość ponad 624 mln zł oraz przekroczenie planowanej wartości inwestycji,
   beneficjenci: podmioty realizujące zadania w sektorze wod-kan,
   typ wsparcia: grant inwestycyjny,
   wnioski: wysoki wolumen zamówień, istotne jest ujednolicenie standardów wymagań i dopuszczenie konkurencyjnej podaży małych dostawców

5. **CyberPL** nabór 4, 367 500 000 zł,
   beneficjenci: administracja i podmioty publiczne,
   typ wsparcia: grant inwestycyjny,
   wnioski: duża alokacja, wymaga mechanizmów interoperacyjności i kryteriów jakości, aby zamówienia nie zamykały rynku i nie wzmacniały wyłącznie największych dostawców
6. **Granty na cyberbezpieczeństwo dla MŚP**, 1,8 mln EUR, grant 30 do 60 tys. EUR,
   beneficjenci: MŚP spełniające kryteria naboru, bez JDG i spółek cywilnych,
   typ wsparcia: grant bezpośredni,
   wnioski: instrument rynkowy o małej skali względem programów publicznych oraz z barierą formalną ograniczającą inkluzywność podaży
7. **Digital Europe Work Programme 2025 do 2027**, 3,2 mld EUR,
   beneficjenci: podmioty UE zależnie od konkursów,
   typ wsparcia: program UE,
   wnioski: kluczowe jest zwiększenie absorpcji przez firmy i MŚP, co wspiera tezę o roli państwa jako katalizatora absorpcji, nie wykonawcy
8. **ECCC call Cyber 09 w ramach Digital Europe**, do 50 mln EUR,
   beneficjenci: podmioty UE, w tym MŚP,
   typ wsparcia: grant UE,
   wnioski: Strategia powinna przewidzieć mechanizmy masowej akceleracji udziału polskich MŚP

Najbardziej istotna obserwacja relacji skali: wielomiliardowe inwestycje w sektor publiczny powinny zostać uzupełnione o masowe instrumenty popytowe dla MŚP oraz o mechanizmy jakości i kierowanie do dostawców rynkowych, aby nie powstał ekosystem, w którym państwo buduje własne platformy i usługi konkurujące z rynkiem.

Bariery dostępu i inkluzywność instrumentów

Najbardziej jednoznaczna bariera formalna w instrumentach adresowanych do rynku została zidentyfikowana w naborze grantowym na cyberbezpieczeństwo dla MŚP, gdzie wprost wskazano wykluczenie JDG oraz spółek cywilnych. [4]

Konsekwencje rynkowe takiej konstrukcji instrumentu:

1. Ogranicza się pula potencjalnych beneficjentów i dostawców w segmencie mikro, co utrudnia skalowanie rozwiązań dla MŚP w modelu blisko klienta
2. Ogranicza się możliwość tworzenia łańcuchów podwykonawczych, gdzie część specjalistycznych usług świadczą mikro podmioty
3. Przy niewielkim budżecie całego instrumentu 1,8 mln EUR ryzyko utraty efektu skali jest wysokie, bo nawet przy pełnym wykorzystaniu alokacji liczba możliwych wdrożeń jest ograniczona

W kontekście Strategii ważne jest, że jednocześnie projekt zawiera zapisy o budowie rozbudowanych narzędzi i usług państwowych oraz o zastępowaniu rozwiązań komercyjnych rozwiązaniami państwowymi, co łącznie może prowadzić do podwójnego efektu: rynek jest formalnie ograniczany w dostępie do instrumentów, a jednocześnie wypierany przez państwową podaż usług. Rekomendacja konsultacyjna w warstwie inkluzywności jest prosta, instrumenty rynkowe powinny obejmować pełne spektrum form prowadzenia działalności, a bariery powinny być uzasadniane wyłącznie ryzykiem prawnym lub mechaniką pomocy publicznej, z preferencją dla minimalizowania wykluczeń.

Udział Polski w programach UE

Projekt Strategii wskazuje Digital Europe oraz Horizon Europe jako potencjalne źródła finansowania. Oficjalnym rejestrem projektów badawczo innowacyjnych UE jest CORDIS, który udostępnia karty projektów i zestawy danych open data o projektach i uczestnikach. [7]

W tym materiale przedstawiamy:

1. minimalny, potwierdzony zestaw przykładów projektów cyberbezpieczeństwa w ramach Horizon Europe z udziałem polskich podmiotów, wraz z wartościami wkładu UE widocznymi na kartach projektów
2. rekomendowaną metodę pełnego przeliczenia, którą można zastosować na podstawie eksportów CORDIS, obejmującą filtrowanie po słowach kluczowych i tematach oraz identyfikację uczestników z Polski poprzez pola kraju i typ organizacji

Minimalnie potwierdzone przykłady Horizon Europe:

1. **MIRACLE**, projekt 101168144,
   polski beneficjent: NASK Państwowy Instytut Badawczy,
   typ: organizacja badawcza,
   wkład UE: 370 000 EUR [8]
2. **AI4CYBER**, projekt 101070450,
   polski beneficjent: ITTI sp z oo,
   typ: podmiot prywatny,
   wkład UE: na karcie widoczny koszt uczestnika 237 075 EUR [8]
3. **PERUN**, projekt 101225653,
   polski beneficjent: Politechnika Warszawska,
   typ: uczelnia,
   wkład UE: dane widoczne na karcie projektu [8]

Rekomendowana metoda pełnego przeliczenia:

1. Pobrać miesięczny eksport CORDIS Horizon Europe projects, pola tytuł, streszczenie, słowa kluczowe, tematy oraz lista uczestników z krajami

2. Zdefiniować kryterium cyberbezpieczeństwa jako kombinację przypisania do obszarów cyber w CORDIS oraz filtrów słów kluczowych cyber security, cybersecurity, incident, SOC, cryptography, vulnerability, secure by design, supply chain security, a następnie ręcznie odfiltrować fałszywe trafienia
3. Policzyć liczbę projektów z co najmniej jednym uczestnikiem z Polski i zsumować EU contribution na poziomie projektu oraz na poziomie uczestników
4. Sklasyfikować typ beneficjenta zgodnie z activity type w CORDIS oraz oznaczeniem SME, jeśli jest dostępne

Analogiczne podejście dla Digital Europe wymaga zastosowania oficjalnych zestawień z programów Digital Europe i instrumentów ECCC oraz krajowego punktu kontaktowego. Strategia powinna zawierać zobowiązanie do publikacji rocznej statystyki absorpcji przez polskie firmy, w tym MŚP, aby wzmacniać rolę państwa jako katalizatora absorpcji funduszy UE na rzecz rynku.

Luka kompetencyjna i ECSF

Projekt Strategii wskazuje, że wykonalność działań zależy od dostępności kadr o wysokich kompetencjach. Jest to szczególnie istotne w MŚP, gdzie zespoły są małe, a koszty pozyskania specjalistów wysokie.

Diagnoza oparta o źródła oficjalne wskazuje trzy bariery

1. Poziom kompetencji cyfrowych społeczeństwa pozostaje ograniczeniem. Według GUS w 2024 roku 48,8 procent osób w wieku 16 do 74 miało podstawowe lub ponadpodstawowe umiejętności cyfrowe. [5]
2. W metrykach UE Digital Decade udział populacji z co najmniej podstawowymi umiejętnościami cyfrowymi wynosi 44,3 procent wobec średniej UE 55,6 procent, co wzmacnia tezę o trudniejszej wykonalności masowych wdrożeń w MŚP bez wsparcia rynku usług i szkoleń. [11]
3. Deficyt specjalistów cyber jest problemem ogólnoeuropejskim. ENISA wskazywała szacunek niedoboru około 300 tys. specjalistów w UE, co oznacza, że Polska konkuruje o talent w warunkach presji płacowej i rosnących cen usług. [12]

Strategia wymaga instrumentów, które zwiększają nie tylko zdolności państwa, ale także popyt MŚP na usługi i technologie cyber, w modelu współdzielenia kosztów i szybkiego dostępu do kwalifikowanych dostawców.

ECSF jako mechanizm porządkowania kompetencji i rynku

ENISA opublikowała European Cybersecurity Skills Framework, którego rdzeniem jest 12 profili ról cyber wraz z misją, zadaniami i wymaganymi kompetencjami. [14] Celem ECSF jest stworzenie wspólnego rozumienia między osobami, pracodawcami i dostawcami programów edukacyjnych w całej UE, czyli mechanizm wspólnego języka rynku zgodny z tezą o roli państwa jako integratora, nie monopolisty szkoleń. [15] ENISA publikuje mapowania certyfikacji do ECSF. To pokazuje praktyczny model: rynek certyfikacji i szkoleń mapuje swoje ścieżki do wspólnej taksonomii, a rola publiczna polega na upowszechnieniu i włączeniu ECSF do standardów, a nie na zastąpieniu rynku. [16] ECSF jest ramą, ale bez wymogu mapowania programów i certyfikacji do ECSF w instrumentach finansowanych publicznie rynek pozostaje

fragmentaryczny. Wtedy rośnie pokusa, aby państwo tworzyło własne scentralizowane ścieżki szkoleniowe, co może wypierać prywatnych dostawców.

Spójność z polityką i strategią UE

Strategia UE w zakresie cyberbezpieczeństwa na Cyfrową Dekadę akcentuje budowę odporności, zdolności i potencjału technologicznego, w tym wzmacnianie współpracy i ekosystemu przemysłowego, nie tylko rozwój zdolności państwowych jako dostawców usług. [19] UE rozwija podejście oparte o sieć i centrum kompetencji cyber, które mają pomagać w utrzymaniu i rozwoju zdolności technologicznych i przemysłowych. [20] W projekcie Strategii są dwa napięcia względem podejścia UE

1. Zapis o zastępowaniu rozwiązań komercyjnych rozwiązaniami udostępnianymi przez instytucje państwowe przesuwa model w stronę państwa jako dostawcy, co jest ryzykowne dla konkurencyjności i innowacji rynku.
2. Zakres portalu cyber.gov.pl oraz Krajowego Cyber Hub opisany jako dostarczanie usług i narzędzi dla przedsiębiorców może w praktyce wejść w obszary typowe dla rynku usług cyber, co wymaga doprecyzowania modelu partnerstw i interoperacyjności.

Wniosek: aby realizować cele UE i wzmocnić wykonalność w MŚP, Strategia powinna wprost zapisać, że państwo jest operatorem standardów, zaufania, interoperacyjności oraz kierunkowania popytu, natomiast usługi wdrożeniowe i operacyjne dla biznesu powinny być zasadniczo realizowane przez rynek w modelu akredytacji i zamówień wynikowych.

Rekomendacje i propozycje instrumentów katalizujących rynek

Architektura ról

Rekomendacja: utrzymać silną centralną koordynację, ale z ograniczeniem funkcji usługowych względem rynku. W praktyce oznacza to rozdzielenie

1. funkcji państwa jako regulatora, nadzorcy systemu, operatora zaufania, integratora danych i standardów interoperacyjności
2. funkcji rynku jako dostawcy usług wdrożeniowych i operacyjnych dla MŚP, realizowanych w oparciu o kryteria jakości, certyfikację i akredytację

Finansowanie i instrumenty rynkowe

Rekomendacja: Priorytetem dla wykonalności w MŚP jest instrument popytowy, a nie tylko inwestycje publiczne. Rekomendowane instrumenty:

1. Bony cyber dla MŚP: voucher na audyt, wdrożenie podstawowych zabezpieczeń, szkolenia i testy, realizowany u akredytowanych dostawców, z komponentem zgodności i dobrowolnej walidacji dojrzałości
2. Współfinansowanie wdrożeń z udziałem usług zarządzanych: zamiast finansować narzędzia państwowe dla przedsiębiorstw, współfinansować zakup usług z rynku, szczególnie dla mikro i małych firm
3. Zamówienia oparte o wyzwania: w sektorze publicznym kupować rozwiązania na podstawie mierzalnych rezultatów i interoperacyjnych wymagań, aby rosła konkurencja i spadały koszty

Uzasadnienie skali: inwestycje publiczne osiągają poziomy miliardów złotych, podczas gdy dedykowany instrument grantowy dla MŚP ma budżet 1,8 mln EUR. Bez korekty rynek będzie rozwijał się głównie jako wykonawca zamówień publicznych, a nie jako ekosystem skalujący produkty i usługi dla MŚP. [22]

Certyfikacja i zaufanie

Rekomendacja: państwo jako nadzorca i gwarant uznawalności, rynek jako wykonawca, przy jednoczesnym uznaniu rynkowej walidacji tam, gdzie jest ona dojrzała i powszechnie stosowana. Korekta interpretacyjna do zapisów Strategii o krajowym systemie certyfikacji

1. Wzmocnić rolę certyfikacji jako mechanizmu zaufania i jakości w łańcuchach dostaw
2. Doprecyzować model: nadzór publiczny, wykonawstwo przez akredytowane jednostki oceny zgodności oraz laboratoria, z otwartym dostępem dla rynku
3. Wprost dopuścić równoważne schematy rynkowe i międzynarodowe, w tym dobrowolne inicjatywy branżowe, o ile spełniają kryteria jakości i transparentności oraz mają potwierdzoną adopcję rynkową
4. Uporządkować zasadę spójności: skoro administracja akceptuje certyfikaty kompetencji wydawane przez organizacje pozarządowe jako dowód kwalifikacji, to analogicznie powinna dopuszczać rynkowe mechanizmy potwierdzania dojrzałości, szczególnie dla MŚP

Istotne doprecyzowanie dla MŚP: w Polsce istnieją oddolne inicjatywy ekosystemowe dedykowane MŚP, które działają jako standard wdrożeniowy i dobrowolny mechanizm potwierdzania dojrzałości. Obejmują one przekład wymagań regulacyjnych na praktyczne kontrole, komponent edukacyjny mapowany do ECSF oraz neutralność vendor-agnostic. Pomijanie tej klasy rozwiązań zwiększa ryzyko centralizacji i utraty tempa wdrożeń w MŚP.

**Transparentność: Sygnalizujemy tę lukę również z perspektywy praktyki wdrożeniowej, ponieważ uczestniczymy w rozwoju jednej z takich rynkowych inicjatyw ekosystemowych dla MŚP. Informacja ta ma charakter transparentności, a rekomendacje pozostają neutralne technologicznie i dostawczo.*

Kompetencje i ECSF

Rekomendacja: ECSF jako standard języka rynku, nie jako narzędzie centralizacji szkoleń. Proponowany model wdrożenia

1. obowiązkowe mapowanie programów szkoleń i certyfikacji finansowanych ze środków publicznych do profili ECSF
2. uznawanie certyfikacji rynkowych mapowanych do ECSF jako równoważnych, z publikowanym katalogiem na portalu państwowym
3. rola państwa ograniczona do jakości, akredytacji, stypendiów i voucherów, a nie do realizacji masowej oferty szkoleniowej

Wykorzystanie funduszy UE

Rekomendacja: Strategia powinna zawierać mechanizm katalizowania absorpcji funduszy UE przez firmy i MŚP. Elementy minimalne

1. roczny standard raportowania absorpcji Digital Europe i Horizon Europe w obszarze cyber przez polskie podmioty, z podziałem na typ beneficjenta i udział MŚP
2. wsparcie aplikacyjne jako usługa państwa, ale realizowana w formule rynku doradców i integratorów, z akredytacją i standardem jakości
3. wykorzystanie programów ECCC oraz naborów Digital Europe jako stałego kanału finansowania innowacji i wdrożeń rynkowych, komplementarnego wobec inwestycji publicznych

Bibliografia źródeł

[1] [6] Rekordowe inwestycje w ochronę przed cyberatakami - https://www.gov.pl/web/cyfryzacja/polska-inwestuje-rekordowe-srodki-w-ochrone-przed-cyberatakami

[2] [22] Cyberbezpieczny Samorząd - Centrum Projektów Polska Cyfrowa - Portal Gov.pl - https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad2

[3] Regulamin_Konkursu_Grantowego_Cyber - https://www.gov.pl/attachment/7c0474b6-c6f7-4d47-b685-8c444643b69d

[4] [29] [33] Granty na cyberbezpieczeństwo dla MŚP - nabór w ramach Programu "Cyfrowa Europa" - Centrum Projektów Polska Cyfrowa - Portal Gov.pl - https://www.gov.pl/web/cppc/nabor-dep010125

[5] [34] Główny Urząd Statystyczny - https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2024-roku%2C2%2C14.html

[7] [9] CORDIS - https://cordis.europa.eu/projects

[8] Monitoring, Investigation and Response to cyber-attacks with - https://cordis.europa.eu/project/id/101168144

[10] ECCC Newsletter - https://ec.europa.eu/newsroom/ECCC/newsletter-archives/view/service/2381/default/latest

[11] Digital Strategy 2024 Poland Digital Decade Report - https://digital-strategy.ec.europa.eu/en/factpages/poland-2024-digital-decade-country-report

[12] ENISA Cybersecurity Skills - https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu

[13] Digital Strategy 2025 Poland Digital Decade Report - https://digital-strategy.ec.europa.eu/en/factpages/poland-2025-digital-decade-country-report

[14] [15] [23] European Cybersecurity Skills Framework Role Profiles – ENISA - https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

[16] [32] Certifications mapped to the ECSF | ENISA - European Union - https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf/certifications-mapped-to-the-ecsf

[17] Relacja z European Cybersecurity Skills Conference 2023 - https://www.gov.pl/web/cyber-nccpl/relacja-z-european-cybersecurity-skills-2023

[18] [26] [31] European Cybersecurity Skills Framework User Manual – ENISA - https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20User%20Manual.pdf

[19] [21] Strategia UE w zakresie cyberbezpieczeństwa na ... - EUR-Lex - https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX%3A52020JC0018&

[20] Europejska Sieć i Centrum Kompetencji w dziedzinie ... - https://digital-strategy.ec.europa.eu/pl/policies/cybersecurity-competence-centre

[24] Centrum Projektów Cyfrowa Polska - https://www.gov.pl/web/cppc/nowy-work-programme-w-ramach-digital-europe-programme

[25] [30] European Cybersecurity Skills Framework Role Profiles.pdf - https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20Role%20Profiles.pdf

[27] 759 projektów w konkursie „Cyberbezpieczne Wodociągi”. ... - https://www.kpo.gov.pl/strony/aktualnosci/759-projektow-w-konkursie-cyberbezpieczne-wodociagi-590-mln-zl-na-cyberbezpieczenstwo/

[28] Inwestycja C3.1.1. Cyberbezpieczeństwo (czwarty nabór) - https://www.gov.pl/web/cppc/inwestycja-c-311-cyberbezpieczenstwo---cyberpl-czwarty-nabor