# Strategia rozwoju Polskiego Klastra Cyberbezpieczeństwa #CyberMadeInPoland

**Kraków 2021**

# Spis treści

## *Wstęp*

Koncepcja klastrów stała się popularnym i kompleksowym sposobem, pozwalającym zarówno na podnoszenie kompetencji, wzrost konkurencyjności, ale także na wzmożony rozwój regionalny. Klastry jako podmioty animujące współpracę przedsiębiorstw, jednostek naukowych i badawczo-rozwojowych, instytucji otoczenia biznesu oraz jednostek samorządu terytorialnego stają się swego rodzaju motorem napędowym rozwoju regionalnego zarówno w przemyśle, działalności usługowej, energetyce, transporcie, ale też w sektorach technologii tradycyjnych i wysokich.

Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland powstał jako odpowiedź na najbardziej naglące kwestie bezpieczeństwa cyfrowego, a także w celu kształtowania i rozwoju bezpiecznej cyberprzestrzeni w Polsce. Klaster działa jako swego rodzaju platforma do współpracy oraz promocji polskiego przemysłu cyberbezpieczeństwa w kraju, ale także poza jego granicami. Ponadto, zadaniem Klastra jest stymulowanie współpracy sektora z instytucjami naukowymi, podmiotami administracji publicznej, międzynarodowymi korporacjami, izbami branżowymi i handlowymi, ale także innymi partnerami.

Cyberbezpieczeństwo w obecnie dynamicznie zmieniającym się świecie jest nie tylko wyzwaniem, ale także szansą dla firm i ośrodków badawczych, które dzięki wiedzy i odwadze innowatorów zabezpieczają transformację cyfrową globalnych rynków.

Niniejsze opracowanie ma na celu przedstawienie strategii rozwoju Polskiego Klastra Cyberbezpieczeństwa #CyberMadeInPoland. Głównym zadaniem strategii jest sprecyzowanie kierunków rozwoju Klastra zgodnie z oczekiwaniami i interesem jego obecnych i przyszłych potencjalnych członków. Opracowanie w pierwszej części (1,2,3 rozdział ) poświęcone jest charakterystyce Klastra oraz omówieniu jego działalności, natomiast druga część (4,5,6,7 rozdział) w oparciu o analizę SWOT, doświadczenie Koordynatora Klastra, Rady Klastra oraz członków tworzących strukturę Klastra traktuje o strategicznych kierunkach rozwoju Klastra.

## 1. *Ogólne informacje o Klastrze*

Dostrzegając potencjał polskiego przemysłu cyberbezpieczeństwa i dążąc do jego rozwoju oraz wzrostu konkurencyjności zarówno na poziomie krajowym, jak i europejskim, czy międzynarodowym uznano że wartościowe byłoby zainicjowanie, a także zorganizowanie trwałej współpracy w formie Klastra. Z inicjatywy Instytutu Kościuszki we wrześniu 2020 roku powstał Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland. Klaster zakładało 37 członków – założycieli, natomiast w ciągu roku działalności do inicjatywy dołączyło 10 nowych firm, które posiadają status członków zwyczajnych. Celem Klastra jest przede wszystkim kształtowanie i rozwój bezpiecznej cyberprzestrzeni w Polsce oraz promowanie polskich technologii w tym zakresie. W dążeniu do realizacji powyższego celu Klaster ułatwia nawiązywanie współpracy pomiędzy firmami reprezentującymi polski przemysł cyberbezpieczeństwa – zrzeszone firmy mają okazję do wymiany doświadczeń, zdobywania kontaktów, czy know – how, ale także bezpośrednio mogą realizować wspólne inicjatywy komercyjne i nie tylko. W ramach działań Klastra firmy mogą angażować się również we współpracę z innymi interesariuszami, którzy mają realny wpływ na rynek cyberbezpieczeństwa (m.in. administracja publiczna, środowisko akademickie, trzeci sektor). Tylko dzięki współpracy wszystkich sektorów możliwe będzie wzmocnienie potencjału polskiego przemysłu cyberbepzieczeństwa.

W ciągu pierwszego roku działalności Klastra zrealizowany został szereg projektów rozwojowych, angażujących członków Klastra oraz interesariuszy zewnętrznych i niosących wartość dodaną zarówno dla samych twórców, jak i partnerów oraz potencjalnych klientów. Na liście projektów znalazły się m.in. :

- Cykl 6 wakacyjnych szkoleń dla Operatorów Usług Kluczowych - #CyberMadeInPoland Academy;
- Wewnętrzny cykl – Virtual Roundtables (networking oraz wymiana wiedzy pomiędzy członkami, a także partnerami Klastra);
- Raport dot. Stanu cyberbezpieczeństwa polskich firm 2021.

Promowanie polskich technologii za granicą wymaga skupienia się na ekspansji zagranicznej, dlatego też Klaster pomaga firmom we wchodzeniu na rynki zagraniczne, m.in. poprzez organizację misji handlowych (misja handlowa do Danii), czy nawiązywaniu kontaktów na rynkach docelowych (wyjazd na targi GITEX w Dubaju). #CMiP współpracuje roboczo z Ministerstwem Spraw Zagranicznych, a także należy do platformy Global EPIC, która zrzesza ponad 25 regionalnych ekosystemów innowacji dla cyberbezpieczenstwa z całego świata. Jako jedyna instytucja w Polsce Klaster posiada akredytację udzieloną przez Europejską Organizację Cyberbezpieczeństwa do nadawania znaku jakości Cybersecurity Made in Europe, który przyznawany jest europejskim podmiotom działającym w dziedzinie cyberbezpieczeńwta, jako narzędzie wspomagające budowanie zaufania do marki i promocji europejskich rozwiązań.

GLOBAL EPIC
Global Ecosystem of Ecosystems Platform in Innovation and Cybersecurity

W celu promocji polskich firm i ich rozwiązań prowadzony jest również comiesięczny newsletter branżowy, social media (Linkedin, Twitter), a także strona internetowa (na bieżąco aktualizowana). Ponadto, Klaster bierze aktywny udział w międzynarodowych (CYBERSEC) i krajowych (CyberGOV) formach wymiany informacji, tym samym budując rozpoznawalność Klastra jako „punktu kontaktowego" oraz *one-stop-shop* w temacie polskiego przemysłu cyberbezpieczeństwa.

## 2. Organizacja i struktura Klastra

Pełna nazwa Klastra w języku polskim brzmi: Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland, w języku angielskim: Polish Cybersecurity Cluster #CyberMadeInPoland. Klaster może posługiwać się nazwą skróconą: #CyberMadeInPoland.


### 2.1 Struktura i forma prawna Klastra

Inicjatorem Polskiego Klastra Cyberbezpieczeństwa #CyberMadeInPoland jest Instytut Kościuszki. Klaster nie posiada osobowości prawnej, a także nie ma charakteru spółki cywilnej. Został powołany na czas nieokreślony i w jego ramach działa: Koordynator Klastra, Rada Klastra, a także organ doradczy – Rada Doradcza. Koordynatorem Klastra jest spółka Polski Klaster Cyberbezpieczeństwa CyberMadeInPoland Sp. Z o.o. z siedzibą w Krakowie, natomiast Rada Klastra składa się z Koordynatora Klastra, Członków Założycieli oraz Członków Zwyczajnych Klastra, z których każdy ma obowiązek wyznaczenia jednego przedstawiciela upoważnionego do przedstawienia stanowiska Członka Klastra na forum Rady Klastra. Posiedzenia Rady Klastra odbywają się online lub fizycznie co najmniej dwa razy w roku i zwoływane są przez Koordynatora Klastra, który im przewodniczy.

Rada Doradcza funkcjonuje, jako ciało doradcze Klastra, zrzeszające ekspertów oraz liderów środowiska ICT. Celem jej działania jest stworzenie bezpośredniego kanału wymiany wiedzy, dobrych praktyk oraz informacji pomiędzy członkami Rady, a polskim przemysłem cyberbezpieczeństwa. Zadaniem Rady jest wsparcie Klastra w wyznaczeniu strategicznych kierunków działania. Członkowie Rady angażują się również operacyjnie i wspierają projekty Klastra leżące w zakresie ich zainteresowań. Członkowie Rady otrzymują na bieżąco materiały dotyczące funkcjonowania Klastra. Rada spotyka się co najmniej dwa razy w roku.

Zakres działalności Klastra obejmuje terytorium Rzeczypospolitej Polskiej oraz terytoria zagraniczne, natomiast siedziba znajduje się w Krakowie i prowadzona jest przez Koordynatora Klastra, czyli spółkę Polski Klaster Cyberbezpieczeństwa CyberMadeInPoland Sp. Z o.o.

## 3. Charakterystyka Klastra

Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland powstał we wrześniu 2020 roku i aktualnie zrzesza 47 członków oraz posiada 22 partnerów krajowych oraz zagranicznych

### 3.1 Członkowie Klastra

Do Klastra dołączyć mogą wszyscy zainteresowani, którzy są:

a) osobą fizyczną, prowadzącą jednoosobową działalność gospodarczą lub prowadzące działalność w formie spółki cywilnej posiadające obywatelstwo polskie;
b) polską osobą prawną;
c) polską jednostką organizacyjną nieposiadająca osobowości prawnej, którym ustawa przyznaje zdolność prawną:

- prowadzącą działalność gospodarczą związaną z branżą cyberbezpieczeństwa, posiadającą siedzibę główną przedsiębiorstwa w Polsce oraz większościowy udział polskiego kapitału;

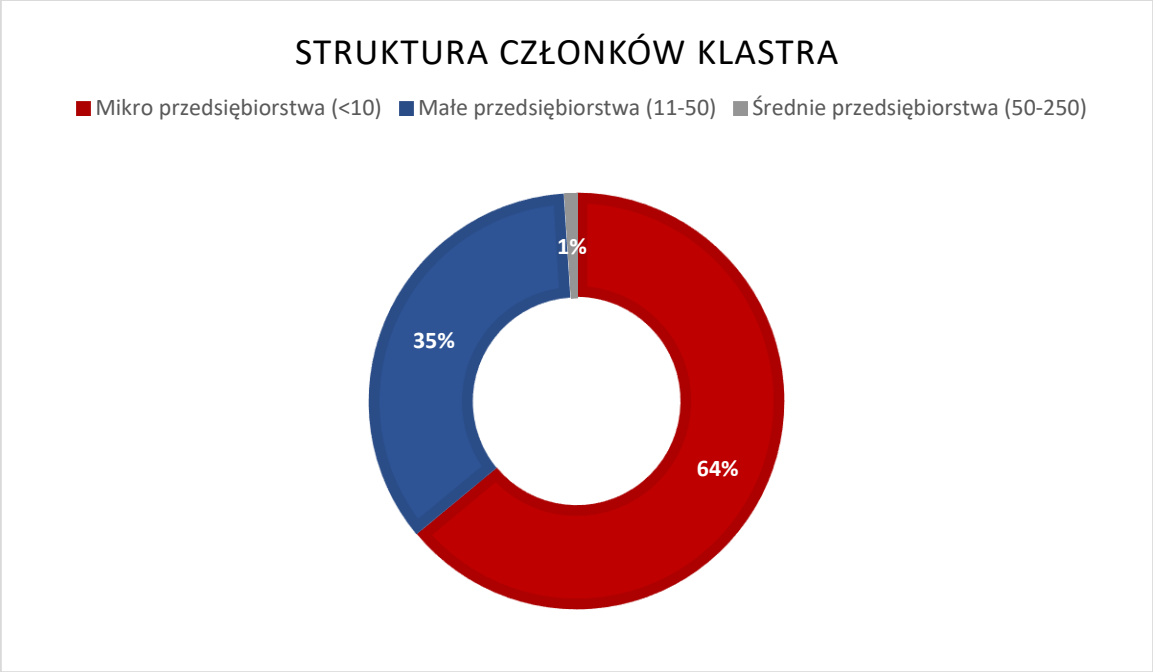
d) polską jednostką naukową.

Podmiot uzyskuje status Członka Klastra po uprzedniej akceptacji treści Regulaminu Klastra, podpisaniu i złożeniu Deklaracji Przystąpienia oraz jej zaakceptowaniu przez Koordynatora Klastra. Firmy przystępujące do Klastra opłacają również roczną składkę członkowską, równą dla wszystkich przedsiębiorców niezależnie od oferowanych produktów i usług oraz wielkości firmy czy długości jej funkcjonowania.

Ze względu na nadrzędny strategiczny cel Klastra, czyli promocję polskich rozwiązań cyberbezpieczeństwa, Członkami Zwyczajnymi Klastra zostać mogą tylko przedsiębiorcy świadczący usługi bądź oferujący

produkty cyberbezpieczeństwa. Regulamin Klastra przewiduje natomiast partnerstwa z organizacjami branżowymi, uczelniami wyższymi, organizacjami trzeciego sektora, administracją publiczną a także innymi podmiotami komercyjnymi zainteresowanymi współpracą z przedsiębiorcami zrzeszonymi w klastrze (patrz: rozdział 3.2)

Aktualnie Klaster zrzesza 47 podmiotów z całej Polski. Są to zarówno mikro i małe przedsiębiorstwa, jak i średnie oraz duże – procentowy udział liczby członków Klastra w poszczególnych sektorach został przedstawiony na Wykresie 1. Członkami Klastra #CyberMadeInPoland są polskie firmy oferujące produkty oraz usługi z branży cyberbezpieczeństwa.




Wykres 1. Struktura członków Klastra

Źródło: opracowanie własne

Członkami Klastra są MŚP co świadczy o wczesnym etapie rozwoju branży w Polsce. Firmy pokrywają wszystkie segmenty cyberbepzieczeństwa, oferując produkty i świadcząc usługi (procentowy podział członków Klastra na oferujących usługę oraz sprzedających produkt został przedstawiony na Wykresie 2.) z zakresu m.in.: ochrony przed złośliwymi oprogramowaniami, bezpieczeństwa aplikacji, Business

Continuity oraz reakcji na incydenty, compliance, informatyki śledczej, szyfrowania, human factors, potwierdzenia tożsamości, bezpieczeństwa IoT, cyberbezpieczeństwa przemysłu, managed services, bezpieczeństwa urządzeń mobilnych, bezpieczeństwa sieci oraz zarządzania ryzykiem.

Klaster jest źródłem korzyści i tworzy nową wartość dla wszystkich podmiotów zrzeszonych w Klastrze. Członkowie uczestniczą w życiu Klastra na równych prawach. Mają prawo do uczestniczenia w działaniach Klastra, brania udziału w pracach Klastra wyznaczając swojego przedstawiciela, korzystania z dorobku i innych form działalności Klastra (za zgodą Koordynatora Klastra), brania udziału w zebraniach, wykładach, czy imprezach organizowanych przez Klaster. Członkowie mogą również zgłaszać wnioski dotyczące zakresu działania Klastra, korzystać z publikacji wewnętrznych Klastra oraz używać w swojej działalności znaków graficznych Klastra, które są przeznaczone do identyfikacji Członków Klastra oraz korzystania z określenia: Członek Polskiego Klastra Cyberbezpieczeństwa #CyberMadeInPoland. Oprócz praw członkowie posiadają obowiązki, które mają przyczyniać się do rozwoju, podnoszenia rangi Klastra oraz zwiększania jego rozpoznawalności i zasięgu działania. Członek ma obowiązek również brać czynny udział w działalności Klastra i realizacji jego celów, jak również przestrzegania Regulaminu Klastra oraz Deklaracji Przystąpienia i uiszczania rocznej opłaty członkowskiej. Obligatoryjne jest również odbieranie korespondencji od Koordynatora Klastra za pomocą różnych kanałów przepływu informacji (wskazanego przez Członka Klastra). Wymagane jest także poinformowanie Koordynatora o zmianie adresu siedziby, zmianie formy prawnej w jakiej działa Członek, połączeniu lub przejęciu przez inny podmiot, zmianie osoby do kontaktu lub danych osoby do kontaktu.

## *3.2 Partnerzy Klastra*

Posiadanie statusu partnera daje możliwość udziału w projektach rozwojowych realizowanych w ramach Klastra oraz uczestnictwa w konsorcjach celowych tworzonych przez firmy zrzeszone w Klastrze w celu realizacji określonych zamówień, projektów lub grantów. Ponadto, partnerzy mogą brać udział lub współorganizować wspólne inicjatywy edukacyjne, szkolenia, konferencje, warsztaty, czy inne inicjatywy merytoryczne z zakresu cyberbezpieczeństwa. Partnerstwo umożliwia również dostęp do szerokiej gamy innowacyjnych rozwiązań członków Klastra oraz networking z liderami branży IT-security w Polsce, tym

samym nawiązując współpracę z ekspertami przy wykonaniu analiz, white papers i materiałów informacyjnych na temat trendów i rynków cyberbezpieczeństwa. #CMiP oferuje również partnerom szereg świadczeń promocyjnych oraz marketingowych, w szczególności jeżeli chodzi o udostępnianie logotypów. Podstawą nawiązania partnerstwa z Klastrem jest podpisania listu intencyjnego, który stanowi wyraz woli współpracy.

Wśród partnerów znajdują się:

- Instytucje Otoczenia Biznesu;
- uczelnie/ instytucje naukowo badawcze;
- organizacje branżowe;
- kancelaria prawna;
- klastry (krajowe ora zagraniczne);
- fundusze inwestycyjne.

Klaster podpisał również porozumienie o współpracy PW Cyber z Kancelarią Prezesa Rady Ministrów. Program Współpracy w Cyberbezpieczeństwie jest zbieżny z założeniami Strategii Cyberbezpieczeństwa Rzeczypospolitej Polski na lata 2019 – 2024. Podpisane porozumienie pozwala na wzmocnienie współpracy państwa i firm zajmujących się technologiami cyberbezpieczeństwa, a co za tym idzie zwiększenie bezpieczeństwa cyfrowych procesów, produktów oraz usług. Obszarami współpracy PW Cyber jest m.in.:

- podnoszenie kompetencji administracji publicznej w zakresie cyberbezpieczeństwa;
- wymiana informacji o cyberzagrożeniach;
- opracowywanie rekomendacji w zakresie cyberbezpieczeństwa;
- przygotowanie, prowadzenie oceny i certyfikacji cyberbezpieczeństwa.

Współpraca ma przede wszystkim na celu zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa.

## *3.3 Łańcuch wartości w Klastrze*

Łańcuch wartości Klastra #CyberMadeInPoland przedstawia w jaki sposób podmioty zrzeszone w Klastrze współpracują ze sobą, a tworzyć wartość dodaną w postaci działań, usług i produktów.

M.E. Porter wyodrębnia funkcje podstawowe oraz funkcje pomocnice, jakie występują w organizacji. Zgodnie z tym podziałem wyróżnione zostały następujące funkcje:

- podstawowe
  a) edukacja rynku – jednym z głównych działań Klastra jest budowanie rozpoznawalności i zaufania do polskich marek, kreowanie świadomości wyzwań cyberbezpieczeństwa u polskich odbiorców, edukacja sektora publicznego w tym Jednostek Samorządu Terytorialnego oraz monitorowanie dynamiki rynku cyberbezpieczeństwa;
  b) certyfikacja i regulacja - #CyberMadeInPoland wspiera tworzenie prorozwojowych polityk publicznych dla sektora IT security, standaryzację wymagań bezpieczeństwa względem określonych sektorów gospodarki, ale także dąży do ułatwiania i wsparcia MŚP oraz startupów w procesach certyfikacyjnych;
  c) ekspansja zagraniczna – zgodnie z założeniem Klastra budowana jest marka #CyberMadeInPoland na rynkach zagranicznych. Klaster wspiera polską dyplomację gospodarczą, działająca na rzecz przemysłu cyberbezpieczeństwa, a także wspiera budowę strategii wchodzenia na rynki zagraniczne dla MŚP oraz startupów;
  d) finansowanie – wsparcie publiczne dla sektora ICT, budowa partnerstw publiczno-prawnych na rzecz cyberbezpieczeństwa, alokacja funduszy krajowych i europejskich, mobilizacja środków prywatnych CVC oraz VC, wypracowanie mechanizmów budżetowych w administracji publicznej dla wydatków na bezpieczeństwo IT.

- wspomagające
  a) marketing – prowadzenie strony internetowej CyberMadeInPoland (w języku polskim oraz angielskim) przez Koordynatora Klastra, w połączeniu z wysyłką comiesięcznego newslettera oraz kanałami społecznościowymi (Linkedin, Twitter), pomoc w organizowaniu udziału członków Klastra w wydarzeniach targowo- wystawienniczych;
  b) integracja – Koordynator Klastra działa na rzecz integracji członków Klastra (networking, matchmaking);
  c) nawiązywanie partnerstw – Klaster czynnie monitoruje możliwości nawiązania partnerstw z instytucjami działającymi w obrębie cyberbezpieczeństwa.

## *3.4 Wyzwania i bariery*

Wyzwania Klastra #CyberMadeInPoland wynikają najczęściej z początkowej fazy rozwoju Klastra i dość krótkiego stażu na rynku (Klaster działa od 01.09.2020), a także z ograniczeń zasobów ludzkich i finansowych. Dodatkowym utrudnieniem jest aktualna sytuacja pandemiczna zarówno w Polsce, jak i na świecie. Wyzwania prezentują się on następująco:

- Brak infrastruktury laboratoryjnej/ badawczej, do której dostęp mieliby członkowie Klastra;
- Ograniczone możliwości spotykania się członków klastra, czy spotykania się z partnerami. Niestety sytuacja pandemiczna stała się jednym z głównych czynników blokujących możliwości spotykania się. Wpływa na to również obszar działalności Klastra – działa on na obszarze całej Polski, zatem przedsiębiorstwa znajdują się w różnych częściach kraju, co na pewno nie ułatwia organizacji spotkań;
- Braki w zasobach ludzkich, wynikające z niewystarczających funduszy Klastra, które nie pozwalają na zatrudnienie większej ilości pracowników, zwłaszcza specjalizujących się w bussines development;
- Ograniczony dostęp do szkoleń dla pracowników, co wiąże się z brakiem możliwości podnoszenia kwalifikacji. Podobnie jak powyższe wyzwanie wiąże się to z brakiem odpowiednich środków, które

mogłyby zostać przeznaczone na uczestnictwo w wydarzeniach podnoszących umiejętności i kompetencje;

- Brak nawiązania współpracy z jednostkami samorządu terytorialnego, co utrudnia, a wręcz uniemożliwia uczestnictwo w procesach współtworzenia, czy konsultacji dokumentów o charakterze strategicznym dla rozwoju regionu, czy realizację wspólnych projektów;
- Ze względu na wczesną fazę rozwoju Klaster utrudnione ma pozyskiwanie funduszy z różnego rodzaju dotacji, czy dofinansowań.

Bariery rozwoju branży cyberbezpieczeństwa zauważalne z perspektywy Klastra:

- Niska świadomość rynkowa dotycząca konieczności stosowania rozwiązań z zakresu cyberbezpieczeństwa;
- Brak odpowiedniej edukacji z zakresu cyberbezpieczeństwa;
- Niewystarczająca ilość dobrze wykwalifikowanej kadry z zakresu cyberbezpieczeństwa;
- Problemy z rekrutacją ekspertów ds. cyberbezpieczeństwa;
- Trudności w dotarciu do kluczowych interesariuszy w procesie sprzedaży;
- Niski poziom zaufania do polskich marek na rynku cyberbezpieczeństwa;
- Mały nacisk na promocję polskich rozwiązań z zakresu cyberbezpieczeństwa;
- Platformizacja rynku ICT;
- Postrzeganie bezpieczeństwa ICT z perspektywy kosztów, nie inwestycji;
- Niska dynamika B+R w dziedzinie cyberbezpieczeństwa;
- Niski poziom zaufania pomiędzy interesariuszami działającymi na rynku IT-sec;
- Mała liczba projektów realizowanych w konsorcjach z uczelniami wyższymi oraz instytucjami badawczo-rozwojowymi.

## 3.5 *Analiza SWOT*

| **Pozytywne** | **Negatywne** |
|---|---|
| **Mocne Strony** | **Słabe strony** |
| S 1 skupienie firm z całej Polski<br>S 2 dostępność przestrzeni biurowej<br>S 3 dostępność baz zasobów i kompetencji klastrowych (portfolio/bazy danych)<br>S 4 aktywne wsparcie internacjonalizacji<br>S 5 trwała współpraca z innymi podmiotami<br>S 6 aktywna działalność marketingowa<br>S 7 duży potencjał rozwoju Klastra poprzez obecność niemalże ¾ przedsiębiorców z obszaru cyberbezpieczeństwa w Klastrze | W 1 brak odpowiedniej infrastruktury laboratoryjnej/ badawczej<br>W 2 brak aktywnego wsparcia w podnoszeniu kompetencji z zakresu zarzadzania klastrem<br>W 3 brak zaangażowania niektórych członków Klastra<br>W 4 brak współpracy z jednostkami samorządu terytorialnego<br>W 5 słaba rozpoznawalność<br>W 6 relatywnie niewielki kapitał i ograniczone możliwości finansowe<br>W 6 brak statusu Kluczowego Klastra Krajowego |
| **Szanse** | **Zagrożenia** |
| O 1 Publiczne programy wsparcia dla inicjatyw klastrowych<br>O 2 możliwość promocji firm oraz Klastra poza granicami kraju<br>O 3 wzrost liczby ataków ransomware oraz wycieku danych, co sprawia, że rośnie świadomość wśród zarządzających przedsiębiorstwami | T 1 Niska świadomość społeczeństwa na temat zagrożeń wynikających z cyber ataków<br>T 2 ciągle ewoluująca sytuacja prawna w obszarze cyberbezpieczeństwa<br>T 3 Ograniczone środki przedsiębiorstw, które niechętnie przeznaczają je na bezpieczeństwo IIT<br>T 4 Zagrożenia pandemiczne, utrudniające networking wśród członków Klastra<br>T5 ograniczone możliwości finansowania (składki) |

Tabela 1. Analiza SWOT

Źródło: opracowanie własne

# 4. Strategia rozwoju Polskiego Klastra Cyberbezpieczeństwa #CyberMadeInPoland

## 4.1 Wizja Klastra

Wizją nazywamy określenie pożądanego stanu i wizerunku Klastra, do którego doprowadzić mają podejmowane przez kierownictwo oraz pracowników działania. Wizja Polskiego Klastra Cyberbezpieczeństwa #CyberMadeInPoland przedstawia się następująco:

Rozpoznawalny i wiarygodny Krajowy Klaster Kluczowy o globalnym potencjale oddziaływania, wspierający rozwój polskiego przemysłu cyberbezpieczeństwa we współpracy z nauką, biznesem, jednostkami samorządowymi i rządowymi, a także kształtujący nowe kierunki rozwoju. cyberbezpieczeństwa wraz z przedstawicielami innych sektorów gospodarki.

## 4.2 Misja Klastra

Misja zawiera w sobie precyzyjny manifest najważniejszych celów Klastra, czyli stanowi swego rodzaju wizytówką, opisującą rolę organizacji. Wartości akcentujące specyficzną rolę Klastra zawarte są w zaprezentowanej poniżej misji Klastra:

Stworzenie platformy współpracy oraz promocji polskiego przemysłu cyberbezpieczeństwa w celu kształtowania i rozwoju bezpiecznej cyberprzestrzeni w Polsce oraz promowania polskich firm poza granicami kraju. Klaster stymulować ma także współpracę sektora z instytucjami naukowymi, podmiotami administracji publicznej, organizacjami wsparcia biznesu, międzynarodowymi korporacjami, izbami branżowymi i handlowymi, oraz innymi partnerami.

## *4.2 Cele strategiczne*

Zgodnie z przyjętym Regulaminem Polskiego Klastra Cyberbezpieczeństwa #CyberMadeInPoland celem strategicznym funkcjonowania Klastra jest tworzenie efektywnego systemu współpracy Członków Klastra prowadzącego do ich dynamicznego rozwoju, wzrostu konkurencyjności na rynku oraz poprawy efektywności ich działania.

## *4.3 Cele szczegółowe*

Cele szczegółowe odnoszą się do celu strategicznego – dopracowują go i odnoszą się bezpośrednio do przedmiotu działalności organizacji. Regulamin Klastra wyróżnia następujące cele szczegółowe:

1) Współpraca Członków Klastra w zakresie docierania do poszczególnych segmentów klientów na polskim rynku;
2) Współpraca Członków Klastra w zakresie docierania do klientów oraz kanałów sprzedaży na rynkach zagranicznych;
3) Uczestnictwo w Programach Współpracy w zakresie cyberbezpieczeństwa tworzonych przez organy polskiej administracji publicznej;
4) Organizacja misji handlowych na wybrane rynki zagraniczne;
5) Monitoring oraz wspólne ofertowanie w ramach zamówień publicznych;
6) Wsparcie tworzenia przez wszystkich lub wybranych członków Klastra, konsorcjów w ramach aplikacji o fundusze krajowe oraz europejskie, w tym m.in. w ramach Programu Cyfrowa Europa, Programu Horyzont Europa, Europejskiego Funduszu Rozwoju Regionalnego i Funduszu Spójności, oraz, innych dostępnych w czasie funkcjonowania Klastra.

## 5. Działania

| Działanie główne | Działanie szczegółowe | Wskaźnik |
|---|---|---|
| **Edukacja rynku** | Budowanie rozpoznawalności i zaufania do polskich marek na rynku cyberbezpieczeństwa | • Portfolio prezentujące i promujące firmy zrzeszone w klastrze oraz ich usługi i produkty,<br>• Portfolio udostępnione na stronie internetowej,<br>• Przesyłanie portfolio do potencjalnych partnerów,<br>• Promocja Klastra poprzez stronę internetową, portale społecznościowe (Linkedin, Twitter) oraz comiesięczny newsletter,<br>• Uczestnictwo w konferencjach (CYBERSEC, CyberGOV, KSC, itp.). |
| | Kreowanie świadomości wyzwań cyberbezpieczeństwa u polskich odbiorców | • Stworzenie raportów na temat stanu cyberbezpieczeństwa,<br>• Webinary dedykowane dla użytkowników końcowych. |
| | Edukacja sektora publicznego, w tym Jednostek Samorządu Terytorialnego | • Szkolenia dla administracji publicznej,<br>• Organizacja webinarów w ramach „Akademii Cyberbezpiecznego Samorządu”, |

| | | |
|---|---|---|
| | | • Kontynuacja projektu szkoleń dla Operatorów Usług Kluczowych,<br>• Podnoszenie kompetencji administracji publicznej w zakresie cyberbezpieczeństwa w ramach PW Cyber. |
| | Monitorowanie dynamiki rynku cyberbezpieczeństwa w Polsce | • Śledzenie portali branżowych,<br>• Monitorowanie nowych dokumentów regulujących cyberbezpieczeństwo. |
| **Współpraca w zakresie certyfikacji oraz regulacji rynku cyberbezpieczeństwa** | Wsparcie rozwoju elementów polskiego systemu certyfikacji | • Wsparcie w opracowaniu procesu certyfikacji dla produktów oraz usług cyberbezpieczeństwa. |
| | Wsparcie tworzenia rozwojowych polityk publicznych dla sektora cyberbezpieczeństwa | • Współpraca z KPRM,<br>• Współpraca z jednostkami samorządu terytorialnego. |
| | Standaryzacja wymagań bezpieczeństwa względem określonych sektorów gospodarki | • Opublikowanie standardów dotyczących wymagań bezpieczeństwa względem określonych sektorów gospodarki. |
| | Promocja ułatwień i wsparcia dla Małych i Średnich Przedsiębiorstw (MŚP) oraz | • Podjęcie współpracy z Regionalnymi Agencjami Rozwoju Regionalnego, |

| | | |
|---|---|---|
| | startupów w procesach certyfikacyjnych | • Współpraca z parkami technologicznymi (Krakowski Park Technologiczny, Kielecki Park Technologiczny). |
| **Współpraca w zakresie ekspansji zagranicznej** | Budowa marki #CyberMadeInPoland na rynkach zagranicznych | • Promowanie polskich firm na rynkach zagranicznych poprzez udział w różnego rodzaju targach (np. GITEX) oraz misjach handlowych (np. misja handlowa do Danii),<br>• Organizacja autorskiego CTF,<br>• Zbudowanie przedstawicielstwa na rynkach zagranicznych,<br>• Zrealizowanie wizyt studyjnych,<br>• Publikacja na temat stanu cyberbezpieczeństwa w ujęciu europejskim/ globalnym,<br>• Organizacja szkoleń, spotkań, publikacji i analiz w zakresie prawnych i gospodarczych uwarunkowań niektórych rynków zagranicznych (np. w ramach wewnętrznego cyklu Virtual Roundtable). |
| | Wsparcie polskiej dyplomacji gospodarczej dla przemysłu cyberbezpieczeństwa | |
| | Wsparcie w budowie strategii wchodzenia na rynki zagraniczne dla MŚP oraz startupów | |
| **Współpraca w zakresie pozyskiwania finansowania** | Budowę Partnerstwa Prywatno – Publicznego (PPP) na rzecz cyberbezpieczeństwa | • Poszukiwanie nowych możliwości finansowania,<br>• Tworzenie konsorcjów celowych, |

| | | |
|---|---|---|
| | Pozyskiwanie dofinansowań oraz inwestycji w ramach dostępnych funduszy, w tym w szczególności:<br>a) Funduszy Unii Europejskiej,<br>b) Krajowych środków publicznych,<br>c) Środków prywatnych, w tym inwestycji wysokiego ryzyka (CVC, VC) | • Rozwój usług konsultingowych z zakresu budowania konsorcjów przetargowych,<br>• Pozyskiwania partnerów VC oraz CVC. |
| **Stymulowanie rozwoju polskich rozwiązań z zakresu cyberbezpieczeństwa** | Wielopoziomowe działania promujące rozpoczęcie kariery w sektorze cyberbezpieczeństwa | • Popularyzacja polskich rozwiązań z zakresu cyberbezpieczeństwa,<br>• Zaangażowanie w procesy związane z tworzeniem innowacji w Klastrze,<br>• Promowanie zatrudniania osób o wysokich kwalifikacjach,<br>• Podnoszenie kompetencji młodych pasjonatów cyberbezpieczeństwa poprzez zorganizowanie autorskiego CTF. |
| **Zarządzanie i rozwijanie inicjatywy klastrowej** | Budowa zasobów i rozwijanie kluczowych kompetencji Klastra | • Pozyskanie nowych podmiotów,<br>• Pozyskanie nowych partnerów ( w szczególności JST),<br>• Podjęcie współpracy z uczelniami wyższymi w zakresie prowadzenia |

| | | |
|---|---|---|
| | | wzajemnych wizyt studyjnych, warsztatów, praktyk, zawodowych,<br>• Opracowanie bazy wiedzy o członkach (mapa kompetencji),<br>• Pozyskanie nowych podmiotów, posiadających rozwinięte zaplecze badawczo-rozwojowe,<br>• Opracowanie Kodeksu Etyki,<br>• Dywersyfikacja przychodów Klastra. |
| | Wprowadzenie zasad Społecznej Odpowiedzialności Biznesu do działalności Klastra | • Tworzenie przyjaznych pracownikom miejsc pracy,<br>• Zwiększanie świadomości na temat CSR wśród członków Klastra,<br>• Promowanie rozwiązań cleantech. |
| | Integracja wewnętrzna członków Klastra | • Prowadzenie i organizowanie spotkań networkingowych,<br>• Prowadzenie matchmakingu (spotkania B2B, B2C, misje gospodarcze itp.),<br>• Zorganizowanie kongresu Klastra,<br>• Organizowanie Rad Klastra, |

| | | |
|---|---|---|
| | | • Opracowanie i promocja standardów etycznego postepowania w Klastrze,<br>• Organizowanie spotkań informacyjnych i kooperacyjnych członków Klastra i instytucji B+R. |
| | Rozwój zasobów ludzkich | • Podnoszenie umiejętności i kompetencji w zakresie zarządzania klastrem,<br>• Aktywniejszy skauting dostępnych na rynku szkoleń,<br>• Przystąpienie do Cluster Collaboration Platform,<br>• Przystąpienie do Mapy Klastrów Polskich,<br>• Pozyskiwanie środków na rozwój kompetencji pracowników,<br>• Pozyskanie/ wyszkolenie pracowników z zakresu eksportu, marketingu, HR. |
| | Wzmacnianie marki Klastra i jego znaczenia w branży cyberbezpieczeństwa na rynku polskim i zagranicznym | • Budowanie partnerstw (merytorycznych i strategicznych) lokalnych, regionalnych, ponadregionalnych, międzysektorowych oraz międzynarodowych istotnych jeżeli chodzi o rozwój cyberbezpieczenstwa, |

| | | |
|---|---|---|
| | | • Partnerstwa z zagranicznymi klastrami zajmującymi się cyberbezpieczeństwem,<br>• Obecność na wydarzeniach branżowych,<br>• Obejmowanie patronatem wydarzeń branżowych i około branżowych,<br>• Aktywność targowo-wystawiennicza,<br>• Organizowanie branżowych konferencji i seminariów,<br>• Kontynuacja prowadzenia projektów rozwojowych oraz zapoczątkowanie nowych,<br>• Opracowanie spójnej strategii wizerunkowej Klastra,<br>• Intensyfikacja działań PR-owych i marketingowych,<br>• Zatrudnienie PR managera,<br>• Przystąpienie do Mapy Klastrów Polskich i European Cluster Collaboration Platform. |

Tabela 2. Działania główne i szczegółowe

Źródło: opracowanie własne

# 6. Źródła finansowania

Założeniem inicjatywy jest finansowanie jej funkcjonowania z różnych źródeł. Aktualnie są to roczne składki członkowskie oraz finansowanie poszczególnych projektów określone na podstawie odrębnych umów. Klaster zakłada również finansowanie działań z funduszy europejskich, funduszy krajowych oraz innych funduszy publicznych i prywatnych.

## 6.1 Analiza potencjalnych instrumentów wsparcia

Analiza możliwości finansowych organizacji wykazała jednoznacznie, że bez wsparcia zewnętrznego możliwości rozwoju są ograniczone i uniemożliwione zostanie realizowanie zaplanowanych celów statutowych. W celu znalezienia alternatywnych instrumentów wsparcia przeanalizowano szereg konkursów oraz działań oferowanych przez instytucje wspierające rozwój przedsiębiorczości oraz organizacji pozarządowych. Potencjalne instrumenty wsparcia prezentują się następująco:

- Sektorowe Rady ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo – rada ma przyczynić się do kompleksowej identyfikacji i prognozowania potrzeb kwalifikacyjno – zawodowych sektora Telekomunikacji i Cyberbezpieczeństwa w Polsce.
- PO WER,
- Projekty B+R (POIR,RPO WSL, NCBiR),
- Krajowy Fundusz Szkoleniowy,
- Dotacje celowe z Ministerstwa Właściwego,
- Wsparcie w ramach RPO,
- Program Fundusze Europejskie dla Nowoczesnej Gospodarki,
- Program Fundusze Europejskie na Rozwój Cyfrowy,
- COSME,
- Horizon Europe.

## 7. *Wdrażanie i monitorowanie strategii*

Wszystkie jednostki, będące uczestnikami działalności klastrowej Polskiego Klastra Cyberbezpieczeństwa #CyberMadeInPoland są odpowiedzialne za wdrażanie założeń strategii. Za realizację strategii bezpośrednio odpowiedzialny jest Koordynator Klastra – nadzoruje on implementacje wskazanych działań, monitoruje je oraz ewaluuje. Dodatkowo, Koordynator odpowiedzialny jest za długoterminowe zarządzanie i monitorowanie strategii, przy czym również koordynuje działania operacyjne konieczne do zrealizowania w celu osiągnięcia celu strategicznego.

Całość podejmowanych działań opierać się musi na zasadzie partnerstwa, gdzie każdy z partnerów jest równy i może uczestniczyć we wdrażaniu strategii. Wypracowane już mechanizmy współpracy wewnątrz Klastra zwiększą efektywność podejmowanych wspólnie wysiłków.
Działania opisane w Tabeli 2. Ogólnie określają ramy realizacji strategii, dzięki czemu możliwe jest elastyczne dostosowanie strategii do zmian w otoczeniu polityczno-prawnym, ekonomicznym, technicznym, społeczno-kulturowym oraz międzynarodowym. Ponadto możliwa będzie reakcja na wyzwania i potrzeby, z którym zmagają się członkowie Klastra.

System monitoringu realizacji Strategii Klastra będzie obejmował procesy zachodzące wewnątrz Klastra oraz wszelkie procesy zachodzące w otoczeniu Klastra (procesy zewnętrzne). Analizowane będą wszystkie obszary związane z działaniami zawartymi w strategii rozwoju Klastra tj. z zakresu edukacji rynku w obszarze cyberbezpieczeństwa, certyfikacji i regulacji rynku cyberbezpieczeństwa, możliwości związanych z internacjonalizacją, możliwości finansowania, rozwoju polskich rozwiązań cyberbezpieczeństwa, możliwości zarządzania i rozwoju klastrów, a także wszelkie możliwości związane z innowacyjnym podejściem do rozwoju MŚP oraz startupów w obszarze cyberbezpieczeństwa. Analiza będzie przeprowadzana na podstawie obserwacji rynku cyberbezpieczeństwa, oficjalnych danych statystycznych, badań własnych (np. stworzenie raportu), czy danych pozyskanych w trakcie dyskusji z uczestnikami Klastra.


Polski Klaster
Cyberbezpieczeństwa
#CyberMadeInPoland
ul. Feldmana 4/9-10
31-130 Kraków, Poland

+48 669 614 854

office@cybermadeinpoland.pl

cybermadeinpoland.pl