Ministerstwo Cyfryzacji

Regulamin Programu Współpracy w Cyberbezpieczeństwie

§ 1.

Cel Programu

Program Współpracy w Cyberbezpieczeństwie (dalej: PWCyber, Program) powstał z inicjatywy Ministra Cyfryzacji[1], a głównym jego celem jest zbudowanie silnego, zintegrowanego podejścia do cyberbezpieczeństwa, które łączy zasoby, wiedzę i doświadczenie administracji publicznej oraz sektora prywatnego w celu skuteczniejszej ochrony przed zagrożeniami w cyberprzestrzeni w skali kraju, poprzez prowadzenie wspólnych działań na rzecz poprawy poziomu bezpieczeństwa cyfrowego, minimalizowania ryzyka cyberzagrożeń i zwiększania odporności na cyberataki.

§ 2.

Założenia Programu PWCyber

1. Dobrowolne i aktywne uczestnictwo w Programie.
2. Wypracowanie długofalowej, trwałej i efektywnej współpracy ministra właściwego ds. informatyzacji z partnerami Programu.
3. Jednakowy format uczestnictwa dla wszystkich partnerów Programu.
4. Brak zobowiązań finansowych.
5. Wzmacnianie zaufania w zakresie ochrony danych i zarządzania cyberzagrożeniami.
6. Ciągłe doskonalenie współpracy oraz adaptacja do zmieniającego się krajobrazu cyberzagrożeń poprzez wspólne monitorowanie sytuacji i aktualizację procedur reagowania.

§ 3.

Obszary współpracy w ramach Programu

1. Program obejmuje V obszarów współpracy:

1) I obszar - podnoszenie kompetencji podmiotów krajowego systemu cyberbezpieczeństwa w zakresie świadomości zagrożeń, metod ataków w cyberprzestrzeni oraz prawnych, organizacyjnych i technicznych umiejętności

[1] Stosownie do § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 grudnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. z 2023 r. poz. 2720) Minister Cyfryzacji kieruje działem administracji rządowej - informatyzacja.

przeciwdziałania zagrożeniom w systemach i sieciach informacyjnych. Działania w tym obszarze mogą obejmować w szczególności:

a) udostępnianie materiałów szkoleniowych oraz informacji o ścieżkach szkoleniowych podnoszących kwalifikacje użytkowników i personelu odpowiadającego za cyberbezpieczeństwo w zakresie korzystania z oferowanych produktów i usług;

b) organizację wydarzeń szkoleniowych i warsztatowych m.in. celem prezentacji metod korzystania z funkcji zabezpieczających, w tym mechanizmów podnoszących odporność na cyberataki oraz zwiększających poziom ochrony informacji;

c) prowadzenie kampanii uświadamiających, organizacja konkursów w zakresie najlepszych praktyk w korzystaniu z produktów i usług podnoszących cyberbezpieczeństwo.

2) II obszar - identyfikacja podatności i zagrożeń, wymiana informacji oraz wypracowywanie metod zgłaszania i obsługi incydentów, w tym również organizacja i udział w ćwiczeniach.

3) III obszar - opracowywanie rekomendacji w zakresie bezpieczeństwa systemów informacyjnych i przetwarzanych informacji oraz usług, konfiguracji urządzeń i oprogramowania w sposób maksymalizujący skuteczność mechanizmów zabezpieczających[2].

4) IV obszar - wymiana wiedzy, doświadczenia w zakresie certyfikacji cyberbezpieczeństwa produktów i usług.

5) V obszar - promowanie innowacyjnych rozwiązań i projektów w dziedzinie cyberbezpieczeństwa oraz budowanie partnerstwa z podmiotami krajowego systemu cyberbezpieczeństwa zainteresowanymi opracowywaniem, testowaniem i wdrażaniem nowych rozwiązań.

2. Minister może dodawać kolejne obszary współpracy w ramach Programu poza ww. w trakcie jego trwania.

§ 4.

Koordynacja i monitorowanie realizacji Programu

1. Koordynatorem Programu jest Departament Cyberbezpieczeńtwa Ministerstwa Cyfryzacji (dalej: koordynator). Dane kontaktowe koordynatora: Departament Cyberbezpieczeństwa, ul. Królewska 27, 00-060 Warszawa, telefon: + 48 22 245 59 22, e-mail: sekretariat.DC@cyfra.gov.pl

[2] ang. *Security Baselines.*

2. Koordynator raz do roku dokonuje ewaluacji funkcjonowania Programu pod kątem osiąganych celów. Przegląd obejmuje ocenę zrealizowanych inicjatyw na rzecz podmiotów krajowego systemu cyberbezpieczeństwa, efektywności i wyników poszczególnych projektów realizowanych przez partnerów w ramach Programu. Weryfikacja ma na celu doskonalenie współpracy.
3. Wyniki ewaluacji wraz z ewentualnymi rekomendacjami dot. dalszych aktywności w ramach Programu przedstawiane są w rocznym raporcie z realizacji Programu.

§ 5.

Warunki przyjęcia i kryteria udziału w Programie

1. Zgłoszenia do Programu przyjmowane są przez cały rok kalendarzowy.
2. W Programie mogą uczestniczyć podmioty oraz firmy technologiczne, których działalność związana jest z cyberbezpieczeństwem, które oferują usługi lub produkty w zakresie cyberbezpieczeństwa od co najmniej 5 lat (dalej: kandydat).
3. Kandydat musi dysponować odpowiednim potencjałem, wiedzą techniczną, doświadczeniem, know-how i uprawnieniami, umożliwiającymi współpracę w ramach Programu.
4. Kandydat powinien cieszyć się dobrą reputacją w swojej branży.
5. Program jest otwarty dla kandydatów z państw Unii Europejskiej, Organizacji Traktatu Północnoatlantyckiego oraz państw partnerskich NATO.
6. Z dniem podpisania porozumienia kandydat zostaje włączony do Programu jako Partner.
7. Kandydat, który dostał odmowę włączenia do Programu może złożyć ponowną aplikację po upływie roku od dnia jej otrzymania.
8. Warunkiem udziału w Programie jest:
   1) przesłanie przez kandydata portfolio dotyczącego prowadzonej działalności oraz wypełnienie ankiety weryfikacyjnej (załącznik nr 2),
   2) pozytywna ocena kandydata dokonana przez koordynatora na podstawie wypełnionej ankiety weryfikacyjnej i przesłanego portfolio,
   3) akceptacja przez kandydata regulaminu Programu,
   4) podpisanie porozumienia o współpracy w zakresie Programu według wzoru ustalonego przez ministra właściwego do spraw informatyzacji.
9. Wszelkie odstępstwa od obowiązującego wzoru porozumienia ustalane są w drodze negocjacji z koordynatorem.
10. W przypadku braku akceptacji przez koordynatora proponowanych przez kandydata zmian we wzorze porozumienia, koordynator może odstąpić od podpisania porozumienia.
11. Do Programu nie będą przyjmowane podmioty, które:
    1) funkcjonują na rynku krócej niż 5 lat oraz takie, które zajmują się wyłączenie odsprzedażą produktów i usług innych firm,
    2) są mikroprzedsiębiorcami,
    3) zostały umieszczone (oraz ich pracownicy) na liście sankcyjnej MSWiA,

4) na które zostały wprowadzone ograniczenia przez państwa sojusznicze (m.in. USA, Wielka Brytania, państwa członkowskie UE), których sprzęt i oprogramowanie zostało wykluczone na podstawie pochodzenia z krajów wysokiego ryzyka ponieważ może być ono wykorzystywane do zagrożenia poufności, integralności i dostępności danych i usług. Zgodnie z Rezolucją Parlamentu Europejskiego z dnia 1 czerwca 2023 r. w sprawie obcych ingerencji we wszystkie procesy demokratyczne w Unii Europejskiej, w tym dezinformacji.

12. Ministerstwo Cyfryzacji zastrzega możliwość odmowy przyjęcia kandydata do Programu, jeśli uzna, że nie gwarantuje on wystarczającego poziomu zaufania w ramach prowadzonej działalności.

§ 6.

Zasady współpracy

1. Partner zobowiązany jest do zachowania bezwzględnej poufności wszelkich informacji udostępnianych i przekazywanych w ramach Programu.
2. Partner wyraża zgodę na wykorzystanie przez Ministra należącego do niego znaku słowno-graficznego (logotypu) w celu promocji wspólnie realizowanych przedsięwzięć i projektów.
3. Minister może zwrócić się z wnioskiem o dołączenie dodatkowych podmiotów administracji publicznej i podmiotów nadzorowanych do porozumienia z danym partnerem, z zastrzeżeniem uzyskania uprzedniej zgody partnera.
4. Partner zobowiązany jest do wyznaczenia osób odpowiedzialnych za kontakty robocze oraz do bieżącego aktualizowania danych kontaktowych, celem zapewnienia sprawnej komunikacji w ramach Programu.
5. Współpraca przewiduje aktywny udział partnerów w organizacji konferencji, seminariów, warsztatów technicznych, kampanii edukacyjnych, szkoleń online dla podmiotów krajowego systemu cyberbepieczeństwa.
6. Współpraca przewiduje cykliczne spotkania z partnerami Programu, których celem będzie ewaluacja wspólnie prowadzonych działań.

§ 7.

Formy współpracy

1. Współpraca partnera z Ministrem może być prowadzona w różnej formie, w zależności od zadeklarowanych propozycji współpracy, zgodnie z podpisanym porozumieniem.
2. Program daje możliwość udziału partnerów w konsultacjach dokumentów strategicznych, aktów normatywnych, bezpośredniej wymiany informacji o cyberzagrożeniach, wymiany informacji o zagrożeniach i incydentach.
3. Partner może dołączyć do rozpoczętych lub zainicjować powstanie nowych działań np. powstanie publikacji (zalecenia, poradniki), kampanii, akcji edukacyjnych oraz konkursów.

4. Partner może inicjować powołanie grup roboczych wspólnie z innymi partnerami będącymi w Programie, których celem będzie wypracowanie np. rekomendacji, procedur i standardów w obszarze Cyberbezpieczeństwa.
5. Powołanie grupy roboczej wymaga uzyskania akceptacji kierunku i zakresu prac przez koordynatora Programu.

§ 8.

Wykluczenie Partnera z Programu

1. Partner zostanie wykluczony z Programu w przypadku:
   1) braku podejmowanych inicjatyw na rzecz współpracy w ramach Programu,
   2) gdy w wyniku rocznej weryfikacji funkcjonowania Programu pod kątem osiąganych celów Partner nie wykazał aktywności na rzecz Programu w danym roku,
   3) złamania postanowień zawartego porozumienia o współpracy,
   4) złamania zasady zachowania w bezwzględnej poufności wszelkich informacji udostępnianych i przekazywanych w ramach Programu,
   5) po osiągnięciu celu współpracy lub na prośbę Partnera.
2. Partner, który został wykluczony z Programu może ubiegać się o ponowne przystąpienie do Programu po upływie 1 roku.
3. Wykluczenie z Programu zostanie stwierdzone na piśmie i staje się skuteczne z dniem doręczenia partnerowi oświadczenia Ministra w tym zakresie.

§ 9.

Postanowienia końcowe

1. Regulamin wchodzi w życie z dniem 3 marca 2025 r.
2. Urząd Ministra Cyfryzacji obsługuje Ministerstwo Cyfryzacji pod adresem: ul. Królewska 27, 00-060 Warszawa.
3. O wszelkich zmianach regulaminu partnerzy będą informowani w formie elektronicznej, wraz z podaniem terminu wejścia zmian w życie.