

PWCyber

Program Współpracy w Cyberbezpieczeństwie

Partnerstwo Publiczno-Prywatne
na rzecz krajowego systemu cyberbezpieczeństwa



Program Współpracy w Cyberbezpieczeństwie (PWCyber) został uruchomiony w 2019 r.

Jest to przedsięwzięcie niekomercyjne o charakterze partnerstwa publiczno-prywatnego, które jest realizowane na rzecz krajowego systemu cyberbezpieczeństwa.



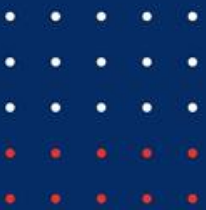
Współpraca w ramach PWCyber ma charakter publiczny, transparentny i pozafinansowy

- Formuła programu partnerskiego jest otwarta dla wszystkich podmiotów, w tym także dla organizacji pozarządowych, które chciałyby pracować nad rozwojem systemu cyberbezpieczeństwa w Polsce.
- Warunkiem przystąpienia do Programu jest zawarcie porozumienia o współpracy, które ma charakter listu intencyjnego.
- Zakres programu jest taki sam dla każdego partnera porozumienia.
- Strony porozumienia zobowiązują się m.in. do współpracy w celu wymiany informacji o potencjalnych cyberzagrożeniach oraz zdarzeniach noszących znamiona zaplanowanych cyberataków na różne sektory gospodarki i sektor publiczny.



Podstawowe założenia PWCyber

1. Dobrowolne i aktywne uczestnictwo w Programie.
2. Format partnerstwa - porozumienie jednakowe dla wszystkich podmiotów.
3. Brak zobowiązań finansowych.
4. Klauzula zachowania poufności wskazanych informacji (NDA).
5. Możliwość przystąpienia innych podmiotów – za zgodą obu stron.



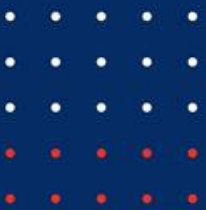


PWCyber – zaufanie i bezpieczeństwo

PWCyber, ze względu na konieczność budowania zaufanych relacji z partnerami technologicznymi, jest otwarty dla firm z państw:

- Unii Europejskiej
- Organizacji Traktatu Północnoatlantyckiego
- państw partnerskich NATO

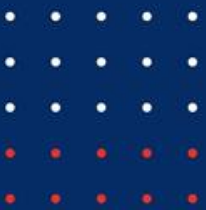
W obecnej fazie rozwoju programu nie jest przewidywany udział firm spoza UE, NATO i państw partnerskich NATO.





Obszary współpracy PWCyber

1. Podnoszenie kompetencji administracji publicznej w zakresie cyberbezpieczeństwa
2. Wymiana informacji o cyberzagrożeniach
3. Opracowywanie rekomendacji w zakresie cyberbezpieczeństwa
4. Przygotowanie i prowadzenie oceny i certyfikacji cyberbezpieczeństwa
5. Upowszechnianie informacji o innowacjach w cyberbezpieczeństwie



1. Podnoszenie kompetencji kadr administracji publicznej w zakresie cyberbezpieczeństwa

Działania w tym obszarze mogą obejmować:

- udostępnianie materiałów szkoleniowych (w tym multimedialnych) oraz informacji o ścieżkach szkoleniowych podnoszących kwalifikacje użytkowników i personelu odpowiadającego za cyberbezpieczeństwo w zakresie korzystania z oferowanych produktów i usług;
- 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;
- prowadzenie kampanii uświadamiających, organizacja konkursów w zakresie najlepszych praktyk w korzystaniu z produktów i usług podnoszących cyberbezpieczeństwo

2. Wymiana informacji o cyberzagrożeniach

- Identyfikacja podatności i zagrożeń
- Wymiana informacji oraz wypracowywanie metod zgłaszania i obsługi incydentów
- Organizacja i udział w ćwiczeniach



3. Opracowywanie rekomendacji w zakresie cyberbezpieczeństwa

Opracowywanie rekomendacji w zakresie:

- konfiguracji urządzeń;
- bezpieczeństwa oprogramowania;
- integracji usług w sposób maksymalizujący skuteczność mechanizmów zabezpieczających (ang. Security Baselines).



4. Przygotowanie i prowadzenie oceny i certyfikacji cyberbezpieczeństwa

- Opracowywanie nowych metod testów
- Przygotowanie nowych kryteriów oceny
- Udział i promowanie certyfikacji cyberbezpieczeństwa produktów i usług



5. Upowszechnianie informacji o innowacjach w cyberbezpieczeństwie

- Promowanie innowacyjnych rozwiązań i projektów w dziedzinie cyberbezpieczeństwa
- Budowanie partnerstwa z podmiotami Krajowego Systemu Cyberbezpieczeństwa zainteresowanymi opracowywaniem, testowaniem i wdrażaniem nowych rozwiązań



Jak dołączyć do Programu PWCyber?

- Skontaktuj się z nami - sekretariat.dc@mc.gov.pl
- Należy umówić się na spotkanie, aby omówić obszary i warunki współpracy w ramach Programu
- Konieczne jest zawarcie porozumienia o współpracy - porozumienie ma charakter listu intencyjnego. Ma ono mało zobowiązujący charakter i nie zakłada przekazywania informacji o charakterze wrażliwym a tylko danych publicznych.

Partnerzy Programu PWCyber

- Samsung Electronics Polska Sp. z o.o.
- Cisco International Limited
- Ericsson Sp. z o.o.
- Nokia Solutions and Networks
- Krypton Polska Sp. z o.o.
- IBM Polska Sp. z o.o.
- Thales Polska Sp. z o.o.
- Dell Sp. z o.o.
- Dynacon Sp. z o.o.
- Smartech IT Sp. z o.o.
- Media Sp. z o.o.,
- Oracle Polska Sp. z o.o.
- Fundacja Bezpieczna Cyberprzestrzeń
- Polski Klaster Cyberbezpieczeństwa Sp. z o.o.
- Securitum Szkolenia Sp. z o.o. (Sekurak.pl)
- HackingDept Sp. z o.o.
- Fudo Security Sp. z o.o.
- ICSec S.A.
- Amazon Web Services EMEA SARL Sp. z o.o.
- PROGET Sp. z o.o.
- Trafford IT Sp. z o.o.
- Integrated Solutions Sp. z o.o.

Zapraszamy do współpracy

Im więcej podmiotów będzie razem działać, tym lepiej dla bezpieczeństwa



Departament Cyberbezpieczeństwa

ul. Królewska 27

00-060 Warszawa

telefon: **+48 22 245 59 22**

e-mail: sekretariat.dc@mc.gov.pl