fundacja instytut
CYBERBEZPIECZEŃSTWA

Współpraca sektora publicznego z sektorem prywatnym w zakresie cyberbezpieczeństwa: ryzyko i korzyści

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Współczesny rozwój technologii niesie ze sobą nowe wyzwania, a jednym z priorytetów staje się zapewnienie bezpieczeństwa w cyberprzestrzeni. Ze względu na siłę wpływu podmiotów prywatnych na kształtowanie sieci internetowej kluczowym elementem skutecznej strategii cyberbezpieczeństwa jest współpraca pomiędzy sektorem publicznym a sektorem prywatnym. Niniejszy artykuł skupia się na analizie korzyści i zagrożeń wynikających z tego partnerskiego podejścia.

Ogólne zalety współpracy

Współpraca sektora publicznego z sektorem prywatnym przynosi wiele korzyści, wynikających z synergii połączenia zasobów obu sektorów. Sektor publiczny dostarcza wiedzę na temat globalnych zagrożeń, podczas gdy przedsiębiorstwa prywatne dysponują zaawansowanymi technologiami i doświadczeniem w monitorowaniu oraz reagowaniu na ataki. Skoordynowane działania umożliwiają szybką identyfikację i neutralizację potencjalnych ataków, zapewniają stałą aktualizację systemów obronnych i efektywne wykorzystanie zasobów publicznych. Wspólne podejście do rozwiązywania problemów i wymiana wiedzy pomiędzy sektorami umożliwiają efektywne wykorzystanie zasobów, co przekłada się na skuteczniejszą ochronę cyberprzestrzeni. Ponadto partnerstwo między sektorem publicznym a sektorem prywatnym wspiera innowacje, co jest niezmiernie istotne w dynamicznym środowisku cybernetycznym.

Istnieje wiele przykładów światowych inicjatyw w zakresie współpracy, takich jak National Cyber Security Centre (NCSC) w Wielkiej Brytanii, InfraGard w Stanach Zjednoczonych czy Joint Cyber Security Centre (JCSC) w Australii. Świadczą one o skuteczności współpracy między sektorem publicznym a sektorem prywatnym w zakresie cyberbezpieczeństwa. Organizacje takie jak CERT Polska czy European Union Agency for Cybersecurity (ENISA) odgrywają istotną rolę w budowaniu partnerstw i wymianie informacji.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Źródło: James Keenan, Flickr (CC 2.0)

Uwarunkowania prawne współpracy

W Polsce zasady współpracy między sektorem publicznym a sektorem prywatnym w zakresie cyberbezpieczeństwa są szczegółowo określone. Ustawy obejmujące ochronę informacji niejawnych, danych osobowych, telekomunikacji, krajowy system cyberbezpieczeństwa, strategię cyberbezpieczeństwa oraz prawo zamówień publicznych stanowią niezbędny fundament, regulujący zasady wspólnego działania oraz wymiany informacji między oboma sektorami. Wartą odnotowania formą współpracy określonej ustawą jest partnerstwo publiczno-prywatne.

Partnerstwo publiczno-prywatne (PPP) to strategiczne sojusze między sektorem publicznym a sektorem prywatnym, oparte na precyzyjnie określonych formach współpracy. Te kompleksowe relacje PPP powstają z różnorodnych powodów, takich jak potrzeba eliminowania barier prawnych barier prawnych dla sektora prywatnego, a także potrzeba współpracy przy wdrażaniu nowych regulacji prawnych. W Polsce najważniejszym aktem prawnym poświęconym tym zagadnieniom jest *Ustawa z dnia 19 grudnia 2008 r. o partnerstwie publiczno-prywatnym* stanowi kluczowe ramy prawne dla tych relacji.

Sektor prywatny decyduje się na uczestnictwo w PPP przede wszystkim w celu uzyskania dostępu do funduszy publicznych, uzyskania wpływu na kształtowanie legislacji krajowej i międzynarodowej oraz aktywnego uczestnictwa w zwalczaniu cyberprzestępczości. Z kolei sektor publiczny przystępuje do PPP głównie dla korzyści płynących z dostępu do specjalistycznej wiedzy w obszarze infrastruktury krytycznej.

Przykłady PPP w Europie obejmują inicjatywę Cyber Growth Partnership w Wielkiej Brytanii, identyfikującą bariery dla rozwoju cyberbezpieczeństwa i zwiększającą aktywność rządu w promocji lokalnych rozwiązań. Kolejnym przypadkiem jest Security Made in Luxembourg (SMILE) w Luksemburgu, dostarczające administracji konkretnych rozwiązań związanych z cyberbezpieczeństwem. W skrócie PPP, wsparte stosownym prawodawstwem, stają się najważniejszym narzędziem do realizacji projektów publicznych, szczególnie w kontekście cyberbezpieczeństwa. To otwarte partnerstwo umożliwia efektywne osiąganie wspólnych celów, z uwzględnieniem różnorodnych korzyści i motywacji dla obu stron.

Warto również zwrócić uwagę na Program Współpracy w Cyberbezpieczeństwie, skrótowo zwany PWCyber, który został uruchomiony w 2019 roku. Jest to niekomercyjne przedsięwzięcie oparte na partnerstwie publiczno-prywatnym, powstałe z myślą o krajowym systemie cyberbezpieczeństwa.

Główne założenia Programu PWCyber obejmują dobrowolne uczestnictwo, ujednolicone porozumienie dla wszystkich uczestników, brak zobowiązań finansowych, klauzulę poufności (NDA) dla wymienianych informacji oraz możliwość dołączenia innych podmiotów za zgodą obu stron. PWCyber kładzie nacisk na zaufanie i bezpieczeństwo, szczególnie w kontekście budowania solidnych relacji z partnerami technologicznymi i krajowymi władzami bezpieczeństwa.

Program jest otwarty dla firm z państw Unii Europejskiej, Organizacji Traktatu Północnoatlantyckiego (NATO) oraz jego państw partnerskich. Obszary współpracy PWCyber obejmują podnoszenie kompetencji krajowego systemu cyberbezpieczeństwa, w tym świadomość zagrożeń, metody ataków, umiejętności prawne, organizacyjne i techniczne przeciwdziałania zagrożeniom w systemach teleinformatycznych. Działania programu mogą dotyczyć udostępniania materiałów szkoleniowych, organizacji szkoleń oraz kampanii uświadamiających, identyfikacji podatności, wymiany informacji, opracowywania rekomendacji dotyczących konfiguracji urządzeń i certyfikacji cyberbezpieczeństwa produktów i usług. Ponadto program promuje innowacyjne rozwiązania i projekty w dziedzinie cyberbezpieczeństwa oraz buduje partnerstwo z podmiotami krajowego systemu cyberbezpieczeństwa.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Zagrożenia wynikające ze współpracy

Pomimo licznych korzyści współpraca między sektorem publicznym a sektorem prywatnym w obszarze cyberbezpieczeństwa niesie ze sobą pewne ryzyko. Jedno z głównych zagrożeń dotyczy kwestii poufności i prywatności danych.

Dyskusja wokół udostępniania informacji publicznych firmom prywatnym w kontekście cyberbezpieczeństwa wydobywa na pierwszy plan złożoność zagadnienia bezpieczeństwa danych. Decyzje o powierzeniu prywatnym podmiotom dostępu do informacji publicznych, zwłaszcza tych wrażliwych, stawiają przed sektorem publicznym i społeczeństwem wiele wyzwań.

Pierwsze z nich wiąże się z ryzykiem potencjalnych nadużyć. Udostępnienie danych firmom prywatnym, które operują na rynku, może rodzić obawy dotyczące właściwego zarządzania tymi informacjami i zabezpieczania ich. Prywatne podmioty mogą być narażone na presję konkurencyjną, co z kolei może skłaniać do niewłaściwego wykorzystania czy też przetwarzania danych dla własnych celów. Skutki nadużyć w tym kontekście mogą sięgać od utraty zaufania społecznego do sektora publicznego po konkretne straty finansowe czy naruszenie prywatności obywateli.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Drugim ważnym aspektem jest ryzyko wycieków danych. Udostępnienie informacji publicznych firmom prywatnym może zwiększać liczbę podmiotów mających dostęp do poufnych danych. Wraz z tym rośnie potencjalne źródło wycieków, zarówno z powodu zewnętrznych ataków, jak i wewnętrznych błędów. Takie incydenty mogą mieć poważne konsekwencje, w tym utratę poufności informacji, szkody dla jednostek czy instytucji, a także poważny uszczerbek dla reputacji sektora publicznego.

Wszystko to stawia decydentów przed sporym wyzwaniem – znalezienia równowagi między potrzebą efektywnego zarządzania cyberbezpieczeństwem a pragnieniem wykorzystania ekspertyzy i zasobów sektora prywatnego. Skuteczne rozwiązania wymagają ustanowienia klarownych ram prawnych, precyzyjnych regulacji i systemów monitorowania, które zapewnią odpowiednie zabezpieczenia przed zagrożeniem związanym z udostępnianiem informacji publicznych firmom prywatnym.

Innym istotnym aspektem jest uzależnienie od podmiotów prywatnych. Możliwość monopolizacji rynku usług cyberbezpieczeństwa oraz ograniczona kontrola sektora publicznego nad najważniejszymi elementami obrony cybernetycznej może doprowadzić do sytuacji, w której decyzje i działania są podyktowane prywatnymi interesami firm.

Dodatkowo pojawiają się kwestie związane z potencjalnymi konfliktami interesów i dylematami etycznymi. Naciski ze strony sektora prywatnego na sektor publiczny mogą wpływać na obiektywność i bezstronność działań w obszarze cyberbezpieczeństwa. Stanowi to wyzwanie utrzymania uczciwej równowagi pomiędzy interesami publicznymi a prywatnymi w kontekście współpracy w cyberprzestrzeni.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Rekomendacje

Aby skutecznie zminimalizować ryzyko i maksymalnie wykorzystać korzyści płynące z współpracy, konieczne są konkretne rekomendacje. Dalsze precyzowanie ram prawnych, wspieranie transparentności, zwiększanie odpowiedzialności oraz edukacja pracowników obu sektorów są niezwykle istotne dla zwiększenia świadomości i umiejętności reagowania na nowe zagrożenia, ale najważniejsza jest elastyczność w podejściu do dostosowywania strategii do zmieniającego się otoczenia cybernetycznego. Umożliwia ona sektorom publicznemu i prywatnemu szybką adaptację do zmieniających się warunków i stawianie czoła nowym wyzwaniom. Ponadto rozwijanie innowacyjnych rozwiązań oraz wspieranie badań i rozwoju w obszarze cyberbezpieczeństwa są bardzo ważne dla utrzymania przewagi w walce z coraz bardziej zaawansowanymi zagrożeniami.

Podsumowanie

Współpraca między sektorem publicznym a sektorem prywatnym w zakresie cyberbezpieczeństwa jest konieczna. Największe wyzwanie to znalezienie równowagi między wymianą zasobów a minimalizacją ryzyka przy jednoczesnym zrozumieniu specyfiki funkcjonowania obu sektorów. Rozwój tej współpracy stanowi nieodłączną część skutecznej ochrony cyfrowej przestrzeni, która jest jednym z najważniejszych elementów współczesnego społeczeństwa. Dalsze doskonalenie i rozwijanie partnerstwa między sektorem publicznym a sektorem prywatnym w obszarze cyberbezpieczeństwa to istotny krok w kierunku budowy bardziej odpornego i bezpiecznego świata.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

www.instytutcyber.pl

fundacja instytut
CYBERBEZPIECZEŃSTWA

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości