

EUROPEJSKIE FORUM CYBERBEZPIECZEŃSTWA

Druga edycja corocznej konferencji poświęconej strategicznym aspektom cyberbezpieczeństwa

26-27 WRZEŚNIA 2016 - KRAKÓW



CYBERSEC 2016

REKOMENDACJE



ŚCIEŻKA
PAŃSTWO



ŚCIEŻKA
WOJSKO



ŚCIEŻKA
PRZYSZŁOŚĆ



ŚCIEŻKA
BIZNES

WWW.CYBERSECFORUM.EU



Rzeczpospolita Polska
Ministerstwo
Spraw Zagranicznych

Projekt współfinansowany przez NATO's Public Diplomacy Division i Ministerstwo Spraw Zagranicznych Rzeczypospolitej Polskiej.

Publikacja wyraża jedynie poglądy autora i nie może być utożsamiana z oficjalnym stanowiskiem Ministerstwa Spraw Zagranicznych RP.

Szanowni Państwo,

Przekazujemy na państwa ręce Rekomendacje wypracowane podczas II Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC. Za jego sprawą Kraków już po raz kolejny stał się centrum międzynarodowej dyskusji o bezpieczeństwie w cyberprzestrzeni.

W ciągu dwóch dni intensywnych obrad w CYBERSEC wzięło udział ponad 700 uczestników, a głos zabrało 120 prelegentów z ponad 20 krajów. W rezultacie decydenci, liderzy opinii, reprezentanci świata nauki i biznesu, z uwzględnieniem specyfiki i interesów każdej z grup, wypracowali praktyczne rekomendacje, które przyczynią się do wzmocnienia jakości współpracy wielopodmiotowej, a w konsekwencji cyberbezpieczeństwa Europy. Wśród wiodących zagadnień znalazły się m.in. kwestie implementacji Dyrektywy NIS, budowy regionalnego systemu cyberbezpieczeństwa Europy Środkowo-Wschodniej, cyberobrony państw NATO, walki z terroryzmem za pomocą cybernarzędzi, czy rosnącego deficytu wśród cyberspecjalistów.

Mamy nadzieję, że lektura Rekomendacji zachęci Państwa do współtworzenia wraz z nami społeczności CYBERSEC i uczestnictwa w przyszłorocznej edycji, która odbędzie się w dniach 9-10 października 2017 r.

Zespół Instytutu Kościuszki

Metodologia

W ramach każdej ścieżki tematycznej – Państwo, Wojsko, Przyszłość i Biznes - odbyły się po dwie Breakout Sessions (BSs) - w oparciu o ich konkluzje powstały prezentowane rekomendacje, a także odpowiednio cztery panele dyskusyjne – w czasie których do rekomendacji mogli odnieść się paneliści. Również ich uwagi uwzględnione zostały w prezentowanym materiale.

Dodatkowo, w tegorocznej edycji CYBERSEC w ścieżce Przyszłość miała miejsce specjalna sesja plenarna poświęcona tematowi inwestycji w sektorze cyberbezpieczeństwa. Odbyła się także sesja specjalna poświęcona problematyce zwalczania cyberprzestępczości. Wnioski z tych dyskusji także zostały uwzględnione w niniejszym dokumencie.

Tworząc rekomendacje Instytut Kościuszki dokonał autorskiej selekcji najbardziej istotnych wątków, nie sposób bowiem uwzględnić wszystkich elementów jakie pojawiały się w dyskusjach. Prosimy mieć również na uwadze, że nie wszystkie rekomendacje odzwierciedlają poglądy wszystkich uczestników.



ŚCIEŻKA PAŃSTWO

CYBERBEZPIECZEŃSTWO REGIONU EUROPY ŚRODKOWO-WSCHODNIEJ – WSPÓŁPRACA I ROZWÓJ ŚRODKÓW BUDOWY ZAUFANIA

Środki budowy zaufania w cyberprzestrzeni stanowią niezwykle istotne narzędzia, które przyczyniają się do utrzymywania stabilności, przejrzystości oraz pokoju w cyberprzestrzeni. Istnieje silna potrzeba opracowania konkretnych i praktycznych instrumentów oraz wdrażania uzgodnionych działań. Dlatego zaleca się podjęcie następujących kroków:

● BUDOWANIE NA FUNDAMENTACH SUBREGIONALNYCH

Inicjatywy subregionalne powinny odgrywać ważną rolę w tworzeniu praktycznych instrumentów oraz promowaniu dobrych praktyk. W celu ponoszenia ogólnej odporności, ich efekty i wyniki prac powinny być one wymieniane z innymi subregionami w ramach współpracy w OBWE. Trwała subregionalna odporność może budować zaufanie na arenie regionalnej jak i międzynarodowej. Grupa Wyszehradzka ma ogromny potencjał, by stać się forum, gdzie wdraża się konkretne środki budowy zaufania w cyberprzestrzeni. Jedną z propozycji zakłada stworzenie solidnych mechanizmów ochrony infrastruktury krytycznej i zarządzania kryzysowego.

● MODERNIZACJA NARZĘDZI

W ramach OBWE utworzona została sieć kontaktów na szczeblu politycznym pomiędzy wszystkimi państwami partycypującymi. Następnym krokiem powinno być podnoszenie zdolności grupy do efektywnej współpracy przez przeprowadzenie wspólnych ćwiczeń. Pozwoli to na sprawdzenie jak sieć współpracuje oraz zachowuje się w różnych sytuacjach i scenariuszach.

● DALSZA INKLUZYWNOŚĆ

Prace nad opracowaniem środków budowy zaufania w cyberprzestrzeni muszą przyjąć wielowymiarowe podejście angażujące wszystkich interesariuszy (z naciskiem na uczestnictwo podmiotów z branży).

● ZAANGAŻOWANIE DECYDENTÓW

Decydenci wysokiego szczebla są kluczowym elementem procesów związanych ze środkami budowy zaufania w cyberprzestrzeni. Stąd też powinni oni uczestniczyć we wszystkich kluczowych działaniach podejmowanych na tym polu.

ŚCIEŻKA PAŃSTWO

DYREKTYWA NIS – JAK WDROŻYĆ PIERWSZĄ UNIJNĄ LEGISLACJĘ DOTYCZĄCĄ CYBERBEZPIECZEŃSTWA?



● KLUCZOWA ROLA HARMONIZACJI

Należy zharmonizować standardy wdrażania Dyrektywy NIS. Ten proces będzie zależał od kilku czynników:

- Skutecznego działania grupy współpracy ustanowionej w ramach Dyrektywy: wszystkie państwa członkowskie powinny intensywnie zaangażować się w prace oraz wykorzystać tę platformę do wypracowania wspólnych stanowisk.
- Aktywnego zaangażowania się branży: rekomenduje się utworzenie sektorowych społeczności wymieniających się informacjami.
- Aktywnej roli ENISA: aby upewnić się, że ENISA będzie miała narzędzia do skutecznego wypełnienia swojej roli, należy przyspieszyć rewizję modelu jej działania. ENISA musi mieć dostęp do wszelkich zasobów, aby skutecznie podołać temu nowemu wyzwaniu.

● DOSTOSOWANIE ŚRODKÓW BEZPIECZEŃSTWA DO POTRZEB SEKTORÓW

- Podczas wdrażania środków cyberbezpieczeństwa w ramach Dyrektywy NIS należy przyjąć podejście sektorowe, które musi uwzględniać różnice oraz charakterystykę poszczególnych sektorów (np. różne ryzyka oraz konsekwencje incydentów)
- Podczas projektowania mechanizmów cyberbezpieczeństwa należy wziąć pod uwagę zależności między sektorami i państwami.

● SEKTOR PUBLICZNY – REALNY PARTNER

Organy państwa odpowiedzialne za wdrożenie Dyrektywy NIS muszą udowodnić, że mają zasoby aby skutecznie prowadzić ten proces oraz że są cennym partnerem dla operatorów usług kluczowych oraz dostawców usług cyfrowych. Podczas implementacji, zarówno jedni, jak i drudzy nie powinni skupiać się wyłącznie na kosztach, lecz postrzegać wdrażanie Dyrektywy NIS jako proces, który może przynieść wiele korzyści.

● UCZENIE SIĘ OD SIEBIE NAWZAJEM

Inicjatywa partnerstwa publiczno-prywatnego na rzecz cyberbezpieczeństwa powinno być potraktowane jako doskonałe forum dla państw członkowskich, agencji bezpieczeństwa narodowego oraz operatorów prywatnych po stronie popytowej do wyrażania swoich oczekiwań względem branży dostarczających usług i produktów z obszaru cyberbezpieczeństwa.

● HUB INFORMACYJNY

Rekomenduje się powołanie centrum informacyjnego, które zmobilizuje podmioty publiczne do większego zaangażowania w wymianę informacji. Tyczy się to takich organizacji jak np. sieć CSIRT, ENISA, CERT UE, Europejskie Centrum ds. Cyberprzestępczości (powstałe przy biurze Europolu).

● CYBERBEZPIECZEŃSTWO TO NIE TYLKO KOSZT

Elementy regulacyjne muszą zostać wsparte systemem zachęt.

● ODPOWIEDZIALNOŚĆ

Należy przedyskutować nowe podejście do odpowiedzialności producenta za jakość i bezpieczeństwo produktu oraz odpowiedzialność przemysłu telekomunikacyjnego.

● AUTOMATYZACJA PROCESÓW WSPÓŁPRACY

Należy szukać okazji do dalszej automatyzacji procesów współpracy w celu podwyższenia wskaźników reakcji oraz bardziej efektywnego zarządzania ryzykami.



ŚCIEŻKA WOJSKO

POLITYKA CYBEROBRONY PO SZCZYCIE NATO W WARSZAWIE

● WDRAŻANIE DECYZJI

W celu wypełnienia zobowiązań zawartych w dokumencie pt. Zobowiązanie w dziedzinie cyberobrony NATO, zaleca się przede wszystkim:

- Zdefiniowanie jasnych celów oraz zakresu obowiązków na poziomie NATO oraz poszczególnych państw członkowskich w zakresie stworzenia narzędzi pomiarowych oraz metryk pozwalających na określenie ich potencjału oraz ocenę poziomu realizacji wyznaczonych celów.
- Zainwestowanie środków w rozwój międzynarodowego potencjału oraz modernizację krajowych mechanizmów obrony, a także w edukację, szkolenie umiejętności oraz budowanie świadomości.

● WALKA Z WYZWANIAM I O CHARAKTERZE HYBRYDOWYM

Budując silne cyberbezpieczeństwo NATO, nie wolno zapominać o wyzwaniach o charakterze hybrydowym.

- Wygrywanie na polu walki informacyjnej wiąże się z rozpoznaniem różnych instrumentów, które zostały wykorzystane do przeprowadzenia wrogich operacji, po to, aby przygotować adekwatną odpowiedź. Wymaga to silnej współpracy na linii UE-NATO oraz skutecznej wspólnej i strategicznej komunikacji opartej na prawdziwych i rzetelnych informacjach.
- Postuluje się, aby każde państwo członkowskie miało instytucję powołaną do tego, aby zintegrować działania mające na celu przeciwdziałanie wojnie informacyjnej.
- NATO wraz z jego państwami członkowskimi powinno położyć większy nacisk na naukę tego, jak reagować i odpowiadać na niekonwencjonalne zagrożenia hybrydowe, zwłaszcza we wczesnej fazie (faza zero), gdy obraz sytuacji jest niejasny, a docierające sygnały niejednoznaczne.
- Należy opracować wczesne wskaźniki ostrzegania dla zagrożeń hybrydowych. To zadanie będzie wymagało zaangażowania różnych aktorów obdarzonych wiedzą oraz umiejętnościami technologicznymi, analitycznymi, wywiadowczymi, oraz znajomością sytuacji. Dobrą praktyką w tym zakresie może być budowanie oraz ćwiczenie różnych scenariuszy na wypadek różnych sytuacji.

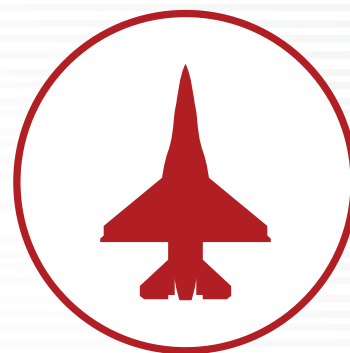
● DYLEMAT ATRYBUCJI

Dylemat atrybucji stanowi poważny problem dla międzynarodowego pokoju. Stąd też należy podjąć następujące działania, aby usprawnić podejmowanie decyzji w tym obszarze:

- Dalsze inwestowanie w rozwój narzędzi wywiadowczych dotyczących cyberzagrożeń.
- Wymianę informacji (pomiędzy różnymi podmiotami, m.in. z sektora prywatnego), która będzie wspierać rozwój technologii;
- Dalsze zwiększanie potencjału wywiadowczego z silnym naciskiem na współpracę pomiędzy cywilnymi oraz wojskowymi agencjami wywiadowczymi.
- Analizę kontekstową, by określić, kto jest faktycznym beneficjentem w danej sytuacji.
- Zbadanie zakresu obowiązków podmiotów państwowych w kwestii dostarczania pomocy i wsparcia, biorąc pod uwagę zasadę należytej staranności (ang. due diligence).

ŚCIEŻKA WOJSKO

WALKA Z TERRORYZMEM ZA POMOCĄ CYBERNARZĘDZI



● BĄDŹMY REALISTAMI

Założenie, że jesteśmy w stanie kompletnie wyeliminować zagrożenia terrorystyczne w cyberprzestrzeni, jest mało realistyczne. Dlatego zaleca się przyjęcie podejścia opartego na ryzyku. Potrzebujemy decyzji politycznej poprzedzonej szeroką debatą publiczną na temat tego, jaki jest najniższy dopuszczalny próg zagrożenia, aby następnie podjąć decyzję w sprawie odpowiednich metod nadzoru i prewencji.

● DOSTOSUJMY NARZĘDZIA DO ZAGROŻEŃ

- Terroryci wykorzystują cyberprzestrzeń do wielu różnych celów. Zatem narzędzia wykorzystywane do ich powstrzymania muszą być dostosowane do rodzaju zagrożenia.
- Walcząc z terrorystami propagującymi swoje idee w Internecie, musimy skupić się nie tylko na usuwaniu niebezpiecznych treści, ale głównie na pracy związanej z tworzeniem przeciw-narracji.
- Terroryci wykorzystują internetowe kanały komunikacji do planowania swoich operacji.
- W celu skutecznego monitorowania tych działań oraz zdobywania istotnych informacji, proaktywna rekrutacja informatorów musi odgrywać kluczową rolę. Powinniśmy korzystać z tradycyjnych metod wywiadowczych i stosować je w warunkach cyberprzestrzeni do zbierania dodatkowych informacji (na przykład prowadzenia tajnych operacji w cyberprzestrzeni). Dlatego też należy przyjąć podejście promujące synergiczne wykorzystanie zarówno narzędzi konwencjonalnych jak i cyfrowych.

● ROLA SEKTORA PRYWATNEGO

To państwa określają, jakie treści publikowane w Internecie mogą być uznane za zgodne z prawem, a jakie za treści o charakterze terrorystycznym. Stanowienie prawa nie leży w gestii prywatnych firm. Jednakże obowiązki sektora prywatnego w kwestiach dotyczących praw człowieka muszą być rozpatrywane zarówno w ramach przepisów krajowych (egzekwowanych przez państwa), jak i polityki firm będącej bezpośrednim zobowiązaniem dotyczącym praw człowieka, zgodnie z dokumentem ramowym ONZ „Chronić, szanować, naprawiać” („Zasady Ruggie'go”).

● PRZYSZŁOŚĆ

W niedalekiej perspektywie ataki podejmowane przez grupy terrorystyczne będą w coraz większym stopniu nakierowane na naruszanie nie tylko poufności i dostępności, ale głównie integralności danych. Oznacza to, że nie będą one ograniczone jedynie do ingerencji w wygląd stron internetowych czy ataki DDoS, ale będą obejmować działania, które są potencjalnie dużo bardziej problematyczne i szkodliwe dla infrastruktury. Zaleca się, aby operatorzy infrastruktury krytycznej zostali prawnie zobowiązani do identyfikacji i kontroli swoich krytycznych zasobów informacyjnych. Operatorzy powinni rozpowszechnić dobre praktyki w tym zakresie oraz oferować narzędzia i rozwiązania ramowe umożliwiające demaskowanie przypadków manipulacji danymi, tj. sposoby identyfikacji i dalszej kontroli swoich krytycznych zasobów informacyjnych. Szacuje się, że owe „krytyczne zasoby” stanowią bardzo ograniczoną grupę informacji posiadanych przez firmy (maksymalnie 2% wszystkich zasobów informacyjnych). Prywatne firmy muszą określić swoje krytyczne zasoby i procesy informacyjne w celu ich ochrony oraz zapewnienia ich rzetelności i wiarygodności.



ŚCIEŻKA PRZYSZŁOŚĆ

PRZYGOTOWANIE ZASOBÓW LUDZKICH NA NADCHODZĄCE CYBERWYZWANIA

Najważniejsze rekomendacje można przedstawić w formie w pełni zintegrowanego łańcucha wartości w edukacji. Z racji tego, że cyberprzestrzeń wywiera wpływ na wszystkie aspekty życia społecznego, powinniśmy przestać mówić o specjalistach do spraw cyberbezpieczeństwa wyłącznie przez pryzmat umiejętności IT, a zacząć myśleć o cyberbezpieczeństwie jako nauce.

Choć traktowanie cyberbezpieczeństwa w kategoriach nauki stanowi cel finalny, to schemat i podejście zaprezentowane poniżej można z powodzeniem zastosować do etapu pośredniego, gdzie cyberbezpieczeństwo rozumiane jest w bardziej konwencjonalny sposób.

ZINTEGROWANY EDUKACYJNY ŁAŃCUCH WARTOŚCI DLA CYBERBEZPIECZEŃSTWA JAKO NAUKI

POSTRZEGANIE I ŚWIADOMOŚĆ

- Postrzeganie cyberbezpieczeństwa jako klarownej i atrakcyjnej ścieżki kariery
- Możliwość wywierania rzeczywistego wpływu na globalną gospodarkę
- Wskazywanie rosnącego popytu na umiejętności
- Wspieranie inkluzywności

PRZYCIĄGANIE TALENTÓW NA WCZESNYCH ETAPACH

- Wyławianie i kreowanie talentów
- Zachęcanie młodych ludzi do podejmowania studiów informatycznych licencjackich i magisterskich
- Walka ze stereotypem męskiej dominacji w sektorze IT
- Ustanowienie programów stypendialnych

NIEWYKWALIFIKOWANA
SIŁA ROBOCZA

EKSPERCI DO SPRAW
CYBERBEZPIECZEŃSTWA

OPRACOWANIE PAKIETU UMIEJĘTNOŚCI INTERDYSCYPLINARNYCH

- Opracowanie standardowego pakietu umiejętności eksperta ds. cyberbezpieczeństwa na szczeblu akademickim
- Programy certyfikacji dla specjalistów w dziedzinie cyberbezpieczeństwa
- Promowanie interdyscyplinarnego podejścia do cyberbezpieczeństwa
- Zwiększanie świadomości i znalezienie jednego wspólnego języka
- Tworzenie centrów doskonałości akademickiej
- Stworzenie sieci programów wymiany studentów

UCZENIE SIĘ OD SIEBIE NAWZAJEM I PRZEWIDYWANIE PRZYSZYŁYCH POTRZEB

- Ćwiczenie ataków w kontrolowanym ekosystemie
- Ciągłe wyszukiwanie umiejętności, by przewidywać przyszłe potrzeby
- Tworzenie interdyscyplinarnych zespołów
- Uczenie się reagowania na transgraniczne zagrożenia

Etap 1 stymulacji łańcucha wartości związany jest z jakościową zmianą w **postrzeganiu dziedziny cyberbezpieczeństwa jako atrakcyjnej, interesującej i lukratywnej ścieżki kariery**, która wywiera realny wpływ zarówno na sferę bezpieczeństwa, jak i globalną gospodarkę czy relacje międzynarodowe. Powinno się ją przedstawiać jako ekscytującą przygodę, a nie tylko jako typowo męski zawód czy pracę na zlecenie.

- **Etap 2** obejmuje **wyławianie i kreowanie talentów wywodzących się z różnych grup społecznych**. Zaleca się, aby poszukiwanie utalentowanych osób obejmowało szerokie spektrum środowisk. Umożliwia to dotarcie do rozległego grona osób, nawet tych, które na pierwszy rzut oka nie wyglądają na oczywistych kandydatów.

Zaleca się też utworzenie różnorodnych programów stypendialnych, które przyciągną młode i obiecujące talenty.

- **Etap 3** obejmuje profesjonalizację zarządzania talentami poprzez **opracowanie bieżącego zestawu potrzebnych umiejętności interdyscyplinarnych**, co pomoże nie tylko kształcić wysokiej klasy specjalistów, ale także umożliwi im efektywną pracę zespołową oraz analizowanie problemów z różnych perspektyw (nie tylko IT, ale zarządzania biznesowego, prawnej, politycznej itd.). W tej fazie różni interesariusze powinni zaangażować się w ciągłą aktualizację i ulepszanie programów nauczania dla cyberspecjalistów (szczególny nacisk należy położyć na aktywny udział w tej fazie przedstawicieli branży). Takie działania pozwoli zrozumieć i nadążać za zmieniającymi się globalnymi wymaganiami i potrzebami (rynkowymi, ale też politycznymi, gospodarczymi itd.).

Aby skutecznie katalizować rozwój talentów, warto zadbać o stworzenie sprzyjającego środowiska naukowego, na przykład poprzez zakładanie centrów doskonałości akademickiej spełniających krajowe standardy. Cennym elementem takiej inicjatywy na tym etapie mogłaby być sieć programów międzynarodowej wymiany studentów.

- **Etap 4 i ostatni związany z przewidywaniem przyszłych potrzeb w dziedzinie cyberbezpieczeństwa poprzez uczenie się od siebie nawzajem w realnych ekosystemach** stanowi największe wyzwanie w momencie, gdy luka w podaży wysoko wykwalifikowanych ekspertów ds. cyberbezpieczeństwa zostanie wypełniona. To najwyższy poziom w rozwoju kariery zawodowej. Narzędziem stymulującym ten proces są różnorodne ćwiczenia zawierające w sobie elementy interdyscyplinarne. Dynamika wzajemnego uczenia się daje najlepszym ekspertom zdolność przewidywania, ale także **umożliwia nieustanne poszukiwanie umiejętności**, które należy włączyć do łańcucha wartości w edukacji.

- Głównym wyzwaniem dla potencjału ludzkiego w sektorze cyberbezpieczeństwa jest stworzenie strumienia przepływu, który uwzględniłby wszystkie wymienione wcześniej etapy i traktował je jako część ustandaryzowanego procesu budowania potencjału profili zawodowych w skali globalnej. Jedynie kompleksowe podejście, obejmujące wszystkie powyższe etapy, może przynieść sukces. Tak skomplikowane wyzwanie musi obejmować wszystkich aktorów, a także być powiązane z istniejącymi już inicjatywami i działaniami, które wspólnie zapewnią ciągłość doskonalenia.



ŚCIEŻKA PRZYSZŁOŚĆ

CYBERINNOWACJE

- PROMOWANIE ROZWOJU I WSPÓŁPRACY

INWESTYCJE

● **Szczebel unijny: instrumenty finansowe muszą być dostosowane do potrzeb podmiotów, które z nich korzystają**

Oferta funduszy unijnych musi być dostosowana do warunków, które sprzyjają innowacjom. Startupy z definicji są przedsięwzięciami charakteryzującymi się oryginalnością, elastycznością oraz silnym etosem pracy.

Kreowanie okoliczności, które stoją w sprzeczności z ich naturą, zabija ich potencjał. Procedura aplikowania o środki unijne, która wymaga od firm wniesienia 50% wkładu własnego i przebrnięcia przez biurokrację po to, aby rozpocząć projekt, który będzie trwał np. 5 lat, przynosi efekt przeciwny do zamierzonego. Dlatego też rekomenduje się, by instrumenty finansowe były lepiej dostosowane do potrzeb małych i innowacyjnych przedsiębiorstw.

● **Szczebel państwowy: sektor publiczny jako dźwignia cyberinnowacji**

Organy administracji publicznej powinny rozwijać swoją wiedzę oraz specjalistyczne kompetencje, aby móc w sposób odpowiedni dokonywać oceny projektów inwestycyjnych oraz podejmować konieczne ryzyko. Podmioty sektora publicznego powinny rozwinąć w sobie mentalność właściwą dla inwestorów VC, a mianowicie przekonanie, że warto inwestować w dobre pomysły pomimo wysokiego ryzyka. Sektor publiczny powinien także przeprowadzić analizę due diligence w celu zwiększenia zaufania oraz inwestycji w cyber startupy. Wspierając startupy w obszarze cyberbezpieczeństwa, podmioty sektora publicznego powinny mieć na względzie to, że cyberbezpieczeństwo może nie tylko zwiększać ogólne bezpieczeństwo, ale także przekształcić się w źródło nowatorskich rozwiązań, które będzie napędzać innowacyjną gospodarkę.

● **Venture Capital jako główny instrument**

Klimat sprzyjający przedsięwzięciom VC powinien być rozwijany na szczeblu UE i przez poszczególne państwa członkowskie.

BUDOWANIE SIECI KONTAKTÓW

● **Przykład Estonii pokazał, iż rząd powinien udzielać wsparcia w nawiązywaniu kontaktów pomiędzy akademickimi ośrodkami badawczymi a małymi, dobrze prosperującymi firmami. Nawiązywanie dobrych relacji z klientami jest istotnym elementem działalności biznesowej, a wsparcie rządu może umożliwić realizację projektów pilotażowych oraz ułatwić budowę początkowej bazy klientów.**

● **Klasy i huby w dziedzinie cyberbezpieczeństwa mogą powstawać w oparciu o wiele różnych modeli. Jednym z nich jest podejście oddolne, które z uwagi na swoją skuteczność, powinno być szerzej propagowane poprzez zaangażowanie możliwie największej liczby interesariuszy.**

PRZEŁAMYWANIE BARIER

● **Istnieje paląca potrzeba opracowania dedykowanych programów, które pomogą startupom rozwinąć skrzydła. Te nowo powstałe i szybko rozwijające się przedsiębiorstwa mają pomysły i umiejętności technologiczne, ale często brakuje im umiejętności miękkich, umożliwiających im dotarcie do klientów i otrzymanie dofinansowania. Bywa, że najlepsi innowatorzy to niekoniecznie świetni przedsiębiorcy. Fundusze VC powinny wносить do tych firm coś więcej niż tylko kapitał. Jako partnerzy, powinny pomagać startupom aranżować spotkania z klientami i wspierać podejmowanie ryzyka.**

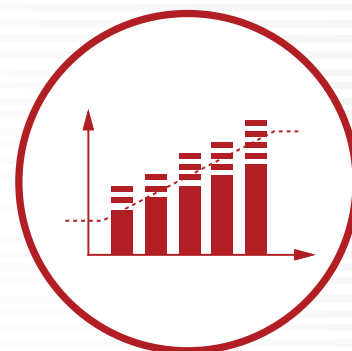
ROZWÓJ TALENTÓW

● **Rola środowiska akademickiego w dziedzinie cyberbezpieczeństwa jest obecnie mocno niedoceniana i należy to zmienić. Uczelnie wyższe powinny stać się ważnymi i uznanymi kuźniami talentów. Należy stworzyć system stypendiów, aby przyciągać najbardziej utalentowanych studentów.**

ZINTEGROWANE ROZWIĄZANIA

● **Istnieje silny trend w kierunku stosowania zintegrowanego podejścia technologicznego w trakcie tworzenia rozwiązań w dziedzinie cyberbezpieczeństwa. Takie podejście powinno uzyskać szerokie poparcie.**

ŚCIEŻKA BIZNES



CYBERBEZPIECZEŃSTWO PRZEMYSŁOWYCH SYSTEMÓW STEROWANIA

● INTEGRACJA SYSTEMÓW IT ORAZ PRZEMYSŁOWYCH SYSTEMÓW STEROWANIA (ICS)

Postrzeganie bezpieczeństwa często różni się znacząco między grupami specjalistów w ramach jednej organizacji. Specjaliści odpowiedzialni za bezpieczeństwo systemów IT i ICS mają tendencję do badania problemu przyjmując różne punkty widzenia. W związku z tym należy dążyć do wzajemnego zrozumienia i ścisłej współpracy w oparciu o regularną komunikację między tymi dwoma grupami.

● SZKOLENIA I ĆWICZENIA

Należy zorganizować wspólne, rutynowe ćwiczenia i szkolenia w skali mikro (firm, operatorów) i makro (państw), które zaangażują wszystkich interesariuszy (specjalistów w dziedzinie IT i OT, operatorów, regulatorów, przedstawicieli rządu czy dostawców rozwiązań).

● ROZWIĄZANIA DOSTOSOWANE DO POTRZEB

Nie istnieje jedno uniwersalne rozwiązanie zapewniające cyberbezpieczeństwo wszystkim systemom ICS. Istniejące ramy i dobre praktyki mogą posłużyć jako baza do opracowania bardziej dojrzałych strategii. Jednak trwałe rozwiązania muszą brać pod uwagę specyfikę sektora i opierać się na skutecznej analizie ryzyka.

● BEZPIECZEŃSTWO PRZEZ PROJEKT (SECURITY BY DESIGN)

Należy opracować standardy cyberbezpieczeństwa dla Internetu rzeczy (ang. IoT) oraz przemysłowych systemów sterowania. Zasada „security by design” ma kluczowe znaczenie.

● PRIORYTYZACJA

Zapewniając cyberbezpieczeństwo, należy rozpocząć od priorytetowych systemów.

● REGULARNA OCENA STANU BEZPIECZEŃSTWA

Zaleca się częste dokonywanie oceny stanu bezpieczeństwa, które pomoże lepiej zrozumieć słabe punkty. Pomoże to podejmować świadome decyzje dotyczące kolejnych kroków.

● UREGULOWANIA PRAWNE I DIALOG ZE ŚRODOWISKIEM BIZNESOWYM

Wszystkie uregulowania prawne muszą być tworzone przy ścisłym udziale biznesu. Tylko wtedy mogą one służyć jako dobry punkt wyjścia do zbudowania dojrzałego systemu cyberbezpieczeństwa. Oprócz przepisów, środowisko biznesowe musi się samoorganizować i stale poprawiać swoje cyberbezpieczeństwo.

● LEPSZE MONITOROWANIE

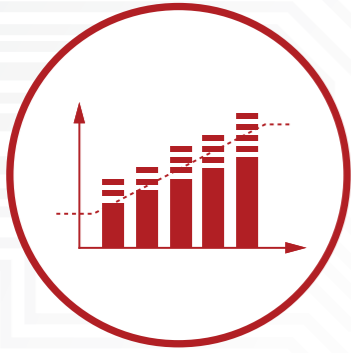
Sieci sterowania przemysłowego powinny być lepiej monitorowane.

● ROLA FIRM UBEZPIECZENIOWYCH

Firmy ubezpieczeniowe mogą odgrywać ważną rolę w regulowaniu bieżących praktyk dotyczących cyberbezpieczeństwa systemów ICS.

● ZESPOŁY ICS-CERT

Należy ustanowić krajowe zespoły ICS-CERT, których zadaniem będzie nie tylko zwiększanie świadomości i wiedzy na temat zagrożeń, ale również ulepszanie procesu wymiany informacji (w anonimowy sposób) i zapewnianie niezbędnej wiedzy eksperckiej.



ŚCIEŻKA BIZNES

HISTORIE SUKCESU WSPÓŁPRACY PUBLICZNO-PRYWATNEJ – POZIOM GLOBALNY, REGIONALNY I KRAJOWY

KRÓTKI PRZEWODNIK JAK REALIZOWAĆ PARTNERSTWA PUBLICZNO-PRYWATNE (PPP)

NAJWAŻNIEJSZE TO ZACZAĆ I STAĆ SIĘ INICJATOREM DZIAŁAŃ!

- To ważne, aby rozpocząć od tworzenia nieformalnych partnerstw w celu budowania zaufania, a w trakcie zawiązywać partnerstwa o charakterze formalnym.

PRZEMYŚLANA KONSTRUKCJA OD POSTAW

- Cele partnerstwa muszą być jasno i konkretnie zdefiniowane.
- Należy jasno określić role i obowiązki różnych interesariuszy.
- PPP powinny korzystać z niezawodnych platform, gdzie interesariusze reprezentujący ten sam sektor mogą podzielić się i przedyskutować swoje problemy.
- Należy zrozumieć, że sektor prywatny jest głównym motorem innowacji i włączyć go w planowanie i projektowanie inicjatyw.

Wysoki poziom zaufania między podmiotami publicznymi i prywatnymi, które ma fundamentalne znaczenie dla sukcesu, przekłada się na wzajemną wiarę w korzyści osiągane przez wszystkich partnerów.

OPTIMALIZACJA PRACY I PROCESÓW

- Należy zdefiniować proste, lecz formalne reguły zarządzania procesem na wczesnym jego etapie.
- PPP muszą być elastyczne. Aby szybko dostosować się do zmian, grupy robocze powinny być małe, ich zakres prac dobrze określony i doprecyzowany, cel końcowy jasny.
- Dla zapewnienia skutecznego działania należy postępować zgodnie z oddolnym podejściem strukturalnym, które pozwala na większą niezależność na niższych poziomach (lokalne potrzeby i zasoby).

TWORZENIE SPRZYJAJĄCEGO ŚRODOWISKA

- Należy zagwarantować zaangażowanie polityczne: jeśli politycy rozumieją wyzwania, jakie stawia cyberprzestrzeń, jest bardziej prawdopodobne, iż będą podejmować decyzje, które będą wspierać PPP.
- Warto zaangażować liderów opinii w tworzenie PPP.
- Należy zaszczepić w partnerstwa publiczno-prywatne „mentalność inwestorów”: sektor prywatny musi postrzegać wspólne inicjatywy nie jako koszt, ale dobrą inwestycję i okazję do uzyskania przewagi konkurencyjnej.

Tworząc przepisy, decydenci muszą zagwarantować, że ustawodawstwo przewiduje jasne wytyczne bazowe. Obowiązki nałożone przez przepisy należy wesprzeć rządowymi programami szkoleniowymi i zachętami finansowymi.

Decydenci powinni rozważyć ustanowienie funduszu cyberbezpieczeństwa na szczeblu UE. Powinien on stanowić mechanizm finansowy powiązany z funduszem badawczo-inwestycyjnym.

WALKA Z CYBERPRZESTĘPCZOŚCIĄ

SESJA SPECJALNA

Świadomość dotycząca zagrożeń jakie płyną z cyberprzestrzeni musi być rozpowszechniona szczególnie wśród małych i średnich przedsiębiorstw. Bardzo często są one celem ataków, a nie inwestują wystarczająco zasobów w działania nakierowane na cyberbezpieczeństwo.

Harmonizacja prawa dotyczącego cyberprzestępstw musi być prowadzona w skali globalnej. Inaczej będziemy mieli do czynienia z powstawaniem rajów dla cyberprzestępców, co znacznie utrudni ich skuteczne ściganie i karanie.

Warto podkreślać, że działania w cyberprzestrzeni wspierają często popełnianie klasycznych przestępstw.

WALKA Z CYBERPRZESTĘPCZOŚCIĄ

Współpraca organów ścigania z podmiotami prywatnymi wciąż jest niewystarczająca i musi być pogłębiana. Podobnie jak kultura wymiany informacji.

Kary za cyberprzestępstwa powinny być surowe i dotkliwe, a przestępcy powinni mieć przekonanie, że nie unikną sprawiedliwości. To czynnik, który może ich powstrzymać i w tym kierunku powinno iść prawodawstwo i działania wymiaru sprawiedliwości.

Podmioty powinny określić najcenniejsze zasoby i skupić się na ich ochronie. Wynika to z faktu, że cyberprzestępcy są niezwykle skuteczni i powinniśmy się przygotować na nowe rodzaje ataków, przed którymi ciężko chronić całe posiadane zasoby.



ŚCIEŻKA PRZYSZŁOŚĆ SPECJALNA SESJA PLENARNA

INWESTOWANIE W CYBERBEZPIECZEŃSTWO: KONIECZNOŚĆ CZY SZANSA? CZY MOŻNA ZAROBIĆ INWESTUJĄC W CYBERTECHNOLOGIE?

- Sektor publiczny odgrywa kluczową rolę w stymulowaniu inwestycji w dziedzinie cyberbezpieczeństwa. Z jednej strony państwa pozostają głównymi inwestorami dostarczającymi kapitał w tym obszarze, z drugiej, z racji sprawowania władzy ustawodawczej i wykonawczej, stymulują rozwój ekosystemu cyberbezpieczeństwa. Szereg strategicznych inwestycji w tej dziedzinie jest stymulowany przez działalność regulacyjną administracji publicznej.
- Kapitał finansowy nie powinien stanowić jedynej wartości wnoszonej przez inwestora. Równie ważne jest wsparcie w zakresie rozwoju sieci kontaktów biznesowych pomagającej nawiązywać relacje z kluczowymi interesariuszami, takimi jak administracja publiczna, uczelnie wyższe czy klienci korporacyjni.
- Inwestowanie w cyberbezpieczeństwo wymaga specjalizacji oraz silnych relacji z głównymi interesariuszami sektora publicznego.
- Nie należy antagonizować różnych interesariuszy na rynku cyberbezpieczeństwa. Inwestorzy, zarówno ogólni, specjalizujący się w sektorze cyberbezpieczeństwa, korporacyjni, czy fundusze funduszy, powinni zostać zaangażowani w rozwój ekosystemu, który umożliwi firmom wzrost.
- Kontraktowe partnerstwo publiczno-prywatne UE w dziedzinie cyberbezpieczeństwa powinno być postrzegane nie tylko jako narzędzie zachęcające do inwestowania w cyberbezpieczeństwo oraz stymulujące działania w obszarze badań i rozwoju, ale również jako szansa na zdefiniowanie wspólnych standardów i potrzeb w tej dziedzinie. Choć cyberbezpieczeństwo pozostaje w zakresie kompetencji państw członkowskich, to nadal istnieje przestrzeń dla współpracy ogólnoeuropejskiej. Przyczyni się ona do wzmocnienia systemu odporności cybernetycznej, wspierania konkurencyjnego i innowacyjnego sektora cyberbezpieczeństwa oraz promowania jednolitego rynku cyfrowego.
- Europejscy innowatorzy w dziedzinie cyberbezpieczeństwa muszą zwrócić uwagę na rozwój umiejętności biznesowych. W Europie jest wiele unikalnych pomysłów, kreatywnych specjalistów w dziedzinie IT oraz startupów, które nie wykorzystują swojego potencjału z powodu braku umiejętności przyciągania potencjalnych inwestorów i klientów.
- Rynek cyberbezpieczeństwa nie powinien być postrzegany jako sektor ograniczony jedynie do określonych produktów czy usług (wyłącznie rozwiązań dotyczących cyberbezpieczeństwa). Wręcz przeciwnie – rynek ten obejmuje również firmy z innych dziedzin branży informatycznej, gdzie cyberbezpieczeństwo stanowi istotny komponent (tzw. „security by design”). Jednym z wymogów czwartej rewolucji przemysłowej jest uwzględnienie elementu bezpieczeństwa w każdej działalności opartej na rozwiązaniach informatycznych.
- Polska musi odnaleźć swoją własną niszę i zbudować unikalną przewagę konkurencyjną. Z tego względu, polski rząd musi zaangażować się w inicjatywy, które promują lokalne rozwiązania i innowacje.
- Polska musi zdefiniować swoją specjalizację sektorową w Europie. Wielka Brytania posiada rozbudowany ekosystem, w skład którego wchodzi najlepsze uniwersytety. Z kolei w Niemczech istnieje wiele firm o ugruntowanej wiarygodności biznesowej. Małe kraje, takie jak Irlandia czy Luksemburg, oferują ustawodawstwo umożliwiające rozwój rozwiązań chroniących prywatność. Polska musi rozwinąć swoją przewagę konkurencyjną w ramach jednolitego rynku cyfrowego.
- Polska powinna wykorzystać swój dobrze prosperujący ekosystem przedsiębiorstw informatycznych jako zasób i źródło krajowej przewagi konkurencyjnej. Wybór strategicznego klastra, który będzie rozwijał technologie wybranego sektora IT, stanowi niewątpliwą kwestię. Oprócz cyberbezpieczeństwa, potencjalnym obszarem rozwoju krajowej specjalności mógłby być Internet rzeczy (ang. IoT).
- Korporacje, duże firmy oraz narodowi czempioni, tj. spółki Skarbu Państwa, powinni korzystać z innowacyjnych rozwiązań w dziedzinie cyberbezpieczeństwa oferowanych przez startupy. Z drugiej strony, startupy powinny dostarczać rozwiązania dopasowane do klienta oraz być gotowe do nawiązania długoterminowej współpracy ze swoimi klientami zamiast liczyć na jednorazowy zysk.



CYBERSEC 2016

W LICZBACH



1
Wyzwanie



2
Dni inspirującej
debaty



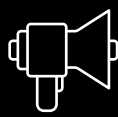
2
Sesje plenarne



2
Sesje
Specjalne



4
Ścieżki
Tematyczne



4
Panele
Dyskusyjne



6
Wydarzeń
Towarzyszących



8
Breakout
Sessions



12
Miesiące
Przygotowań



16
Godzin Tłumaczeń
Symultanicznych



20
Godzin
Networkingu



20
Państw



35
Wywiadów
dla CYBERSEC TV



40
Akredytowanych
Dziennikarzy



>50
Członków Ekipy
CYBERSEC



>120
Prelegentów



>400
Artukółów
o CYBERSEC



>700
Uczestników



2800
Zdjęć

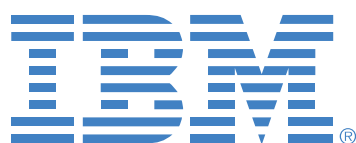


79K
Impresji
na Twitterze

DOWIEDZ SIĘ WIĘCEJ O @CYBERSECEU:



PARTNERZY STRATEGICZNI



Bank Polski



PARTERZY GŁÓWNI

COMARCH

 **EXATEL**
people behind technology

 **PGNiG**

 **PKPCARGO**

 **TAURON**

THALES

PARTNERZY

4ATP GROUP
 **paloalto networks**

 **25 YEARS GPW**
WARSAW STOCK EXCHANGE

arp 
Agencja
Rozwoju
Przemysłu
S.A.

CRAY
THE SUPERCOMPUTER COMPANY

 **ORLEN**

PSE

SIEMENS
Ingenuity for life

PARTNER CYBERSEC STARTUP DAYS



PARTNERZY MERYTORYCZNI



PARTNERZY WSPIERAJĄCY



PARTNER LOGISTYCZNY



PATRONI HONOROWI



PATRONI INSTYTUCJONALNI



PATRONI MEDIALNI



ORGANIZATOR



PARTNER PROGRAMOWY



POWERED BY



WSPÓŁFINANSOWANIE



Rekomendacje zostały współfinansowane ze środków prewencyjnych PZU SA.

Podstawą do opracowania rekomendacji były ustalenia konferencji CYBERSEC 2016.

Chcielibyśmy podziękować wszystkim partnerom CYBERSEC 2016, a także firmie Raytheon za wsparcie projektu.

BREAKOUT SESSION „CYBERBEZPIECZEŃSTWO REGIONU EUROPY ŚRODKOWO-WSCHODNIEJ – WSPÓŁPRACA I ROZWÓJ ŚRODKÓW BUDOWY ZAUFIANIA” ORAZ PANEL DYSKUSYJNY W ŚCIEŻCE PAŃSTWO SA DOSTĘPNE NA LICENCJI CREATIVE COMMONS UZNANIE AUTORSTWA 3.0 POLSKA. PEWNE PRAWA ZASTRZEŻONE NA RZECZ INSTYTUTU KOŚCIUSZKI. UTWÓR POWSTAŁ W RAMACH KONKURSU WSPARCIE WYMIARU SAMORZĄDOWEGO I OBYWATELSKIEGO POLSKIEJ POLITYKI ZAGRANICZNEJ – 2016. ZEZWALA SIĘ NA DOWOLNE WYKORZYSTANIE UTWORU, POD WARUNKIEM ZACHOWANIA WW INFORMACJI, W TYM INFORMACJI O STOSOWANEJ LICENCJI, O POSIADACZACH PRAW ORAZ O KONKURSIE WSPARCIE WYMIARU SAMORZĄDOWEGO I OBYWATELSKIEGO POLSKIEJ POLITYKI ZAGRANICZNEJ - 2016.

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

SUBSCRIBE ECJ

[HTTP://CYBERSECFORUM.EU/EN/SUBSCRIPTION](http://cybersecforum.eu/en/subscription)

CONTRIBUTE TO THE NEXT ISSUE!
CALL FOR PAPERS:
EDITOR@CYBERSECFORUM.EU

ANALYSES - POLICY REVIEWS - OPINIONS



THE KOSCIUSZKO INSTITUTE

FOLLOW US ON TWITTER  @ECJOURNAL

[WWW.CYBERSECFORUM.EU/EN/ABOUT-ECJ/](http://www.cybersecforum.eu/en/about-ecj/)



CYBERSEC
EUROPEAN
CYBERSECURITY
FORUM

SAVE THE DATE

CYBERSEC
EUROPEAN
CYBERSECURITY
FORUM

III Europejskie Forum Cyberbezpieczeństwa
CYBERSEC 2017

9-10 PAŹDZIERNIKA 2017
KRAKÓW, POLSKA

CYBERSEC
EUROPEAN
CYBERSECURITY
FORUM

WWW.CYBERSECFORUM.EU

WWW.CYBERSECFORUM.EU



@CYBERSECEU



/CYBERSECEU