POLSKIE FORUM CYBERBEZPIECZEŃSTWA

Konferencja poświęcona strategicznym aspektom cyberbezpieczeństwa

8 KWIETNIA 2016 – WARSZAWA

CYBERSEC PL 2016

REKOMENDACJE

ŚCIEŻKA **PAŃSTWO**

ŚCIEŻKA **WOJSKO**

ŚCIEŻKA **PRZYSZŁOŚĆ**

ŚCIEŻKA **BIZNES**

WWW.CYBERSECFORUM.PL

CYBERSEC EU

EUROPEJSKIE FORUM CYBERBEZPIECZEŃSTWA

Druga edycja corocznej konferencji poświęconej strategicznym aspektom cyberbezpieczeństwa

26-27 WRZEŚNIA 2016, KRAKÓW

WWW.CYBERSECFORUM.EU

\CYBERSECEU

@CYBERSECEU

Wstęp

Polskie Forum Cyberbezpieczeństwa – CYBERSEC PL 2016 to pierwsza edycja corocznej konferencji poświęconej budowaniu narodowych zdolności służących wzmacnianiu krajowego systemu cyberbezpieczeństwa i pozwalających na prowadzenie skutecznych i suwerennych działań w cyberprzestrzeni. CYBERSEC PL powstał w oparciu o formułę Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC EU. Założeniem obydwu konferencji jest stworzenie praktycznych rekomendacji dla zapewnienia bezpieczeństwa w cyberprzestrzeni w wymiarze globalnym (CYBERSEC EU) i narodowym (CYBERSEC PL). Bazą do tworzenia rekomendacji każdorazowo są sesje i panele dyskusyjne o charakterze warsztatów w ramach czterech ścieżek tematycznych tj. Państwo, Wojsko, Przyszłość, Biznes.

W tym roku CYBERSEC PL zgromadziło ponad 300 uczestników, a zainteresowanie konferencją przerosło nasze najśmielsze oczekiwania. Rekomendacje, które trzymacie Państwo w ręku są efektem dyskusji ekspertów i praktyków, dla których narodowy system cyberbezpieczeństwa stanowi najwyższy priorytet. W tym miejscu, mamy przyjemność jeszcze raz podziękować wszystkim panelistom i uczestnikom, którzy dzięki udziałowi w CYBERSEC PL przyczynili się do rozwoju debaty na ten aktualny temat. Mamy nadzieję, że rok do roku w podobnym gronie omawiać będziemy kolejne wyzwania dla narodowego cyberbezpieczeństwa, a także podsumowywać realizację złożonych na CYBERSEC PL 2016 strategicznie ważnych deklaracji.

Zespół Instytutu Kościuszki

Metodologia

Niniejsze rekomendacje powstały w oparciu o najważniejsze konkluzje Polskiego Forum Cyberbezpieczeństwa - CYBERSEC PL.

Dokument podzielony został na cztery główne części odpowiadające panelom dyskusyjnym w ramach ścieżek tematycznych Państwo, Wojsko, Przyszłość, Biznes. W każdej części wyszczególniono uczestników sesji, których wypowiedzi stały się bazą do opracowanych przez zespół Instytutu Kościuszki rekomendacji. Poprzedzone zostały one rekomendacjami strategicznymi tj. najważniejszymi spostrzeżeniami dotyczącymi systemu cyberbezpieczeństwa w wymiarze ogólnym.

Ponadto, na początku dokumentu wskazano deklaracje poszczególnych decydentów złożone podczas konferencji. Wyodrębnienie ich w osobnym rozdziale ma na celu ułatwienie monitorowania procesu ich wdrażania.

Tworząc rekomendacje Instytut Kościuszki starał się uwzględnić stanowiska jak największej ilości prelegentów. Prosimy mieć na uwadze, iż nie wszystkie zapisy odzwierciedlają poglądy każdego z uczestników.

ŚCIEŻKA
PAŃSTWO

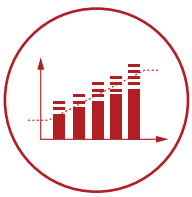
Poszukiwanie skutecznych rozwiązań, mających na celu ochronę infrastruktury krytycznej – wzmacnianie roli państwa, współpraca publiczno-prywatna.

ŚCIEŻKA
WOJSKO

Zwiększenie roli polskiej armii w zapewnianiu cyberbezpieczeństwa, lipcowy szczyt NATO w Warszawie i konieczność podjęcia dalszych kroków w polityce cyberbezpieczeństwa Sojuszu.

ŚCIEŻKA
PRZYSZŁOŚĆ

Podnoszenie świadomości w zakresie rosnącej luki zatrudnienia w dziedzinie IT i cyberbezpieczeństwa oraz wyznaczenie priorytetów systemu edukacji w tym obszarze.



ŚCIEŻKA
BIZNES

Inicjatywy podejmowane w zakresie bezpieczeństwa cybernetycznego w Polsce, problematyka zarządzania ryzykiem cybernetycznym z perspektywy ubezpieczyciela, ubezpieczenie konsekwencji ataku cybernetycznego.

DEKLARACJE ZŁOŻONE NA CYBERSEC PL 2016

- Uruchomienie tymczasowego ośrodka koordynującego działania związane z ochroną cyberprzestrzeni w Ministerstwie Cyfryzacji, który z czasem zastąpiony zostanie przez strukturę docelową.
- Stworzenie Strategii Cyberbezpieczeństwa RP (do końca 2016 r.).
- Stworzenie ustawy o krajowym systemie cyberbezpieczeństwa (projekt do końca 2016 r.).
- Skoncentrowanie działań Ministerstwa Cyfryzacji w zakresie budowania systemu cyberbezpieczeństwa na trzech filarach (do czasu przyjęcia odpowiednich krajowych aktów prawnych lub dokumentów strategicznych):
  - 1. stworzenie procedur na szczeblu centralnym, które sięgać będą w głąb struktur administracyjnych kraju i będą kompatybilne ze strukturami, które funkcjonują w sektorze cywilnym m.in. w transporcie i energetyce.
  - 2. uruchomienie programu „złota setka", mającego na celu wykreowanie w administracji odpowiednich zasobów kadrowych z wysokimi cyberkompetencjami i wiedzą.
  - 3. utworzenie następujących podmiotów:
    - Narodowego Centrum Kompetencji (nadążanie za zmianami technologicznymi)
    - CERTu Narodowego (realizowanie przedsięwzięć z zakresu ochrony cyberprzestrzeni RP i odpowiedzialność za krajowy system szybkiego ostrzegania obejmującego międzynarodowe i międzyoperatorskie punkty wymiany ruchu internetowego)
    - klastra bezpieczeństwa administracji rządowej (mającego na celu ograniczyć ilość dróg i dojść do systemu ICT administracji państwowej; polegającego na dwustopniowym systemie zabezpieczeń dla rejestrów państwowych, systemów bankowych oraz regionalizacji ochrony cyberbezpieczeństwa dla jednostek samorządowych i służb zespolonej administracji państwowej).
- Biuro Bezpieczeństwa Narodowego przygotuje nową wersję Doktryny Cyberbezpieczeństwa, która adresować będzie m.in. potrzebę skutecznej, konsekwentnej współpracy w sektorze publicznym (do końca 2016 r.).
- Ministerstwo Finansów stworzy projekt zmian do ustawy o przeciwdziałaniu praniu brudnych pieniędzy zakładający ścisłą współpracę w tym zakresie z instytucjami finansowymi (do końca 2016 r.).
- Centrum Doktryn i Szkolenia Sił Zbrojnych stworzy doktrynę działań militarnych w cyberprzestrzeni (do końca 2016 r.).
- W polskich prokuraturach, na wszystkich poziomach powstaną komórki do zwalczania cyberprzestępczości (o charakterze międzynarodowym i terrorystycznym; krajowym i wieloosobowym, powodującej straty w wielkich rozmiarach; o charakterze wieloosobowym i lokalnym i powodujących straty w znacznych rozmiarach). Wyodrębniona zostanie także kadra wyspecjalizowanych prokuratorów, którzy we współpracy z funkcjonariuszami służb specjalnych i służb porządku publicznego będą zwalczać zagrożenia w zakresie cyberprzestępczości i zmniejszać je.

REKOMENDACJE STRATEGICZNE

- Z punktu widzenia budowania systemu cyberbezpieczeństwa kluczowe jest pokonanie problemu silosowego podejścia. Należy skupić się na koordynacji i integracji wysiłków.
- Potrzebna jest ustawa podejmująca kwestie związane z cyberbezpieczeństwem, która będzie szeroko konsultowana ze wszystkimi najważniejszymi interesariuszami.
- Powinien powstać ośrodek koordynujący strategiczne działania związane z budową systemu cyberbezpieczeństwa RP. System ten powinien na poziomie operacyjnym wykorzystywać w najbardziej efektywny sposób wszystkie rozproszone zasoby.
- Istnieje konieczność budowy narodowego operatora sieci strategicznych.
- Polska powinna przeciwdziałać praniu brudnych pieniędzy w cyberprzestrzeni i generowaniu zysku z cyberprzestępstw. Tak pozyskany dochód niejednokrotnie służy finansowaniu działalności terrorystycznej. Konieczne jest również odpowiednie przygotowanie się na zagrożenia związane z obiegiem kryptowalut.
- Niezbędne jest stworzenie sprawnego, skutecznego i kompleksowego systemu zapobiegania łamaniu prawa oraz prowadzenia działalności przestępczej w cyberprzestrzeni, a także systemu ujawniania i ścigania takiej działalności. Konieczne jest nadanie odpowiedzialnym instytucjom odpowiednich kompetencji. Działania takie będą miały także istotne znaczenie prewencyjne.
- Należy określić zapotrzebowanie na konkretne kompetencje zawodowe w powiązaniu z wyznaczeniem kierunku rozwoju gospodarczego, w jakim powinna podążać Polska. W procesie tym należy wziąć pod uwagę dwa najważniejsze uwarunkowania:
  - 1. zapotrzebowanie rynkowe – popyt na produkty i usługi ICT zapewniające bezpieczeństwo użytkowania sieci i systemów teleinformatycznych tak ze strony nabywców indywidualnych, przedsiębiorstw wszystkich sektorów gospodarczych, jak i instytucji sektora publicznego, lawinowo rośnie.
  - 2. specjalne „narodowe" umiejętności i predyspozycje – historyczne złamanie Enigmy predestynuje nas do zbudowania zasobu intelektualnego w zakresie narodowej kryptologii. Tradycja „polskiej szkoły matematycznej" owocuje tym, że na krajowych uczelniach i politechnikach kształcą się najlepsi specjaliści w dziedzinie matematyki i informatyki. Ogromny kapitał intelektualny Polski, który, choć już teraz stanowi o naszym narodowym potencjale, powinien być stale rozwijany.
- Wykształcenie armii cyberspecjalistów, stworzenie im szansy rozwoju zawodowego oraz zatrzymanie w kraju tych już działających, pozwoli zbudować silny sektor cyberbezpieczeństwa. Rynek usług i produktów IT dla bezpieczeństwa może być wartością dodaną dla polskiej gospodarki oraz jednym z filarów wzrostu gospodarczego, który pozwoli Polsce wyjść z pułapki średniego dochodu. Software (ofensywny i defensywny) może być naszym towarem eksportowym, na przykład na potrzeby NATO.

- Należy uruchomić program zamówień rządowych i wojskowych w zakresie bezpieczeństwa narodowego, które zbudują wewnętrzny rynek na produkty cyberbezpieczeństwa i pozwolą zagospodarować polski kapitał intelektualny. Finansowanie takich projektów zapewnić można z m.in. budżetu programu „Innowacyjna Polska" czy przeznaczenia pewnej puli budżetu MON – ok. 2% PKB. Te kwoty pozwoliłyby zbudować polski odpowiednik DARPA.
- Polski sektor cyberbezpieczeństwa powinien stać się strategicznym polem rozwoju oraz eksportu rodzimych technologii ICT.
- Kompetencje oraz produkty i usługi dla sektora cyberbezpieczeństwa powinny być rozwijane i tworzone w cyberhubach - organizmach skoncentrowanych na tworzeniu zachęt dla rozwoju sektora cyberbezpieczeństwa, edukujących zasoby ludzkie, łączących popyt z podażą i tworzących R&D w tym sektorze. Taka kumulacja potencjału technologicznego, inwestycyjnego oraz naukowego, niezbędna dla wytworzenia przewagi konkurencyjnej produktów cybersecurity, jest zgodna z koncepcją Cyberparków Enigma, które zostały przewidziane w ramach Strategii Zrównoważonego Rozwoju Ministerstwa Rozwoju. Instytut Kościuszki animuje powstanie CYBERSEC HUB w Krakowie.
- Poziom unijny i prawo unijne należy traktować jedynie jako wspomagające i pomocnicze w budowie narodowego systemu cyberbezpieczeństwa, a także do wzmacniania współpracy międzynarodowej w zakresie zwalczania zagrożeń transgranicznych.
- Współpraca międzynarodowa w zakresie cyberzagrożeń i cyberbezpieczeństwa jest potencjalną szansą dla Polski aby budować wiedzę opartą na dobrych praktykach naszych partnerów z UE. Szansę na to daje dyrektywa NIS (ang. Network and Information Security).
- Konieczne jest prowadzenie aktywnej polityki Polski na arenie międzynarodowej – Polska powinna przygotować stanowisko wobec pytań zawartych w Rezolucji Narodów Zjednoczonych z 23 grudnia 2015 r.

ŚCIEŻKA PAŃSTWO

PANEL DYSKUSYJNY „OCHRONA INFRASTRUKTURY KRYTYCZNEJ”

UCZESTNICY:

Albert Borowski – Dyrektor Pionu Cyberbezpieczeństwa i Zarządzania Ryzykiem - COMP S.A., **Tomasz Chodor** – Zastępca Dyrektora Departamentu Bezpieczeństwa - Polskie Górnictwo Naftowe i Gazownictwo S.A., **Piotr Januszewicz** – Zastępca Dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji, **Janusz Kowalski** – Wiceprezes Zarządu ds. Korporacyjnych - Polskie Górnictwo Naftowe i Gazownictwo S.A., **Maciej Pyznar** – Szef Wydziału Ochrony Infrastruktury Krytycznej w Rządowym Centrum Bezpieczeństwa, **dr hab. inż. Konrad Świrski, prof. nadzw.** – Kierownik Zakładu Maszyn i Urządzeń Energetycznych Politechniki Warszawskiej, **Marek Wójcik** – Poseł RP, wiceprzewodniczący Komisji Administracji i Spraw Wewnętrznych, **Tomasz Zdzikot** – Podsekretarz Stanu w Ministerstwie Spraw Wewnętrznych i Administracji

Moderator: **Tomasz Szewczyk** – Ekspert Instytutu Kościuszki

Tworząc rekomendacje Instytut Kościuszki starał się uwzględnić stanowiska jak największej ilości prelegentów. Prosimy mieć na uwadze, iż nie wszystkie zapisy odzwierciedlają poglądy każdego z uczestników.

- Z punktu widzenia zapewniania bezpieczeństwa infrastruktury krytycznej konieczne będzie wypracowanie procedur szeroko rozumianej współpracy między wszystkimi najważniejszymi interesariuszami. Procedury te powinny być sprawdzane i praktykowane w ramach organizowanych ćwiczeń. Istnienie procedur współpracy będzie skutecznym narzędziem walki z problemem fragmentaryzacji działań.
- Cyberbezpieczeństwo powinno być traktowane jako jeden z elementów całościowej, komplementarnej strategii zapewniania bezpieczeństwa infrastruktury krytycznej.
- Oprócz koniecznych działań planistycznych powinny być wdrażane realne działania nakierowane na zapewnianie bezpieczeństwa.
- Operatorzy i właściciele infrastruktury krytycznej powinni aktywnie włączać się w procesy pracy nad dobrymi praktykami, które uczestnicy systemu zapewniania bezpieczeństwa infrastruktury krytycznej powinni stosować.
- Operatorzy powinni wdrażać istniejące branżowe standardy, a na straży ich implementowania powinni stać przede wszystkim regulatorzy sektorowi.
- W Polsce powinno się wdrożyć przynajmniej elementy sankcyjnego podejścia w odniesieniu do nieprzestrzegania standardów.
- Cyberbezpieczeństwo infrastruktury krytycznej powinno być zapewnianie na całym łańcuchu dostaw. Odpowiednie podmioty powinny dokonywać certyfikacji funkcjonujących produktów, także w odniesieniu do możliwości istnienia backdoorów.

- Ministrowie odpowiedzialni za systemy infrastruktury krytycznej powinni aktywniej włączać się w działania związane z podnoszeniem jej bezpieczeństwa.
- Należyte działania w zakresie cyberbezpieczeństwa infrastruktury krytycznej wymagają odpowiedniego finansowania.
- Konieczny jest rozwój polskich prac badawczo rozwojowych, szczególnie nakierowanych na bezpieczeństwo automatyki przemysłowej.

ŚCIEŻKA WOJSKO

PANEL DYSKUSYJNY

„MODERNIZACJA POLSKIEJ ARMII A KWESTIE CYBERBEZPIECZEŃSTWA”

UCZESTNICY:

dr hab. inż. Ryszard Antkiewicz, prof. nadzw. – Kierownik Zakładu Badań Operacyjnych i Wspomagania Decyzji w Wojskowej Akademii Technicznej, **płk dr Karol Dymanowski** – p.o. Dyrektora Departamentu Polityki Zbrojeniowej w Ministerstwie Obrony Narodowej, **kmdr por. Sylwester Filipczak** – Zastępca Szefa Oddziału Rozwoju Koncepcji w Centrum Doktryn i Szkolenia Sił Zbrojnych, **Borys Iwaszko** – Dyrektor Biura Bezpieczeństwa Cybernetycznego Służby Kontrwywiadu Wojskowego, **ppłk dr inż. Bartosz Jasiul** – Kierownik Laboratorium Analiz Ataków Cybernetycznych w Wojskowym Instytucie Łączności, **Mirosław Maj** – Prezes Fundacji Bezpieczna Cyberprzestrzeń, **Paweł Prokop** – Wiceprezes Zarządu, Dyrektor Sektora Publicznego Comarch, **Janusz Sobolewski** – Dyrektor Programu C4ISR, PGZ Polska Grupa Zbrojeniowa S.A., **prof. dr hab. inż. Ryszard Szpyra** – Kierownik studiów doktoranckich Akademii Obrony Narodowej, **płk Robert Walkowski** – Służba Wywiadu Wojskowego

Moderator: **dr hab. Tomasz Siemiątkowski, prof. nadzw.** – Szkoła Główna Handlowa w Warszawie, Uniwersytet Kardynała Stefana Wyszyńskiego

Tworząc rekomendacje Instytut Kościuszki starał się uwzględnić stanowiska jak największej ilości prelegentów. Prosimy mieć na uwadze, iż nie wszystkie zapisy odzwierciedlają poglądy każdego z uczestników.

- Skuteczne działanie państwa w cyberprzestrzeni wymaga sprecyzowania misji, wizji i wynikającej z tego strategii. Na tej podstawie powinny być określone role i kompetencje poszczególnych podmiotów.
- W ramach strategii narodowej powinno się dążyć do wypracowania i określenia jasnych zadań jakie w cyberprzestrzeni powinny prowadzić Siły Zbrojne RP.
- Działania nakierowane na zwiększanie bezpieczeństwa cyberprzestrzeni, realizowane przez podmioty ze świata cywilnego i militarnego nie powinny być traktowane oddzielnie. Ponieważ są to raczej działania komplementarne, powinny być ustanowione mechanizmy współpracy, pozwalające osiągać efekt synergii. Obszarami współpracy mogłoby być m.in. wykrywanie zagrożeń i wymiana informacji w tym zakresie, czy też wypracowywanie mechanizmów przeciwdziałania zagrożeniom.
- Kluczowe z punktu widzenia efektywnego działania Sił Zbrojnych RP w cyberprzestrzeni będzie odpowiednie wyszkolenie nie tylko „cyber wojowników” ale także kadry dowódczej.
- Z punktu widzenia wzmacniania zdolności Sił Zbrojnych RP do prowadzenia działań w cyberprzestrzeni, kluczowe jest korzystanie z doświadczenia sojuszników.
- Zanim przystąpimy do budowania zdolności Sił Zbrojnych RP do działania w cyberprzestrzeni należy określić jakie cele należy osiągnąć i przed jakimi wyzwaniami stoi Polska. Kluczowe jest zdefiniowanie zagrożeń.

ŚCIEŻKA WOJSKO

- Szczególnym obszarem gdzie współpraca między obszarem cywilnym i militarnym jest niezbędna jest walka z zagrożeniami hybrydowymi.
- Konieczny jest rozwój sektora R&D w zakresie tworzenia rozwiązań wzmacniających cyberbezpieczeństwo także dla obszaru militarnego. Ważnym elementem tego procesu jest faza wdrożeniowa, którą należy wzmacniać. Interesariusze projektów powinni dążyć do weryfikacji takich rozwiązań na wczesnym studium wykonalności projektu, w warunkach zbliżonych do operacyjnych.
- Siła armii wynika z czterech elementów:
  1. Efektywnej struktury organizacyjnej – przede wszystkim właściwego systemu dowodzenia
  2. Systemu łączności i informatyki wspierającego efektywną strukturę organizacyjną
  3. Procedur i ludzi
  4. Sprzętu

  Sektor prywatny może realnie wesprzeć Siły Zbrojne RP w zakresie budowy tych elementów (szczególnie punktów 2 i 3).
- Winno się dążyć do rozwoju i budowy bezpiecznych, narodowych produktów z obszaru cyberbezpieczeństwa.
- By sektor prywatny mógł wspierać rozwój cyberzdolności Sił Zbrojnych RP, konieczne jest stworzenie właściwych ram prawnych. Na przykład Rozporządzenie Rady Ministrów z dnia 4 października 2010 r. w sprawie wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym powinno zostać uzupełnione o sektor IT i cyberbezpieczeństwa.
- W ramach Sił Zbrojnych RP powinny zostać utworzone efektywnie funkcjonujące rodzaje sił zbrojnych dedykowane do prowadzenia działań w cyberprzestrzeni.
- Wsparcie ze strony organizacji pozarządowych – inicjatywy takie jak CYBERSEC PL, Polska Obywatelska Cyberobrona – powinny być rozwijane.
- Konieczne jest jak najszybsze sfinalizowanie programu operacyjnego „Bezpieczeństwo w cyberprzestrzeni i wsparcie kryptologiczne" - priorytet Programu Modernizacji Technicznej Sił Zbrojnych.
- Progres prac wymaga uregulowania obszaru wymiany informacji między ekspertami cywilnymi i militarnymi.
- Rekomenduje się stworzenie polskiego odpowiednika DARPA - ośrodka R&D w sektorze prywatnym, który na zlecenie wojska tworzyłby cyberrozwiązania. Polska DARPA nie powinna być usytuowana w lub przy Ministerstwie Obrony Narodowej, ale np. przy Polskiej Grupie Zbrojeniowej (PGZ).

ŚCIEŻKA PRZYSZŁOŚĆ

PANEL DYSKUSYJNY „BUDOWA CYFROWEGO ZASOBU KADROWEGO – WYZWANIE DLA POLSKIEJ EDUKACJI”

UCZESTNICY:

Jacek Cichocki – DELab Uniwersytet Warszawski, **prof. dr hab. n. mat. Jerzy Gawinecki** – Dziekan Wydziału Cybernetyki Wojskowej Akademii Technicznej, **dr Paweł Modrzyński** – Dyrektor Departamentu Innowacji i Rozwoju w Ministerstwie Nauki i Szkolnictwa Wyższego, **Grzegorz Poznański** – Dyrektor Departamentu Polityki Bezpieczeństwa Ministerstwa Spraw Zagranicznych, **Krzysztof Silicki** – Doradca Dyrektora NASK, Dyrektor ds. Współpracy z ENISA w Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji, **dr hab. inż. Marek Stanuszek** – Dziekan Wydziału Fizyki, Matematyki i Informatyki Politechniki Krakowskiej, **dr hab. inż Jerzy Surma** – Kierownik studiów podyplomowych Zarządzanie Cyberbezpieczeństwem w Szkole Głównej Handlowej, **Zdzisław Wiater** – Zastępca Dyrektora Pionu Administracji Publicznej, Dyrektor Departamentu Organizacji Międzynarodowych i Rozwiązań dla Sektora Bezpieczeństwa - Asseco Poland S.A

Moderator: **Izabela Albrycht** – Prezes Zarządu Instytutu Kościuszki, Przewodnicząca Komitetu Organizacyjnego CYBERSEC EU

Tworząc rekomendacje Instytut Kościuszki starał się uwzględnić stanowiska jak największej ilości prelegentów. Prosimy mieć na uwadze, iż nie wszystkie zapisy odzwierciedlają poglądy każdego z uczestników.

WYZWANIA I PROBLEMY

- Aktualna dynamika rozwoju sektora ICT i cyberbezpieczeństwa wymaga wielopokoleniowego namysłu nad budową cyberkadr. Dzisiejszy niedostatek wiedzy i edukacji, będzie niczym w porównaniu z brakami, które odczuwać będziemy za 50 lat.
- Państwo powinno oszacować jakie zdolności w zakresie cyberochrony i cyberobrony chce osiągnąć i paralelnie do tego określić zapotrzebowanie na specjalistów i ich kompetencje.
- Potrzebni są specjaliści o profilu technicznym, ale również cyberprawnicy, cybermenedżerowie czy cyberdyplomaci, a także „integratorzy rozwiązań” – posiadający „cyfrową wyobraźnię” - umiejętność rozpoznania i zrozumienia globalnych cyfrowych trendów oraz projektowania całościowych rozwiązań w dziedzinie cyberbezpieczeństwa, by być gotowym na coś czego jeszcze nie znamy.
- Nie wszyscy pracownicy sfery publicznej będą jednak cyberspecjalistami, dlatego istotne jest budowanie powszechnej cyberświadomości i wiedzy, którą przedstawiciele administracji będą potrafili przełożyć na podejmowane działania dyplomatyczne czy polityczne, takie jak tworzenie środków budowy zaufania (ang. Confidence Building Measures - CBMs) czy legalnych ram funkcjonowania w cyberprzestrzeni i układania stosunków miedzy państwami.

WYZWANIA I PROBLEMY

- Państwo powinno zabezpieczyć adekwatne środki budżetowe zapewniające utrzymanie odpowiedniego potencjału ludzkiego do ochrony systemów i sieci teleinformatycznych polskiej administracji. Proces budowania systemu cyberbezpieczeństwa nie może być dłużej traktowany jako „bezkosztowy", a zabezpieczenie środków na wynagrodzenia jest jego najważniejszym elementem.
- Wynagrodzenia branży cybersecurity są najwyższymi w sektorze ICT i żadna administracja państwowa na świecie nie posiada wystarczających zasobów finansowych, aby konkurować z rynkiem. Dlatego państwo nie może konkurować wyłącznie warunkami finansowymi zatrudnienia. Specjaliści ds. cyberbezpieczeństwa są zainteresowani nie tylko wysokością wynagrodzeń, ale także uczestnictwem w realizacji pewnej długofalowej wizji budowania cyberbezpieczeństwa państwa. Zatem kluczowym zadaniem dla rządu, który odpowiedzialny jest za stworzenie Strategii Cyberbezpieczeństwa RP jest zaprojektowanie działań dedykowanych budowie systemu ochrony cyberprzestrzeni Polski i zaangażowanie do pracy na rzecz dobra wspólnego jak największej liczby cyberspecjalistów.

WSPÓŁPRACA

- W sektorze komercyjnym i środowisku naukowym jest największy potencjał wiedzy i kompetencji, które mogą wesprzeć państwo. Niedostatek kadr oraz braki budżetowe można wyrównywać rozwijając formuły i modele współpracy biznesu, administracji i uczelni. Dlatego, współpraca oparta na synergii celów, zaufaniu, przejrzystości i przekonaniu o potrzebie zintegrowania działań na rzecz budowy cyberbezpieczeństwa jest najważniejszą rekomendacją CYBERSEC PL 2016.
- Rząd powinien pozostawać w kontakcie z ekspertami i zadawać im pytania. Jedną z form przepływu wiedzy i platformą dialogu może być CYBERSEC PL.
- Poszerzenie bazy cyberkadr mogłoby być wynikiem integracji administracji i sektora prywatnego np. poprzez stworzenie organizacji na kształt estońskiej Ligii Obrony – oddziałów cybernetycznych złożonych ze specjalistów na co dzień funkcjonujących w swoich firmach i instytucjach, a na czas wojny mających przypisane określone obowiązki i zadania cybernetyczne. Integracja tych dwóch sektorów powinna dotyczyć nie tylko fazy reagowania na zagrożenia, ale również wykrywania ich. W Polsce funkcjonuje stowarzyszenie Polska Obywatelska Cyberobrona, która może pełnić taką funkcję.
- Potencjał tkwiący w przemyśle trzeba stale rozbudowywać. Dobrym przykładem wsparcia instytucjonalnego są np. grupy robocze w NATO. NATO definiuje pewien problem do rozwiązania i zaprasza do współpracy podmioty prywatne. Dzięki temu rośnie potencjał wiedzy firm. Również UE prowadzi grupy robocze związane z bezpieczeństwem cybernetycznym, które zajmują się podobnymi konsultacjami.

WSPÓŁPRACA

- Strategiczne programy rozwojowe czy modernizacyjne, jak np. program modernizacji Sił Zbrojnych RP powinien obejmować także oprogramowanie, a tym samym angażować potencjał narodowy, wypełniając lukę ambitnych, motywujących projektów. Aktualnie można zaobserwować odpływ ludzi do np. programów NATO.
- Współpraca uczelni z biznesem powinna być katalizatorem przemiany oferty edukacyjnej w kierunku kształcenia specjalistów odpowiednich dla potrzeb rynku, jest to przemiana długoterminowa.
- Współpraca ośrodków naukowych i sektora komercyjnego potrzebna jest również do tworzenia sylwetki absolwentów na przykład na wzór Rady Kwalifikacji ds. Absolwentów Wojskowej Akademii Technicznej, złożonej z przedstawicieli instytucji rządowych i prezesów firm. Ważne jest także to, aby wbrew dominującemu trendowi, uczelnie nie tylko z sobą konkurowały, ale również współpracowały na rzecz realizacji ważnych projektów.

CYBEREDUKACJA

- Konieczne jest budowanie świadomości w społeczeństwie, że cyberprzestrzeń jest elementem dobra narodowego i gospodarki narodowej, w której wypracowywana jest duża część PKB kraju, a poprzez systemy teleinformatyczne realizowane są podstawowe potrzeby obywateli. Najistotniejszy kapitał ludzki konieczny do budowania cyberbezpieczeństwa kraju stanowi, de facto, całe społeczeństwo.
- Edukację na rzecz cyberbezpieczeństwa należy rozpocząć już w szkołach podstawowych, jeśli nie w domu. Polskie społeczeństwo, a także dydaktycy nie są w tym momencie na to przygotowani. Tymczasem, promowanie wiedzy o cyberzagrożeniach, nauka bezpiecznych zachowań w Internecie i umiejętności bezpiecznego korzystania z jego zasobów jest podstawą bezpieczeństwa w cyberprzestrzeni. Edukację w tym zakresie należy kontynuować na kolejnych poziomach nauczania.
- Obok higieny korzystania z Internetu, ważne jest aby program nauczania bardziej koncentrował się na tzw. przedmiotach STEM (ang. Science, Technology, Engineering, Mathematics, pl. Nauka, Technologia, Inżynieria i Matematyka), dzięki czemu wzrośnie również zainteresowanie kontynuacją kształcenia na tych specjalnościach.
- Dla wykształcenia armii cyberspecjalistów konieczne jest stworzenie kierunków studiów dedykowanych cyberbezpieczeństwu. Aktualne, wyrywkowe umieszczenie zagadnień związanych z bezpieczeństwem sieci i systemów teleinformatycznych w programach nauczania informatyki daje niepełny obraz zagrożeń i wyzwań i nie jest w pełni komplementarne do potrzeb. Konieczne jest tworzenie bloków programowych o cyberbezpieczeństwie od początku studiów informatycznych.

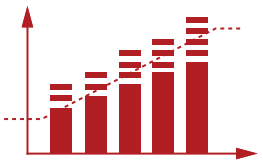
CYBEREDUKACJA

- Potrzebne jest stworzenie „zespołów łowców" – cyberspecjalistów o najwyższych kwalifikacjach którzy będą potrafili skojarzyć wybrane elementy, tworząc innowacyjną całość. Polska ma taki potencjał, gdyż polscy specjaliści są cenieni na całym świecie odnosząc sukcesy w międzynarodowych konkursach tj. RobotChallenge, Hello World Open, University Rover Challenge i innych. Aby zatrzymać ich w kraju należy zapewnić im szanse dalszego rozwoju. Najlepsi uczestniczą w międzynarodowych konferencjach, spotykają się ze specjalistami z innych krajów i poświęcają czas na samorozwój. Trzeba stworzyć z nich kadrę dydaktyków i także na tej bazie rozbudowywać nasz narodowy cyberpotencjał.
- Jednym z modeli, w którym można zatrzymać cyberspecjalistów jest stworzenie mechanizmu stypendiów dla wybitnie zdolnych studentów oraz zapewnienie im udziału w projektach dużej kategorii. Ministerstwo Nauki i Szkolnictwa Wyższego przy wsparciu pozostałych relewantnych resortów, biorąc pod uwagę potrzeby naszego kraju oraz posiadany potencjał intelektualny, zdolny do stworzenia własnych zasobów technologicznych, powinno podjąć działania zmierzające do tego abyśmy własnymi technologiami lepiej zabezpieczyli krajową cyberprzestrzeń.
- Konieczne jest wspieranie programów naukowych prowadzonych na uczelni we współpracy z firmami komercyjnymi.

ŚCIEŻKA BIZNES

PANEL DYSKUSYJNY

„JAK ZWIĘKSZYĆ POZIOM DOJRZAŁOŚCI W SFERZE CYBERBEZPIECZEŃSTWA”



UCZESTNICY:

Dariusz Gołębiewski – Dyrektor ds. Inżynierii Ryzyka i Rozwoju Współpracy z Przemysłem w PZU S.A., **Piotr Kalbarczyk** – Dyrektor Biura Bezpieczeństwa Informatycznego w Departamencie Bezpieczeństwa - PKO Bank Polski, **Robert Kępiński** – Pełnomocnik ds. Ochrony Infrastruktury Krytycznej - Polskie Górnictwo Naftowe i Gazownictwo S.A., **dr inż. Andrzej Kozak** – Radca Prezesa w Urzędzie Dozoru Technicznego, **dr Maciej Majewski** – Prezes Zarządu Pentacomp S.A., **Piotr Ratajczak** – Kierownik Zespołu Operacyjnego Monitorowania Bezpieczeństwa IT w PZU S.A., **dr hab. Roman Szwed** – Członek Rady Polskiej Izby Informatyki i Telekomunikacji

Moderator: **Artur Piechocki** – Fundacja Bezpieczna Cyberprzestrzeń

Tworząc rekomendacje Instytut Kościuszki starał się uwzględnić stanowiska jak największej ilości prelegentów. Prosimy mieć na uwadze, iż nie wszystkie zapisy odzwierciedlają poglądy każdego z uczestników.

- Należy pamiętać, że rozwój rynku cyberubezpieczeń jest ważny także z punktu widzenia bezpieczeństwa infrastruktury krytycznej, a tym samym bezpieczeństwa narodowego. Cyberpolisy mogą znacznie przyczynić się do podniesienia jego poziomu.
- W ramach dojrzałego procesu ubezpieczania danego podmiotu prowadzone są działania weryfikujące poziom szeroko rozumianego cyberbezpieczeństwa. Między innymi wskazywane są elementy wymagające poprawy, oraz przekazywane są rekomendacje odpowiednich rozwiązań. Zastosowanie elementów związanych z podejściem proaktywnym (co może obniżyć składkę, lub być warunkiem ubezpieczenia) przyczynia się do podniesienia ogólnego poziomu cyberbezpieczeństwa. Takie podejście ubezpieczycieli powinno być w Polsce powszechnie stosowane.
- W ramach wspierania rozwoju rynku cyberubezpieczeń powinno się rozważyć stworzenie przez rząd funduszu reasekuracji.
- Ubezpieczyciele powinni oferować produkty dostosowane do specyfiki funkcjonowania danego podmiotu, a nie produkty „z półki”.
- Powinno się rozważyć zmianę prawa zamówień publicznych i włączyć w ich katalog cyberubezpieczenia.
- Z punktu widzenia operatorów infrastruktury krytycznej, pozytywnie przyjmowane są wszystkie zachęty sprzyjające podnoszeniu poziomu cyberbezpieczeństwa. Jedną z takich zachęt mogą być zniżki przysługujące danemu podmiotowi po spełnianiu standardów cyberbezpieczeństwa.
- Z punktu widzenia operatorów infrastruktury krytycznej, w sytuacji braku obowiązkowego przeprowadzania audytów zewnętrznych, dodatkowy audyt przeprowadzony przez ubezpieczyciela (wraz z rekomendacjami), może nieść dużą wartość dodaną.

CYBERSEC PL 2016

W LICZBACH

KONFERENCJA

1
Wyzwanie dla Polski

4
Ścieżki tematyczne

5
Paneli dyskusyjnych

10
Godzin networkingowych

LUDZIE

41
Akredytowanych dziennikarzy

15
Osób zespołu organizacyjnego

43
Prelegentów

>300
Uczestników

MEDIA & SPOTKANIA

20
Wywiadów dla CYBERSEC TV

>1000
Zdjęć

>900
Filiżanek kawy

64100
Impresji na Twitterze

Instytut Kościuszki – think tank kreujący nowe idee dla Polski i Europy – jest niezależnym, pozarządowym instytutem naukowo-badawczym o charakterze non-profit, założonym w 2000 r. Instytut Kościuszki opierając się na pogłębionej, interdyscyplinarnej analizie, propaguje rozwiązania w postaci rekomendacji programowych i ekspertyz, których odbiorcami są instytucje unijne, rządowe i samorządowe, polscy i europejscy politycy i decydenci, a także media, przedsiębiorcy oraz pasjonaci niezależnej myśli i otwartej debaty.

Misją Instytutu Kościuszki jest działanie na rzecz społeczno-gospodarczego rozwoju i bezpieczeństwa Polski, jako aktywnego członka Unii Europejskiej oraz partnera sojuszu euroatlantyckiego.

Działalność Instytutu koncentruje się wokół siedmiu obszarów programowych tj. Instytucje i Prawo RP i UE, Energia i Klimat, Państwo Prawa, Stosunki Międzynarodowe, Promocja Polski, Bezpieczeństwo i Obrona, Gospodarka i Finanse.

INSTYTUTKOSCIUSZKI @IKOSCIUSZKI

INSTYTUT KOŚCIUSZKI

jest organizatorem

CYBERSEC EU
EUROPEJSKIE
FORUM CYBERBEZPIECZEŃSTWA

PARTNERZY GŁÓWNI

COMARCH

asseco

EXATEL
people behind technology

PARTNER

Comp

PATRONI MEDIALNI

POLSKIE RADIO

TVP INFO

pap
centrum prasowe

CyberDefence24

BIZNES ALERT

CIRE.PL
Centrum Informacji o Rynku Energii

BEZPIECZEŃSTWO

polska-zbrojna.pl

PATRONI HONOROWI

Ministerstwo Spraw Wewnętrznych i Administracji

Rzeczpospolita Polska Ministerstwo Spraw Zagranicznych

RCB Rządowe Centrum Bezpieczeństwa

Ministerstwo Cyfryzacji

MSP Ministerstwo Skarbu Państwa

Ministerstwo Infrastruktury i Budownictwa

BBN Biuro Bezpieczeństwa Narodowego

Prokuratura Krajowa

Ministerstwo Nauki i Szkolnictwa Wyższego

Ministerstwo Rozwoju

Ministerstwo Finansów

PARTNERZY STRATEGICZNI

PGNiG

PZU

PGZ Polska Grupa Zbrojeniowa

PKO Bank Polski

TAURON

ORGANIZATOR

Instytut Kościuszki

PARTNER PROGRAMOWY

Fundacja bezpieczna cyberprzestrzeń

I Polskie Forum Cyberbezpieczeństwa zostało współfinansowane ze środków prewencyjnych PZU.