CYBERSEC PL

POLSKIE FORUM CYBERBEZPIECZEŃSTWA

Warszawa 06. 04. 2017

Druga edycja corocznej konferencji poświęconej strategicznym aspektom narodowego cyberbezpieczeństwa Polski

REKOMENDACJE

ŚCIEŻKA **PAŃSTWO**

ŚCIEŻKA **OBRONA**

ŚCIEŻKA **PRZYSZŁOŚĆ**

ŚCIEŻKA **BIZNES**

WWW.CYBERSECFORUM.PL

#CSPL17

#RazemDlaCyberbezpieczeństwa

Szanowni Państwo,

CYBERSEC PL 2017 zgromadził ponad 500 uczestników reprezentujących administrację publiczną, sektor prywatny, środowiska eksperckie, liderów opinii i wiodące ogólnopolskie media. Dzięki naszym wspólnym wysiłkom, dziś możemy cieszyć się sukcesem Forum, które stało się jednym z najważniejszych wydarzeń dedykowanych strategicznym aspektom cyberbezpieczeństwa w Polsce.

W temacie cyberbezpieczeństwa musimy grać do jednej bramki – podkreślali zgodnie eksperci zaproszeni na CYBERSEC PL. Cieszymy się, że wzajemna współpraca i koordynacja były słowami, które podczas forum padały najczęściej.

Mamy również nadzieję, że CYBERSEC PL przyczyni się do budowy narodowych zdolności naszego kraju w tym obszarze. To dla nas ogromna satysfakcja móc stymulować krajową debatę z udziałem kluczowych interesariuszy cyberprzestrzeni oraz tworzyć platformę wymiany wiedzy i doświadczeń skupiającą przedstawicieli różnorodnych podmiotów, sektorów i środowisk.

Aby osiągnąć ten cel, Instytut Kościuszki opracował strategiczne rekomendacje dla wzmocnienia cyberbezpieczeństwa Polski, w oparciu o ustalenia Forum. Życząc owocnej lektury, mamy nadzieję, że będą one istotnym wsparciem w wytyczaniu kierunków rozwoju i narodowych polityk bezpieczeństwa.

Z pozdrowieniami,

Zespół Instytutu Kościuszki

INSTYTUT KOŚCIUSZKI

REKOMENDACJE STRATEGICZNE

PANEL OTWIERAJĄCY – STRATEGIA CYBERBEZPIECZEŃSTWA RP – JAK WDROŻYĆ W ŻYCIE KLUCZOWE DZIAŁANIA

UCZESTNICY:

Tomasz Szatkowski – Podsekretarz Stanu w Ministerstwie Obrony Narodowej

Tomasz Zdzikot – Podsekretarz Stanu w Ministerstwie Spraw Wewnętrznych i Administracji

Jadwiga Emilewicz – Podsekretarz Stanu w Ministerstwie Rozwoju

Piotr Januszewicz – Dyrektor Departamentu Cyberbezpieczeństwa, Ministerstwo Cyfryzacji

Dariusz Gwizdała – Zastępca Szefa Biura Bezpieczeństwa Narodowego

Marek Kubiak – Dyrektor Rządowego Centrum Bezpieczeństwa

dr Arkadiusz Marchewka – Poseł na Sejm, członek sejmowej Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii

Nikodem Bończa Tomaszewski – Prezes Zarządu w Exatel

Moderacja: dr Joanna Świątkowska – Dyrektor Programowy CYBERSEC, Ekspert Instytutu Kościuszki

Tworząc rekomendacje Instytut Kościuszki starał się uwzględnić stanowiska jak największej liczby prelegentów.

Prosimy mieć na uwadze, iż nie wszystkie zapisy odzwierciedlają poglądy każdego z uczestników.

RAMY INSTYTUCJONALNO-PRAWNE DLA CYBERBEZPIECZEŃSTWA

1. Konieczne jest jak najszybsze opracowanie planu działań Krajowych Ram Polityki Cyberbezpieczeństwa oraz przyjęcie ustawy implementującej dyrektywę NIS;
2. Projektując konkretne rozwiązania legislacyjne dla cyberbezpieczeństwa nie należy pominąć kwestii zapewnienia prywatności użytkowników sieci;

3. W systemie cyberbezpieczeństwa nie ma miejsca na jednowładztwo i właściwe mu sztywne i hierarchiczne podejście. Potrzebne są systemowe i elastyczne rozwiązania;
4. System cyberbezpieczeństwa musi zostać oparty na dwóch głównych filarach. Po pierwsze, zarządzaniu strategicznym, które musi być ponadresortowe – tworząc ten filar należy wziąć pod uwagę koncepcję ponadresortowego podejścia do koordynacji cyberbezpieczeństwa opracowaną przez ekspertów Zespołu ds. Cyberbezpieczeństwa Biura Bezpieczeństwa Narodowego. Po drugie, na zarządzaniu operacyjnym, które musi być oparte na standardowych procedurach operacyjnych i współpracy pomiędzy wszystkimi podmiotami.

CYBERBEZPIECZEŃSTWO TO GRA ZESPOŁOWA

Są różne modele zarządzania działaniami prowadzonymi w cyberprzestrzeni, a tym samym podziału odpowiedzialności między jej interesariuszami. Zawsze jednak potrzebny jest koordynator krajowego systemu cyberbezpieczeństwa, który będzie odpowiedzialny za wdrożenie strategii i współpracę z intere-sariuszami, a także wyposażony w narzędzia oddziaływania na uczestników systemu.

BUDOWANIE CYBERSUWERENNOŚCI

1. Polska powinna zmierzać do zbudowania cybersuwerenności w oparciu o 6 elementów – własną infrastrukturę i kadry, ochronę własnych danych, świadczenie publicznych e-usług, zapewnienie cyberbezpieczeństwa, zbudowanie własnego narodowego sektora informatycznego jako zaplecza gospodarczego, dzięki któremu możliwe będzie zrealizowanie części tych zadań (należy to uczynić w modelu państwowo-prywatnym);
2. Konieczne jest wypracowanie synergii telekomunikacyjnej w ramach sektora publicznego – strukturalne rozproszenie jest nieefektywne kosztowo i organizacyjne.

BUDOWANIE POTENCJAŁU OBRONNEGO - DZIAŁANIA CYBEROFENSYWNE I CYBERDEFENSYWNE

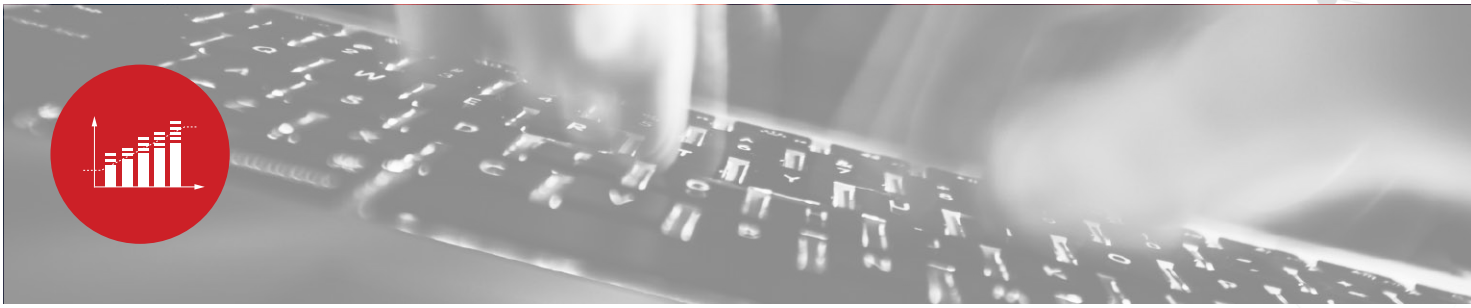
W wymiarze militarnym konieczne jest dokonanie zmian doktrynalnych (wizja działań w cyberprzestrzeni) i strukturalnych (stworzenie i zaadaptowanie struktur dowodzenia zdolnościami cyber tak, aby wkomponowały się w istniejący system kierowania i dowodzenia), a także budowanie zasobów i kompetencji (szkolenia oraz ćwiczenia - wewnątrzresortowe; z rożnymi rodzajami wojsk oraz międzyresortowe z różnymi segmentami administracji publicznej zapewniające interoperacyjność elementów państwa).

BUDOWANIE POTENCJAŁU NAUKOWO – PRZEMYSŁOWEGO

1. Zapewnienie cyberbezpieczeństwa jest wyzwaniem dla rozwoju przemysłu 4.0. Sektor cyberbezpieczeństwa to także ocean możliwości gospodarczych, dlatego konieczne jest pobudzanie innowacyjności tego sektora w Polsce i tworzenie usług i produktów na rynek krajowy i jako towar eksportowy;
2. Należy rozwijać nowe technologie dla cyberbezpieczeństwa w ramach modelu otwartości na świat i we współpracy między startupami, MŚP i dużymi firmami tak, aby partycypować w globalnym wyścigu technologicznym;
3. Konieczne jest uruchomienie akceleratora dla startupów cybersecurity oraz centrum badawczo-rozwojowego dla cyberbezpieczeństwa;
4. Polska posiada potencjał kapitału ludzkiego dla cyberbezpieczeństwa, dlatego musimy stworzyć adekwatny system kształcenia na potrzeby rynku oraz administracji publicznej, a następnie stawiać ambitne cele informatykom w zakresie tworzenia unikatowych rozwiązań m.in. dla administracji, które mogą stać się towarem eksportowym.

OPERATORZY INFRASTRUKTURY KRYTYCZNEJ I USŁUG KLUCZOWYCH ORAZ ADMINISTRACJA PUBLICZNA NA PIERWSZEJ LINII CYBERZAGROŻEŃ

1. Należy dostosować procedury i legislacje w zakresie postępowań przygotowawczych i prokuratorskich do skali zagrożeń i specyfiki zagrożeń cyberprzestępstwami;
2. Te elementy systemu ochrony infrastruktury krytycznej, które zostały przez ostatnie lata wypracowane i są efektywne, należy zaimplementować do planu realizacji Krajowych Ram Polityki Cyberbezpieczeństwa, tak aby nie dublować obowiązków nałożonych na operatorów;
3. Budowa systemu cyberbezpieczeństwa powinna uwzględniać integrację usług kluczowych z infrastrukturą krytyczną, co wymagało będzie przeglądu przepisów, które regulują te kwestie i modernizacji systemu ochrony infrastruktury krytycznej – system jest ułomny w związku z tym, że ustawodawca nie przewidział żadnych możliwości egzekwowania obowiązków operatorów w zakresie przygotowania się na zagrożenia, nie ma możliwości prowadzenia audytów i kontroli. System w tym zakresie należy zmienić poprzez wprowadzenie sankcji obejmujących operatorów, którzy nie spełnialiby stawianych przed nimi wymagań i minimalnych standardów w zakresie bezpieczeństwa teleinformatycznego;
4. Należy odejść od kryterium obiektowego w zakresie identyfikacji obszarów infrastruktury krytycznej.



ŚCIEŻKA BIZNES

OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH OSOBOWYCH – OCHRONA DANYCH W ERZE SPOŁECZEŃSTWA CYFROWEGO

UCZESTNICY:

dr Wojciech Rafał Wiewiórowski – Z-ca Europejskiego Inspektora Ochrony Danych (nagrane wystąpienie)

dr Maciej Kawecki – Doradca w gabinecie politycznym Ministra Cyfryzacji

Tomasz Soczyński – Z-ca Dyrektora Departamentu Informatyki w Biurze Generalnego Inspektora Danych Osobowych

Jędrzej Niklas – Ekspert ds. prawnych Fundacji Panoptykon

Moderacja: dr Paweł Litwiński – Adwokat, członek Rady ds. Cyfryzacji II kadencji

Tworząc rekomendacje Instytut Kościuszki starał się uwzględnić stanowiska jak największej liczby prelegentów.

Prosimy mieć na uwadze, iż nie wszystkie zapisy odzwierciedlają poglądy każdego z uczestników.

1. Przedsiębiorcy przetwarzający dane osobowe stoją przed koniecznością dostosowania zasad ochrony danych do nowych europejskich ram prawnych ochrony danych osobowych. Ten proces dostosowania powinien już trwać, a ostateczny termin to rozpoczęcie stosowania nowego prawa, czyli 25 maja 2018 r.;
2. Przygotowywane przez Ministerstwo Cyfryzacji nowe polskie przepisy o ochronie danych osobowych stanowią uzupełnienie regulacji europejskich;
3. Podejście oparte na ryzyku (risk based approach) jest charakterystyczne dla nowych zasad ochrony danych osobowych – podmioty przetwarzające dane będą musiały ustalić poziom ryzyka dla danych osobowych i dobrać odpowiednie środki zabezpieczenia danych, celem zminimalizowania tego ryzyka;

4. Z punktu widzenia wdrożenia nowych zasad ochrony danych osobowych kluczowe jest przejście z filozofii zarządzania istniejącym ryzykiem dla bezpieczeństwa danych osobowych na filozofię minimalizacji tego ryzyka. Przedsiębiorcy będą musieli więc każdorazowo ocenić ryzyko związane z przetwarzaniem danych oraz samodzielnie zdecydować, jakie środki zabezpieczające podjąć, by ryzyko takie ograniczyć. Trafność takiego wyboru, oceniania będzie z kolei w dalszej kolejności przez krajowy organ ochrony danych osobowych w toku ewentualnego, prowadzonego przez niego postępowania;
5. Przedsiębiorcy będą również zobowiązani do wykonania tzw. oceny skutków dla ochrony danych osobowych. Jej elementem będzie ustalenie poziomu ryzyka dla danych osobowych;
6. Prawidłowo przeprowadzona ocena skutków dla ochrony danych osobowych może skutkować koniecznością tzw. uprzednich konsultacji z organem ochrony danych osobowych. W wyniku takich konsultacji administrator danych może zostać zobowiązany do przedsięwzięcia środków zabezpieczenia danych wskazanych przez regulatora;
7. Już dzisiaj należy rozpocząć prace w kierunku wdrożenia nowych zasad ochrony danych osobowych.
8. Bazy danych osobowych mają ogromne znaczenie z punktu widzenia zapewnienia cyberbezpieczeństwa.
9. Działając w oparciu o podejście oparte na ryzyku należy uwzględnić zagrożenia dla bezpieczeństwa danych osobowych wynikające z możliwych cyberataków.

ŚCIEŻKA OBRONA

CYBEROBRONA POLSKI PO SZCZYCIE NATO W WARSZAWIE

UCZESTNICY:

płk Paweł Dziuba – Szef Inspektoratu Systemów Informacyjnych w Ministerstwie Obrony Narodowej

Mirosław Maj – Prezes Fundacji Bezpieczna Cyberprzestrzeń

Zdzisław Wiater – Zastępca Dyrektora Pionu Administracji Publicznej, dyrektor Departamentu Organizacji Międzynarodowych i Rozwiązań dla Sektora Bezpieczeństwa w Asseco Poland S. A.

Moderacja: kmdr por. Wiesław Goździewicz – Radca Prawny w NATO Joint Force Training Centre w Bydgoszczy

Tworząc rekomendacje Instytut Kościuszki starał się uwzględnić stanowiska jak największej liczby prelegentów.

Prosimy mieć na uwadze, iż nie wszystkie zapisy odzwierciedlają poglądy każdego z uczestników.

1. Dalsza ewolucja podejścia NATO do operacji w cyberprzestrzeni jest nieunikniona. Należy bacznie przyglądać się kierunkowi tej ewolucji i za nią nadążać;
2. Rozwijanie krajowej doktryny działań cybernetycznych powinno być zsynchronizowane z pracami nad sojuszniczą Doktryną Operacji Cybernetycznych AJP-3.20 dla zapewnienia maksymalnej możliwej zbieżności doktryny krajowej i sojuszniczej;
3. Polska ma szansę być krajem innowacyjnym również w zakresie działań cybernetycznych, a jak pokazał Szczyt NATO w Warszawie, potrafi być swego rodzaju „trendsetterem" w tym obszarze. Każda okazja w tym zakresie powinna być wykorzystywana;
4. Dążyć należy nie tyle do dotrzymywania kroku czołówce państw Sojuszu rozwijającej swoje zdolności do działania w cyberprzestrzeni, co raczej do znalezienia się w ścisłej czołówce. Dysponując dużym potencjałem intelektualnym i technologicznym Polska ma spore szanse ten cel osiągnąć;

5. Biorąc pod uwagę zapisy Cyber Defence Pledge i Art. 3 Traktatu Waszyngtońskiego, należy zintensyfikować prace nad budowaniem narodowego potencjału obronnego w cyberprzestrzeni;
6. Potencjał obronny musi uwzględniać posiadanie zdolności ofensywnych jako niezbędnego elementu skutecznego systemu obrony. Nie da się na dłuższą metę bronić wyłącznie pasywnie – niezbędne jest posiadanie środków umożliwiających osłabianie, redukcję bądź zniszczenie potencjału przeciwnika. Należy więc kontynuować, a być może również zintensyfikować prace nad rozwijaniem ofensywnych zdolności cybernetycznych, ponieważ:
    - Ofensywne zdolności cybernetyczne mogą w niektórych okolicznościach w większym stopniu niż środki konwencjonalne spełniać wymogi międzynarodowego prawa konfliktów zbrojnych;
    - Posiadanie ofensywnych zdolności cybernetycznych może stanowić skuteczny instrument odstraszania potencjalnych przeciwników;
    - NATO nie wyklucza już możliwości skorzystania z dobrowolnej kontrybucji państwa posiadającego takie zdolności w celu wsparcia operacji sojuszniczej;
    - Odpowiednio użyte środki cybernetyczne mogą wyeliminować bądź znacząco zredukować ryzyko dla własnych sił;
    - Środki cybernetyczne powszechnie używane są w tzw. działaniach hybrydowych i mogą być również skutecznym instrumentem odpowiedzi na zagrożenia hybrydowe.
7. Polityka „cyberodstraszania" powinna być wielotorowa i uwzględniać nie tylko racjonalne informowanie o rozwijanych bądź posiadanych zdolnościach, ale też np. maksymalne nagłośnianie sukcesów Polaków w ćwiczeniach typu Locked Shields czy Cyber Coalition oraz konkursach takich jak Hackathon;
8. Dla wzmocnienia cyberbezpieczeństwa niezbędna jest ścisła współpraca sektora militarnego z cywilnym i dotyczy to między innymi:
    - Prac badawczo-rozwojowych sponsorowanych bądź współfinansowanych przez wojsko;
    - Realizacji kluczowych programów zbrojeniowych przez krajowe podmioty sektora IT;
    - Stworzenia ram prawnych umożliwiających włączenie obywatelskich formacji cyberobrony do szerokiego systemu cyberbezpieczeństwa państwa, w szczególności na wypadek konfliktu zbrojnego, gdzie kluczowe będzie ustanowienie relacji dowodzenia i kontroli między siłami zbrojnymi i formacjami obywatelskimi dla uniknięcia samowoli, jaka stała się udziałem takich formacji obywatelskich na Ukrainie;
    - Stworzenia ram dla partnerskich relacji między wojskiem a przemysłem, umożliwiających między innymi tworzenie rozwiązań dla wojska bez konieczności transferu wszystkich praw własności intelektualnej i przemysłowej do opracowanych rozwiązań – jest to kluczowe jeżeli partner przemysłowy ma kontynuować rozwijanie danego rozwiązania;
    - Wymiany informacji o zagrożeniach i incydentach cybernetycznych z cywilnymi służbami

ochrony porządku publicznego, a także podmiotami sektora prywatnego, w szczególności operatorami systemów infrastruktury krytycznej;

9. Narodowe zdolności cybernetyczne należy budować w miarę możliwości w oparciu o krajowe rozwiązania technologiczne:
    - W celu wspierania krajowych podmiotów sektora IT, posiadających duży potencjał intelektualny i technologiczny, ale pod względem potencjału ekonomicznego niejednokrotnie niemających szans w konkurencji ze światowymi gigantami;
    - Dla zminimalizowania ryzyka, że zagraniczny producent pozostający pod kontrolą obcego rządu na jego zlecenie pozostawi w oprogramowaniu luki i furtki, jednocześnie odmawiając dostępu do kodów źródłowych;
    - W celu pozyskania rozwiązań unikatowych, nieopartych na komercyjnych lub rozpowszechnionych produktach (które zwiększają ryzyko penetracji przez osoby niepowołane), a jednocześnie uwzględniających specyficzne potrzeby zamawiającego.
10. Projektowana ustawa o cyberbezpieczeństwie ma potencjał stać się kluczowym dokumentem odpowiednio zakreślającym i rozgraniczającym role oraz kompetencje poszczególnych instytucji odpowiedzialnych za funkcjonowanie systemu bezpieczeństwa cybernetycznego państwa, a także tworzącym definicje legalne pojęć kluczowych z perspektywy cyberbezpieczeństwa, np. cyberprzestrzeni, suwerenności w cyberprzestrzeni, infrastruktury cybernetycznej itp. Powinna również regulować kwestie możliwości użycia wojskowych zdolności cybernetycznych do wsparcia działań służb ochrony porządku publicznego w przypadku wystąpienia najpoważniejszych kryzysów cyberbezpieczeństwa.

ŚCIEŻKA PRZYSZŁOŚĆ

KRAJOWE INNOWACJE DLA CYBERBEZPIECZEŃSTWA

dr Lior Tabansky – Pracownik naukowy w Blavatnik Interdisciplinary Cyber Research Center, Uniwersytet Telawiwski

POLSKI RYNEK CYBERBEZPIECZEŃSTWA - W POSZUKIWANIU INNOWACJI

UCZESTNICY:

dr Jacek Orzeł – Dyrektor Departamentu Bezpieczeństwa i Zarządzania Kryzysowego, pełnomocnik ds. Ochrony Informacji Niejawnych w Ministerstwie Rozwoju

Paweł Surówka – Prezes Zarządu PZU Życie S.A.

dr Karel Obluk – Partner w Evolution Equity

George Slawek – Współzałożyciel i Dyrektor Generalny Cyberus Labs

Grzegorz Wójcik – Założyciel i Dyrektor Generalny Autenti

Moderacja: Robert Siudak – Koordynator projektu CYBERSEC HUB, Ekspert Instytutu Kościuszki

Tworząc rekomendacje Instytut Kościuszki starał się uwzględnić stanowiska jak największej liczby prelegentów.

Prosimy mieć na uwadze, iż nie wszystkie zapisy odzwierciedlają poglądy każdego z uczestników.

1. Skutecznie ochronić przed „nieznanym” - dynamicznie ewoluującymi zagrożeniami płynącymi z cyberprzestrzeni mogą tylko nieszablonowe, innowacyjne rozwiązania. Dlatego konieczne jest wsparcie rozwoju startupów i producentów niekonwencjonalnych technologii;
2. Przykład Izraela pokazuje, że rola państwa w rozwoju krajowych produktów i usług z dziedziny

cyberbezpieczeństwa to stworzenie ram narodowego systemu innowacji, który musi być oparty na planie strategicznym:

- Strategia rozwoju narodowego systemu innowacji nie może być wyłącznie pustą polityczną deklaracją. Nie może tylko przedstawiać pożądanej wizji przyszłości, ale musi też uwzględniać zastane realia i wiążące się z nimi zagrożenia i trendy;
- Strategii nie można traktować jako jednorazowego produktu. Jej realizacja musi być stale monitorowana i na tej podstawie aktualizowana. W Izraelu istnieje specjalna agencja rządowa odpowiedzialna za adaptowanie strategii do nowych wyzwań.

3. Warunkiem koniecznym rozwoju innowacji jest zwiększenie wydatków publicznych na działalność badawczo-rozwojową. Izrael jest drugim państwem na świecie pod względem odsetka PKB wydawanego na tego typu działalność;
4. Inwestycje w innowacyjne rozwiązania nie tylko zwiększają poziom cyberbezpieczeństwa, ale co pokazuje przykład Izraela, mogą też być jednym z napędów rozwojowych gospodarki;
5. Innowacja to nie tylko technologia – konieczna jest również innowacyjność w dziedzinie polityk publicznych. Poleganie na zastanych metodach zarządzania stanowi blokadę w pobudzaniu i wykorzystywaniu innowacyjnego potencjału krajowej gospodarki;
6. Najbardziej obiecujące technologie w dziedzinie cyberbezpieczeństwa to te oparte na sztucznej inteligencji (wykorzystujące tzw. big data do wykrywania anomalii), matematyce stosowanej oraz technologii blockchain;
7. We wspieraniu krajowych startupów należy pamiętać, iż ich celem jest rozwój i eksport. Dlatego trzeba wyważyć dbałość o ich narodowy charakter (własność intelektualna, lokalizacja siedziby) z wymogami konkurencji na globalnym rynku;
8. Startupy powinny szukać inwestorów oferujących „mądre pieniądze" – umożliwiające rozwój i zdobywanie wiedzy;
9. Startup, aby pozyskać atrakcyjnego inwestora musi posiadać zaangażowany zespół, motywację do osiągnięcia sukcesu i cel polegający na wejściu na rynek globalny. Startupy z Polski (i UE) muszą bardziej skupić się na działalności eksportowej i rozwoju umiejętności biznesowych. Bez strategii eksportowej i umiejętności sprzedaży swojego rozwiązania, zaawansowane technologie z UE nie są w stanie konkurować na globalnym rynku;
10. Działalność na globalnym rynku wymaga dostosowywania swojej oferty i rozwiązania do różnorodnych klientów i specyfiki lokalnych rynków;
11. Obecnie, w przeciwieństwie do początków sektora ICT, na polskim rynku jest wielu partnerów chętnych do współpracy w ramach różnorodnych modeli biznesowych. Jedna rzecz pozostaje niezmienna – kluczem do sukcesu jest entuzjastyczny zespół, który potrafi się uczyć;
12. Problemem polskiego ekosystemu jest brak bezpośredniego połączenia między startupami a dużymi firmami, które są skłonne testować ich rozwiązania. W USA istnieją akceleratory (np.

Mach 37), które mają rozbudowane relacje z korporacjami otwartymi na innowacje i wdrożenia rozwiązań oferowanych przez startupy;

13. Dodatkowo duże firmy i administracja publiczna wymagają spełnienia różnorodnych wymogów formalnych (certyfikaty, doświadczenie, sukcesy sprzedażowe, wiarygodność finansowa), które stanowią istotną blokadę dla innowacyjnych startupów. Należy wypracować mechanizmy ułatwiające relacje biznesowe pomiędzy małymi, nowymi przedsiębiorstwami i dużymi organizacjami. Polska może stać się rynkiem testowym dla rodzimych innowacji o globalnym potencjale;
14. Fundusze venture capital lub corporate venture capital posiadające siatkę kontaktów wśród dużych firm, znające rynek, mogą stanowić pomost pomiędzy startupami i globalnymi graczami. Są one w stanie zagwarantować długoterminową niezbędną stabilność finansową startupu, dzięki czemu będzie on wiarygodnym partnerem biznesowym;
15. Polska podejmuje liczne działania na rzecz wsparcia innowacji w dziedzinie cyberbezpieczeństwa, które uczyniono jedną z krajowych inteligentnych specjalizacji. Innowacje stanowią jeden z pięciu filarów Strategii Odpowiedzialnego Rozwoju zakładającej realizacje 200 projektów o łącznej wartości 2 bln zł. Wśród nich 4 projekty dotyczą wyłącznie cyberbezpieczeństwa, m.in. Cyberpark Enigma. Również w projekcie Krajowych Ram Polityki Cyberbezpieczeństwa RP na lata 2017-2022 dostrzeżono strategiczny charakter rozbudowy zasobów technologicznych na potrzeby cyberbezpieczeństwa. W ramach Polskiego Funduszu Rozwoju utworzono 5 funduszy-funduszów PFR ventures. Nowa tzw. "mała ustawa o innowacyjności" zawiera ulgi podatkowe dla podmiotów podejmujących działalność badawczo-rozwojową. Rozwijany jest także Narodowy Instytut Technologiczny.

ŚCIEŻKA BIZNES

CYBERBEZPIECZEŃSTWO POLSKIEGO PRZEMYSŁU

UCZESTNICY:

dr Piotr Dardziński – Podsekretarz Stanu w Ministerstwie Nauki i Szkolnictwa Wyższego

dr inż. Piotr Pacyna – Pracownik naukowy w Katedrze Telekomunikacji Akademii Górniczo-Hutniczej im. S. Staszica w Krakowie

Izabela Lewandowska-Wiśniewska – Koodynator projektu „Cyber Industry", koordynator-starszy inżynier ryzyka w PZU Lab

Jarosław Sordyl – Kierownik Wydziału Cyberbezpieczeństwa w Departamencie Audytu i Bezpieczeństwa PSE S.A.

Tomasz Chodor – Z-ca Dyrektora Departamentu Bezpieczeństwa Grupy Kapitałowej PGNiG

Szymon Kowalczyk – Dyrektor Wykonawczy ds. IT w TAURON Polska Energia

Moderacja: dr Andrzej Kozłowski – Ekspert Fundacji im. Kazimierza Pułaskiego, redaktor prowadzący portal Cyberdefence24.pl

Tworząc rekomendacje Instytut Kościuszki starał się uwzględnić stanowiska jak największej liczby prelegentów.

Prosimy mieć na uwadze, iż nie wszystkie zapisy odzwierciedlają poglądy każdego z uczestników.

1. Przedstawiciele przemysłu funkcjonujący w różnych sektorach wspólnie podkreślają, że administracja publiczna powinna jak najszybciej przygotować regulacje i wymagania związane z cyberbezpieczeństwem. Pozwoli to na realizowanie działań zgodnych z ogólną wizją i celami, a także przyczyni się do ograniczenia niepewności, którą odczuwają poszczególne podmioty. Przedstawiciele sektorów powinni być czynnie zaangażowani w opracowanie wymagań i rozwiązań legislacyjnych związanych z cyberbezpieczeństwem. Autentyczny i konstruktywny dialog to warunek osiągnięcia sukcesu;
2. Rozliczanie w zakresie wypełniania wymagań nie powinno sprowadzać się wyłącznie do weryfikacji dokumentacji, gdyż może to sfałszować obraz cyberbezpieczeństwa;

3. Rozporządzenie o Ochronie Danych Osobowych przyniesie wiele zmian w sposobie myślenia o cyberbezpieczeństwie. Groźba dotkliwych sankcji nie powinna jednak sprawić, że operatorzy infrastruktury krytycznej położą nacisk wyłącznie na działania związane z bezpieczeństwem systemów IT. Z ich punktu widzenia, krytycznym elementem bezpieczeństwa są systemy OT;
4. Wyzwaniem dla zapewniania cyberbezpieczeństwa, szczególnie w kontekście zapewniania ciągłości dostępności usług, jest zrozumienie nie tylko funkcjonowania własnych systemów, ale także poznania systemów, od których dany podmiot jest uzależniony. Wiedza ta powinna mieć głębszy wymiar, a nie sprowadzać się wyłącznie do zdiagnozowania punktów styku.
5. Przedstawiciele przemysłu podkreślają potrzebę kontynuacji prac sektorowych oraz tworzenia szkoleń w zakresie cyberbezpieczeństwa;
6. Wskazuje się na konieczność tworzenia polskich rozwiązań w zakresie cyberbezpieczeństwa, skoncentrowanych szczególnie na systemach OT. Należy poszukiwać nisz i trendów tam, gdzie innowacyjne rozwiązania znajdą odbiorców. W sposób szczególny zaakcentowano problematykę Internetu Rzeczy;
7. Wdrażanie rozwiązań związanych z Internetem Rzeczy musi być poprzedzone analizą ryzyka i przeprowadzaniem testów. Istnieją obszary krytyczne, gdzie zastosowanie Internetu Rzeczy powinno być ograniczone;
8. Pożądanym jest tworzenie sektorowych Zespołów Reagowania na Incydenty Komputerowe na wzór CERT-u aktualnie tworzonego w sektorze elektroenergetyki. Będzie on pełnił funkcje koordynacyjno-usługowe i przyczyni się do bardziej proaktywnego, synergicznego i skutecznego zapewniania cyberbezpieczeństwa;
9. W kontekście niedoboru kadr zajmujących się cyberbezpieczeństwem, pojawiający się problem to zapotrzebowanie na dydaktyków kształcących przyszłych specjalistów. Ta kwestia powinna być rozwiązana na poziomie systemowym;
10. Proponuje się stworzenie wyspecjalizowanych konsorcjów, które oferowałyby permanentne, modułowe kształcenie, odpowiadające w sposób elastyczny na dynamicznie zmieniające się potrzeby rynku. Konsorcja tworzyłyby zarówno firmy jak i uczelnie;
11. Zaawansowane prace badawcze muszą być współfinansowane z nakładów publicznych.

CYBERSEC PL 2017

W LICZBACH

1 kluczowe wyzwanie dla Polski

4 ścieżki tematyczne

2 wydarzenia specjalne

5 paneli dyskusyjnych

4 prezentacje

9 godzin tłumaczenia symultanicznego

12 godzin możliwości networkingowych

12 wywiadów dla CYBERSEC TV

15 startupów

33 prelegentów

50 osób z zespołu CYBERSEC PL

56 akredytowanych dziennikarzy

>180 publikacji na temat wydarzenia

>500 uczestników

1294 zdjęć

1282 filiżanek kawy

60 K impresji na Twitterze

SAVE THE DATE

III Europejskie Forum Cyberbezpieczeństwa
- CYBERSEC 2017

9-10 PAŹDZIERNIKA 2017
KRAKÓW, POLSKA

WWW.CYBERSECFORUM.EU @CYBERSECEU /CYBERSECEU

PARTNERZY

asseco

COIG

COMARCH

GALACH CONSULTING

GPW

T

PARTNERZY WSPIERAJĄCY

EVERCOM

IGT iGRID TECHNOLOGY

Spica Solutions

PATRONI INSTYTUCJONALNI

FUNDACJA IM. KAZIMIERZA PUŁASKIEGO

KRAKOWSKI PARK TECHNOLOGICZNY

NASK

PKN POLSKI KOMITET NORMALIZACYJNY

POLSKA PLATFORMA BEZPIECZEŃSTWA WEWNĘTRZNEGO

STARTUP HUB POLAND

PATRONI MEDIALNI

POLSKIE RADIO

pap POLSKA AGENCJA PRASOWA

TVP INFO

RZECZPOSPOLITA

300POLITYKA

DO RZECZY

BIZNES ALERT

wysokieNapiecie.pl

TELIX.PL PORTAL TELEKOMUNIKACYJNY

ZAUFANA TRZECIA STRONA.PL

di24.pl

CyberDefence24

PATRONI HONOROWI

Ministerstwo Cyfryzacji

Minister Spraw Wewnętrznych i Administracji

Rzeczpospolita Polska Minister Spraw Zagranicznych

Ministerstwo Rozwoju

Ministerstwo Nauki i Szkolnictwa Wyższego

Ministerstwo Obrony Narodowej

Wojska Polskie

Ministerstwo Finansów

Ministerstwo Infrastruktury i Budownictwa

Biuro Bezpieczeństwa Narodowego

Prokuratura Krajowa

RCB Rządowe Centrum Bezpieczeństwa

PARTNER STRATEGICZNY

PZU

PARTNERZY GŁÓWNI

EXATEL

PGNiG

PGZ

TAURON

ORGANIZATOR

Instytut Kościuszki

PARTNER PROGRAMOWY

Fundacja bezpieczna cyberprzestrzeń

POWERED BY

EVEREST360