DZIEŃ 1

WTOREK, 06 GRUDZIEŃ, 2022

Punkt Programu	Godz.	Prelegent	Opis
REJESTRACJA	8:30 9:00		
OTWARCIE KONFERENCJI	9:00 9:15		
PODPISANIE DEKLARACJI PRZYSTĄPIENIA MIASTA OPOLA DO SINOTAIC - POLSKIEGO KLASTRA IOT & AI	09:15 09:25		Podpisanie deklaracji przystąpienia Miasta Opola do SINOTAIC – polskiego klastra IoT & AI
REFERAT OTWIERAJĄCY - WYZWANIA BEZPIECZEŃSTWA IT	9:30 10:10	Adam Czubak	Aktualne wyzwania dla domen bezpieczeństwa IT i rola projektu CyberEva w ich adresowaniu
PORÓWNANIE TECHNIK BADANIA BEZPIECZEŃSTWA W OPARCIU O RED, BLUE I PURPLE TEAMING	10:15 11:00	Tomasz Turba	Podczas prezentacji zostaną omówione aktualne trendy i problemy związane z tematyką cyberbezpieczeństwa przedsiębiorstw. Przedstawiony zostanie sposób realizacji zaawansowanego testu penetracyjnego w oparciu o walkę dwóch drużyn – atakujących hakerów i broniących się administratorów oraz dlaczego ww. podejście do zabezpieczania przedsiębiorstw powinno zostać zrewidowane i udoskonalone.
PRZERWA KAWOWA	11:00 11:10		
BEZPIECZEŃSTWO TELEINFORMATYCZNE, TO ZADANIE DLA NAS WSZYSTKICH	11:10 11:35	Marcin Szyłko oraz Krzysztof Trawiński	O poziomie bezpieczeństwa każdego systemu informatycznego decyduje jego najsłabsze ogniwo. Każdy z Nas może stanąć na drodze cyberprzestępcy. Zostaniesz bohaterem czy ofiarą? Podnieś poziom swojej świadomości zagrożeń czyhających w sieciach teleinformatycznych. Poznaj Program Budowy Systemu Cyberbezpieczeństwa w ZUS od strony użytkownika.
SINOTAIC "SMART CITY"	11:40 12:25	Agnieszka Łasut/Marek Ostafil	Realna współpraca pomiędzy samorządem, biznesem a nauką – czy to możliwe? Showroom Innowacji IoT i jego rola w lokalnym ekosystemie
PRZERWA OBIADOWA	12:25 13:00		
OCHRONA ORGANIZACJI W ZAKRESIE: SIECI, SYSTEMÓW I DANYCH.	13:00 13:40	Łukasz Skibniewski	Podczas wykładu omówione będą niektóre technologie i procedury wykorzystywane przez specjalistów ds. cyberbezpieczeństwa w zakresie ochrony sieci, sprzętu i danych organizacji. Na początku krótko przedstawione są różne rodzaje zapór sieciowych, urządzenia bezpieczeństwa i aktualnie używane oprogramowanie antywirusowe, a także omówione są najlepsze praktyki postępowania w zakresie zabezpieczania systemu teleinformatycznego. Następnie wyjaśnione będzie czym są botnety, model Kill Chain oraz zabezpieczenia oparte na analizie zachowań. Omówiony będzie także protokół NetFlow służący do monitorowania sieci. Trzecia część wykładu porusza sposób działania firmy Cisco wobec cyberbezpieczeństwa, tworzenie zespołu ekspertów do spraw

			bezpieczeństwa komputerowego (ang. CSIRT) oraz krótki przewodnik bezpieczeństwa. W treści wykładu wymienione będą także narzędzia wykorzystywane przez specjalistów ds. cyberbezpieczeństwa do wykrywania i zapobiegania atakom sieciowym.
PROGRAM RAMOWY HORIZON EUROPE I MECHANIZM EIC ACCELERATOR	13:45 14:00	Ewa Mendec i Katarzyna Markiewicz-Śliwa	Wprowadzenie do programu ramowego Horizon Europe ze szczególnym uwzględnieniem Klastra 3 (“Civil security for society” – innovation projects on crisis management, fight against crime and terrorism, external and border security, cybersecurity, privacy and trust) Mechanizm EIC Accelerator – wsparcie dla małych i średnich przedsiębiorstw (wysoki potencjał do wzrostu, przełomowe rozwiązania np. technologia, produkt, usługa, znajdujące się w fazie bezpośrednio poprzedzającej skalowanie i wdrożenie na rynek europejski i globalny.)
ZAKOŃCZENIE DNIA PIERWSZEGO	14:00		Zakończenie spotkania.

DZIEŃ 2

ŚRODA, 07 GRUDZIEŃ, 2022

Punkt Programu	**Godz.**	**Prelegent**	**Opis**
REJESTRACJA	8:30 - 9:00		
PROFILING IOT	9:00 - 9:25	Adam Czubak	Wyzwania identyfikacji urządzeń w bezpośrednim otoczeniu i ich poziomu bezpieczeństwa przy niepełnych danych
WYKRYWANIE MOBILNEGO BOTNETU	9:30 - 9:55	Jarosław Kobiela i Piotr Urbaniec	W naszej prezentacji opowiemy o początkowych pracach związanych z udziałem w projekcie CyberEva, które dotyczyły wykrywania mobilnych botnetów. W literaturze przedmiotu problem ten nie jest nowy, ale szybko rozwijająca się technologia wywiera nacisk na ciągłą rewizję istniejących i szukanie nowych metod działania. Naszym celem było sprawdzenie, jak funkcjonuje mobilny botnet w rzeczywistych warunkach. Wykorzystaliśmy do tego dostępne zasoby sprzętowe i serwer Command & Control, udostępniony przez społeczność na serwisie Github. Pozwoliło to nam na zasymulowanie pracy botnetu w realnych warunkach w obrębie sieci LAN, w której funkcjonowały także inne niezainfekowane urządzenia. Podczas pracy botnetu zebraliśmy dane dotyczące ruchu sieciowego w całej sieci, a także informacje z poszczególnych urządzeń dotyczące wszystkich zdarzeń, jakie były na nich wykonywane. Następnie pliki i dane poddaliśmy analizie, próbując zlokalizować wzorce oraz zależności, które pozwoliłby na identyfikację urządzeń, które są częścią botnetu. Wyniki tych analiz nie pozwalają na jednoznaczne wskazanie potencjalnego zagrożenia, a jednocześnie zmuszają do postawienia nowych pytań, na które to pytania odpowiedzi będziemy poszukiwać w dalszych badaniach. Rozwiązanie tego problemu jest o tyle istotne, że botnety mogą posłużyć do wielu niepożądanych działań, takich jak: kradzieże z kont

			bankowych, ataki cybernetyczne, czy dostęp do poufnych informacji.
OCHRONA URZĄDZEŃ IT	10:00 - 10:45	Tadeusz Więckowski	Wpływ na urządzenia z branży IT, jak chronić je przed impulsami elektromagnetycznymi i zabezpieczyć przed ulotem sygnałów, które niosą te informacje.
PRZERWA KAWOWA	10:45 - 11:00		
AI I CYBERBEZPIECZEŃSTWO – WYZWANIA BADAWCZE NA POLITECHNICE ŚLĄSKIEJ	11:00 - 11:40	Adrian Kapczyński	W ramach wykładu przedstawiony zostanie potencjał Politechniki Śląskiej związany z cyberbezpieczeństwem, ze szczególnym uwzględnieniem podejmowanych wyzwań badawczych.
ZASTOSOWANIA PROSTEJ STATYSTYKI OPISOWEJ ORAZ PEWNEGO PROCESU STOCHASTYCZNEGO DO OKREŚLANIA PRZYSZŁEJ WARTOŚCI LICZBOWEJ CHARAKTERYSTYKI OPISUJĄCEJ WYBRANY ASPEKT BEZPIECZEŃSTWA SIECI.	11:45 - 13:30	Tomasz Michael	Referat przedstawia możliwości zastosowania metod statystycznych w prognozowaniu przyszłej wartości charakterystyk liczbowych opisujących stan bezpieczeństwa (niebezpieczeństwa) sieci. Przedstawione zostaną dwa podejścia. Pierwsze z nich, bardzo elementarne, bazuje na podstawowych statystykach opisowych; drugie, dużo bardziej zaawansowane, zakłada wykorzystanie pewnego autorskiego algorytmu wykorzystującego ideę procesu stochastycznego.
LUNCH + NETWORKING	13:30 - 14:00		
ZWALCZANIE CYBERPRZESTĘPCZOŚCI I CYBERBEZPIECZEŃSTWO – DWA OBSZARY DZIAŁAŃ.	14:00 - 14:45	Michał Podpora	Rosnąca popularność cyberbezpieczeństwa jako obszaru kompetencji lub oferty edukacyjnej powoduje że istnieje tendencja nadmiarowego rozszerzania danego obszaru działań, często ze szkodą dla obszarów pokrewnych. W świetle dzisiejszej popularności cyberbezpieczeństwa warto zauważyć i zaznaczyć, że jest ono zagadnieniem rozdzielnym względem wielu pokrewnych obszarów. Ponieważ każdy obszar działań w czasie swojego życia podlega kształtowaniu i ewolucji, warto prowadzić dyskusję pomagającą wyjaśniać i precyzować. Wieloletnie doświadczenie prelegenta w projektowaniu i realizowaniu oferty edukacyjnej na potrzeby służb zainteresowanych Informatyką Śledczą stanowi istotny i ciekawy głos pozwalający lepiej nazwać i lepiej przygotowywać ofertę edukacyjną z zakresu również Cyberbezpieczeństwa.
ZAKOŃCZENIE KONFERENCJI	14:45		