AKADEMIA ROZWOJU PRZEMYSŁU 4.0

Cyberbezpieczeństwo w samorządzie terytorialnym

w ramach Akademii Rozwoju Przemysłu 4.0

29 marca 2023 roku, g. 10:00 – 12:00
Webinar na platformie ZOOM

Udział w webinarze jest BEZPŁATNY.
Wystarczy się zarejestrować, aby otrzymać dostęp do udziału w wydarzeniu.

Rejestracja na spotkanie: https://forms.gle/CUcrqCYk3eqH82yq6
Dodaj wydarzenie do kalendarza Google
Dodaj wydarzenie do kalendarza Outlook ICal

Na dzień przed wydarzeniem osoby zarejestrowane otrzymają link do spotkania.
Serdecznie zapraszamy!

Cyberbezpieczeństwo to proces, którego celem jest ochrona danych i systemów wewnętrznych przed zagrożeniami, jakie niosą za sobą ataki w przestrzeni cyfrowej. Wdrożenie odpowiednich procedur w tym zakresie pozwala zapobiec skutkom działań, które mogą wyrządzić organizacji wiele szkód. Celem seminarium jest podniesienie świadomości kadr JST o cyberbezpieczeństwie, obowiązkach wynikających z prawa oraz dostarczenie wiedzy o narzędziach, standardach i projektach w celu zapewniania cyberbezpieczeństwa w organizacji.

Dla kogo:

- **Starostowie**
- **Prezydenci Miast**
- **Burmistrzowie**
- **Wójtowie**
- **Osoby zarządzające w JST,**
- **Służby informatyczne JST**

Podczas webinaru zostaną poruszone zagadnienia takie jak:

- **Obowiązki JST w zakresie cyberbezpieczeństwa – Krajowy system cyberbezpieczeństwa;**
- **Projekty oraz programy dla JST – rozwój kompetencji cyfrowych;**
- **Cyberbezpieczeństwo w praktyce (Podstawy poruszania się w cyberprzestrzeni; Bezpieczeństwo w sieci; Zaawansowane zabezpieczenie systemów/organizacji).**

Prosimy o potwierdzenie obecności do dnia 28 marca 2023 r. Rejestracja zostanie zamknięta o 12:00.

Szczegółowy program oraz informacje na temat Prelegentów znajdziecie pod linkiem
https://pracodawcy.pl/cyberbezpieczenstwo-w-samorzadzie-terytorialnym/

Akademia Rozwoju Przemysłu 4.0
ul. F. Chopina 2, 59-300 Lubin
Tel. 76/8478585; e-mail: sekretariat@pracodawcy.pl

Masz pytanie? Napisz do nas: szkop@pracodawcy.pl

ORGANIZATOR

ZWIĄZEK PRACODAWCÓW POLSKA MIEDŹ
THE POLISH COPPER EMPLOYERS' ASSOCIATION

PARTNER MERYTORYCZNY

CENTRUM CYBERBEZPIECZEŃSTWA

PRELEGENCI

Jan Kostrzewa, Dyrektor Centrum Cyberbezpieczeństwa

Współtwórca pierwszego polskiego satelity PW-Sat. W latach 2018 – 2021 Dyrektor Biura Cyberbezpieczeństwa w Ministerstwie Sprawiedliwości. Pomysłodawca konkursu Capture the flag „153+1" skierowanego do młodych pasjonatów cyberbezpieczeństwa. Autor wielu publikacji naukowych m. in. *Influence of the Sampling Frequency in Duffing Time Series on Prediction's Error*.

Rafał Szkop, Manager ds. Analiz, Legislacji i Współpracy Międzynarodowej, Związek Pracodawców Polska Miedź

Absolwent Wydziału Prawa Uniwersytetu Łódzkiego oraz Uniwersytetu im. Adama Mickiewicza w Poznaniu. Certyfikowany manager projektów wg metodologii TenStep.

Uczestnik wielu projektów międzynarodowych z dziedziny prawa pracy, stosunków przemysłowych, ekonomii. Współautor kilku artykułów w publikacjach krajowych i zagranicznych.

W latach 2017-2021 Prezydent Europejskiej Platformy Technologicznej Zrównoważonych Surowców Mineralnych. Manager Projektu „Akademia Rozwoju Przemysłu 4.0" prowadzonego przez Związek Pracodawców Polska Miedź. Entuzjasta innowacji i nowych technologii „z ludzką twarzą".

Michał Rzeźnikiewicz, Naczelnik Wydziału Funkcjonowania Krajowego Systemu Cyberbezpieczeństwa, Departament Cyberbezpieczeństwa, Cyfryzacja KPRM, Kancelaria Prezesa Rady Ministrów

Łukasz Białek, Naczelnik Wydziału Departamentu Strategii Centrum Projektów Polska Cyfrowa

ORGANIZATOR – LIDER PROJEKTU

Związek Pracodawców Polska Miedź

Samorządna organizacja pracodawców, która powstała w 1996 roku z inicjatywy KGHM Polska Miedź S.A. Związek początkowo miał charakter stowarzyszenia branżowego, a obecnie zrzesza 119 firm z różnych sektorów gospodarki, zatrudniających ponad 38 000 pracowników. Zadaniem Związku jest ochrona i reprezentowanie interesów pracodawców.

Nasza struktura pozwala na współpracę firm w duchu społecznej odpowiedzialności biznesu, przy poszanowaniu różnorodności interesów bez względu na wielkość, strukturę czy formę prawną. Naszym zadaniem jest ochrona praw i reprezentowanie interesów zrzeszonych pracodawców. Jednym z elementów poprawiających konkurencyjność jest stałe podnoszenie kompetencji. ZPPM organizuje konferencje, seminaria i szkolenia, z których skorzystało ponad pięć tysięcy osób. Pomagamy uzyskiwać wiedzę, pozwalającą na budowanie przewagi rynkowej. Mamy ogromny potencjał intelektualny, ze względu na wsparcie naszego założyciela - Grupy Kapitałowej KGHM i innych firm członkowskich, posiadających unikalne kompetencje. Oprócz organizacji różnego rodzaju form rozwoju skutecznie upowszechniamy także dobre praktyki zarządzania.

www.pracodawcy.pl; M: sekretariat@pracodawcy.pl

PARTNER MERYTORYCZNY

CENTRUM CYBERBEZPIECZEŃSTWA

O Nas

Centrum Cyberbezpieczeństwa to instytucja powstała w 2020 roku, świadcząca szeroki zakres usług w dziedzinie bezpieczeństwa informatycznego. Pracownicy CC to doświadczeni specjaliści w branży, których głównym zadaniem jest dbanie o bezpieczeństwo cybernetyczne klientów oraz zwiększanie ich świadomości w tym zakresie. Zespół posiada certyfikaty takie jak: Offensive Security Certified Expert (OSCE), Offensive Security Certified Professional (OSCP), Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker oraz CompTIA Security+.

W ostatnim kwartale 2022 roku przetestowaliśmy nasz **autorski produkt SecureBox**, *który ma za zadanie chronić Instytucje i Firmy przed zagrożeniami przenoszonymi na zewnętrznych nośnikach o niewiadomej zawartości i pochodzeniu.*

Ważne sukcesy 2022 roku

• Skutecznie chroniliśmy resort sprawiedliwości przed atakami hakerskimi, które nasiliły się po wybuchu wojny na Ukrainie.

• Wykonaliśmy wiele testów penetracyjnych, między innymi ogólnopolskiego systemu zdalnych rozpraw sądowych.

• Przeszkoliliśmy ponad 5000 osób w ponad 100 szkoleniach na temat podstaw cyberbezpieczeństwa, osiągając poziom zadowolenia uczestników na poziomie średnim 94%.

• Dopracowaliśmy i przetestowaliśmy nasz autorski produkt SecureBox, który ma za zadanie chronić instytucje i firmy przed zagrożeniami przenoszonymi na zewnętrznych nośnikach o niewiadomej zawartości i pochodzeniu.

• Rozpoczęliśmy utrzymywanie i rozwijanie projektu „Nieodpłatna pomoc prawna" dla Ministerstwa Sprawiedliwości.

• Pod koniec 2022 roku rozpoczęliśmy wdrażanie systemu ochrony urządzeń mobilnych.

Zajmujemy się:

- Usługami informatycznymi związanymi z pisaniem aplikacji obejmujące projektowanie, programowanie i wdrażanie aplikacji komputerowych dla różnych systemów operacyjnych i urządzeń mobilnych.

- Produkcją i wdrożeniem usługi SecureBox, która wspomaga ochronę Organizacji Klienta przed zagrożeniami przenoszonymi na nośnikach danych USB oraz płytach CD/DVD.

- Szkoleniami z podstaw cyberbezpieczeństwa, gdzie poruszamy szeroko pojętą tematykę cyberbezpieczeństwa w prosty i zrozumiały sposób. Od bezpieczeństwa plików i haseł po inżynierię społeczną, przedstawiając popularne zagrożenia oraz najskuteczniejsze sposoby obrony przed nimi.

- Analizą cyberprzestrzeni nieruchomości należącej do Organizacji, która ma na celu wykrycie niewystarczająco zabezpieczonych punktów dostępu o dużym znaczeniu.

- Ochroną bezpieczeństwa cybernetycznego urządzeń mobilnych.

- Monitoringiem i SOC świadczonymi w trybie 24/7 polegającym na zbieraniu i analizowaniu incydentów w infrastrukturze sieciowej Klienta, właściwej ich interpretacji oraz podjęciu stosownych działań, za pomocą zaawansowanych narzędzi.

- Testami penetracyjnymi, które sprawdzają kompleksowo wskazany system, infrastrukturę teleinformatyczną lub wybrane jej segmenty. Dzięki temu Organizacja może poznać słabe punkty wybranych elementów infrastruktury oraz uzyskać rekomendacje w zakresie ich naprawy.

- RED Teamingiem, czyli symulacją ataku cybernetycznego w oparciu o techniki wykorzystywane przez rzeczywistych atakujących. Jej efektem jest wskazanie podatności oraz sformułowanie zaleceń, dzięki którym Organizacja może w szybki sposób podnieść poziom bezpieczeństwa i uniemożliwić osiągnięcie celów przestępcom.

- Organizowaniem Konkursu 153+1, w którym młodzi pasjonaci cyberbezpieczeństwa z całej Polski mogą sprawdzić swoje umiejętności rywalizując między sobą w formule Capture The Flag.

OFERTA

KONKURS CTF 153+1

Polscy etyczni hakerzy należą do najlepszych na świecie. Chcemy, aby młodzi ludzie, idąc za ich przykładem, rozwijali zainteresowania kwestiami cyberbezpieczeństwa i wykorzystywali swoje umiejętności zgodnie z prawem.

Specjalnie z myślą o młodych pasjonatach stworzyliśmy ogólnopolski konkurs w popularnej formule Capture The Flag „153+1”. Przedsięwzięcie jest skierowane do uczniów szkół ponadpodstawowych i dorosłych. Konkurs został objęty patronatem Ministerstwa Sprawiedliwości oraz Ministra Edukacji i Nauki. Każdego roku zapisy do konkursu rozpoczynają się na jesieni. Na zwycięzców czekają atrakcyjne nagrody pieniężne.

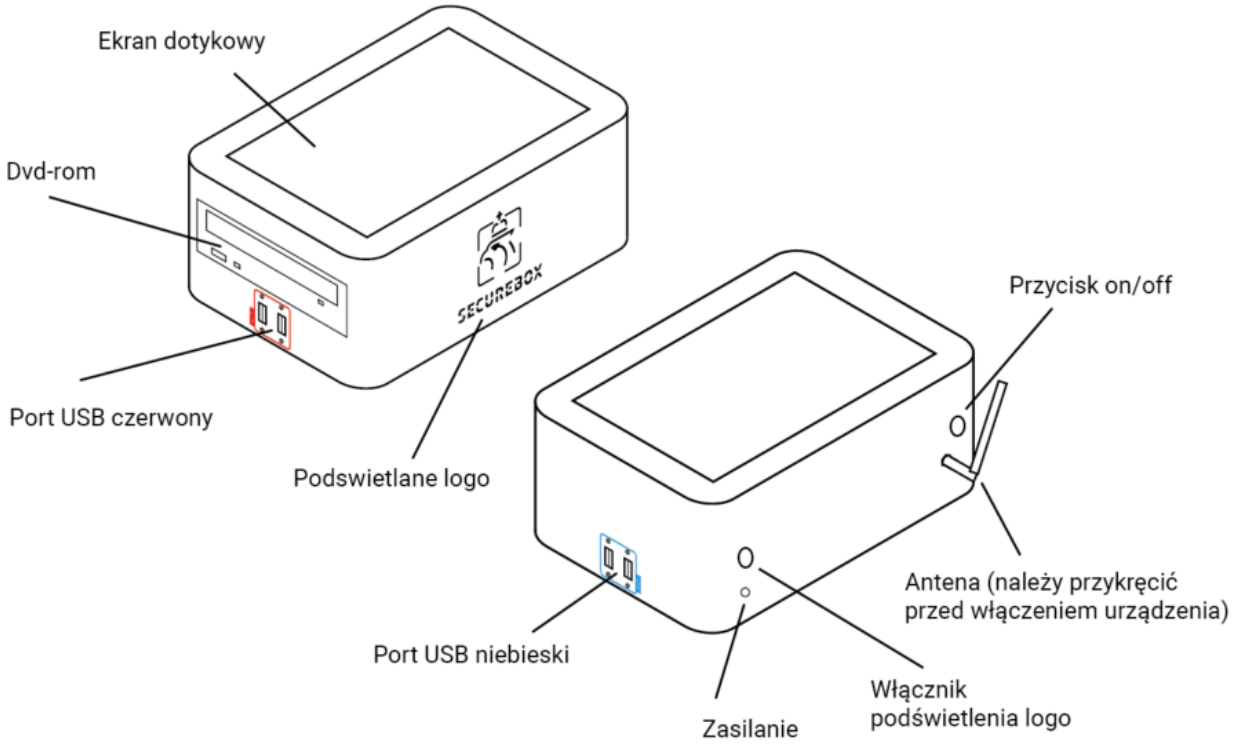
SZKOLENIA

Prowadzimy szkolenia Security Awareness, mające na celu przybliżenie podstaw cyberbezpieczeństwa pracownikom Organizacji Klienta. Od bezpieczeństwa plików i haseł po inżynierię społeczną – przedstawimy popularne zagrożenia oraz najważniejsze zasady obrony przed nimi. Czynnik ludzki jest częstą przyczyną udanych ataków hakerskich, dlatego przeprowadzane przez nas szkolenia skupiają się na podniesieniu świadomości pracowników oraz przekazaniu im prostych wskazówek, które mogą znacząco poprawić bezpieczeństwo teleinformatyczne Organizacji.

SECUREBOX

Autorski produkt Centrum Cyberbezpieczeństwa, który wspiera ochronę Organizacji przed zagrożeniami przenoszonymi na nośnikach danych.

Wychodząc naprzeciw potrzebom Klientów, zmierzyliśmy się z wyzwaniami zaprojektowania urządzenia oraz aplikacji analizujących dane na potencjalnie niebezpiecznych nośnikach zewnętrznych. Przeskanowane i niezainfekowane pliki są kopiowane na nośnik oznaczony jako „bezpieczny”.



Projekt został już wdrożony w aplikacji lubelskiej.

Ekran dotykowy i przejrzysty interfejs zapewniają prostotę obsługi, a wykorzystanie sprawdzonych technologii wykrywania zagrożeń - bezpieczeństwo Organizacji.

VIP MONITORING - Ochrona urządzeń mobilnych

Chronimy przed oprogramowaniem szpiegującym typu Pegasus. Usługa ochrony jest dostarczona wraz z nowoczesnym telefonem (iPhone 14; Samsung Galaxy s23).

Oferujemy system cyfrowej ochrony urządzeń mobilnych złożony z centralnego serwera oraz aplikacji klienckich zainstalowanych na urządzeniach komórkowych, pozwalający na monitorowanie procesów w systemach operacyjnych z rodzin

Android i iOS, filtrowanie ruchu sieciowego oraz przesyłanie alertów o zagrożeniach do zdalnego operatora.

Dzięki zespołowi operatorów pracujących przez całą dobę, jesteśmy w stanie odpowiadać na pojawiające się zagrożenia w czasie rzeczywistym oraz elastycznie dopasowywać filtrowanie treści do potrzeb Klienta. System zapewnia przy tym całkowitą anonimowość użytkownikowi.

SOC - Security Operations Center dostępna w trybie 24/7/365

SOC to wyspecjalizowany zespół, którego głównym celem jest świadczyć najwyższej jakości usługi w obszarach monitoringu sieci, zarządzania platformami bezpieczeństwa i zarządzania incydentami. Nasi pracownicy dbają o nieustanny rozwój i utrzymywanie odpowiedniego poziomu umiejętności. Zatrudniamy kilkanaście osób z certyfikatami. Pracujemy w systemie zmianowym na pierwszej linii obrony przed atakami cybernetycznymi.

Analityk bezpieczeństwa to przede wszystkim osoba, która potrafi interpretować i reagować na zdarzenia, które obserwuje. Ma również za zadanie podejmować decyzje, które mają ogromny wpływ na bezpieczeństwo monitorowanej infrastruktury, takich jak: właściwa interpretacja zdarzeń, analiza szkodliwego oprogramowania, załączników i treści e-maili.

Dzięki monitoringowi IT zapewniamy ciągłość działania usług w resorcie i inicjujemy niemal natychmiastową reakcję na zagrożenia, co ma kluczowe znaczenie w przypadku ataków cybernetycznych

Trzy filary wsparcia:

1. Wyspecjalizowany zespół w obsłudze klienta, monitoringu stanu bezpieczeństwa ICT, selekcji i priorytetyzacji incydentów.

2. Komórka odpowiedzialna za obszar zarządzania platformami bezpieczeństwa oraz zarządzanie incydentami.

3. Grupa ekspertów od zaawansowanych technik ataku i najbardziej skomplikowanych zagrożeń, w tym administratorzy platform bezpieczeństwa.

Nieodłączną częścią SOC jest również **monitorowanie i obsługa incydentów** – to podstawowa usługa SOC Centrum Cyberbezpieczeństwa. Składa się z trzech elementów:

1. **monitorowanie** zdarzeń w sieci klienta – czyli zbierania, analizowania oraz korelacji zdarzeń, które zachodzą w sieciach oraz systemach klienta. Zebrane dane najpierw są automatycznie analizowane przez systemy analityczne. Następnie są badane przez naszych ekspertów do spraw bezpieczeństwa,
2. **wykrywanie** zdarzeń lub incydentów bezpieczeństwa,
3. **ocena** wpływu zdarzenia lub incydentu bezpieczeństwa IT na system klienta – jeśli nasz system wykryje zdarzenie lub incydent bezpieczeństwa, ekspert w dziedzinie bezpieczeństwa ICT wstępnie je analizuje. Sprawdza, czy nie jest to fałszywy alarm. Po analizie podejmuje działania zgodne z procedurami.

REKONESANS CYBERPRZESTRZENI

Dodatkowa usługa rekonesansu nieruchomości pod kątem urządzeń infrastruktury internetowej, które są coraz częstszym wektorem ataku.

Połączenie wiedzy naszych dwóch zespołów: Blue Team oraz Red Team oferuje specjalistyczną usługę rekonesansu cyberprzestrzeni nieruchomości należącej do Organizacji, która ma na celu wykrycie niewystarczająco zabezpieczonych punktów dostępu o dużym znaczeniu.

Usługa powstała jako odpowiedź na coraz częstsze zagospodarowanie sieci bezprzewodowej przy użyciu urządzeń IoT (Internet of Things), które są coraz częstszym wektorem ataku.

W naszym zakresie jest analiza faktycznego stanu cyberbezpieczeństwa przestrzeni z poziomu Internetu jak i przestrzeni fizycznej, która należy do danej Organizacji.

Dzięki naszej usłudze dowiesz się o istniejących urządzeniach widocznych z poziomu Internetu, należących do Twojej Organizacji. Poznasz również słabe punkty takie jak nieprawidłowo zabezpieczone sieci bezprzewodowe, błędnie skonfigurowane urządzenia kontroli dostępu oraz wiele innych, które mogą stać się celem przestępców.

USŁUGI OFENSYWNE

1. **TESTY PENETRACYJNE – siła cyberodporności**

   Nasz zespół specjalistów oferuję usługi z zakresu testów penetracyjnych aplikacji webowych oraz infrastruktury, zgodnie z przyjętymi standardami testowania takimi jak OWASP oraz OSSTMM oraz własnymi wypracowanymi metodologiami. Testy penetracyjne sprawdzają kompleksowo wskazany system, infrastrukturę teleinformatyczną lub wybrane jej segmenty. Dzięki temu Organizacja może poznać słabe punkty wybranych elementów infrastruktury oraz uzyskać rekomendacje w zakresie ich naprawy.

Centrum Cyberbezpieczeństwa to przede wszystkim specjaliści z doświadczeniem, którzy wiedzą, że dzięki pentestom przedsiębiorstwa mogą lepiej zarządzać cyberbezpieczeństwem, planować strategię dotyczącą zarządzania cyklem życia oprogramowania, oraz przede wszystkim uniknąć ataków hakerskich.

Rodzaje testów:

- Black – box (brak wiedzy o testowanych systemach),
- Grey – box (częściowa wiedza o testowanych systemach informatycznych),
- White – box (audyt kodu źródłowego),
- Wewnętrzne i zewnętrzne,
- Zdalne i w siedzibie Klienta, Informując administratorów lub bez informowania administratorów – w celu sprawdzenia ich reakcji.

2. **RED TEAMING**

Oferujemy również usługę klasy Red Teaming, czyli symulacje prawdziwego ataku na Organizacje z wykorzystaniem technik używanych powszechnie przez zorganizowane grupy przestępców. Efektem symulacji jest wskazanie podatności oraz rekomendacji, dzięki którym Organizacja może w szybki sposób podnieść poziom bezpieczeństwa uniemożliwiając osiągnięcie celów atakującym.