Oferta szkoleń PIH.

Kontakt: 22 440 83 23 pih@pih.org.pl

ZAPEWNIENIE BEZPIECZEŃSTWA DZIAŁANIA SYSTEMÓW INFORMATYCZNYCH WYKORZYSTYWANYCH DO REALIZACJI ZADAŃ PUBLICZNYCH

Warsztaty będą poruszały tematykę, związana z „dobrymi praktykami w administracyjnej sieci komputerowej, jako przyczynek do podnoszenia kwalifikacji ASI".

- najważniejsze aspekty prawne (ochrona danych osobowych),

- analiza bezpieczeństwa fizycznego i logicznego,

- identyfikacja zagrożeń, ze szczególnym uwzględnieniem socjotechnik,

- zabezpieczenia sieci IT (podstawowe i zaawansowane),

- analiza najczęściej spotykanych incydentów,

- Instrukcja Zarządzania Systemem Informatycznym, czyli jak przygotować listę kontrolną działań, zleconych pracownikowi działu teleinformatycznego:

- kontrola awaryjnego zasilania komputerów,
- nadzór nad naprawą, konserwacją oraz likwidacją urządzeń komputerowych,
- kontrola systemów antywirusowych oraz aktualności baz wirusów oraz innych zabezpieczeń,
- kontrola wykonywania kopii awaryjnych danych osobowych i systemów do ich przetwarzania,
- kontrola przeglądu i konserwacji systemów informatycznych,
- kontrola uaktualnienia systemów informatycznych,
- kontrola mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrola poziomu dostępu do danych osobowych.

W trakcie szkolenia uczestnik ma dostęp do środowiska testowego na którym może praktyczne wykorzystać pozyskaną wiedzę z części teoretycznej.

CYBERZAGROŻENIA W UJĘCIU OCHRONY INFORMACJI FINANSOWYCH REALIZOWANYCH W SAMORZĄDACH

1. **Wprowadzenie, omówienie zagrożeń i ogólne zasady przeciwdziałania: (1,5h)**

   - podstawowe pojęcia dotyczące cyberbezpieczeństwa (cyberprzestrzeń, malware) - krótkie wprowadzenie,
   - omówienie zagrożeń (typy i rodzaje) – diagramy, statystyki (np.: co to jest: ransomware, ataki kierowane, itp.) - interakcja z uczestnikami (pytania i odp.),
   - metodyka ataków i konsekwencje (socjotechnika, phishing) - przykłady ataków,
   - wykorzystywane narzędzia do ataków (key-loggery, nośniki pamięci, otwarte sieci publiczne) - demonstracja narzędzi,
   - ocena sytuacji, reagowanie i ogólne zasady działań – np.: schemat działania w przypadku infekcji - co wybrać: przywracanie danych, czy tryb awaryjny?

2. **Jak poruszać się bezpiecznie w internecie: (1h)**

   - bankowość elektroniczna - czego nie robić?
   - niebezpieczne linki (pharming) i reklamy,
   - bezpieczna konfiguracja przeglądarki (auto-uzupełnianie, cookies, hasła, tryb "incognito", wtyczki) - demonstracja i ćwiczenia,
   - poczta elektroniczna - demonstracja i ćwiczenia.

3. **Aplikacje użytkowe i biurowe: (1,5h)**

   - zasady pobierania i instalowania - przykład instalacji programu do odtwarzania muzyki Winamp,
   - hasła i szyfrowanie - jak szyfrować programem „7 zip” + opcjonalnie true-crypt, demonstracja łamania haseł, przydatne informację, Webowa aplikacja sprawdzająca jakość hasła,
   - makra - instrukcja jak włączać i wyłączać funkcję w np.: w Excelu, zabezpieczanie dokumentów np.: pdf-ów bezpłatnymi rozwiązaniami,
   - BOD (bring you own device) - prywatny sprzęt w miejscu pracy (możliwości i zagrożenia).

4. **Podstawowe zabezpieczenia: (1h)**

   - program antywirusowy, firewall, aktualizacja systemu i dodatków – prezentacja,
   - narzędzia wykrywające zaawansowane zagrożenia demonstracja podstawowych narzędzi, i ćwiczenia + przedstawienie najnowocześniejszych narzędzi oraz trendów,
   - archiwizacja - demonstracja bezpłatnego programu, ćwiczenia,
   - zalecane zabezpieczenia - porównanie ceny do jakości,
   - nowości na rynku zabezpieczeń: Moving Target Defense - MORPHISEC.

ZATROSZCZ SIĘ O SWOJE DANE, CZYLI WARSZTATY NIE TYLKO DLA INFORMATYKÓW

1. Wdrożenie systemu do automatycznego szyfrowania korespondencji mailowej przy wykorzystaniu bezpłatnych narzędzi: (1h)

- ważne aspekty szyfrowania,
- krótkie omówienie systemu PGP,
- instalacja systemu GPG wraz klientem poczty(Thunderbird) i konfiguracja na komputerach (GNU GPL),
- ćwiczenia i testy (szyfrowanie korespondencji),
- szyfrowane bezpieczne skrzynki i komunikatory (ProtonMail, Tutanota, Signal, Wire),
- inne rozwiązania.

2. Szyfrowanie danych przy wykorzystaniu bezpłatnych narzędzi: (1h)

- dostępne narzędzia,
- co i gdzie szyfrować,
- instalacja oprogramowania do szyfrowania danych (VeraCrypt, TrueCrypt),
- konfiguracja i testy,
- inne rozwiązania (AxCrypt, CloudFogger).

3. Anonimowość w świecie inwigilacji a dostępne zabezpieczenia: (1h)

- przeglądarka i wyszukiwarka internetowa,
- proxy i anonimowy VPN,
- trasowanie cebulowe i inne techniki kryptograficzne (Riffle, TOR),
- inne rozwiązania.

4. Instalacja systemu do automatycznej archiwizacji danych: (1,5h)

- najważniejsze aspekty archiwizacji,
- dostępne oprogramowanie (analiza funkcjonalności , testy..),
- miejsce przechowywania lokalnej kopii zapasowej,
- instalacja systemu do archiwizacji (Cobian),
- opracowanie harmonogramu archiwizacji na podstawie przykładowych zadań,
- szyfrowanie (testy – szyfrowanie/deszyfrowanie),
- testy (przywracanie),
- przechowywanie kopii poza siecią lokalną (chmura, serwer dedykowany…).

5. Dodatkowa/alternatywna tematyka: (0,5 – 1,0h)

1. permanentne usuwanie danych przy wykorzystaniu "open sourcowego" oprogramowania.