

Tworzenie i zarządzanie zespołami obsługi incydentów naruszenia bezpieczeństwa CERT/CSIRT

Omówienie

Szkolenie z Tworzenia i Zarządzania Zespołami Obsługi Incydentów Naruszenia Bezpieczeństwa obejmuje wszystkie etapy pracy zespołu, od projektowania jego struktury, przez aspekty techniczne obsługi bieżących incydentów po najlepsze praktyki wykorzystywane w codziennej pracy. Uczestnicy szkolenia posiadają wiedzę pozwalającą na zbudowanie sprawnie działającego zespołu CERT lub zostanie członkiem takiego zespołu.

Adresaci szkolenia

Członkowie i pełnomocnicy zarządów odpowiedzialni za reagowanie na incydenty naruszające bezpieczeństwo, kadra kierownicza pionów IT odpowiedzialna za tworzenie i utrzymanie zespołów CERT, kandydaci na członków zespołów CERT.

Zakres tematyczny

Podstawy działania zespołów CERT / CSIRT

- Podstawowe pojęcia dotyczące zespołów CERT / CSIRT
- Tworzenie zespołu CSIRT – od określania podległości do pozyskiwania rozgłosu
- Klasyfikacja i priorytety incydentów
- Procedury i ich wykorzystywanie w zadaniach
- Systemy rejestracji incydentów
- Narzędzia wykorzystywane w pracy zespołów
- Działania pozaoperacyjne
- Współpraca z innymi zespołami

Wprowadzenie do obsługi incydentów – case studiem

- Analiza zgłoszeń incydentów
- Określanie przyczyn i skutków incydentu
- Weryfikacja informacji ze zgłoszenia
- Klasyfikacja i nadawania priorytetów
- Poszukiwanie informacji kontaktowych

- Wprowadzenie do obsługi incydentów – gra symulacyjna
- Zrozumienie ról poszczególnych aktorów w procesie obsługi incydentu
- Eskalacja
- Rozwiązywanie konfliktów interesów pomiędzy aktorami
- Responsible disclosure

Czas trwania

Szkolenie prowadzone jest w formie warsztatów, wykładów i gier symulacyjnych, na omówienie wybranych zagadnień potrzebne jest 16 godzin zajęć.

Prowadzący

Ekspertami prowadzącymi szkolenie są członkowie działającego w obrębie NASK zespołu CERT Polska. Osoby te zajmują się na co dzień reagowaniem na pojawiające się w sieci incydenty zagrażające bezpieczeństwu, posiadają wybitną wiedzę specjalistyczną oraz doświadczenie prelegentów międzynarodowych konferencji poświęconych bezpieczeństwu teleinformatycznemu.