Bezpieczeństwo cyfrowe

Szkolenie zamknięte

Szkolenie rekomendujemy: właścicielom MŚP, kadrze zarządzającej, zarządom spółek, managerom, pracownikom wobec których właściciele mają plany związane z awansem na kierownicze stanowiska.

Szkolenie przygotowuje do identyfikowania i rozumienia zróżnicowanych źródeł zagrożeń ataków cyfrowych, wyboru i stosowania zasad zabezpieczeń technicznych i organizacyjnych w celu przeciwdziałania atakom i/lub łagodzenia ich skutków, nadzorowania ustanawiania, wdrażania, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji.

Uczestnik po zakończonym szkoleniu:
- charakteryzuje potencjalne źródła ataków cyfrowych w firmie (zagrożenia);
- definiuje zalecenia ENISA do osiągniecia wysokiego poziomu bezpieczeństwa cybernetycznego;
- charakteryzuje podstawy zabezpieczania przesyłania danych w przedsiębiorstwie i w całym łańcuchu wartości;
- charakteryzuje normy: ISO/IEC 27001,
- charakteryzuje przykłady podstawowej dokumentacji opisującej zasady bezpieczeństwa w firmie (np. przykład metodologii szacowania ryzyka, dokumenty dotyczące zarządzania zidentyfikowanym ryzykiem, czy przykład analizy zabezpieczeń systemów teleinformatycznych).
- charakteryzuje różnice pomiędzy różnymi systemami IT i OT oraz podstawy sposobów ich zabezpieczania.
- definiuje podstawowe różnice pomiędzy modelem zabezpieczeń oprogramowania typu open-source i closed-source.
- opisuje podstawy zagadnień dotyczące zagrożeń cyberbezpieczeństwa wynikających ze stosowania nowych rozwiązań cyfrowych, w tym algorytmów sztucznej inteligencji, przetwarzania w chmurze, rozwiązań mobilnych.
- zapewnia ciągłość działania organizacji w procesie transformacji cyfrowej
- szacuje ryzyko w odniesieniu do poszczególnych aktywów informatycznych firmy i wpływ wystąpienia potencjalnych ryzyk na działanie firmy
- współpracuje ze specjalistami ds. cyberbezpieczeństwa danych i systemów w zakresie projektów realizowanych w transformacji cyfrowej firmy
- wdraża odpowiednie procedury bezpieczeństwa.
- identyfikuje niezbędne akty prawne, dokumenty i zapisy w nich zawarte, określające podstawy bezpieczeństwa cyfrowego w firmie

Czas trwania szkolenia: 16 godzin

Program szkolenia
1. Mapowanie potrzeb i rozmowa motywacyjna na temat korzyści z kompetencji cyfrowych w zakresie bezpieczeństwa informatycznego.
2. Dbałość o sprzęt informatyczny. Aktualizacja systemów operacyjnych i programów:
a) komputer
b) tablet

c) smartfon
3 Zalecenia ENISA do osiągniecia wysokiego poziomu bezpieczeństwa cybernetycznego
4 Modele zabezpieczeń oprogramowania typu open-source i closed-source.
5 Ochrona przed złośliwym oprogramowaniem. Możliwe sposoby zainfekowania (komputer, tablet, smartfon) i sposoby ochrony.
6 Bezpieczeństwo w Internecie. Zabezpieczenie przeglądarki internetowej.
7 Kopie bezpieczeństwa. Przechowywanie danych i ich bezpieczeństwo.
8 Ochrona sprzętu przed kradzieżą danych. Ustawienie zabezpieczeń antykradzieżowych
9 Ochrona haseł. Zabezpieczenia programowe i sprzętowe.
10 Ochrona danych osobowych i informacji poufnych
11 Bezpieczeństwo finansów i operacji finansowych dokonywanych za pośrednictwem Internetu i aplikacji
12 Piractwo cyfrowe – rodzaje zagrożeń i sposoby przeciwdziałania