Cyberbezpieczeństwo w organizacji – ochrona danych i ciągłość działania

Nowoczesne szkolenie, które przygotowuje firmy do funkcjonowania w świecie rosnących zagrożeń cyfrowych. Skupiamy się na praktycznych rozwiązaniach, realnych scenariuszach oraz budowaniu odporności organizacji – nie tylko na poziomie technologii, ale także procesów i ludzi.

Dla kogo?
Dla właścicieli MŚP, kadry zarządzającej, managerów oraz osób przygotowywanych do ról kierowniczych, które odpowiadają za bezpieczeństwo informacji i ciągłość działania organizacji.

Cel szkolenia
Zwiększenie poziomu bezpieczeństwa cyfrowego w firmie poprzez rozwój kompetencji w zakresie identyfikacji zagrożeń, zarządzania ryzykiem oraz wdrażania skutecznych zabezpieczeń organizacyjnych i technicznych.

Efekty dla uczestników
Po szkoleniu uczestnicy:

- identyfikują kluczowe zagrożenia cybernetyczne i ich źródła
- rozumieją standardy i dobre praktyki, w tym wytyczne ENISA oraz normę ISO/IEC 27001
- potrafią ocenić ryzyko i jego wpływ na funkcjonowanie firmy
- wdrażają procedury bezpieczeństwa i podstawową dokumentację
- zwiększają bezpieczeństwo danych, systemów i procesów biznesowych
- rozumieją zagrożenia związane z AI, chmurą i rozwiązaniami mobilnymi
- potrafią współpracować ze specjalistami IT i cyberbezpieczeństwa
- dbają o ciągłość działania organizacji w procesie transformacji cyfrowej

Zakres tematyczny
Szkolenie obejmuje najważniejsze obszary współczesnego cyberbezpieczeństwa:

- identyfikacja zagrożeń i budowanie świadomości cyberbezpieczeństwa
- ochrona urządzeń i systemów (komputery, smartfony, aplikacje)
- bezpieczeństwo danych, kopie zapasowe i zarządzanie dostępem
- ochrona przed phishingiem, malware i wyciekiem danych
- bezpieczeństwo pracy w internecie i aplikacjach biznesowych
- zarządzanie hasłami i dostępem do zasobów
- podstawy norm i systemów zarządzania bezpieczeństwem informacji
- różnice i zabezpieczenia systemów IT i OT
- bezpieczeństwo w chmurze, AI i środowisku mobilnym
- ochrona operacji finansowych i przeciwdziałanie nadużyciom

Forma pracy
Szkolenie ma charakter praktyczny – uczestnicy analizują realne zagrożenia, pracują na przykładach z życia firm oraz uczą się wdrażać konkretne rozwiązania możliwe do zastosowania od razu w organizacji.

Czas trwania: 2 dni (16 godzin)
Forma: szkolenie zamknięte, dopasowane do specyfiki firmy

To szkolenie daje nie tylko wiedzę, ale przede wszystkim **realne narzędzia do ochrony firmy w cyfrowym świecie**.