

E-Cyberbezpieczeństwo dla Kadry zarządzającej

Cele szkolenia

Szkolenie z zakresu cyberbezpieczeństwa zostało przygotowane z myślą o kadrze zarządzającej, która podejmuje strategiczne decyzje i odpowiada za bezpieczeństwo informacji w organizacji. Głównym celem jest wyposażenie liderów w wiedzę niezbędną do podejmowania świadomych decyzji strategicznych w obszarze bezpieczeństwa informacji.

Zrozumienie roli lidera w budowaniu kultury bezpieczeństwa w organizacji.

Identyfikacja ryzyk biznesowych, prawnych i wizerunkowych wynikających z incydentów cybernetycznych.

Przygotowanie do zarządzania kryzysowego w przypadku wystąpienia ataku.

Umiejętności

Uczestnik po szkoleniu będzie potrafił:

Podjmować decyzje pod presją czasu

Zadawać właściwe pytania działom IT/Security i egzekwować raportowania opartego na metrykach biznesowych

Stosować zaawansowane metody ochrony własnej tożsamości cyfrowej

Profil uczestników

Szkolenie jest dedykowane osobom, które nie muszą posiadać wiedzy technicznej, ale odpowiadają za strategię i ciągłość działania firmy:

- Członkowie zarządów i Rad Nadzorczych.
- Właściciele średnich i dużych przedsiębiorstw.
- Dyrektorzy operacyjni, finansowi , oraz HR.
- Kierownicy kluczowych działów biznesowych.

Przygotowanie uczestników

Uczestnik powinien:

- Posiadać znajomość struktury organizacyjnej i odpowiedzialności r a także rozumieć różnicę między trzymaniem danych u siebie a u zewnętrznego dostawcy.
- Wiedzieć czym jest tożsamość cyfrowa, posiadać świadomość, że login i hasło to "cyfrowe klucze" do firmy
- Posiadać podstawowa wiedzę o tym, czym jest phishing (odróżnianie oczywistego spamu od komunikacji służbowej).

Szczegółowy program szkolenia

Cyberbezpieczeństwo - Rola kadry zarządzającej

- Wprowadzenie do tematyki i omówienie roli menedżerów w zapewnianiu bezpieczeństwa cyfrowego.

NIS2 – obowiązki kadry zarządzającej

- Omówienie wymogów wynikających z dyrektywy NIS2 i konkretnych obowiązków, jakie nakłada ona na osoby zarządzające.

Normy ISO 27001 - wsparcie bezpieczeństwa informacji w organizacji

- Przedstawienie standardów ISO 27001 jako narzędzia wspierającego system bezpieczeństwa informacji w firmie.

Normy ISO a NIS2

- Analiza korelacji między normami ISO a wymogami dyrektywy NIS2.

Metoda realizacji szkolenia

Szkolenie realizowane jest w modelu nauki samodzielnej. Uczestnik realizuje program w trybie asynchronicznym, co pozwala na pełną elastyczność i dopasowanie nauki do własnego kalendarza przy jednoczesnym zachowaniu wysokiej interaktywności materiału.

Liczba dni, liczba godzin szkoleniowych

Łączny czas materiału: ok. 120 minut

Ścieżka rozwoju po szkoleniu

- szkolenia z oferty CSC z zakresu Cyberbezpieczeństwa