

Cybersecurity dla kadry zarządzającej

Szkolenie **Cybersecurity dla kadry zarządzającej** to praktyczny program dla osób decyzyjnych, które chcą zrozumieć ryzyka cyfrowe i skutecznie zarządzać bezpieczeństwem informacji w organizacji. Nie wymaga wiedzy technicznej – skupia się na aspektach biznesowych, prawnych i strategicznych.

Uczestnicy poznają najważniejsze zagrożenia, nauczą się oceniać ryzyko oraz podejmować świadome decyzje dotyczące **bezpieczeństwa IT, zarządzania incydentami i ciągłości działania**. Szkolenie pokazuje, jak budować odporność organizacji oraz jak współpracować z działem IT i dostawcami usług.

Program uwzględnia aktualne regulacje (m.in. **NIS2, RODO**) oraz realne scenariusze ataków, dzięki czemu uczestnicy rozumieją konsekwencje biznesowe cyberzagrożeń.



Zakres tematyczny

Cybersecurity w kontekście biznesowym

- Dlaczego cyberbezpieczeństwo to problem zarządu
- Najważniejsze trendy i statystyki
- Koszty incydentów – finansowe i wizerunkowe

Kluczowe zagrożenia dla organizacji

- Typy ataków (ransomware, wycieki danych, ataki na łańcuch dostaw)
- Scenariusze realnych incydentów
- Czynniki ryzyka w organizacji

Zarządzanie ryzykiem cybernetycznym

- Identyfikacja i klasyfikacja ryzyk
- Ocena wpływu na biznes
- Podejmowanie decyzji (akceptacja, redukcja, transfer)

Regulacje i odpowiedzialność

- NIS2, RODO – co musi wiedzieć zarząd
- Odpowiedzialność prawna kadry zarządzającej
- Audyty i compliance

Zarządzanie incydentami

- Jak reagować na incydent krok po kroku
- Komunikacja kryzysowa
- Współpraca z zespołem IT i partnerami



Budowanie strategii bezpieczeństwa

- Polityki bezpieczeństwa
- Kultura bezpieczeństwa w organizacji
- Rola zarządu w cyberbezpieczeństwie