**PROGRAM SZKOLENIA**

**CYBERBEZPIECZEŃSTWO DLA PODMIOTÓW ADMINISTRACJI SAMORZĄDOWEJ**

1. Bezpieczeństwo cyberprzestrzeni - uregulowania prawne w RP i UE oraz zadania i struktura instytucji zajmujących się w RP bezpieczeństwem cyberprzestrzeni, a także wybrane dla niej zagrożenia i ich charakterystyka.
2. Systemy bezpieczeństwa teleinformatycznego - podstawowe zasady, systemy i rozwiązania organizacyjno-techniczne bezpieczeństwa IT, potrzeba zmiany filozofii myślenia o bezpieczeństwie IT oraz przykłady przyszłych rozwiązań dla architektur bezpieczeństwa teleinformatycznego
3. Najpowszechniejsze ataki cybernetyczne – charakterystyka najczęstszych ataków hakerskich, profilaktyka i minimalizacja ich skutków
4. Rodzaje zagrożeń cybernetycznych i terrorystycznych dla teleinformatycznej infrastruktury krytycznej - identyfikacja zagrożeń o charakterze ataków cyberterrorystycznych i terrorystycznych wymierzonym w krajową infrastrukturę krytyczną, elementy teleinformatycznej infrastruktury krytycznej najbardziej narażone na ataki, rodzaje ataków terrorystycznych i ich potencjalne skutki dla tego elementu infrastruktury krytycznej, a także organizacyjne i techniczne metody zapobiegania atakom i ochrony

Szkolenie realizowane jest w formule online i trwa 5h.