Oferta na przeprowadzenie **szkolenia on-line** pt.

WYBRANE PROBLEMY ZWIĄZANE Z BEZPIECZEŃSTWEM INFORMACJI I OCHRONY DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH I TRADYCYJNYCH FORMACH PRZETWARZANIA

1. **Bezpieczeństwo informacji - polskie realia**
2. **Bezpieczeństwo jako wypadkowa zabezpieczeń:**

    a) fizycznych;
    b) prawnych;
    c) teleinformatycznych;
    d) osobowo – organizacyjnych.

3. **Elementy bezpieczeństwa informacji**
4. **Przyczyny naruszeń bezpieczeństwa na podstawie raportu cert**
5. **Najczęściej występujące nieprawidłowości ma podstawie NIK**
6. **Przykłady zagrożeń na podstawie normy ISO/IEC 29134:2017 w odniesieniu do:**

    a) sprzętu;
    b) oprogramowania i kanałów łączności komputerowej;
    c) personelu;
    d) dokumentów papierowych i kanałów obiegu dokumentów.

7. **Przykładowe podatności wg. Normy PN-ISO/IEC 27005**
8. **Złośliwe i niebezpieczne oprogramowanie m.in.:**

    a) Spyware;
    b) Adware;

c) Ransomware;
d) Key loggery;
e) Trojany;
f) Backdory.

9. **Przykłady cyberataków**
10. **Bezpieczeństwo urządzeń mobilnych**
11. **Kopie zapasowe**
12. **Zarządzanie ryzykiem**
13. **Zarządzanie naruszeniami**
14. **Wymagania systemu zarządzania bezpieczeństwem**
15. **PN**
16. **ISO/IEC 27001 norma standaryzująca systemy zarządzania bezpieczeństwem – omówienie**
17. **Polityki, dokumenty, procedury i instrukcje w zakresie zarządzania bezpieczeństwem**
18. **Okresowe analizy ryzyka utraty integralności, dostępności lub poufności – działania minimalizujące ryzyko**
19. **Procedury przywracania sprawności systemu informatycznego po awarii**
20. **Zasady zgłaszania incydentów, problemów, awarii związanych z systemem informatycznym**
21. **Zalecenia dla użytkowników**