

Program szkolenia

Cyberbezpieczeństwo dla kadry zarządzającej

<https://bloomwise.pl/consulting/training/cyberbezpieczenstwo-dla-kadry-zaradzajacej>

Poniższy zakres stanowi bazę, którą możemy dopasować do specyfiki Twojej marki, zespołu i modelu pracy z klientem.

Moduł 1. Wprowadzenie, czyli jak działają cyberprzestępcy?

Moduł 2. Podstawowe obowiązki, regulacje, odpowiedzialności i sankcje w zakresie cyberbezpieczeństwa.

Moduł 3. Skutki cyberataków – case study.

Moduł 4. Podstawowe informacje o atakach na użytkowników (z uwzględnieniem roli kadry zarządzającej) – m. in. socjotechnika, phishing, spearphishing, malware, pharming, spoofing, spam, spim, scam. Przykłady z życia.

Moduł 5. Podstawowe informacje o atakach na infrastrukturę teleinformatyczną organizacji: DDos, XSS, ransomeware, brute force

Moduł 6. Cyberbezpieczeństwo

[6.1](#) Bezpieczeństwo teleinformatyczne

[6.2](#) Bezpieczeństwo osobowe

[6.3](#) Bezpieczeństwo fizyczne

[6.4](#) Bezpieczeństwo prawno-organizacyjne

Moduł 7. Zarządzanie cyberbezpieczeństwem: szacowanie ryzyka, standardy (m.in.KSC, ISO 27001, ISO 22301, NIST)

Moduł 8. Dyskusja na temat działań jakie uczestnicy chcą podjąć po szkoleniu.

Moduł 9. Moduły personalizowane - do uzgodnienia.