

Szkolenie Podstawy prawne w obszarze cyberbezpieczeństwa

Opis szkolenia: Szkolenie wprowadzające do zagadnień prawnych i organizacyjnych w zakresie cyberbezpieczeństwa oraz przygotowanie do pełnienia roli lidera w zarządzaniu bezpieczeństwem informacji.

Kod szkolenia: SEC-PWN-01

Kategoria: Security awareness / Cyberbezpieczeństwo / Edukacja pracowników

Trenerka: Beata Zalewa

Czas trwania: 4 godziny (np. 9:00 – 13:00)

Poziom zaawansowania: Podstawowy

Język wykładowy: język polski

Forma szkolenia: zdalne. Po wcześniejszym uzgodnieniu możliwe szkolenie w siedzibie klienta.

Materiały: w języku polskim. Na życzenie klienta materiały w języku angielskim.

Wymagania wstępne: Brak wymagań technicznych - szkolenie dla każdego pracownika.

Grupa docelowa: Kadra kierownicza i menedżerska.

Cel szkolenia: Zwiększenie świadomości prawnej w zakresie cyberbezpieczeństwa oraz przygotowanie do pełnienia roli lidera w zarządzaniu bezpieczeństwem informacji.

Efekty szkolenia:

- Uczestnik zna kluczowe polskie i europejskie akty prawne oraz regulacje w obszarze cyberbezpieczeństwa, w tym wymagania dyrektywy NIS2, ustawy o krajowym systemie cyberbezpieczeństwa (KSC) oraz przepisy RODO.
- Potrafi prawidłowo zidentyfikować obowiązki prawne ciążyące na jego organizacji, dokonać klasyfikacji incydentów bezpieczeństwa oraz przeprowadzić procedurę ich zgłaszania do odpowiednich organów (np. CSIRT) w ustawowych terminach.
- Potrafi ocenić wewnętrzne procedury oraz dokumentację firmy pod kątem zgodności (*compliance*) z aktualnymi normami prawnymi i wskazać obszary wymagające dostosowania do nowych regulacji.
- Rozumie osobistą odpowiedzialność kadry zarządzającej oraz konsekwencje prawne, finansowe i wizerunkowe, jakie grożą organizacji w przypadku niedopełnienia obowiązków z zakresu ochrony cyberprzestrzeni.
- Rozumie bezpośredni związek między technicznymi środkami bezpieczeństwa a wymogami prawnymi, traktując zgodność z regulacjami jako strategiczny element budowania odporności cyfrowej biznesu.

Co otrzymasz?

- Materiały szkoleniowe.
- Szkolenie kończy się certyfikatem uczestnictwa.

Agenda szkolenia

Godzina	Czas trwania	Moduł	Forma
9:00 - 9:15	15 minut	Wstęp	Dyskusja
9:15 - 9:45	30 minut	Wprowadzenie do cyberbezpieczeństwa w kontekście prawnym	Wykład, dyskusja
9:45 - 10:15	30 minut	Kluczowe akty prawne regulujące cyberbezpieczeństwo	Wykład, dyskusja
10:15 - 11:00	45 minut	Obowiązki firmy jako operatora usług kluczowych / podmiotu publicznego	Wykład, dyskusja
11:00 - 11:15	15 minut	Przerwa kawowa	-
11:15 - 11:45	30 minut	Rola kadry zarządzającej w systemie bezpieczeństwa informacji	Wykład, dyskusja
11:45 - 12:15	30 minut	Studium przypadku i analiza incydentów	Studium przypadku, dyskusja
12:15 - 12:45	30 minut	Warsztat: ocena zgodności i plan działań	Warsztat
12:45 - 13:00	15 minut	Sesja pytań i odpowiedzi	Q&A, ankieta końcowa

Szczegółowy program szkolenia

Moduł 1: Wstęp

Wprowadzenie do tematu i przedstawienie agencji.

- Przedstawienie prowadzącego i uczestników.
- Omówienie celów i struktury szkolenia.
- Zasady współpracy i interaktywności.

Moduł 2: Wprowadzenie do cyberbezpieczeństwa w kontekście prawnym

- Definicje i podstawowe pojęcia (cyberbezpieczeństwo, incydent, dane wrażliwe).
- Znaczenie cyberbezpieczeństwa w firmie.
- Obowiązki kadry kierowniczej w świetle przepisów.

Moduł 3: Kluczowe akty prawne regulujące cyberbezpieczeństwo

- Ustawa o krajowym systemie cyberbezpieczeństwa.
- RODO (GDPR) – ochrona danych osobowych w kontekście incydentów.
- Kodeks karny i odpowiedzialność za naruszenia.
- Przepisy sektorowe.

Moduł 4: Obowiązki firmy jako operatora usług kluczowych / podmiotu publicznego

- Wymogi dotyczące systemów informatycznych.
- Zgłaszanie incydentów do CSIRT.
- Współpraca z organami nadzorczymi.

Moduł 5: Rola kadry zarządzającej w systemie bezpieczeństwa informacji

- Tworzenie i nadzorowanie polityk bezpieczeństwa.
- Zarządzanie ryzykiem i odpowiedzialność za decyzje.
- Współpraca z inspektorem ochrony danych (IOD) i zespołem IT.

Moduł 6: Studium przypadku i analiza incydentów

- Przykłady realnych incydentów w firmach.
- Analiza błędów i działań naprawczych.
- Dyskusja: co można było zrobić inaczej?

Moduł 7: Warsztat: Ocena zgodności i plan działań

- Praca w grupach: identyfikacja luk w zgodności z przepisami.
- Opracowanie planu działań naprawczych.
- Prezentacja i omówienie wyników.

Moduł 8: Podsumowanie, Q&A i kolejne kroki

- Podsumowanie i wnioski.
- Sesja pytań i odpowiedzi.
- Ankieta końcowa i informacje o certyfikacie.
- Rekomendacje dla kadry zarządzającej.

Zarejestruj się na szkolenie: szkolenia@zalnet.pl

<https://zalnet.pl/edu/podstawy-prawne-w-obszarze-cyberbezpieczenstwa/>

