ODPOWIEDZIALNOŚĆ OSOBISTA CZŁONKÓW ZARZĄDU ZA WDROŻENIE NIS2 I KSC

Wejście w życie dyrektywy NIS2 oraz nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa istotnie zmieniają zakres odpowiedzialności organizacji oraz kadry zarządzającej w obszarze cyberbezpieczeństwa.

Nowe regulacje:

- wprowadzają bezpośrednią, osobistą odpowiedzialność kierownictwa za nadzór nad systemem zarządzania bezpieczeństwem,
- rozszerzają katalog podmiotów objętych obowiązkami,
- przewidują administracyjne wielomilionowe kary pieniężne,
- umożliwiają organom nadzorczym prowadzenie kontroli oraz wydawanie wiążących decyzji.

W PRAKTYCE KLUCZOWE STAJE SIĘ USTALENIE, CZY PAŃSTWA ORGANIZACJA PODLEGA POD NOWE PRZEPISY I W JAKIM ZAKRESIE. JEŚLI TAK - PRZYGOTOWANIE WDROŻENIA W CELU UNIKNIĘCIA ODPOWIEDZIALNOŚCI.

Proponujemy następujące kroki:

Opinia prawna w zakresie określenia statusu podmiotu na gruncie NIS2/KSC

Przedmiotem usługi jest przeprowadzenie kompleksowej analizy prawno-regulacyjnej w celu ustalenia, czy oraz w jakim zakresie Spółka podlega przepisom dyrektywy NIS2 oraz ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC).

Pre-audyt gotowości na NIS2/KSC

Umożliwia organizacji wstępne określenie, na ile jej obecny poziom bezpieczeństwa informacji i cyberodporności odpowiada wymaganiom dyrektywy NIS2 oraz KSC. Wynikiem jest klarowna lista luk i rekomendacji, które stanowią fundament planu wdrożeniowego.

Wsparcie we wdrożeniu NIS2/KSC

Usługa wsparcia we wdrożeniu NIS2/KSC pomaga organizacji sprawnie osiągnąć zgodność z wymaganiami regulacyjnymi, zwiększyć poziom cyberbezpieczeństwa oraz zminimalizować ryzyko incydentów i kar administracyjnych.

Pełnienie funkcji Pełnomocnika Zarządu ds. cyberbezpieczeństwa

Pełnomocnik Zarządu koordynuje i nadzoruje działania związane z przygotowaniem i realizacją spełniania wymogów NIS2/KSC oraz zapewnia Zarządowi wsparcie prawne, informacyjne, szkoleniowe i doradcze.

Realnie możemy wesprzeć Twoją organizację. Porozmawiaj z nami już dziś!

SKONTAKTUJ SIĘ Z NAMI

JDS CONSULTING

23 LATA DOŚWIADCZENIA

5 największych ryzyk dla zarządu w przypadku braku wdrożenia NIS2/KSC

Ryzyko wysokich kar finansowych
Niespełnienie wymagań wynikających z NIS2/KSC może skutkować wielomilionowymi karami administracyjnymi oraz dodatkowymi kosztami związanymi z obsługą incydentów, przestojami operacyjnymi czy utratą danych.

Ryzyko osobistej odpowiedzialności członków zarządu
Dyrektywa NIS2 wzmacnia odpowiedzialność kadry zarządzającej za nadzór nad cyberbezpieczeństwem. Brak odpowiednich mechanizmów zarządzania bezpieczeństwem może prowadzić do osobistej odpowiedzialności członków zarządu.

Ryzyko negatywnych wyników kontroli organów
Organizacje objęte NIS2/KSC muszą być przygotowane na audyty oraz kontrole organów nadzorczych. Brak uporządkowanych procesów, dokumentacji i dowodów zgodności zwiększa ryzyko negatywnych wyników kontroli.

Ryzyko utraty reputacji i zaufania rynku
Poważny incydent cyberbezpieczeństwa może znacząco wpłynąć na wizerunek organizacji, obniżyć zaufanie klientów i partnerów biznesowych oraz mieć długotrwałe konsekwencje reputacyjne.

Ryzyko utraty kontraktów i relacji biznesowych
Coraz więcej organizacji wymaga od swoich partnerów spełnienia określonych standardów cyberbezpieczeństwa. Brak zgodności z NIS2/KSC może ograniczyć możliwość udziału w przetargach lub prowadzić do utraty kluczowych kontraktów.

Dlaczego zarządy wybierają nasze wsparcie

- **Pewność regulacyjna**

Dostarczamy jasną opinię prawną oraz praktyczne rekomendacje, które pozwalają zarządowi szybko zrozumieć skalę obowiązków i podjąć właściwe decyzje strategiczne.

- **Sprawne wdrożenie wymagań**

Prowadzimy organizację przez cały proces dostosowania do nowych regulacji.

- **Gotowość na kontrolę regulatora**

Organizacja jest przygotowana na kontrole organów nadzorczych oraz potrafi wykazać spełnienie obowiązków.

- **Stałe wsparcie zarządu**

Pełnomocnik Zarządu ds. cyberbezpieczeństwa pomaga kierownictwu organizacji w nadzorze nad wdrożeniem wymagań NIS2 oraz podejmowaniu świadomych decyzji w obszarze bezpieczeństwa, ograniczając na bieżąco ryzyko odpowiedzialności zarządu.

WWW.JDS.COM.PL
OFFICE@JDS.COM.PL

SKONTAKTUJ SIĘ Z NAMI