Szanowni Państwo,

w związku z pojawiającymi się pytaniami dotyczącymi wdrożenia dyrektywy NIS2 w Polsce przygotowaliśmy zestawienie najważniejszych informacji.

Jako firma świadcząca usługi IT na bieżąco monitorujemy proces legislacyjny oraz rozwój wytycznych, ze szczególnym uwzględnieniem ich przełożenia na wymagania techniczne i organizacyjne.

Czym jest NIS2 i dlaczego to ważne?

NIS2 to unijna dyrektywa dotycząca cyberbezpieczeństwa, która znacząco podnosi wymagania w zakresie ochrony systemów IT i zarządzania ryzykiem. **W Polsce została wdrożona 3.04.2026 r. poprzez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa (KSC).**

Kluczowe zmiany to **rozszerzenie zakresu firm objętych regulacją** (również poprzez łańcuch dostaw) oraz **zwiększenie odpowiedzialności kadry zarządzającej** – obejmujące zarówno wysokie **kary finansowe** (do 10 mln € lub 2% globalnego obrotu), jak i **środki o charakterze osobistym**, w tym możliwość odsunięcia od pełnienia funkcji kierowniczych.

W praktyce oznacza to, że coraz więcej organizacji będzie musiało spełniać określone standardy bezpieczeństwa IT – również w relacjach z dostawcami.

Warto, aby każda firma przeanalizowała, czy i w jakim zakresie nowe regulacje mogą mieć do niej zastosowanie.

Kogo dotyczy NIS2?

Nowe przepisy obejmują szerokie grono organizacji, dzieląc je na **podmioty kluczowe** (np. energetyka, bankowość, zdrowie, infrastruktura cyfrowa) oraz **podmioty ważne** (np. produkcja, branża spożywcza, chemia, logistyka).

- Główne kryteria objęcia regulacją to przede wszystkim prowadzenie działalności w określonych sektorach oraz wielkość organizacji (zazwyczaj powyżej 50 pracowników lub 10 mln EUR obrotu rocznego).

- Mniejsze podmioty również mogą zostać objęte regulacją, jeśli pełnią istotną rolę dla funkcjonowania gospodarki lub państwa.

- Dodatkowo, NIS2 wprowadza obowiązek zarządzania ryzykiem w łańcuchu dostaw, co w praktyce oznacza, że firmy objęte regulacją będą wymagały odpowiednich standardów bezpieczeństwa od swoich dostawców.

Harmonogram wdrożenia

3 IV 2026

START
Wejście w życie nowelizacji ustawy o KSC
- od tego momentu rozpoczyna się bieg terminów ustawowych

do 3 X 2026

REJESTRACJA
Zgłoszenie do wykazu podmiotów
- samoidentyfikacja oraz zgłoszenie do właściwego rejestru

do 3 IV 2027

OPERACYJNOŚĆ
Wdrożenie wymogów bezpieczeństwa
- dokumentacja, analiza ryzyka i zabezpieczenia techniczne

RAPORTOWANIE
Gotowość do zgłaszania incydentów
- raportowania incydentów w określonym czasie

EDUKACJA
Szkolenia z zakresu cyberbezpieczeństwa
- zapewnienie kompetencji kadry zarządzającej

do 3 IV 2028

WERYFIKACJA
Pierwszy audyt bezpieczeństwa, a następnie cykliczne
- przeprowadzenie audytu zewnętrznego

Najważniejsze wymogi

Obszar	Co to oznacza w praktyce?	Ryzyko/odpowiedzialność
Zarządzanie ryzykiem	Systematyczna weryfikacja bezpieczeństwa (audyty, skanowanie podatności), wdrożone polityki haseł, backupu i aktualizacji	Zarząd odpowiada za zatwierdzenie i nadzór nad środkami bezpieczeństwa, a naruszenia mogą skutkować wysokimi karami finansowymi oraz odpowiedzialnością osobistą
Łańcuch dostaw	Weryfikacja bezpieczeństwa dostawców IT oraz podwykonawców, kontrola dostępu firm zewnętrznych do systemów	Ryzyko utraty współpracy z klientami objętymi NIS2 w przypadku niespełnienia wymagań
Obsługa incydentów	Wdrożone procedury wykrywania i reagowania na incydenty oraz gotowość do ich zgłaszania w terminach (24h/72h)	Ryzyko kar finansowych oraz konsekwencji prawnych w przypadku niewłaściwego raportowania
Edukacja i świadomość	Regularne szkolenia z zakresu cyberbezpieczeństwa, szczególnie dla kadry zarządzającej i administratorów systemów	Brak szkoleń może skutkować niespełnieniem wymogów oraz zwiększonym ryzykiem incydentów

Podział kompetencji przy wdrożeniu NIS2

Zgodność z dyrektywą to gra zespołowa. Wymaga połączenia trzech różnych ról:

- **Kancelaria prawna (obszar prawno-compliance)**. Interpretacja wymagań NIS2, określenie statusu organizacji, dostosowanie umów z kontrahentami oraz doradztwo w zakresie odpowiedzialności zarządu.

- **Audytor/konsultant (procesy i zgodność operacyjna)**. Analiza luk, opracowanie podejścia do zarządzania ryzykiem, przygotowanie procedur oraz uporządkowanie dokumentacji zgodnie z wymaganiami.

- **Partner IT (technologia).** Wdrożenie i utrzymanie rozwiązań technologicznych (systemy monitoringu, zabezpieczeń i reagowania na incydenty). Doradza też w zakresie architektury IT i pomaga budować długoterminową strategię cyberbezpieczeństwa.

Wniosek: prawnik określa wymogi, audytor przekłada je na procedury, a partner IT wdraża rozwiązania, które zamieniają te wytyczne w realne cyberbezpieczeństwo.

O ile wsparcie prawne i procesowe często realizowane jest przez jeden podmiot doradczy, o tyle kompetencje technologiczne zwykle stanowią odrębny, kluczowy fundament bezpieczeństwa organizacji.

Pierwsze kroki – od czego zacząć?

Wdrożenie NIS2 warto rozpocząć od uporządkowanej, etapowej analizy.

1. Ocena wpływu i statusu prawnego
Sprawdzenie, czy organizacja podlega NIS2 (bezpośrednio lub w łańcuchu dostaw) oraz potwierdzenie statusu (podmiot kluczowy/ważny) w oparciu o kryteria ustawowe.

2. Analiza luk i ryzyka (gap analysis)
Porównanie obecnych praktyk z wymaganiami NIS2, identyfikacja braków oraz określenie priorytetów działań (organizacyjnych i technicznych).

3. Ocena środowiska IT i plan wdrożenia
Przegląd zabezpieczeń, dostępu i monitoringu oraz przygotowanie planu wdrożenia środków technicznych i organizacyjnych.

Potencjalny podział kompetencji w praktyce

Obszar NIS2	Kancelaria/konsultant	Partner IT	Co konkretnie zapewnia firma IT
Analiza ryzyka	Identyfikuje procesy biznesowe oraz ryzyka prawne i regulacyjne	Przeprowadza inwentaryzację zasobów IT i techniczne skanowanie podatności	Audyt zerowy IT, audyt bezpieczeństwa infrastruktury, skanowanie podatności
Polityki i procedury	Opracowuje polityki i procedury zgodne z wymaganiami NIS2 oraz nadzoruje ich zgodność formalną	Konfiguruje narzędzia tak, aby wymuszały te procedury (np. polityki haseł, blokady)	Systemy zarządzania politykami, szyfrowanie danych, DLP (Data Loss Prevention)
Ciągłość działania (BCP/DR)	Tworzy plany (BCP) "na papierze": procesy decyzyjne i komunikację kryzysową	Projektuje i wdraża architekturę wysokiej dostępności oraz mechanizmy odtwarzania	BaaS (Backup), DRaaS (Disaster Recovery), testowe odtworzenie (raport RTO/RPO)
Zarządzanie dostępem	Definiuje matrycę uprawnień: kto, do czego i dlaczego ma mieć dostęp	Wdraża techniczne środki kontroli (uwierzytelnianie) i zarządza tożsamością	np. MFA (logowanie dwuetapowe), Azure/AD, systemy PAM
Obsługa incydentów	Opracowuje ramy prawne zgłaszania incydentów do CERT/CSIRT (24h/72h)	Wdraża systemy monitorowania (SOC), które wykrywają atak i reagują technicznie	np. EDR/XDR, SIEM (logi), umowy SLA na Incident Response
Bezpieczeństwo łańcucha dostaw	Tworzy bezpieczne zapisy w umowach z dostawcami i weryfikuje ich prawnie	Wdraża bezpieczne tunele (VPN/SD-WAN) i monitoruje dostępy firm zewnętrznych	Bezpieczny VPN, segmentacja sieci, audyty techniczne poddostawców

Jako partner IT zapewniamy kompleksowe zaplecze technologiczne niezbędne do spełnienia wymogów NIS2. Przekładamy wymagania regulacyjne na konkretne rozwiązania, które realnie podnoszą poziom bezpieczeństwa organizacji.

W przypadku pytań zachęcamy do kontaktu:

Maciej Kóska
tel. +48 605 311 424
e-mail: mkoska@intelion.pl

Ze względu na dynamiczny charakter regulacji niniejszy materiał ma charakter informacyjny i może podlegać aktualizacjom wraz ze zmianami przepisów oraz kształtowaniem się praktyki rynkowej.