TOMASZ OCHOCKI

Przewodnik po NIS2

CO DYREKTYWA NIS2 OZNACZA DLA ZARZĄDU?

Stan na 2.03.2026

SPIS TREŚCI

01

Dlaczego NIS2?

Wdrożenie dyrektywy NIS2 do polskiego prawa wyznacza nowe ramy odpowiedzialności za bezpieczeństwo informacji.

Tu i teraz najważniejsze są:

- **Osobista odpowiedzialność zarządów** za nadzór nad cyberbezpieczeństwem.
- **Obowiązek raportowania incydentów** w rygorystycznych reżimach czasowych.
- **Konieczność audytowania łańcucha dostaw**.

Czy Państwa firma podlega nowym przepisom? Jak wdrożyć te zmiany? Oto krótkie podsumowanie kluczowych założeń znowelizowanej ustawy.

Tomasz Ochocki
Wiceprezes Zarządu ODO 24 sp. z o .o.
Koordynator Zespołu Merytorycznego

02

Czy NIS2 mnie dotyczy?

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa rozszerza zakres sektorów gospodarki, które będą podlegać nowym przepisom.

Oto lista sektorów objętych nowelizacją:

1. Energia
2. Transport
3. Bankowość
4. Infrastruktura rynków finansowych
5. Ochrona zdrowia
6. Zaopatrzenie w wodę pitną i jej dystrybucja
7. Infrastruktura cyfrowa
8. Ścieki
9. Zarządzanie usługami ICT
10. Podmioty publiczne
11. Przestrzeń kosmiczna
12. Usługi pocztowe i kurierskie
13. Gospodarowanie odpadami
14. Produkcja, wytwarzanie i dystrybucja chemikaliów
15. Produkcja, przetwarzanie i dystrybucja żywności
16. Produkcja
17. Dostawcy usług cyfrowych
18. Badania naukowe.

03

NIS2 – 5 zmian kluczowych dla zarządu

1 Samoidentyfikacja

Podmioty kluczowe i ważne będą musiały same zgłaszać się do wykazu podmiotów kluczowych i podmiotów ważnych, co zwiększa ich odpowiedzialność za zgodność z przepisami.

2 Obowiązki kierownictwa

Kierownictwo najwyższego stopnia w firmach ponosi osobistą odpowiedzialność za wykonywanie obowiązków z zakresu cyberbezpieczeństwa. Jest zobowiązane m.in. do:

- zapewnienia systemu zarządzania bezpieczeństwem informacji i zarządzania ryzykiem oraz sprawowania nad tym nadzoru,
- odbywania regularnych szkoleń i zapewnienia odpowiedniego przeszkolenia personelu,
- zabezpieczenia odpowiednich środków finansowych na cele z tym związane,
- właściwego rozdzielania zadań i nadzoru nad ich wykonaniem

3 Zgłaszanie incydentów

NIS2 wprowadza obowiązek zgłaszania incydentów mających poważny wpływ na świadczenie usług już w ciągu 24 godzin od ich wykrycia (wczesne ostrzeżenie), następnie zgłoszenie właściwe w ciągu 72 godz. (24 godz. dla dostawców usług zaufania) oraz sprawozdanie końcowe w ciągu miesiąca od zgłoszenia incydentu. Dodatkowo na wezwanie obowiązkowe jest złożenie także sprawozdania okresowego z obsługi incydentu.

4 Środki bezpieczeństwa

Firmy są zobowiązane do wdrażania środków bezpieczeństwa opartych na przeprowadzonej analizie ryzyka. Oznacza to identyfikację potencjalnych zagrożeń, ocenę ich wpływu oraz wdrożenie adekwatnych środków zapobiegawczych i ochronnych, które minimalizują ryzyko wystąpienia incydentów cybernetycznych.

5 Wyznaczenie osób odpowiedzialnych

Organizacje muszą wyznaczyć odpowiednie osoby do kontaktów i wymiany informacji związanych z cyberbezpieczeństwem. Osoby te będą odpowiedzialne za komunikację z odpowiednimi organami i zespołami reagowania na incydenty (CSIRT), zapewniając szybkie i skuteczne przekazywanie informacji o zagrożeniach i incydentach.

04

Jakie kary wprowadza NIS2?

Za naruszenie przepisów NIS2 grożą kary finansowe. **Podmioty kluczowe mogą zostać ukarane:**

- grzywną **do 10 milionów euro lub do 2% całkowitego rocznego światowego obrotu** uzyskanego w poprzednim roku obrotowym –

w zależności od tego, która z tych wartości jest wyższa.

Podmioty ważne:

- do 7 milionów euro lub do 1,4% całkowitego rocznego światowego obrotu uzyskanego w poprzednim roku obrotowym – w zależności od tego, która z tych wartości jest wyższa. Niezależnie od wymierzenia kary za naruszenia ustawy, organ właściwy może ukarać podmiot kluczowy lub ważny okresową karą pieniężną, jeżeli opóźnia się on z wykonaniem obowiązków nałożonych na niego w ramach czynności nadzorczych lub środków egzekwowania przepisów. Taka kara wynosi od 500 do 100 000 złotych za każdy dzień opóźnienia.

W sytuacji, gdy podmiot kluczowy lub ważny narusza przepisy ustawy, powodując:

- bezpośrednie i poważne cyberzagrożenie dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi,
- zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług,

wówczas może być nałożona kara w wysokości **do 100 000 000 zł.**

Jaką odpowiedzialność ponosi zarząd?

Według nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (UKSC), karze pieniężnej może podlegać kierownik podmiotu kluczowego lub ważnego za niewykonanie wskazanych w ustawie obowiązków, jeżeli przemawia za tym czas, zakres lub charakter naruszenia.

Maksymalna kwota kary

Zwiększeniu ulega również maksymalna kwota kary możliwej do wymierzenia – **do 300%** (a w odniesieniu do podmiotów publicznych – do 100%) otrzymywanego przez kierownika wynagrodzenia, obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop (dotychczasowa kara wynosiła max. 200% miesięcznego wynagrodzenia).

W rażących sytuacjach nieprzestrzeganie przepisów skutkować może nawet zawieszeniem niezbędnych dla prowadzenia działalności certyfikacji, zezwoleń, czy nawet czasowym zakazem sprawowania funkcji zarządczych.

05

NIS2 – obowiązki zarządu

ART. 8C

Odpowiedzialność za cyberbezpieczeństwo

1. Kierownik podmiotu kluczowego lub ważnego jest **odpowiedzialny za wykonywanie obowiązków w zakresie cyberbezpieczeństwa** przez podmiot, obejmujących m.in. zarządzanie systemami bezpieczeństwa informacji oraz raportowanie incydentów.
2. **Odpowiedzialność kolektywna** – w przypadku organu wieloosobowego, wszyscy członkowie ponoszą odpowiedzialność, jeśli nie wskazano jednej osoby odpowiedzialnej.
3. **Delegowanie obowiązków** – kierownik odpowiada również, gdy obowiązki zostały powierzone innej osobie za jej zgodą.

NIS2 – obowiązki zarządu

ART. 8D

Decyzje i zarządzanie bezpieczeństwem informacji

1. Decyzje strategiczne – kierownik podejmuje kluczowe decyzje dotyczące przygotowania, wdrażania, stosowania i przeglądu i nadzorowania systemu zarządzania bezpieczeństwem informacji.
2. Planowanie finansowe – zapewnienie odpowiednich środków finansowych na realizację obowiązków z zakresu cyberbezpieczeństwa.
3. Przydzielanie i nadzór zadań – rozdzielanie zadań związanych z cyberbezpieczeństwem oraz nadzorowanie ich realizacji.
4. Podnoszenie świadomości – zapewnienie, że personel jest świadomy obowiązków oraz przepisów i regulacji wewnętrznych podmiotu dotyczących cyberbezpieczeństwa.
5. Zgodność z przepisami – upewnienie się, że działania podmiotu są zgodne z obowiązującym prawem i wewnętrznymi regulacjami.

NIS2 – obowiązki zarządu

ART. 8E

Szkolenia

Obowiązkowe szkolenia – kierownik podmiotu kluczowego lub podmiotu ważnego oraz osoba, której powierzono obowiązki kierownika w zakresie cyberbezpieczeństwa, musi raz w roku przejść szkolenie z zakresu obowiązków związanych z cyberbezpieczeństwem, a udział w szkoleniu musi być odpowiednio udokumentowany.

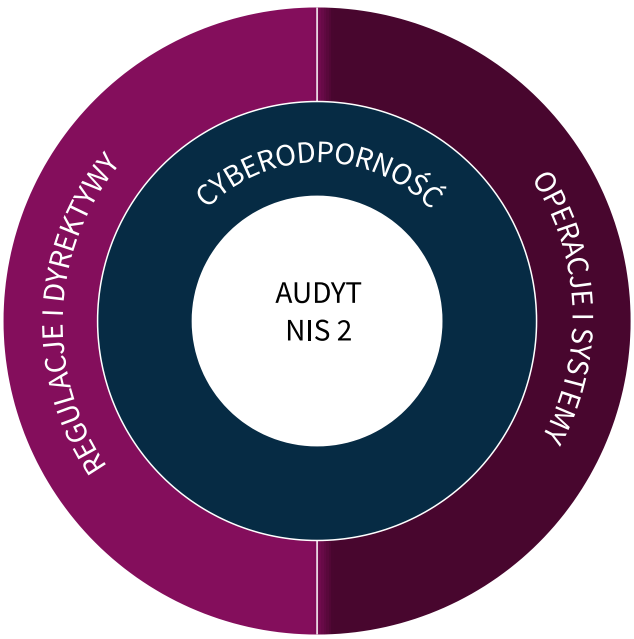
06

Co dalej?

W naszej ocenie znowelizowana ustawa o krajowym systemie cyberbezpieczeństwa prawdopodobnie będzie miała zastosowanie w Państwa przypadku. Sygnalizujemy, że choć ustawa została już podpisana przez Prezydenta RP, to została skierowana do kontroli następczej przez Trybunał Konstytucyjny. Nie wstrzymuje to jednak jej ogłoszenia i wejścia w życie.

Uważamy, że samo wdrożenie przepisów będzie przypominać proces implementacji norm z rodziny ISO, dlatego sugerujemy realizację tego przedsięwzięcia według sprawdzonego schematu:

1. Przeprowadzenie audytu (opcjonalnie).
2. Analiza ryzyka.
3. Opracowanie dokumentacji.
4. Szkolenie personelu i zarządu.



Co dalej?

Wdrożenie NIS2

Jeśli potrzebują Państwo wsparcia w tym procesie, chętnie służymy pomocą. Dysponujemy odpowiednimi kompetencjami i zasobami, aby Państwa w tym wesprzeć. Zapraszamy do zapoznania się z naszą ofertą:

Wdrożenie NIS2

Kontakt

Marcin Kuźniak
tel. +48 690 957 665

Cezary Lutyński
tel. +48 690 957 609

ODO 24 sp. z o.o.
22 740 99 96
oferty@odo24.pl

ul. Kamionkowska 45
03-812 Warszawa
KRS: 0000434350