Knoxtera

CYBERBEZPIECZEŃSTWO
jako odpowiedzialność Zarządu

Praktyczny przewodnik po UKSC i NIS2
dla członków zarządu

Zawartość

Knoxtera

01 Dlaczego ten przewodnik trafia właśnie **do Ciebie**?

Ten materiał powstał z jednego powodu: **nowelizacja Ustawy o Krajowym Systemie Cyberbezpieczeństwa (UKSC) implementująca dyrektywę NIS2** zmienia fundamentalnie, kto odpowiada za cyberbezpieczeństwo w organizacji.
Odpowiedź brzmi: Zarząd.
Nie dział IT. Nie CISO.
Zarząd.

> Art. 20 dyrektywy NIS2 wprost stanowi, że organy zarządzające podmiotów kluczowych i ważnych są zobowiązane do zatwierdzania środków zarządzania ryzykiem cyberbezpieczeństwa i nadzoru nad ich wdrożeniem. Za naruszenie tego obowiązku grozi osobista odpowiedzialność.

Niniejszy przewodnik nie jest opracowaniem prawnym ani technicznym podręcznikiem IT. To praktyczne narzędzie dla osób, które:

- zasiadają w zarządzie organizacji działającej w sektorach objętych NIS2/UKSC,
- chcą zrozumieć swoje obowiązki bez wchodzenia w techniczne szczegóły,
- potrzebują konkretnych pytań, które powinni zadać swojemu CISO lub dyrektorowi IT,
- chcą uniknąć sankcji – finansowych i reputacyjnych.

> *„Zarząd, który traktuje cyberbezpieczeństwo jako kwestię techniczną i deleguje je wyłącznie do IT, naraża organizację – i siebie – na poważne konsekwencje prawne. NIS2 tę odpowiedzialność formalizuje."*

Michał Tomaszewski
CIO
Knoxtera

02 Dwie regulacje – **jeden obowiązek zarządu**

Wiele osób pyta: "**Czy NIS2 i UKSC to to samo?**".

Krótka odpowiedź: nie, ale są ściśle powiązane. Rozumienie tej relacji jest kluczowe dla prawidłowego działania.

NIS2

dyrektywa europejska

NIS2 (Network and Information Security Directive 2) to dyrektywa Unii Europejskiej przyjęta w grudniu 2022 roku. Zastępuje pierwotną dyrektywę NIS z 2016 roku i znacznie rozszerza zakres obowiązków oraz podmiotów nim objętych. Dyrektywa sama w sobie **nie obowiązuje bezpośrednio - musi zostać wdrożona do prawa krajowego** każdego państwa członkowskiego.

UKSC

polska ustawa implementująca NIS2

Ustawa o Krajowym Systemie Cyberbezpieczeństwa (UKSC) to polska ustawa, która wdraża NIS2 do krajowego porządku prawnego. Nowelizacja UKSC weszła w życie 3 kwietnia 2026 roku i **w niektórych obszarach wychodzi poza wymagania dyrektywy**, dostosowując przepisy do specyfiki polskiego sektora publicznego i prywatnego.

> "W mojej praktyce regularnie spotykam zarządy, które słyszały o NIS2, ale nie zdają sobie sprawy, że nowelizacja **UKSC jest już faktem i nakłada konkretne obowiązki z konkretnymi terminami**. **Czas na działanie jest teraz.**"

Kamil Bryłka
Dyrektor Handlowy | Chief Commercial Officer
Knoxtera

	NIS2 (Dyrektywa UE 2022/2555)	**UKSC** (Ustawa o KSC - nowelizacja 2026)
Podstawa prawna	Dyrektywa Parlamentu Europejskiego, wdrożona do prawa krajowego	Polska ustawa o Krajowym Systemie Cyberbezpieczeństwa – nowelizacja implementująca NIS2
Termin obowiązywania	W Polsce od daty wejścia w życie nowelizacji UKSC	Od dnia 03.04.2026
Kto podlega?	Podmioty kluczowe i ważne w 18 sektorach (energia, transport, zdrowie, finanse, IT, woda, infrastruktura cyfrowa i in.)	Te same podmioty co NIS2, plus operatorzy usług kluczowych z dotychczasowego UKSC
Maks. kara finansowa	10 mln EUR lub 2% globalnego obrotu (dla podmiotów kluczowych)	Analogicznie – ustalona w nowelizacji UKSC; dodatkowe kary krajowe nawet do 100 000 000 PLN
Odpowiedzialność osobista zarządu	TAK - art. 20 NIS2: zarząd zatwierdza środki, odpowiada za ich wdrożenie	TAK - przepisy krajowe potwierdzają i rozszerzają tę odpowiedzialność

Oś czasu zmian

Styczeń 2023
NIS 2
Wprowadzony w życie w całej Uni Europejskiej

17 października 2024
Deadline transpozycji
Deadline transpozycji do prawa lokalnego w całej Unii Europejskiej

3 kwietnia 2026
KSC 2.0
Wprowadzenie w życie nowelizacji ustawy o KSC

3 października 2026
Deadline rejestracji
Samookreślenie się i rejestracja organizacji w ramach S46 jako podmioty kluczowe i ważne

3 kwietnia 2027
Deadline implementacyjny
Pełna implementacja w obrębie cyberbezpieczeństwa

3 kwietnia 2028
Pierwsze audyty i kary
Rozpoczęcie pierwszych audytów zgodności z regulacjami i pierwsze możliwe kary dla organizacji niezgodnych z regulacjami.

NIS2 pyta o zarząd, nie o dział IT.
Sprawdź gotowość swojej organizacji.

Wypełnij ankietę »

03 Czy Twoja organizacja **podlega regulacjom?**

NIS2 i UKSC wprowadzają podział na dwie kategorie podmiotów objętych regulacją: podmioty kluczowe (essential entities) i podmioty ważne (important entities). Przynależność do danej kategorii **determinuje zakres obowiązków i wysokość potencjalnych sankcji.**

Podmioty kluczowe (essential entities)

Do podmiotów kluczowych zaliczają się duże organizacje działające w sektorach o wysokim znaczeniu:

- **energia,**
- **transport,**
- **bankowość,**
- **woda pitna,**
- **ścieki,**
- **usługi ICT B2B,**
- **administracja publiczna**
- **infrastruktura rynków finansowych,**
- **ochrona zdrowia,**
- **infrastruktura cyfrowa,**
- **przestrzeń kosmiczna.**

Podmioty ważne

Podmioty ważne to średnie organizacje z sektorów kluczowych oraz podmioty średnie i duże z dodatkowych sektorów:

- **wybrana produkcja (wyroby medyczne, maszyny, pojazdy, elektronika),**
- **dostawcy usług cyfrowych,**
- **organizacje badawcze,**
- **usługi pocztowe i kurierskie,**
- **zarządzanie odpadami**
- **produkcja i dystrybucja chemikaliów**
- **produkcja i dystrybucja żywności.**

DOBRA PRAKTYKA

Nawet jeśli Twoja organizacja nie spełnia bezpośrednio kryteriów podmiotu kluczowego lub ważnego, może podlegać wymaganiom pośrednio – jako dostawca usług dla podmiotów objętych NIS2/UKSC. Warto to zweryfikować.

Dodatkowo, niektóre podmioty niezależnie od swojej wielkości mogą być traktowane jako podmioty ważne lub kluczowe.

Szybka checklista dla Zarządów

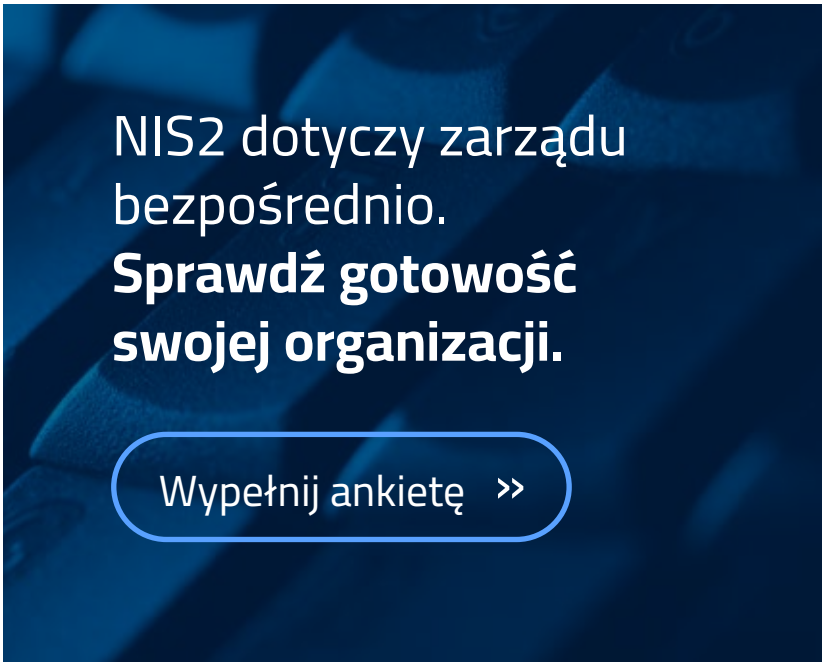
Skorzystaj z poniższej tabeli, aby wstępnie ocenić, **czy Twoja organizacja podlega regulacjom**:

NIS2 (Dyrektywa UE 2022/2555)	Pytanie sprawdzające	Dotyczy mnie?
Sektor działalności	Czy Twoja organizacja działa w jednym z 18 sektorów NIS2/UKSC? (energia, transport, bankowość, infrastruktura rynków finansowych, ochrona zdrowia, woda pitna, ścieki, infrastruktura cyfrowa, usługi ICT, administracja publiczna, przestrzeń kosmiczna, usługi pocztowe, zarządzanie odpadami, chemia, żywność, produkcja, dostawcy cyfrowi, badania)	TAK | NIE
Wielkość organizacji	Jesteś średnim przedsiębiorcą w rozumieniu przepisów lub przewyższasz progi dla średniego przedsiębiorcy?	TAK | NIE
Infrastruktura krytyczna	Czy Twoja organizacja dostarcza usługi uznane za krytyczne dla funkcjonowania państwa lub społeczeństwa?	TAK | NIE
Łańcuch dostaw	Czy jesteś dostawcą lub podwykonawcą dla podmiotów podlegających NIS2/UKSC?	TAK | NIE
Dotychczasowy OUK/DSP	Czy Twoja organizacja była już wcześniej zidentyfikowana jako Operator Usług Kluczowych lub Dostawca Usług Cyfrowych?	TAK | NIE

Jeśli wśród Twoich odpowiedzi znalazły się odpowiedzi "TAK" - Warto przeprowadzić dokładniejszą analizę aby potwierdzić czy Twoja organizacja podlega regulacjom. Jeśli chcesz sprawdzić dokładniej wypełnij ankietę gotowości na NIS2.

> "Przeprowadziliśmy w ciągu ostatniego roku kilkanaście projektów identyfikacji podmiotowości NIS2. **Przynajmniej w jednej trzeciej przypadków organizacja była przekonana, że regulacje jej nie dotyczą – i się myliła**. Autoidentyfikacja na podstawie checklisty to absolutne minimum."

Michał Tomaszewski
CIO
Knoxtera



04 Co Zarząd musi zrobić **osobiście?**

To jest serce tego przewodnika. NIS2 - a za nią UKSC - precyzyjnie określają, czego przepisy oczekują od organu zarządzającego (zarządu, rady dyrektorów). **Poniżej omawiamy pięć kluczowych obszarów**.

Zatwierdzenie polityki zarządzania ryzykiem cyberbezpieczeństwa

Zarząd jest zobowiązany do **formalnego zatwierdzenia polityki zarządzania ryzykiem cyberbezpieczeństwa**. Oznacza to, że polityka musi:

- zostać przedstawiona zarządowi **w zrozumiałej formie**,
- być **zatwierdzona uchwałą** lub innym formalnym dokumentem,
- być regularnie przeglądana – **co najmniej raz w roku** lub po istotnych zmianach lub incydentach,
- obejmować **ocenę ryzyka dla łańcucha dostaw**, nie tylko wewnętrznych systemów.

> Podpisanie polityki bezpieczeństwa przez CISO lub dyrektora IT NIE jest wystarczające. **Wymogiem jest zatwierdzenie przez organ zarządzający – czyli zarząd.**

Obowiązkowe szkolenia dla zarządu

NIS2 wprowadza bezprecedensowy wymóg: **szkolenia z cyberbezpieczeństwa są obowiązkowe nie tylko dla pracowników IT, ale dla samych członków zarządu**. Celem nie jest wiedza techniczna, lecz zdolność do oceny ryzyk i podejmowania decyzji.

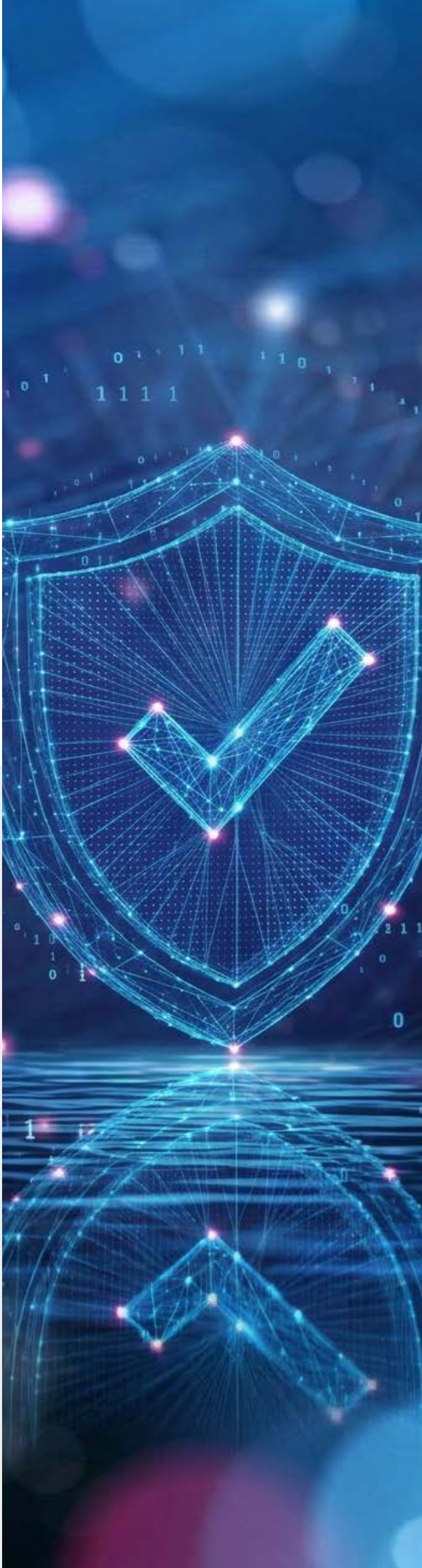
Rekomendujemy szkolenia, które obejmują:

- **zrozumienie krajobrazu zagrożeń i trendów** w cyberprzestępczości,
- **znajomość obowiązków** wynikających z NIS2 i UKSC,
- **umiejętność oceny** raportów bezpieczeństwa i **zadawania właściwych pytań**,
- **procedury postępowania** w przypadku poważnego incydentu cybernetycznego.
- Dodatkowo Zarząd musi być **cyklicznie szkolony z wymagań, jakie NIS2 oraz UKSC** nakładają na podmioty podlegające. Celem tych szkoleń jest uświadomienie Zarządom jakie obowiązki ustawowe na nich spoczywają oraz jaka jest ich rola w procesie zarządzania bezpieczeństwem IT.

Nadzór nad wdrożeniem i raportowanie do zarządu

Zarząd nie może jednorazowo zatwierdzić polityki i zapomnieć o temacie. NIS2 wymaga ciągłego nadzoru, co w praktyce oznacza:

- regularne (**rekomendujemy raz na kwartał**) raporty bezpieczeństwa dla zarządu,
- wskaźniki KPI pozwalające **ocenić stan bezpieczeństwa bez wiedzy technicznej**,
- formalny punkt **"cyberbezpieczeństwo" w agendzie posiedzeń** zarządu,
- **dokumentowanie decyzji zarządu dotyczących akceptacji lub ograniczania ryzyk**.



Zarządzanie incydentami - rola zarządu

W przypadku poważnego incydentu cybernetycznego **zarząd powinien być włączony w proces reagowania**. Zgodnie z NIS2 i UKSC:

- poważne incydenty **muszą być zgłoszone do właściwego CSIRT w ciągu 24 godzin** (wczesne ostrzeżenie),
- pełne zgłoszenie następuje **w ciągu 72 godzin**,
- przygotowanie sprawozdania końcowego **nie później niż miesiąc po zgłoszeniu** incydentu
- **zarząd powinien być poinformowany o incydencie natychmiast** - przed zgłoszeniem do regulatora,
- w przypadku incydentów o krytycznym wpływie na działalność, zarząd podejmuje decyzje o eskalacji i komunikacji zewnętrznej.

> Brak zgłoszenia incydentu w terminie lub błędy w zgłoszeniu **mogą skutkować oddzielnymi sankcjami**, niezależnymi od sankcji za samo naruszenie bezpieczeństwa.

Bezpieczeństwo łańcucha dostaw

NIS2 i UKSC **rozszerzają odpowiedzialność organizacji na jej dostawców i podwykonawców**. Zarząd jest odpowiedzialny za zapewnienie, że organizacja:

- **identyfikuje kluczowych dostawców IT i OT,**
- **ocenia ryzyko** związane z każdym z nich,
- **wdraża wymagania** bezpieczeństwa w umowach z dostawcami,
- **regularnie weryfikuje** zgodność dostawców z wymaganiami.

> "Widzę zarządy, które zainwestowały miliony we własne systemy bezpieczeństwa, a zostały sparaliżowane przez lukę u małego dostawcy oprogramowania. NIS2 słusznie wymusza spojrzenie na bezpieczeństwo całego ekosystemu, nie tylko własnej organizacji."

Kamil Bryłka
Dyrektor Handlowy | CCO
Knoxtera

Budżet i zasoby

Przepisy nie pozostawiają wątpliwości: to **organ zarządzający odpowiada za zapewnienie organizacji zasobów adekwatnych do zidentyfikowanych ryzyk**. Cyberbezpieczeństwo przestaje być pozycją "do negocjacji" w budżecie IT - staje się obowiązkiem ustawowym zarządu. W praktyce oznacza to, że zarząd powinien:

- **zatwierdzać budżet** na cyberbezpieczeństwo w powiązaniu z wynikami oceny ryzyka - a nie jako stały procent budżetu IT,
- zapewniać zasoby rozumiane szeroko: nie tylko środki finansowe, ale także **kompetencje, liczebność zespołu i narzędzia**,
- weryfikować, **czy planowane wydatki pokrywają wszystkie obszary** wymagane przez NIS2 i UKSC (m.in. zarządzanie incydentami, ciągłość działania, łańcuch dostaw, szkolenia),
- **dokumentować decyzje budżetowe** - w tym decyzje o odroczeniu lub ograniczeniu wydatków na bezpieczeństwo.
- regularnie **weryfikować zgodność dostawców** z wymaganiami.

Przydzielanie ról w obszarze cyberbezpieczeństwa

Skuteczny nadzór wymaga jasnej struktury odpowiedzialności. NIS2 i UKSC oczekują, że w organizacji nie będzie wątpliwości, kto za co odpowiada - **od poziomu operacyjnego po zarząd**. Do obowiązków zarządu należy zapewnienie, że:

- wyznaczona jest **osoba odpowiedzialna za obszar cyberbezpieczeństwa** (CISO lub funkcja równoważna) z jasno określonym mandatem, zakresem decyzyjności i linią raportowania,
- **role są rozdzielone zgodnie z zasadą separacji obowiązków** - osoba wdrażająca zabezpieczenia nie powinna być jedyną osobą oceniającą ich skuteczność,
- **wyznaczona jest osoba do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa** (w tym właściwym CSIRT), wraz z zastępstwem na wypadek jej nieobecności,
- **odpowiedzialność** za cyberbezpieczeństwo powinna być **przypisana konkretnemu członkowi zarządu** w ramach podziału kompetencji - tak, aby temat miał swojego "właściciela" na najwyższym poziomie organizacji.

Przydzielenie ról i delegowanie zadań NIE zwalnia zarządu z odpowiedzialności.
NIS2 wprost wskazuje, że odpowiedzialność organu zarządzającego za zatwierdzenie środków i nadzór nad ich wdrażaniem nie podlega pełnej delegacji - można delegować wykonanie, nie można delegować odpowiedzialności.

05 Ryzyko i sankcje - co realnie grozi

Regulacje NIS2 i UKSC wprowadzają jeden z najbardziej rygorystycznych reżimów sankcyjnych w obszarze cyberbezpieczeństwa w historii prawa europejskiego. Poniżej zestawienie kluczowych konsekwencji.

Rodzaj sankcji	Podmioty kluczowe	Podmioty ważne	Kogo dotyczy
Kara administracyjna	Do 10 mln EUR lub 2% globalnego obrotu (wyższa kwota)	Do 7 mln EUR lub 1,4% globalnego obrotu	Organizacja
Odpowiedzialność osobista	Zakaz pełnienia funkcji kierowniczych przez określony czas	Nie przewidziano wprost	Członkowie zarządu, dyrektor generalny
Zawieszenie działalności	Tymczasowe zawieszenie certyfikatów lub zezwoleń	Nie przewidziano wprost	Organizacja
Publiczne ogłoszenie naruszenia	TAK – organy nadzorcze mogą opublikować informację	TAK	Organizacja (ryzyko reputacyjne)
Kara finansowa nakładana na poszczególne osoby zarządzające	Do 300% miesięcznego uposażenia przedstawiciela kierownictwa	Do 300% miesięcznego uposażenia przedstawiciela kierownictwa	Członkowie zarządu, dyrektor generalny

Odpowiedzialność osobista - co to oznacza w praktyce?

Dla zarządu szczególnie istotny jest mechanizm odpowiedzialności osobistej przewidziany w NIS2. Organ nadzorczy może:

- **tymczasowo zawiesić możliwość pełnienia funkcji kierowniczych** przez konkretną osobę (np. prezesa lub członka zarządu),
- **publicznie wskazać osobę odpowiedzialną** za naruszenie przepisów,
- **nakazać organizacji publiczne ogłoszenie naruszenia i jego skutków.**

Odpowiedzialność osobista dotyczy konkretnych osób - nie tylko organizacji jako całości. Oznacza to, że niewiedza nie stanowi wystarczającego usprawiedliwienia. NIS2 nakłada obowiązek aktywnego nadzoru.

Ryzyko reputacyjne

Obok sankcji finansowych i prawnych, NIS2 przewiduje obowiązkowe mechanizmy transparentności. Organy nadzorcze mogą opublikować informacje o naruszeniu, co w praktyce oznacza:

- **utratę zaufania klientów** i partnerów biznesowych,
- **negatywne konsekwencje dla wartości rynkowej** i pozycji w przetargach publicznych,
- **presję inwestorską** i pytania ze strony akcjonariuszy.

> „Z perspektywy lat doradztwa widzę, że dla większości zarządów to nie kara finansowa jest największym strachem – **to publiczne ogłoszenie naruszenia.** Jeden artykuł w branżowym medium potrafi zniszczyć relacje budowane latami."

Michał Tomaszewski
CIO
Knoxtera

NIS2 dotyczy zarządu bezpośrednio.
Sprawdź gotowość swojej organizacji.

Wypełnij ankietę »

06 Plan działania w 5 krokach

Poniższy plan jest adresowany do zarządu, który chce systematycznie wdrożyć wymagania NIS2 i UKSC. To nie jest lista zadań dla działu IT - **to mapa decyzji, które zarząd musi podjąć** i których wdrożenie musi nadzorować.

Krok 1

Oceń swoją sytuację wyjściową

Zarząd powinien zlecić przeprowadzenie formalnej analizy luk (gap analysis), która odpowie na pytania:

- **Czy i w jakiej kategorii** podlegamy NIS2/UKSC?
- Jakie wymagania już spełniamy, a **czego brakuje**?
- Jakie są nasze **najpoważniejsze luki** bezpieczeństwa?

Wynik gap analysis powinien zostać formalnie przedstawiony zarządowi - nie jako raport techniczny, ale jako ocena ryzyka biznesowego i prawnego.

Krok 2

Powołaj odpowiedzialnych i sformalizuj nadzór

Zarząd powinien formalnie:

- **wyznaczyć lub potwierdzić osobę odpowiedzialną** za cyberbezpieczeństwo (CISO lub ekwiwalent),
- **ustalić cykl raportowania** bezpieczeństwa do zarządu,
- wprowadzić punkt **„cyberbezpieczeństwo" do agendy posiedzeń** zarządu,
- rozważyć powołanie komitetu ds. ryzyka.

Krok 3

Zatwierdź i wdróż SZBI

(system zarządzania bezpieczeństwem informacji)

Wdrożenie SZBI w zakresie i formie, które wynikają z posiadanych ryzyk, a w szczególności SZBI powinien co najmniej składać się z polityki ryzyka, zarządzania incydentami i zarządzania dostawcami.

Na podstawie gap analysis należy opracować i formalnie zatwierdzić uchwałą zarządu:

- **Politykę zarządzania ryzykiem** cyberbezpieczeństwa,
- **Politykę zgłaszania i reagowania** na incydenty,
- **Wymagania bezpieczeństwa** dla dostawców i podwykonawców.

Krok 4

Wdróż monitoring i procedury zgłaszania incydentów

Zarząd powinien zapewnić, że organizacja dysponuje:

- **ciągłym monitoringiem bezpieczeństwa** (na przykład SOC lub usługą MDR/SOC-as-a-Service),
- **procedurą klasyfikacji incydentów** - kto decyduje, że incydent jest „poważny" i wymaga zgłoszenia do CSIRT,
- **gotowym szablonem zgłoszenia incydentu** - dostosowanym do wymagań właściwy CSIRT sektorowy,
- testem tej procedury - **co najmniej jednym ćwiczeniem w roku.**

Krok 5

Weryfikuj dostawców i aktualizuj ocenę ryzyka

Bezpieczeństwo łańcucha dostaw to nie jednorazowe zadanie. Zarząd powinien zapewnić:

- **roczny przegląd rejestru kluczowych dostawców IT i OT,**
- włączenie wymagań NIS2/UKSC **do nowych umów z dostawcami,**
- renegocjację istniejących umów z kluczowymi dostawcami,
- **procedurę weryfikacji zgodności dostawców** z deklarowanymi standardami.

DOBRA PRAKTYKA

Wszystkie pięć kroków powinno być udokumentowane. W razie kontroli organu nadzorczego lub dochodzenia po incydencie, dokumentacja decyzji zarządu jest kluczowym dowodem na zachowanie należytej staranności.

07 **Pytania,** które zarząd powinien **zadać swojemu IT / CISO**

Jedną z kluczowych kompetencji zarządu w obszarze cyberbezpieczeństwa jest umiejętność zadawania właściwych pytań – i egzekwowania konkretnych odpowiedzi. Poniżej zestaw pytań, które warto zadać na najbliższym posiedzeniu zarządu lub spotkaniu z CISO.

Obszar	Pytanie dla CISO / dyrektora IT	Oczekiwana odpowiedź / dowód
Ocena gotowości	Czy przeprowadziliśmy formalną analizę luk (gap analysis) pod kątem NIS2/UKSC?	Raport z gap analysis lub harmonogram jego wykonania
Polityki bezpieczeństwa	Czy mamy zatwierdzone przeze mnie (zarząd) polityki bezpieczeństwa informacji?	Dokument polityki z podpisem zarządu i datą
Zgłaszanie incydentów	Jaka jest nasza procedura zgłoszenia incydentu w ciągu 24 godzin? Kto konkretnie ją uruchamia?	Procedura IR z przypisanymi rolami i numerami kontaktowymi
Łańcuch dostaw	Czy zidentyfikowaliśmy i oceniliśmy ryzyko u naszych kluczowych dostawców IT/OT?	Rejestr dostawców z oceną ryzyka
Szkolenia zarządu	Kiedy odbyło się ostatnie szkolenie z cyberbezpieczeństwa dla zarządu?	Harmonogram szkoleń i certyfikaty ukończenia
Testy odporności	Kiedy ostatnio testowaliśmy zdolność do odtworzenia działalności po cyberataku?	Raport z ćwiczenia / testu BCP/DR
Monitoring	Czy mamy ciągły monitoring bezpieczeństwa (SOC lub MDR) 24/7?	Umowa z dostawcą lub opis własnych zasobów
Budżet	Czy budżet na cyberbezpieczeństwo odzwierciedla nowe wymogi regulacyjne?	Porównanie budżetu bieżącego z szacunkiem kosztów compliance

Jak ocenić odpowiedź?

Dobra odpowiedź jest konkretna: **zawiera datę, dokument lub osobę odpowiedzialną**. Jeśli odpowiedź brzmi "pracujemy nad tym" lub "mamy to w planach" - zapytaj o termin i osobę odpowiedzialną. Jeśli nie wiesz, jak ocenić odpowiedź techniczną - możesz poprosić o zewnętrzną niezależną opinię.

Korzyści z bycia organizacją zgodną z UKSC i NIS2

Wokół UKSC i NIS2 dominuje język obowiązku i ryzyka. To perspektywa uzasadniona, ale niepełna – świadome wdrożenie wymogów nie jest wyłącznie kosztem zgodności, lecz inwestycją zwracającą się w obszarach istotnych dla zarządu niezależnie od samej regulacji.

Przewaga konkurencyjna

Klienci, zwłaszcza w sektorach regulowanych, coraz częściej oceniają dostawców nie tylko przez pryzmat ceny i jakości, ale także poziomu zabezpieczeń i zgodności z prawem. NIS2 dodatkowo zobowiązuje objęte podmioty do weryfikacji swoich dostawców, więc dojrzałość w tym obszarze czyni organizację partnerem niższego ryzyka i mocniejszym kandydatem w przetargach. Zgodność przestaje być kosztem, a staje się argumentem sprzedażowym.

Uporządkowanie procesów

Droga do zgodności wymusza inwentaryzację zasobów, mapowanie procesów i jednoznaczne przypisanie odpowiedzialności. Ten wysiłek niemal zawsze ujawnia obszary wcześniej nieuporządkowane, dając realne uporządkowanie i optymalizację procesów wewnętrznych – wartość działającą niezależnie od kontekstu regulacyjnego.

Ochrona wartości i ciągłość działania

Sednem obu regulacji jest ochrona tego, co najcenniejsze: danych, reputacji i zdolności do nieprzerwanego świadczenia usług. Wymóg planowania ciągłości działania (BCP) oznacza przygotowanie na sytuacje kryzysowe, zanim wystąpią, a w efekcie wymierne ograniczenie ryzyka kosztownych przestojów.

08 Jak Knoxtera pomaga zarządom?

Knoxtera to firma specjalizująca się w cyberbezpieczeństwie w modelu always-on, ciągłego, czynnego wsparcia dla organizacji, które traktują bezpieczeństwo jako element strategii biznesowej, nie tylko techniczny obowiązek.

Dla zarządów i organizacji stojących przed wdrożeniem NIS2/UKSC oferujemy:

Warsztaty dla zarządu (Board-Level Cyber Awareness)

Dedykowane, 4-godzinne sesje przygotowane specjalnie dla członków zarządu. **Bez technicznego żargonu.** Z konkretnymi scenariuszami z polskiego rynku. **Zakończone certyfikatem** potwierdzającym odbycie szkolenia wymaganego przez NIS2.

Analiza luk (NIS2/UKSC Gap Analysis)

Kompleksowa analiza gotowości organizacji na wymagania regulacyjne. Raport przedstawiany zarządowi w formie mapy ryzyk i priorytetowego planu działań. **Realizowana w ciągu 4–6 tygodni.**

Always-on Security Monitoring (SOC-as-a-Service)

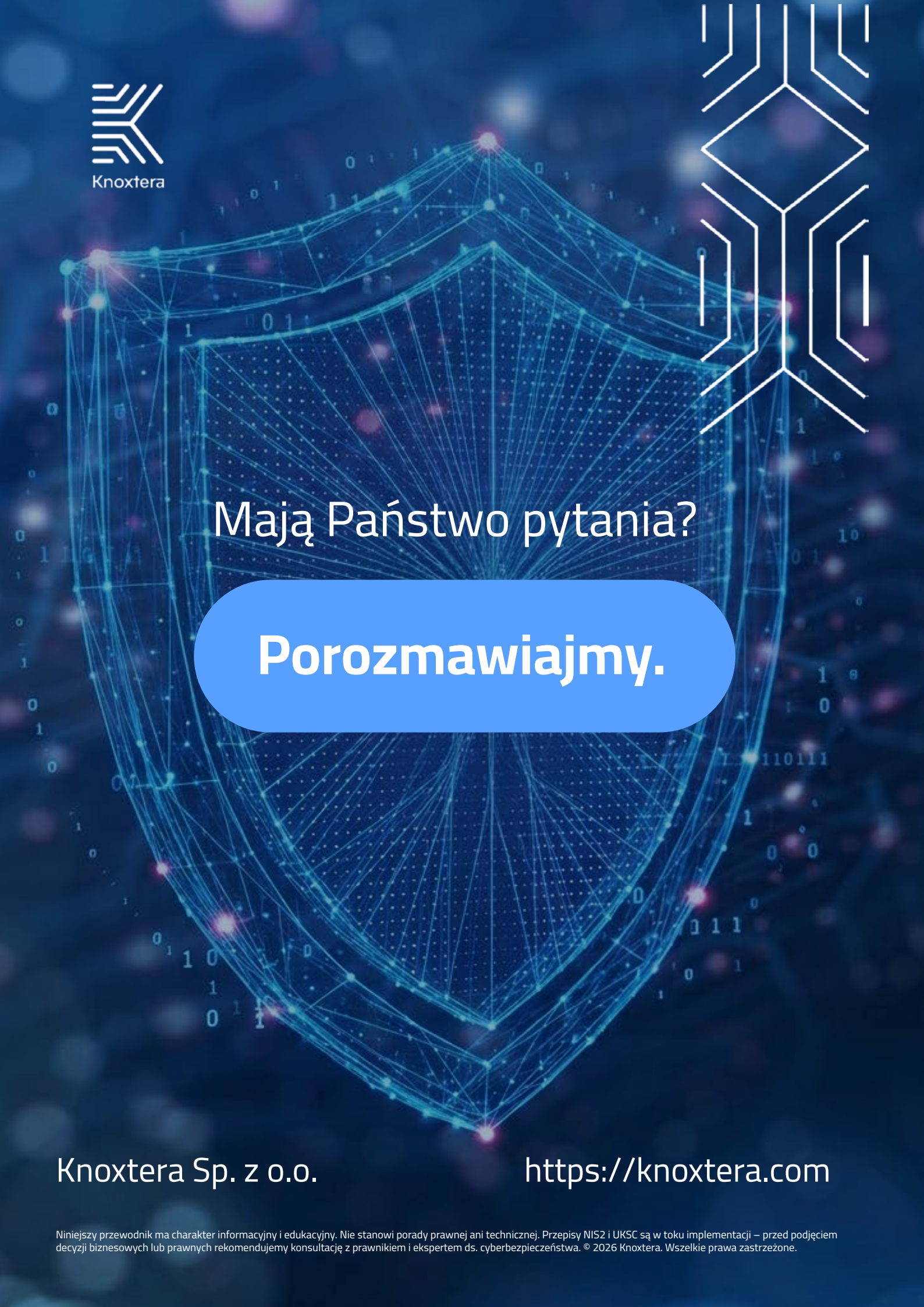
Ciągły monitoring bezpieczeństwa 24/7, który zapewnia zarządowi pewność, że w każdej chwili ktoś czuwa nad bezpieczeństwem organizacji. Włącza procedurę zgłaszania incydentów zgodną z NIS2/UKSC.

Compliance Advisory i wsparcie przy wdrożeniu

Doradztwo od identyfikacji podmiotowości, przez opracowanie polityk, po wdrożenie techniczno-organizacyjne. **Knoxtera towarzyszy organizacji na każdym etapie – od diagnozy do certyfikacji.**

DOBRA PRAKTYKA

Pierwsze spotkanie konsultacyjne jest bezpłatne. Podczas 60-minutowej rozmowy z ekspertem Knoxtery dowiesz się, czy i w jakim zakresie Twoja organizacja podlega NIS2/UKSC oraz jakie są Twoje priorytety.



Niniejszy przewodnik ma charakter informacyjny i edukacyjny. Nie stanowi porady prawnej ani technicznej. Przepisy NIS2 i UKSC są w toku implementacji – przed podjęciem decyzji biznesowych lub prawnych rekomendujemy konsultację z prawnikiem i ekspertem ds. cyberbezpieczeństwa. © 2026 Knoxtera. Wszelkie prawa zastrzeżone.