XOPERO
Backup&Recovery

NIS2 w pigułce

Przygotuj się na nadchodzące zmiany z Xopero

O wymaganiach, obowiązkach i wpływie NIS2
na organizacje w sektorach kluczowych



NIS2 to dyrektywa Parlamentu Europejskiego i Rady (UE 2016/1148), która podnosi wspólny poziom cyberbezpieczeństwa organizacji działających w kluczowych sektorach gospodarki europejskiej.

Dyrektywa ujednolica też minimalne standardy bezpieczeństwa w państwach członkowskich.

Wdrożenie NIS2 wiąże się z jasnym podziałem odpowiedzialności, przeglądem architektury bezpieczeństwa, reakcji na incydenty, ciągłości działania i bezpieczeństwa dostawców oraz uporządkowaniem systemów.

Jak przebiega wdrożenie NIS2 w Polsce?

Październik 2024

Państwa członkowskie miały zacząć stosować wymagania NIS2. **Polska nie dotrzymała terminu.**

19 lutego 2026

Prezydent podpisał nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), która wdraża NIS2. Jednocześnie skierował ją w trybie kontroli następczej do Trybunału Konstytucyjnego.

3 kwietnia 2026

Termin wejścia w życie regulacji.

Sprawdź, czy Twoja organizacja podlega NIS2

Jeśli Twoja organizacja należy do jednej z poniższych grup, musi się dostosować do wymogów NIS2 i znowelizowanej ustawy o KSC oraz obowiązkowo złożyć wniosek o wpis do wykazu podmiotów kluczowych i podmiotów ważnych do 3 października 2026 r.



Podmioty kluczowe ↓



Podmioty ważne



Wyjątki

>250
pracowników

>50 mln EUR
obrót roczny

Branże:

- energetyka
- transport
- brankowość
- finanse
- ochrona zdrowia
- zaopatrzenie w wodę
- odprowadzanie ścieków
- infrastruktura cyfrowa
- zarządzanie usługami informatycznymi i telekomunikacyjnymi (ICT)
- przemysł kosmiczny
- administracja

Sprawdź, czy Twoja organizacja podlega NIS2

Jeśli Twoja organizacja należy do jednej z poniższych grup, musi się dostosować do wymogów NIS2 i znowelizowanej ustawy o KSC oraz obowiązkowo złożyć wniosek o wpis do wykazu podmiotów kluczowych i podmiotów ważnych do 3 października 2026 r.



Podmioty kluczowe



Podmioty ważne ↓



Wyjątki

>50
pracowników

>10 mln EUR
obrót roczny

Branże:

- usługi pocztowe i kurierskie
- gospodarowanie odpadami
- badania naukowe
- dostawcy usług cyfrowych
- produkcja wytwarzanie i dystrybucja chemikaliów

w tym produkcja:

- produkcja, wytwarzanie i dystrybucja żywności
- wyrobów medycznych
- komputerów
- elektroniki
- urządzeń elektrycznych
- urządzeń optycznych
- maszyn i urządzeń
- samochodów, przyczep i pozostałego sprzętu transportowego

Sprawdź, czy Twoja organizacja podlega NIS2

Jeśli Twoja organizacja należy do jednej z poniższych grup, musi się dostosować do wymogów NIS2 i znowelizowanej ustawy o KSC oraz obowiązkowo złożyć wniosek o wpis do wykazu podmiotów kluczowych i podmiotów ważnych do 3 października 2026 r.



Podmioty kluczowe



Podmioty ważne



Wyjątki ↓

<50
pracowników

<10 mln EUR
obrót roczny

Działają w jednym z sektorów kluczowych lub ważnych oraz:

- świadczą usługi o znaczeniu krytycznym,
- są jedynymi dostawcami w kraju,
- mają znaczenie dla bezpieczeństwa publicznego,
- należą do łańcucha dostaw podmiotu kluczowego lub ważnego,
- decyzją Ministerstwa Cyfryzacji zostały uznane za podmiot kluczowy lub ważny.

Wymagane środki i działania

Zarządzanie ryzykiem

- Wprowadzenie polityk i procedur służących ocenie skuteczności środków zarządzania ryzykiem.
- Przygotowanie organizacji do zbierania informacji o cyberzagrożeniach i podatnościach oraz do obsługi incydentów.

Tworzenie polityk bezpieczeństwa

- Opracowanie i wdrożenie polityki bezpieczeństwa systemu informacyjnego oraz metodyki szacowania ryzyka.
- Opracowanie i wdrożenie dokumentacji dotyczącej bezpieczeństwa łańcucha dostaw, w tym polityk bezpieczeństwa stron trzecich.
- Wprowadzenie polityk i procedur stosowania kryptografii.

Raportowanie incydentów

- Opracowanie i wdrożenie procesu zarządzania incydentami i innych polityk tematycznych.

Wdrożenie zabezpieczeń technicznych i organizacyjnych

- Opracowanie i wdrożenie planów działania oraz polityk awaryjnych umożliwiających ciągłe i niezakłócone świadczenie usługi, np. wykorzystaniem rozwiązania do backupu i przywracania danych.
- Zapewnienie bezpieczeństwa w procesie nabywania, rozwoju i utrzymania sieci oraz systemów.
- Monitorowanie bezpieczeństwa systemów teleinformatycznych w trybie ciągłym.



Szczegółową listę środków i działań wskazanych na etapie wdrożenia i po wdrożeniu wymogów NIS2 wraz z listą kontrolną znajdziesz na naszym blogu:

NIS2 w praktyce

Kary i odpowiedzialność za brak zgodności



Podstawy sankcji

Sankcje grożą m.in za brak adekwatnych zabezpieczeń, zaniedbania w zarządzaniu ryzykiem lub nieterminowe raportowanie incydentów.



Podmioty kluczowe

Maksymalne kary dla podmiotów kluczowych to 10 mln EUR lub 2% ich całkowitego rocznego światowego obrotu.



Podmioty ważne

Dla podmiotów ważnych maksymalna kara to 7 milionów EUR lub 1,4% ich całkowitego rocznego światowego obrotu.



Kara dzienna

Niezależnie od limitów za niezastosowanie się do nakazu organu cyberbezpieczeństwa będzie grozić kara od 500 zł do 100 tys. zł za każdy dzień opóźnienia.



Kadra kierownicza

Przy rażących naruszeniach przewidziano kary finansowe dla kadry kierowniczej, a także możliwość nałożenia czasowego zakazu pełnienia funkcji na członków zarządu.



Odroczenie kar

Kary pieniężne za brak realizacji obowiązków wynikających z ustawy o KSC będą nakładane dopiero po 2 latach od wejścia w życie nowelizacji.



Jak Xopero wspiera zgodność z wymaganiami NIS2?

Xopero oferuje **zaawansowane rozwiązania klasy enterprise i disaster recovery**, które wspierają spełnienie wymogów NIS2 w zakresie ciągłości działania i zarządzania kryzysowego.

Zarządzanie backupem



Wdrożenie rozwiązania do tworzenia i przywracania kopii zapasowych

Xopero dostarcza kompletny mechanizm backupu i odtwarzania jako centralny filar ciągłości działania. Umożliwia przywrócenie danych i środowisk po awarii lub ataku.

Pomocne funkcjonalności:

- ✓ Kompleksowy backup dowolnej infrastruktury
- ✓ Centralne zarządzanie (konsola webowa)
- ✓ Zautomatyzowane kopie oparte na politykach
- ✓ Retencja i wersjonowanie
- ✓ Kompresja i globalna deduplikacja na źródle



Regularne wykonywanie kopii i ich bezpieczne przechowywanie poza infrastrukturą

Xopero ułatwia strategię wielu kopii w niezależnych lokalizacjach i ogranicza ryzyko, że atak zaszyfruje lub usunie kopie zapasowe. Wspiera odporność na ransomware i scenariusze “najgorszego dnia”.

Pomocne funkcjonalności:

- ✓ Multi-storage i plany replikacji do niezależnych magazynów
- ✓ Replikacja i georedundancja danych
- ✓ Immutable storage
- ✓ Air Gap backup (izolacja)
- ✓ Format kopii ograniczający możliwość uruchomienia złośliwego kodu
- ✓ Ograniczony dostęp do danych uwierzytelniających magazynu

Odzyskiwanie danych



Testowanie przywracania danych z kopii zapasowej

Xopero wspiera udokumentowaną gotowość odtworzeniową. Planujesz testy, mierzysz parametry i masz dowód, że odtwarzanie działa.

Pomocne funkcjonalności:

- ✓ Kontrolowane próby odtwarzania (test restore)
- ✓ Pomiar RTO i RPO
- ✓ Raporty na potrzeby audytu i kontroli



Przywrócenie normalnego działania po awarii lub incydencie

Skraca czas powrotu do pracy, ponieważ oferuje kilka trybów odtwarzania, od selektywnego przywracania po scenariusze DR. Możesz odtworzyć dane elastycznie, także przy zmianie środowiska.

Pomocne funkcjonalności:

- ✓ Odtwarzanie danych między różnymi systemami
- ✓ (nawet o innych parametrach)
- ✓ Uruchomienie VM z kopii
- ✓ Granularne przywracanie
- ✓ Mechanizmy automatycznej odbudowy po awarii
- ✓ Zdalny Bare Metal Restore
- ✓ Opcja szybkiego odtwarzania systemów ICS/OT

Przygotowanie polityk i procedur



Polityki i procedury oceny skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie

Xopero dostarcza dane i ślad audytowy do wskaźników (KPI) w obszarze ochrony danych, np. pokrycie backupem, skuteczność zadań, wyniki testów odtworzenia, czasy RTO/RPO. To ułatwia przeglądy i utrzymanie kontroli.

Pomocne funkcjonalności:

- ✓ Zaawansowany monitoring
- ✓ Zaawansowane logi i powiadomienia (e-mail, Slack i integracje za pośrednictwem webhooków)
- ✓ Wizualne statystyki i dashboardy



Polityki i procedury stosowania kryptografii i szyfrowania

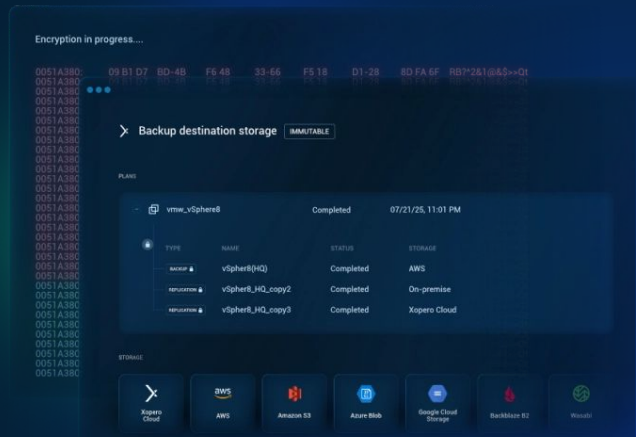
Xopero wspiera szyfrowanie kopii i ogranicza ryzyko przejęcia danych z backupu.

Pomocne funkcjonalności:

- ✓ Kompresja i szyfrowanie danych w procesie tworzenia kopii
- ✓ Format kopii ograniczający możliwość uruchomienia złośliwego kodu (niewykonywalne pliki)

XOPERO
Backup&Recovery

Atuty Xopero to poufność i integralność



Nie ograniczamy bezpieczeństwa jedynie do uprawnień użytkowników. **Stosujemy politykę Zero Trust** także w zakresie przechowywania danych, umożliwiając dostęp do danych wyłącznie na podstawie żądań agenta backupu podczas tworzenia kopii zapasowych, replikacji lub odzyskiwania.

Gwarantujemy integralność kopii bez stosowania dodatkowych warstw sprzętowych. **Nasze rozwiązania zabezpieczają dane już od pierwszej kopii sprawiając, że dane są niezmienne.**

Stosujemy szyfrowanie w całym procesie tworzenia kopii (AES-256 „in-flight" i „at-rest"). Oferujemy także możliwość stworzenia własnego klucza szyfrującego, który wykorzystywany jest wyłącznie na czas wykonywania kopii i uniemożliwia jej odszyfrowanie osobom trzecim.

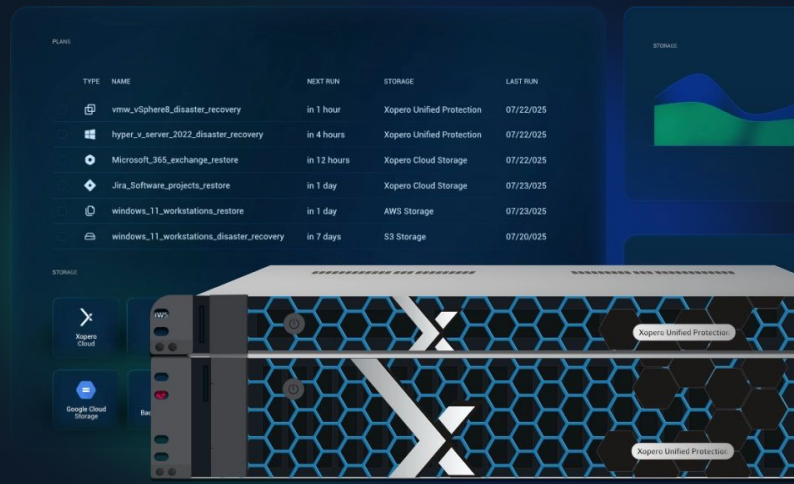
XOPERO
Backup&Recovery

Twój partner we wdrożeniu NIS2

Xopero Software S.A. jest polską firmą i partnerem instytucji państwowych. Aktywnie wspiera krajowe inicjatywy w zakresie cyberbezpieczeństwa i suwerenności cyfrowej. Nasze produkty są projektowane z myślą o wymaganiach UE i wspierają spełnienie wymogów regulacyjnych, w tym NIS2 i RODO. Firma posiada certyfikaty ISO 27001 oraz SOC 2 Type II.

Sprawdź, jak Xopero ułatwi Twojej organizacji dostosowanie się do wymogów NIS2.

Umów demo



Materiał ten został opracowany w lutym 2026 r. w celu wsparcia organizacji w procesie wdrażania wybranych wymogów wynikających z dyrektywy NIS2. Zawarte w nim informacje mają charakter ogólny i orientacyjny. Xopero Software S.A. nie ponosi odpowiedzialności za kompletność, aktualność i zgodność materiałów z pełnym zakresem obowiązków wynikających z NIS2 oraz z przepisami krajowymi wdrażającymi tę dyrektywę. Zaleca się, aby każda organizacja samodzielnie przeprowadziła szczegółową analizę ryzyka oraz skonsultowała się z odpowiednimi specjalistami lub organami nadzorczymi w celu zapewnienia pełnej zgodności z obowiązującymi regulacjami.