REGUVARA · BEZPŁATNY PORADNIK PRAKTYCZNY

NIS2: przygotowanie ścieżek zgłoszeń i dowodów

Praktyczny punkt wyjścia dla kierownictwa, IT/bezpieczeństwa, działu prawnego i compliance. Informacje o zakresie, najważniejszych terminach zgłoszeń i pięciu pierwszych działaniach.

Cel: szybko wskazać właściwe pytania. Ten poradnik nie rozstrzyga wiążąco, czy dana osoba prawna podlega NIS2.

1. Najpierw wstępnie oceń zakres

• Przyporządkuj działalność, usługę i osobę prawną do sektorów z załączników I i II do dyrektywy NIS2. Sama nazwa sektora nie przesądza o objęciu przepisami.

• Sprawdź wielkość, powiązania grupowe, rodzaj usługi, status podmiotu krytycznego, wyjątki i szczególne przepisy danego państwa członkowskiego. Niektóre podmioty lub usługi mogą podlegać przepisom niezależnie od zwykłego progu wielkości.

• Dla każdej potencjalnie objętej osoby prawnej udokumentuj państwa, lokalizacje, usługi, właściwy organ, obowiązki rejestracyjne i kontaktowe oraz uzasadnienie.

2. Unijne etapy zgłaszania poważnego incydentu

Etap	Podstawa UE zgodnie z art. 23	Pytanie przygotowawcze
Wczesne ostrzeżenie	Bez zbędnej zwłoki, nie później niż w ciągu 24 godzin od powzięcia wiadomości o poważnym incydencie.	Kto rozpoczyna pomiar czasu, podejmuje decyzję i wskazuje właściwy organ?
Zgłoszenie incydentu	Bez zbędnej zwłoki, nie później niż w ciągu 72 godzin od powzięcia wiadomości; wstępna ocena powagi i skutków oraz wskaźniki, jeśli są dostępne.	Jak równolegle gromadzić fakty, znaczniki czasu i niewiadome?
Sprawozdanie pośrednie	Jeśli zażąda go CSIRT lub właściwy organ.	Kto śledzi zmiany i odpowiada na pytania uzupełniające?
Sprawozdanie końcowe	Co do zasady w ciągu miesiąca od zgłoszenia incydentu. Jeśli incydent nadal trwa, w tym terminie należy złożyć sprawozdanie z postępów, a sprawozdanie końcowe w ciągu miesiąca od zakończenia obsługi.	Kto potwierdza krajowy termin i wymagane treści?

Terminy dotyczą poważnych incydentów oraz chwili powzięcia o nich wiadomości. Dostawcy usług zaufania podlegają szczególnej zasadzie 24-godzinnego zgłoszenia incydentu. Sprawdź przepisy krajowe, regulacje sektorowe i inne mające zastosowanie akty UE.

ARKUSZ ROBOCZY

Od tekstu prawa do pierwszego procesu

NIS2 wymaga proporcjonalnych do ryzyka środków technicznych, operacyjnych i organizacyjnych. To zestawienie pomaga zebrać pierwsze osoby odpowiedzialne.

3. Obszary wskazane w art. 21

Środki chronią sieci i systemy informatyczne używane do świadczenia usług, w tym ich środowisko fizyczne. Zakres i sposób działania zależą od ryzyka i proporcjonalności.

Obszar	Przykładowe pytanie robocze
Analiza ryzyka i bezpieczeństwo systemów	Jakie usługi, systemy, zagrożenia i zależności obejmuje analiza? Kto ją aktualizuje?
Obsługa incydentów	Jak zorganizowano wykrywanie, klasyfikację, ograniczanie, eskalację, zabezpieczanie dowodów i analizę po incydencie?
Ciągłość działania i kryzys	Czy kopie zapasowe, odtwarzanie, role kryzysowe i cele przywrócenia działania są udokumentowane i testowane?
Łańcuch dostaw	Czy ujęto bezpośrednich dostawców, krytyczne zależności i informacje o bezpieczeństwie?
Bezpieczne zakupy i rozwój	Jak bezpiecznie wybiera się i utrzymuje systemy oraz obsługuje lub ujawnia podatności?
Ocena skuteczności	Jak organizacja ustala, czy środki bezpieczeństwa działają?
Higiena cyberbezpieczeństwa i szkolenia	Jakie podstawowe praktyki i szkolenia są planowane i dokumentowane?
Kryptografia	Jakie zasady dotyczą kryptografii i, w stosownych przypadkach, szyfrowania?
Personel, dostęp i aktywa	Jak kontroluje się uprawnienia, zmiany kadrowe, aktywa i dostęp?
Uwierzytelnianie i komunikacja	Gdzie właściwe są MFA lub ciągłe uwierzytelnianie, bezpieczna komunikacja i kanały awaryjne?

4. Pięć przydatnych pierwszych działań

- Wyznacz osobę odpowiedzialną za koordynowanie pytań o zakres i nierozstrzygniętych kwestii.
- Sporządź wykaz usług, osób prawnych, systemów i krytycznych bezpośrednich dostawców.
- Wyznacz kierownictwo, lidera incydentu, IT/bezpieczeństwo, dział prawny/compliance i komunikację oraz zastępców.
- Zweryfikuj krajowy właściwy organ, CSIRT, rejestrację, kanał zgłoszeń i ewentualne obowiązki sektorowe.
- Przeprowadź krótkie ćwiczenie: wykryj incydent, zapisz moment powzięcia wiadomości, uruchom eskalację i zbierz fakty.

NIS2 nie dotyczy automatycznie każdej firmy. Zakres zależy m.in. od działalności, wielkości, osoby prawnej, państwa członkowskiego, szczególnych przypadków i przepisów sektorowych.

ŹRÓDŁA I STAN PRAWNY

Źródło podstawowe: dyrektywa (UE) 2022/2555, w szczególności art. 2-4, 20, 21 i 23 oraz załączniki I-II. Wniosek COM(2026) 13 final nie jest obowiązującym prawem. 8 października 2026 r. procedura Parlamentu Europejskiego 2026/0012(COD) oczekiwała na decyzję komisji; 24 września 2026 r. opublikowano projekt sprawozdania komisji. Wdrożenie krajowe i przepisy sektorowe nie zostały sprawdzone osobno dla każdego państwa.
NIS2 Directive (EUR-Lex) · European Commission FAQ · National transposition · EP procedure 2026/0012(COD) · COM(2026) 13 proposal