

RAPORT SPRAWDZAJĄCY GOTOWOŚĆ FIRMY

Sprawdzian gotowości na przepisy *NIS2*

Raport z analizy luk · wersja przykładowa v1.0

PRZYKŁADOWY KLIENT

DANE ZANONIMIZOWANE

Producent żywności, 320 osób

Kategoria wg przepisów: firma objęta obowiązkami (tzw. „podmiot ważny”) · Branża: produkcja i przetwórstwo żywności

Województwo pomorskie · Termin na spełnienie wymogów: **17 kwietnia 2027**

Podsumowanie dla zarządu

Ten raport pokazuje, jak dużo brakuje badanej firmie do spełnienia nowych, unijnych przepisów o cyberbezpieczeństwie (przepisy te nazywa się **NIS2**; w Polsce zostały wdrożone jako ustawa o Krajowym Systemie Cyberbezpieczeństwa, w skrócie **UKSC**). Firma to producent żywności zatrudniający 320 osób. Ponieważ jest średniej wielkości firmą działającą w branży uznanej przez przepisy za istotną dla kraju (produkcja żywności), prawo klasyfikuje ją jako tzw. „**podmiot ważny**” — czyli firmę, na którą nałożono konkretne obowiązki, choć nieco łagodniejsze niż na największych graczy strategicznych (tzw. „podmioty kluczowe”). Sprawdzenie zajęło 3 tygodnie i objęło rozmowy z zespołem, przegląd dokumentów oraz test zabezpieczeń technicznych.

CZAS SPRAWDZENIA

3 tyg.

od pierwszego spotkania do
gotowego raportu

CZAS DO PEŁNEJ ZGODNOŚCI

11 tyg.

od akceptacji planu
działania

ZNALEZIONE BRAKI

17

w tym 6 pilnych
(krytycznych)

MOŻLIWA REDUKCJA RYZYKA

−1,4 mln €

po wdrożeniu
najpilniejszych poprawek

W skali od 1 do 5 (gdzie 5 oznacza pełną gotowość) ogólny poziom przygotowania firmy oceniliśmy na **2,4** — to etap, który można nazwać „w budowie”: część zabezpieczeń już działa, ale wielu wciąż brakuje. Znaleźliśmy 17 braków, w tym 6 pilnych. Jeśli nic się nie zmieni, firmie grozi kara finansowa do 2% rocznego obrotu (w tym przypadku ok. 2,4 mln EUR), a dodatkowo — zgodnie z nowymi przepisami — za brak nadzoru nad bezpieczeństwem **osobiście mogą odpowiadać członkowie zarządu**.

⚠ TRZY NAJWIĘKSZE RYZYKA

- **Dostawcy firmy** — brak ustalonych zasad zgłaszania awarii przez partnerów biznesowych. Jeśli coś pójdzie nie tak u dostawcy, firma może się o tym nie dowiedzieć na czas.
- **Świadomość zarządu** — nikt z 12-osobowego grona kierowniczego nie przeszedł jeszcze wymaganego szkolenia z cyberbezpieczeństwa.
- **Brak rejestracji** — firma nie jest jeszcze zgłoszona do krajowego rejestru podmiotów objętych przepisami; termin na to mija 90 dni od zakwalifikowania.

Pełne dojście do zgodności zajmie ok. **11 tygodni** od zaakceptowania planu działania. Trzy najprostsze, najszybsze kroki (tzw. *quick wins*) obniżają ekspozycję na kary o ok. **1,4 mln EUR** już w pierwszych 4 tygodniach — jeszcze przed pełnym wdrożeniem. Szczegółowy plan i podział zadań w zespole — w rozdziale 06.

CO ZROBIĆ NAJPIERW

Zacząć od trzech najprostszych, a zarazem najważniejszych kroków: zgłoszenia firmy do wymaganego rejestru, włączenia podwójnego logowania (tzw. *MFA*) na najważniejszych systemach oraz spisania prostej procedury na wypadek ataku. Te trzy działania od razu zamykają połowę najpilniejszych braków.

Jak przebiegało sprawdzenie

Sprawdziliśmy, czy firma spełnia wymogi dotyczące zabezpieczeń (art. 21 NIS2) oraz obowiązki formalne i zgłoszeniowe wynikające z polskiej ustawy UKSC.

Na jakich przepisach się opieramy

- **Unijna dyrektywa NIS2** (UE 2022/2555) — europejskie przepisy o cyberbezpieczeństwie dla firm z branż uznanych za ważne dla funkcjonowania gospodarki.
- **Polska ustawa o Krajowym Systemie Cyberbezpieczeństwa (UKSC)** — polska wersja tych przepisów, z konkretnymi terminami i obowiązkami: m.in. rejestracją firmy oraz zgłaszaniem poważnych awarii w ciągu 24 i 72 godzin.
- **Norma ISO/IEC 27001** — międzynarodowy, dobrowolny standard zarządzania bezpieczeństwem informacji. Jego wdrożenie pokrywa 70–80% wymagań NIS2, dlatego sprawdzamy oba tematy razem.

Metodyka

ETAP	NA CZYM POLEGAŁ
Rozmowy	9 spotkań z IT, zarządem, HR, działem jakości i osobą odpowiedzialną za zgodność z przepisami — sprawdzenie procesów, świadomości i codziennych nawyków.
Przegląd dokumentów	Polityki, procedury, rejestry ryzyk, umowy z dostawcami, plany działania na wypadek awarii.
Test zabezpieczeń	Sprawdzenie kontroli dostępu, podwójnego logowania (MFA), szyfrowania, kopii zapasowych, podziału sieci i monitoringu.
Ocena ryzyka	Wskazanie najważniejszych zasobów, zagrożeń i słabych punktów; ocena każdego obszaru w skali 1–5 i mapa ciepła (rozdział 03).

Co dokładnie sprawdziliśmy

Firmę oceniliśmy w **5 obszarach** (zasady i dokumenty, codzienne procesy, technologia, ludzie, kontrola/audyt) oraz w **5 rodzajach działań** (wykrywanie zagrożeń, zarządzanie nimi, reagowanie, ciągłość pracy, bezpieczeństwo dostawców) — razem 25 punktów kontrolnych, każdy oceniony w skali od 1 (wszystko w porządku) do 5 (poważny brak).

DLACZEGO TA FIRMA JEST OBJĘTA PRZEPISAMI

Firma zatrudnia ponad 50 osób i ma obrót powyżej 10 mln EUR rocznie, a działa w branży produkcji żywności — a to jedna z branż wskazanych wprost w przepisach (tzw. Załącznik II do NIS2) jako ważna dla funkcjonowania kraju. Dlatego prawo klasyfikuje ją jako „**podmiot ważny**”, co oznacza obowiązek rejestracji, wdrożenia konkretnych zabezpieczeń oraz zgłaszania poważnych awarii.

Mapa: gdzie są największe braki

Poniższa mapa pokazuje wielkość braku w każdym z 25 sprawdzonych punktów. Im wyższa liczba i ciemniejszy kolor, tym większa rozbieżność względem wymogów NIS2.

	Wykrywanie	Zarządzanie	Reagowanie	Ciągłość pracy	Dostawcy
Zasady i dokumenty	3	2	1	2	3
Codziennie procesy	2	4	2	1	3
Technologia	1	2	3	2	2
Ludzie	2	3	1	3	4
Kontrola / audyt	3	2	2	1	2

Skala: 1 — w porządku 2 — drobne braki 3 — wyraźny brak 4 — poważny brak 5 — bardzo pilne

Co z tego wynika

- **Najslabsze punkty:** kontrola nad bezpieczeństwem dostawców przez pracowników (4) oraz procedury reagowania na awarie w codziennych procesach (4) — tu jest największe ryzyko.
- **Najmocniejsze punkty:** wykrywanie zagrożeń po stronie technologii oraz ciągłość pracy w procesach i audycie (1) — techniczne podstawy są solidne.
- **Wniosek:** większość braków to kwestia brakujących procedur i przeszkolenia ludzi, a nie brakującej technologii — takie braki są zwykle tańsze i szybsze do naprawienia.

Co dokładnie znaleźliśmy

Spośród 17 znalezionych braków, poniżej pokazujemy podział wg pilności i obszaru. Szczegóły 6 najpilniejszych — w rozdziale 05.

PILNE

6

działanie natychmiastowe

WYSOKA WAGA

5

do 4 tygodni

ŚREDNIA WAGA

4

do 8 tygodni

NISKA WAGA

2

może poczekać

Podział braków wg obszaru

OBSZAR	ILE	NA CZYM POLEGA PROBLEM
Reagowanie na awarie	4	Brak spisanej procedury, brak jasnych terminów zgłaszania (24 / 72 godz.), brak rejestru zdarzeń.
Bezpieczeństwo dostawców	3	Firma nie sprawdza dostawców pod kątem bezpieczeństwa ani nie ma odpowiednich zapisów w umowach.
Ludzie i świadomość	3	Brak programu szkoleń; zarząd i kluczowe osoby nie zostały jeszcze przeszkolone.
Dostęp i szyfrowanie	3	Brak podwójnego logowania (MFA) na części ważnych systemów; nikt nie sprawdzał, czy kopie zapasowe faktycznie się odtwarzają.
Porządek i dokumentacja	2	Nieaktualne zasady wewnętrzne; nie wiadomo jasno, kto za co odpowiada.
Obowiązki formalne (UKSC)	2	Firma nie jest zarejestrowana; nie ma wyznaczonej osoby kontaktowej dla urzędu.

⚠ CO GROZI, JEŚLI NIC SIĘ NIE ZMIENI

Przy obecnym stanie rzeczy maksymalna kara dla firmy tej wielkości sięga **1,4% rocznego obrotu lub 7 mln EUR** (obowiązuje kwota wyższa). Dodatkowo nowe przepisy przewidują, że za brak nadzoru nad bezpieczeństwem **osobiście mogą odpowiadać osoby zarządzające firmą**.

Dobra wiadomość: warstwa technologiczna (monitoring, podział sieci, kopie zapasowe) jest już dojrzała. Większość braków dotyczy procesów i dokumentacji, więc można je zamknąć bez dużych wydatków inwestycyjnych.

Sześć najpilniejszych spraw

Sześć braków, które wymagają działania w pierwszej kolejności — z konkretną rekomendacją, co z nimi zrobić.

PRZEPIS	CZEGO BRAKUJE	WAGA	CO ZROBIĆ
NIS2 art. 21(2)(d)	Brak zasad postępowania na wypadek awarii u dostawców firmy.	PILNE kara do 2% obrotu	Spisać procedurę i dodać zapisy o bezpieczeństwie do umów; sprawdzić 12 kluczowych dostawców.
NIS2 art. 21(2)(g)	Brak szkoleń dla zarządu i kluczowych osób — obecnie 0 z 12 osób przeszkolonych.	PILNE ryzyko osobiste zarządu	Szkolenie dla zarządu (4 godz.) + szkolenie ogólne dla pracowników; powtarzane co roku.
UKSC art. 8(3)	Firma nie jest jeszcze zgłoszona do wymaganego rejestru krajowego (tzw. system S46).	PILNE termin: 90 dni	Zgłoszenie do rejestru i wyznaczenie osoby kontaktowej — najszybszy krok, poniżej tygodnia.
NIS2 art. 21(2)(b)	Brak spisanego planu reagowania na awarie i jasnych terminów zgłaszania (24 / 72 godz.).	PILNE ryzyko spóźnionych zgłoszeń	Przygotować plan reagowania na incydenty z jasnym podziałem ról; przeciwiczyć go na sucho (tzw. próba stołowa).
NIS2 art. 21(2)(i)	Brak podwójnego logowania (MFA) na części ważnych systemów (ERP, poczta, dostęp zdalny).	PILNE ryzyko przejęcia konta	Włączyć podwójne logowanie na wszystkich kontach z szerokim dostępem i połączeniach zdalnych.
NIS2 art. 21(2)(j)	Nikt nie sprawdzał, czy kopie zapasowe faktycznie da się odtworzyć.	PILNE ryzyko utraty danych	Ustalić regularny harmonogram testowania kopii (co kwartał); trzymać też kopię offline.

NAJSZYBSZE EFEKTY (ZAMYKAJĄ 3 Z 6 PILNYCH SPRAW W MNIEJ NIŻ 4 TYGODNIE)

Rejestracja w wymaganym rejestrze · włączenie podwójnego logowania na najważniejszych kontach · spisanie podstawowego planu reagowania na awarie. Niski koszt, a od razu wyraźnie mniejsze ryzyko kary (~1,4 mln EUR).

Pełna wersja raportu zawiera analogiczne opisy pozostałych 11 braków (wysoka / średnia / niska waga) wraz z dowodami (zrzuty konfiguracji, fragmenty dokumentów) — pominięte w tej wersji przykładowej.

Plan działania

Droga do pełnej zgodności w 11 tygodni, podzielona na cztery etapy. Najpilniejsze działania obniżają największe ryzyko już w pierwszym etapie.

TYDZIEŃ 1–2 · ETAP 1 — NAJSZYBSZE EFEKTY

Zamknięcie 3 pilnych spraw przy minimalnym koszcie

Rejestracja w wymaganym rejestrze · podwójne logowanie na najważniejszych kontach · podstawowy plan reagowania na awarie · wyznaczenie osoby kontaktowej.

TYDZIEŃ 3–6 · ETAP 2 — PROCEDURY I DOKUMENTY

Reagowanie na awarie, dostawcy, zasady wewnętrzne

Pełna procedura reagowania z terminami 24 / 72 godz. · sprawdzenie 12 dostawców i zapisy w umowach · aktualizacja zasad wewnętrznych i rejestru ryzyk.

TYDZIEŃ 7–10 · ETAP 3 — TECHNIKA I LUDZIE

Wdrożenie i szkolenia

Testy odtwarzania kopii zapasowych · dodatkowy podział sieci w newralgicznych miejscach · szkolenie zarządu (4 godz.) i program dla 320 pracowników.

TYDZIEŃ 11 · ETAP 4 — WERYFIKACJA

Sprawdzenie wewnętrzne i potwierdzenie gotowości

Wewnętrzny przegląd wdrożonych zabezpieczeń · ponowna ocena mapy braków · raport gotowości dla zarządu i potwierdzenie zgodności z UKSC.

Kto za co odpowiada

R = wykonuje zadanie · A = ostatecznie odpowiada za efekt · C = pytamy o zdanie · I = informujemy na bieżąco

DZIAŁANIE	ZARZĄD	IT / BEZPIECZEŃSTWO	HR	DS. ZGODNOŚCI
Nadzór i akceptacja planu	A	R	I	C
Rejestracja i obowiązki formalne	A	C	I	R
Podwójne logowanie, plan reagowania, testy kopii	I	R / A	I	C
Sprawdzenie dostawców i zapisy w umowach	A	C	I	R
Szkolenia zarządu i pracowników	A	C	R	C

Co dalej

Kolejność działań

PRIORYTET	DZIAŁANIE	EFEKT
P1	Najszybsze efekty: rejestracja, podwójne logowanie, plan reagowania	–3 pilne sprawy, –1,4 mln € ryzyka kary, poniżej 4 tygodni.
P2	Procedury reagowania na awarie i bezpieczeństwo dostawców	Spełnienie kluczowych wymogów NIS2 dotyczących zgłaszania awarii.
P3	Szkolenia zarządu i pracowników	Ograniczenie osobistej odpowiedzialności osób zarządzających.
P4	Testy odtwarzania danych, aktualizacja zasad, jasny podział ról	Pełna dokumentacja i ciągłość pracy firmy.

DODATKOWA KORZYŚĆ

Realizacja powyższych działań załatwia „przy okazji” 70–80% wymagań międzynarodowego standardu ISO/IEC 27001 — więc jeśli firma zechce się kiedyś certyfikować, nie zaczyna od zera.

KOLEJNY KROK

Bezpłatna rozmowa — 30 minut

Omówimy wyniki dla Twojej firmy, ustalimy zakres i harmonogram. Bez zobowiązań.

E-MAIL

kontakt@eurokompas.pl

TELEFON

[\[numer telefonu\]](#)

UMÓW ONLINE

eurokompas.pl/kontakt

Zastrzeżenie: niniejszy dokument jest przykładem poglądowym ilustrującym format i zakres raportu przygotowywanego przez Euro Kompas. Nazwa klienta, dane liczbowe oraz wszystkie ustalenia są fikcyjne / zanonimizowane i nie odnoszą się do żadnej rzeczywistej organizacji. Raport rzeczywisty przygotowywany jest indywidualnie na podstawie sprawdzenia konkretnej firmy.