CYBERBEZPIECZEŃSTWO · ZGODNOŚĆ NIS2 / KSC

Ocena zakresu i luk — NIS2 / KSC

Podmiot: **„Metalpol" Sp. z o.o.** (fikcyjny) Sektor: **produkcja** Wielkość: **~110 osób**

Autor: **Bartek Binder — FatDot** Poufność: **Zastrzeżone**

STRESZCZENIE DLA ZARZĄDU

Spółka **podlega** ustawie o KSC (wdrożenie NIS2) jako **podmiot ważny** (sektor produkcji, próg wielkości spełniony). Obowiązek wpisu do wykazu KSC mija **3 października 2026**; pełne środki zarządzania bezpieczeństwem – do 3 kwietnia 2027. Ocena wykazała **3 luki wysokiego ryzyka** (brak MFA na kontach uprzywilejowanych, brak testowanych kopii zapasowych, brak procedury zgłaszania incydentów w wymaganych oknach 24/72 h) oraz szereg braków proceduralnych. Żadna z luk nie wymaga dużych nakładów sprzętowych – kluczowy jest projekt SZBI, procedur i wdrożenie kilku kontroli technicznych. Rekomendacja: rejestracja przed 3.10, następnie 90-dniowy plan zamknięcia luk wysokiego ryzyka.

1 · USTALENIE STATUSU

WYNIK: podmiot ważny — podlega

Działalność w sektorze produkcji objętym załącznikiem do ustawy o KSC, przy spełnieniu progu wielkości (średnie przedsiębiorstwo). Klasyfikacja: **podmiot ważny**. Nadzór i sankcje łagodniejsze niż dla podmiotów kluczowych, ale obowiązki wpisu, zarządzania ryzykiem i raportowania incydentów – identyczne co do istoty.

2 · KLUCZOWE TERMINY DLA PODMIOTU

3.10.2026	Wpis do wykazu KSC (system S46) – samorejestracja. **Termin krytyczny.**
od 3.04.2026	Obowiązek zgłaszania poważnych incydentów (24 h / 72 h / 30 dni) – już obowiązuje.
3.04.2027	Wdrożenie środków zarządzania bezpieczeństwem informacji (SZBI).
3.04.2028	Pierwszy audyt (dot. podmiotów kluczowych; dla ważnych – na żądanie organu).

3 · ANALIZA LUK

OBSZAR	STAN OBECNY	WYMÓG	RYZYKO	PRIO
Kontrola dostępu / MFA	Brak MFA na kontach administracyjnych i VPN.	Uwierzytelnianie wieloskładnikowe dla dostępu uprzywilejowanego i zdalnego.	WYSOKIE	P1
Kopie zapasowe	Kopie istnieją, brak testów odtworzenia od 12 mies.	Kopie odporne na ransomware + regularne testy odtworzenia.	WYSOKIE	P1
Zgłaszanie incydentów	Brak procedury i osoby odpowiedzialnej.	Procedura zgłoszenia do CSIRT w 24/72 h; punkt kontaktowy.	WYSOKIE	P1

OBSZAR	STAN OBECNY	WYMÓG	RYZYKO	PRIO
Polityki / SZBI	Brak sformalizowanego SZBI i polityk.	System zarządzania bezpieczeństwem informacji, zatwierdzony przez zarząd.	ŚREDNIE	P2
Zarządzanie podatnościami	Aktualizacje ad-hoc, brak skanowania.	Proces zarządzania podatnościami i aktualizacjami.	ŚREDNIE	P2
Ciągłość działania	Brak planu BCP/DRP.	Plan ciągłości i odtwarzania po awarii.	ŚREDNIE	P2
Łańcuch dostaw	Brak oceny bezpieczeństwa dostawców ICT.	Ocena i wymogi bezpieczeństwa dla kluczowych dostawców.	ŚREDNIE	P2
Świadomość / szkolenia	Brak szkoleń w ostatnich 24 mies.	Cykliczne szkolenia i podnoszenie świadomości.	NISKIE	P3
Monitorowanie / logi	Logi częściowe, brak centralizacji.	Zbieranie i przegląd logów zdarzeń bezpieczeństwa.	NISKIE	P3

4 · OBOWIĄZEK ZGŁASZANIA INCYDENTÓW

Zgłaszanie poważnych incydentów obowiązuje już od 3.04.2026 – niezależnie od okresu na wdrożenie SZBI. Poniższe terminy (SLA) i droga zgłoszenia muszą znaleźć się we wdrażanej procedurze (luka P1).

≤ 24 h	**Wczesne ostrzeżenie** – wstępny sygnał do CSIRT od wykrycia incydentu.
≤ 72 h	**Zgłoszenie incydentu** – ocena wstępna: dotkliwość, wpływ, wskaźniki kompromitacji.
co 30 dni	**Raporty pośrednie** – dla incydentów trwających (np. ransomware), na żądanie CSIRT.
≤ 1 mies.	**Raport końcowy** – przyczyny, skutki, zastosowane środki zaradcze.

Droga zgłoszenia: CSIRT NASK – portal `incydent.cert.pl` lub system S46. (Administracja / infrastruktura krytyczna: CSIRT GOV.) Dodatkowo – obowiązek poinformowania odbiorców usług, których incydent może dotyczyć.

W ramach wdrożenia projektuję procedurę z przypisaniem ról (kto wykrywa, kto zgłasza, kto decyduje), progami kwalifikacji „poważnego" incydentu i gotowymi szablonami zgłoszeń – tak, by okno 24 h nikogo nie zaskoczyło.

5 · ROADMAPA

0-30 DNI

- Wpis do wykazu KSC (przed 3.10).
- Wyznaczenie osoby odpowiedzialnej + punktu kontaktowego.
- Uruchomienie MFA na kontach uprzywilejowanych i VPN (P1).
- Test odtworzenia kopii zapasowych (P1).

30-90 DNI

- Procedura zgłaszania incydentów 24/72 h (P1).
- Szkielet SZBI i kluczowe polityki (P2).
- Skan podatności + plan aktualizacji (P2).

3–12 MIES.	• Pełne SZBI, BCP/DRP, ocena dostawców (do 3.04.2027). • Centralizacja logów, cykliczne szkolenia. • Przegląd gotowości przed ewentualnym audytem.

NASTĘPNY KROK

Wdrożenie — projekt i nadzór

Na bazie tej oceny projektuję SZBI, procedury i playbooki oraz nadzoruję wdrożenie luk P1–P2. Prace techniczne realizują sprawdzeni wykonawcy pod moją kontrolą; odpowiadam za działający, zgodny system — nie za sam dokument. Wycena wdrożenia wg zakresu, ustalona przed startem.

Bartek Binder — FatDot
bartek@fatdot.pl · +48 609 737 000 · fatdot.pl