Checklista zgodności KSC/NIS 2

Operacyjne narzędzie dla dyrektora szpitala - 10 kroków wdrożenia w 12-miesięcznym oknie (do 3.04.2027) + protokół reakcji 24h + skład zespołu kryzysowego. Format gotowy do druku.

Trzy najważniejsze daty 2026-2027

Od 3 kwietnia 2026 r. szpital publiczny jest podmiotem kluczowym KSC/NIS 2 (każdy podmiot świadczący opiekę szpitalną, niezależnie od wielkości). Termin samoidentyfikacji w wykazie CSIRT: 3.10.2026 r. Termin pełnego wdrożenia SZBI: 3.04.2027 r. Kary: do 10 mln EUR (kluczowe) lub 7 mln EUR (ważne). Odpowiedzialność: osobista dyrektora szpitala - nieprzekazywalna.

10 kroków wdrożenia w 12-miesięcznym oknie

- ☐ Krok 1. Audyt cyberbezpieczeństwa - I kwartał
  Zlecenie audytu przez zewnętrznego, certyfikowanego audytora. Dokument oczekiwany przez organ nadzorczy. Termin krytyczny.
- ☐ Krok 2. Wyznaczenie CISO - I kwartał
  CISO lub kierownik IT z explicit pełnomocnictwem, raportujący bezpośrednio do dyrekcji. Pisemne powierzenie obowiązków.
- ☐ Krok 3. Klasyfikacja podmiotu - I kwartał
  Formalna samoidentyfikacja: podmiot kluczowy (szpitale - z reguły tak) czy ważny. Rejestracja w systemie S46 CSIRT.
- ☐ Krok 4. Wdrożenie/aktualizacja SZBI - II kwartał
  System Zarządzania Bezpieczeństwem Informacji: polityka, rejestr zasobów, procedury, instrukcje robocze. Podpisuje dyrektor.
- ☐ Krok 5. BCP / DRP + ćwiczenie sztabowe - II kwartał
  Plan ciągłości działania (BCP) i odtwarzania awaryjnego (DRP) z RPO/RTO. Pierwsze ćwiczenie tabletop w pełnym składzie zespołu kryzysowego.
- ☐ Krok 6. MFA dla wszystkich + PAM dla admin - II kwartał
  Wieloskładnikowe uwierzytelnianie dla wszystkich kont (nie tylko admin). Privileged Access Management dla kont uprzywilejowanych. Bez tego MFA jest fikcją.
- ☐ Krok 7. Backup immutable 3-2-1 - III kwartał
  3 kopie danych łącznie, 2 różne nośniki, 1 kopia poza siedzibą lub immutable. Regularne testy odtwarzania (nie tylko backupu). Bez tego = negocjacje z atakującym.
- ☐ Krok 8. SIEM/SOC 24/7 - III kwartał
  Własny SOC lub usługa zewnętrzna. Warunek dotrzymania 24h terminu zgłoszenia incydentu do CSIRT. Bez monitoringu 24/7 nie wykryjesz ataku weekend/nocą.
- ☐ Krok 9. Szkolenia zarządu + ciągłe szkolenia personelu - cały rok
  Pierwsze szkolenie zarządu w I kwartale (osobista odpowiedzialność NIS 2). Symulacje phishingu co miesiąc dla personelu. Tabletop półrocznie.
- ☐ Krok 10. Lista dostawców wysokiego ryzyka - IV kwartał
  Inwentaryzacja dostawców (HIS, LIS, RIS, PACS, sprzęt). Klasyfikacja ryzyka. Plan wymiany sprzętu od dostawców wysokiego ryzyka w terminach z decyzji organu.

Plan reakcji - pierwsze 24h po wykryciu incydentu

Czas	Działanie techniczne	Działanie organizacyjne
0-1 h	Izolacja zainfekowanych segmentów sieci, odcięcie połączeń zewnętrznych	Aktywacja zespołu kryzysowego, powiadomienie dyrekcji
1-6 h	Identyfikacja wektora ataku, zabezpieczenie logów, ocena zakresu	Decyzja o przejściu na tryb papierowy, komunikacja wewnętrzna do oddziałów
6-24 h	Próba odtworzenia z kopii zapasowych, kontakt z CSIRT NASK / CERT Polska	Wczesne powiadomienie organu nadzorczego (24h), komunikacja z pacjentami
24-72 h	Odbudowa systemów krytycznych, śledztwo techniczne, eradykacja	Pełne zgłoszenie incydentu (72h RODO + NIS 2), powiadomienie pacjentów
72h - 30 dni	Pełne odtworzenie środowiska, twardy reset poświadczeń, hardening	Raport końcowy do organu (1 miesiąc), lekcje, aktualizacja BCP

Skład zespołu kryzysowego - lista nazwisk i kontaktów

Zespół kryzysowy NIE jest tworzony "na żywo" w momencie ataku - to udokumentowana lista nazwisk z numerami kontaktowymi (także prywatnymi, na wypadek gdy systemy szpitalne nie działają), aktualizowana co kwartał.

- ☐ Dyrektor / wicedyrektor ds. zarządzania - decyzje strategiczne, kontakt z mediami, organem właścicielskim
- ☐ CISO / kierownik IT - koordynacja techniczna, kontakt z CSIRT NASK
- ☐ IOD (Inspektor Ochrony Danych) - ocena obowiązku zgłoszenia do UODO, komunikacja z pacjentami
- ☐ Radca prawny - odpowiedzialność cywilna i karna, postępowanie z UODO i CSIRT
- ☐ Rzecznik prasowy / specjalista ds. komunikacji - komunikacja zewnętrzna, media
- ☐ Naczelna pielęgniarka / kierownik administracji medycznej - koordynacja pracy oddziałów w trybie awaryjnym
- ☐ Zewnętrzny partner IR (Incident Response) - w idealnym scenariuszu na umowie retainerskiej 24/7

Najczęstsze pułapki wdrożeniowe

1. Delegowanie NIS 2 w całości na dział IT - dyrektor osobiście podpisuje SZBI i osobiście odpowiada.
2. Brak immutable backup - jeśli atakujący zaszyfruje backup, jedyne wyjście to okup.
3. MFA tylko dla adminów - 95% ataków zaczyna się od konta zwykłego użytkownika.
4. Pomijanie IoMT (pompy, monitory, MRI) - segmentacja VLAN to wymóg, nie opcja.
5. Brak SOC 24/7 - atak weekendowy = przekroczenie 24h terminu CSIRT = osobna kara.
6. Audyty "papierowe" - bez technicznego pentestu organ uzna SZBI za niewystarczające.

Kluczowe kontakty i źródła

CSIRT NASK: incydent.cert.pl (zgłaszanie incydentów 24h/72h)
Centrum e-Zdrowia: ezdrowie.gov.pl, ankieta dojrzałości cyberbezpieczeństwa
Ministerstwo Cyfryzacji: gov.pl/web/cyfryzacja (lista podmiotów KSC)
UODO: uodo.gov.pl (zgłoszenia naruszeń RODO)
KPO D1.1.2: finansowanie cyberbezpieczeństwa szpitali (1-12 mln zł)

Artykuł źródłowy

Pełny artykuł z dokładnym omówieniem zagrożeń, ataków na polskie placówki w 2025-2026, finansowania KPO i pełną listą obowiązków znajdziesz pod adresem:

https://wsparciedlaszpitala.pl/ai-w-szpitalu/cyberbezpieczenstwo-szpitala-jak-chronic-dane-pacjentow-i-systemy-medyczne-przed-atakami-hakerow/

Materiał ma charakter informacyjny i nie stanowi porady prawnej. Stan prawny i organizacyjny na 26.05.2026 r. Dokument przygotowała redakcja wsparciedlaszpitala.pl na podstawie znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa z 19.02.2026 (NIS 2), wytycznych CSIRT NASK, Centrum e-Zdrowia oraz Ministerstwa Cyfryzacji.