CYBERBEZPIECZEŃSTWO · NIS2 · SEKTOR ZDROWIA

Checklista gotowości NIS2 dla szpitala

22 punkty kontrolne, które pomogą Ci ocenić, gdzie szpital naprawdę jest w gotowości na wymagania dyrektywy NIS2 - bez kosztownego audytu zewnętrznego.

22
PUNKTY KONTROLNE

9
OBSZARÓW NIS2

10 mln €
MAKS. KARA ZA NIEZGODNOŚĆ

Opracowanie: OneCare Sp. z o.o.
Strategiczny partner cyfryzacji szpitali

onecare.com.pl

Po co ta checklista

Dyrektywa **NIS2** (Network and Information Security Directive 2) klasyfikuje szpitale i podmioty lecznicze jako **podmioty kluczowe** sektora zdrowia. Oznacza to konkretne, mierzalne obowiązki w zakresie cyberbezpieczeństwa - z karami do **10 mln EUR lub 2% rocznych przychodów światowych** (art. 34 NIS2) oraz **osobistą odpowiedzialnością członków zarządu** (art. 20 NIS2).

W Polsce dyrektywę implementuje nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC). Pełne przepisy obowiązują od **17 października 2024 r.**, ale praktyczne wdrożenie w polskich szpitalach jest dopiero w trakcie.

Ta checklista pomoże Ci

- Ocenić, gdzie Twój szpital faktycznie jest w gotowości NIS2
- Zidentyfikować luki bez kosztownego audytu zewnętrznego
- Przygotować plan działania na najbliższe 6-12 miesięcy
- Pokazać zarządowi konkretny obraz ryzyka i potrzeb inwestycyjnych

Jak korzystać

Zaznacz ☑ dla każdego punktu, który jest **udokumentowany i działa w praktyce**. Sama deklaracja „mamy" bez dowodu - pozostaw puste.

Na końcu policz wynik:

Wynik	Status	Co dalej
20-22	Gotowy	Utrzymuj poziom, audytuj raz w roku
16-19	W trakcie	Uzupełnij luki w 3 miesiące
10-15	Ryzyko podwyższone	Plan naprawczy w 6 miesięcy, raportowanie do zarządu
0-9	Krytyczne	Pilne działania, ryzyko kary i przerwania działalności

Checklista - 22 punkty kontrolne

A · Zarządzanie ryzykiem cyberbezpieczeństwa

1. Aktualny rejestr ryzyk cyberbezpieczeństwa

- [ ] Mamy formalny rejestr zidentyfikowanych ryzyk (zagrożenia + podatności + skutki + prawdopodobieństwo).

Przegląd nie rzadziej niż raz na 12 miesięcy.

2. Zatwierdzona polityka bezpieczeństwa informacji

- [ ] Polityka jest spisana, aktualna i podpisana przez dyrektora/zarząd. Pracownicy mają do niej dostęp i są o niej szkoleni.

3. Wyznaczona osoba odpowiedzialna za bezpieczeństwo IT

- [ ] Mamy formalnie wskazaną osobę (CISO, kierownik bezpieczeństwa IT) z zakresem obowiązków na piśmie.

W placówce poniżej 500 łóżek może to być rola łączona, ale musi być nazwana.

4. Szkolenie zarządu z odpowiedzialności za cyberbezpieczeństwo

- [ ] Członkowie zarządu/dyrekcji przeszli szkolenie z obowiązków NIS2 (art. 20) - z dokumentem potwierdzającym (lista obecności, certyfikat).

B · Obsługa incydentów

5. Procedura reagowania na incydenty (IRP)

- [ ] Mamy spisaną procedurę: kto co robi w pierwszych 60 minutach, w pierwszych 24 godzinach, w 72 godzinach. Procedura była testowana (tabletop exercise) co najmniej raz.

6. Wiemy jak zgłosić incydent do organu (CSIRT MZ / GOV)

- [ ] Wiemy do kogo i jakim kanałem zgłaszać incydenty istotne (próg 24h dla wczesnego ostrzeżenia, 72h dla raportu). Mamy gotowy szablon zgłoszenia.

  Aktualny kontakt: CSIRT GOV / sektorowy CSIRT NASK / CSIRT MZ.

7. Rejestr incydentów z analizą

- [ ] Każdy incydent ma wpis w rejestrze z analizą przyczyn i wnioskami (post-mortem). Rejestr przechowywany min. 24 miesiące.

C · Ciągłość działania i odporność

8. Plan ciągłości działania (BCP) i odtwarzania po awarii (DRP)

☐ Mamy aktualne dokumenty BCP i DRP, znane RTO i RPO dla krytycznych systemów (HIS, LIS, PACS). Aktualizacja co najmniej raz w roku.

9. Backup w schemacie 3-2-1

☐ Co najmniej **3 kopie** danych, na **2 różnych mediach**, z czego **1 offline / off-site** (immutable, zabezpieczone przed ransomware). Backup automatyczny, monitorowany alertami.

10. Test odtwarzania z backupu w ostatnich 12 miesiącach

☐ Wykonaliśmy faktyczny test odtworzenia kluczowego systemu z kopii - z dokumentem potwierdzającym (data, osoba, wynik).

„Robimy backup" bez testu odtworzenia - pozostaw puste.

D · Bezpieczeństwo łańcucha dostaw

11. Lista kluczowych dostawców IT z oceną krytyczności

☐ Mamy zinwentaryzowanych dostawców systemów, sprzętu, łączy, hostingu, serwisu - z oznaczeniem poziomu krytyczności (A/B/C). Dla dostawców kategorii A: dane kontaktowe SOC 24/7, czasy reakcji w SLA.

12. Klauzule bezpieczeństwa w umowach z dostawcami

☐ Umowy z dostawcami klasy A i B zawierają zapisy o: SLA bezpieczeństwa, prawie audytu, obowiązku notyfikacji incydentu w 24h, miejscu przetwarzania danych, podwykonawcach.

Stare umowy (sprzed 2024) sukcesywnie aktualizowane.

13. Wiemy gdzie fizycznie są przetwarzane nasze dane

☐ Dla każdego krytycznego systemu wiemy: kraj/lokalizacja serwerowni, podmiot odpowiedzialny, czy występuje transfer poza EOG. Mamy mapę przepływu danych.

E · Bezpieczeństwo systemów i sieci

14. Proces aktualizacji oprogramowania (patch management)

- [ ] Mamy udokumentowany proces aktualizacji systemów operacyjnych, baz danych, aplikacji medycznych. Krytyczne łatki bezpieczeństwa wdrażane w określonym SLA (np. ≤14 dni dla CVSS ≥9.0). Inwentaryzacja zasobów IT (CMDB) jest aktualna.

15. Segmentacja sieci

- [ ] Sieć kliniczna (urządzenia medyczne, HIS) jest oddzielona od sieci administracyjnej (księgowość, HR) i sieci gościnnej. Komunikacja między segmentami przez firewall z regułami min-priv.

16. Logi audytu (audit trail) zbierane i przechowywane

- [ ] Logi z systemów krytycznych (HIS, AD, firewall, VPN, dostęp do EDM) trafiają do centralnego repozytorium (SIEM lub równoważne). Retencja minimum 12 miesięcy. Logi są chronione przed manipulacją.

F · Kontrola dostępu i zarządzanie tożsamością

17. MFA dla kont administracyjnych i zdalnego dostępu

- [ ] Wszystkie konta z uprawnieniami administracyjnymi (AD, bazy danych, systemy medyczne, infrastruktura) wymagają drugiego składnika. Wszystkie połączenia VPN/RDP z zewnątrz wymagają MFA.

18. Off-boarding pracownika i wykonawcy

- [ ] Mamy procedurę natychmiastowej deaktywacji kont po zakończeniu zatrudnienia/umowy (≤24h). Cykliczny przegląd kont nieaktywnych (raz na kwartał).

19. Polityka silnych haseł + cykl życia konta

- [ ] Wymuszone minimum 12 znaków, lockout po nieudanych próbach, brak haseł zapisanych w plikach jawnym tekstem. Przegląd uprawnień użytkowników nie rzadziej niż raz na 6 miesięcy.

G · Kryptografia

20. Szyfrowanie danych w spoczynku i w tranzycie

- [ ] Bazy danych z danymi osobowymi i medycznymi mają szyfrowanie na poziomie storage lub aplikacji. Każda komunikacja webowa/API używa TLS 1.2+. Backupy są szyfrowane.

H · Cyberhigiena i kompetencje

21. Szkolenie personelu z cyberhigieny w ostatnich 12 miesiącach

- [ ] Cały personel mający dostęp do systemów IT (pielęgniarki, lekarze, administracja) przeszedł szkolenie z phishingu, haseł, zgłaszania incydentów - z listą obecności / wynikiem testu.

I · Audyt i przegląd

22. Plan audytu / przeglądu zgodności z NIS2

- [ ] Mamy zaplanowany audyt wewnętrzny lub zewnętrzny zgodności z wymaganiami NIS2 - co najmniej raz w roku. Wynik audytu trafia do zarządu z planem działań naprawczych.

Wynik i co dalej

Liczba zaznaczonych punktów: _____ / 22

Status: _____

Interpretacja wyniku

Jeśli wynik 16-22: Gratulacje. Utrzymuj poziom - najwięcej szpitali wpada w pułapkę „mamy to" bez utrzymania (kontrole compliance ujawniają to po 18-24 miesiącach od audytu wstępnego).

Jeśli wynik 10-15: Plan naprawczy w 6 miesięcy. Priorytetowo: punkty 5-10 (incydenty + ciągłość) - najczęstsze źródło realnych strat finansowych.

Jeśli wynik poniżej 10: Pilna mobilizacja. Skontaktuj się z dostawcą systemu medycznego - w wielu przypadkach kluczowe braki to konfiguracja istniejących narzędzi, nie nowe zakupy.

Pomoc OneCare

OneCare jest dostawcą systemu OpenCARE i potencjalnym wykonawcą w postępowaniach na HIS/EDM. Z tego względu nie pełnimy roli doradcy zamawiającego ani audytora postępowania (art. 56 ust. 1 pkt 4 PZP). To, co możemy zaoferować:

- **Materiały edukacyjne** - kolejne checklisty, białe księgi i webinary o cyberbezpieczeństwie w sektorze zdrowia
- **Demo OpenCARE** - 30-minutowa prezentacja mechanizmów wspierających punkty 8, 14, 16, 17, 19, 20 z tej checklisty
- **Wizyta referencyjna** - możliwość zobaczenia OpenCARE w pracującym szpitalu
- **Złożenie oferty** - w postępowaniu otwartym, jako jeden z wykonawców na warunkach jednakowych dla wszystkich

kontakt@onecare.com.pl · +48 601 821 612 · onecare.com.pl

> **Zastrzeżenie.** Niniejszy materiał ma charakter edukacyjny i nie stanowi porady prawnej. Zalecamy konsultację z kancelarią prawną oraz audytorem ds. cyberbezpieczeństwa przed podjęciem wiążących decyzji w zakresie zgodności z dyrektywą NIS2 i ustawą o krajowym systemie cyberbezpieczeństwa. OneCare Sp. z o.o. nie gwarantuje zgodności z NIS2 - pomaga ją osiągnąć i utrzymać.
