

Pierwsza godzina po cyberataku

Na ekranach żądanie okupu, system szpitalny nie odpowiada, izba przyjęć dzwoni co minutę. W pierwszej godzinie rozstrzyga się, czy będzie z czego odtworzyć dane, czy zostaną ślady i czy zgłoszenia pójdą na czas. Wypełnijcie kartę teraz, a w trakcie incydentu zaznaczajcie punkty.

ZAPISZ OD RAZU

Data i godzina wykrycia:

Kto wykrył i na czym:

Dowodzący incydem:

MINUTY 0 DO 15

Odciąć, ale nie niszczyć

- ☐ **Odłącz zainfekowany komputer lub serwer od sieci: wyjmij kabel, wyłącz Wi-Fi. Zasilania nie wyłączaj.**
Po wyłączeniu znika zawartość pamięci, z której odczytuje się, którądy wszedł napastnik. Dowód: lista odłączonych urządzeń.
- ☐ **Odłącz od sieci serwer kopii zapasowych i sprawdź datę ostatniej kopii.**
RODO wymienia wśród środków bezpieczeństwa zdolność do szybkiego przywrócenia dostępności danych po incydencie (art. 32 ust. 1 lit. c).
- ☐ **Zapisz godzinę wykrycia. Od niej bieżą terminy 24 i 72 godzin.**
KSC liczy od wykrycia incydentu (art. 11 ust. 1 pkt 4 i 4a), RODO od stwierdzenia naruszenia (art. 33 ust. 1).
- ☐ **Wstrzymaj dostęp zdalny: VPN dostawców, pulpity zdalne, konta serwisowe. Hasła kont administracyjnych zmieniaj z komputera spoza zaatakowanej sieci.**
Dowód: wpis w dzienniku, kto i o której wyłączył dostęp.
- ☐ **Powiadom dowodzącego telefonicznie, nie firmową pocztą.**
Zaatakowaną skrzynkę i komunikator zalogowany kontem z domeny szpitala może czytać napastnik.

MINUTY 15 DO 30

Zabezpieczyć ślady

- ☐ **Sfotografuj telefonem ekran z żądaniem okupu i komunikaty błędów, tak żeby było widać godzinę.**
- ☐ **Skopiuj dzienniki zapory, VPN, serwera domeny i systemu kopii na czysty nośnik poza siecią, zanim się nadpiszą.**
- ☐ **Prowadź dziennik działań na papierze: godzina, kto, co zrobił, na jakim urządzeniu.**
Administrator dokumentuje każde naruszenie, skutki i działania zaradcze (art. 33 ust. 5 RODO); wczesne ostrzeżenie podaje moment wystąpienia i wykrycia (art. 12 ust. 1 pkt 4 KSC).

MINUTY 30 DO 60

Decyzja o pracy awaryjnej

- ☐ **Kierownik akcji (w nocy lekarz kierujący dyżurem) ogłasza pracę na papierze bez czekania na dyrektora i zapisuje godzinę.**
Za obowiązki z KSC, w tym zgłoszenia, odpowiada kierownik podmiotu, także gdy powierzył je innej osobie (art. 8c ust. 1 i 3).
- ☐ **Izba przyjęć, SOR, apteka i laboratorium przechodzą na formularze papierowe. Zapisz, od której godziny.**
Papier jest dopuszczalny, gdy warunki organizacyjno-techniczne uniemożliwiają postać elektroniczną; ten sam dokument nie może być prowadzony w obu postaciach naraz (§ 1 ust. 2 i 3 rozporządzenia MZ o dokumentacji medycznej).
- ☐ **Ustalcie, czy ograniczacie przyjęcia, i kto informuje dyspozytornię medyczną, lekarza koordynatora ratownictwa medycznego i podmiot tworzący.**
- ☐ **Dowodzący, inspektor ochrony danych i dyrektor oceniają: czy to incydent poważny i czy doszło do naruszenia ochrony danych osobowych.**
Incydent poważny: m.in. poważne obniżenie jakości lub przerwanie ciągłości usług (art. 2 pkt 7 KSC). Naruszenie danych: m.in. zniszczenie, utracenie, nieuprawnione ujawnienie lub dostęp (art. 4 pkt 12 RODO).

ZEGAR OBOWIĄZKÓW

Kto, do kogo i w jakim terminie

0	Wykrycie incydentu. Godzina w dzienniku działań. (art. 11 ust. 1 pkt 4 KSC; art. 33 ust. 1 RODO)
bez zbędnej zwłoki	Dostawca, który przetwarza dane pacjentów, zgłasza szpitalowi naruszenie po swojej stronie bez zbędnej zwłoki. Zadzwońcie, jeśli milczy. (art. 33 ust. 2 RODO)
do 24 h	Wczesne ostrzeżenie o incydencie poważnym do CSIRT sektorowego, przez system S46. Zawiera m.in. dane zgłaszającego, osoby do wyjaśnień, moment wystąpienia i wykrycia, ocenę, czy to działanie bezprawne, jeśli da się ją już dokonać. (art. 11 ust. 1 pkt 4 i ust. 2, art. 12 ust. 1 KSC)
do 72 h	Zgłoszenie incydentu poważnego, m.in.: wpływ na usługi i liczba użytkowników, przyczyny, działania zapobiegawcze i naprawcze. Podajecie to, co wiecie, i uzupełniacie w trakcie. (art. 11 ust. 1 pkt 4a, art. 12 ust. 3 i 5 KSC)
do 72 h	Zgłoszenie naruszenia ochrony danych do Prezesa UODO, chyba że ryzyko dla osób jest mało prawdopodobne. Po 72 h tylko z wyjaśnieniem opóźnienia; brakujące informacje wolno dosyłać. (art. 33 ust. 1, 3 i 4 RODO)
bez zbędnej zwłoki	Zawiadomienie pacjentów, gdy naruszenie może powodować wysokie ryzyko dla ich praw lub wolności. (art. 34 ust. 1 RODO)
bez terminu	Informacja dla użytkowników usług o incydencie poważnym, który ma niekorzystny wpływ na świadczenie tych usług; ustawa nie podaje terminu. (art. 11 ust. 2b KSC)
1 miesiąc	Sprawozdanie końcowe od dnia zgłoszenia. Gdy obsługa trwa dłużej: sprawozdanie z postępu, a końcowe w miesiąc od zakończenia obsługi. (art. 11 ust. 1 pkt 4c, art. 12b KSC)

Terminy KSC dotyczą podmiotów kluczowych i ważnych (nowelizacja Dz.U. 2026 poz. 252, w mocy od 3.04.2026). Obowiązki trzeba wdrożyć do 3.04.2027 (art. 33 ust. 1 ustawy nowelizującej); byli operatorzy usług kluczowych przechodzą na nowe zasady zgłaszania w ciągu 6 miesięcy od wejścia nowelizacji w życie (art. 33 ust. 4). Kary, także dla kierownika podmiotu, od 3.04.2028 (art. 35 ustawy nowelizującej, art. 73a ust. 1 pkt 9 KSC). RODO dotyczy każdej placówki.

TYPOWE BŁĘDY

Czego nie robić

- ☒ **Nie restartuj serwerów, nie formatuj dysków, nie reinstaluj systemów przed zabezpieczeniem śladów.** Restart kasuje ślady, a szyfrowanie może ruszyć od nowa.
- ☒ **Nie przywracaj z kopii, dopóki nie wiecie, którądy wszedł napastnik i czy kopia jest czysta.** Przywrócony system może zostać zaszyfrowany drugi raz.
- ☒ **Nie odpowiadaj na żądanie okupu.** Kontakt z przestępcami to decyzja kierownika po rozmowie z CSIRT i organami ścigania.
- ☒ **Nie czekaj z decyzją o zgłoszeniu na pełną wiedzę.** Wczesne ostrzeżenie i zgłoszenie do UODO zawierają to, co wiecie w danej chwili.
- ☒ **Nie odłączaj na ślepo urządzeń medycznych, od których zależy leczenie.** Kolejność ustalcie wcześniej z działem aparatury.

TELEFONY: WPISZCIE NUMERY, SPRAWDŹCIE, CZY ODBIERAJĄ W NOCY I W ŚWIĘTA

Dowodzący incydem	Zastępca dowodzącego	Dyżur IT, administrator sieci	Dyrektor albo zastępca	Inspektor ochrony danych
Pielęgniarka naczelna, kierownik SOR	Serwis całodobowy dostawcy systemu szpitalnego	Dostawca łączy i zapory sieciowej	Firma od analizy powłamaniowej lub monitorowania	Policja, komenda właściwa dla placówki
Podmiot tworzący lub właściciel	Osoba do kontaktu z mediami	CSIRT CeZ (CSIRT sektorowy ochrony zdrowia) S46; csirt.cez.gov.pl/pl/zglos-incydent; incydent@csirt.cez.gov.pl; tel.:	Prezes UODO formularz zgłoszenia naruszenia na biznes.gov.pl	Kto ma dostęp do konta S46 (dwie osoby)

Skala ma znaczenie. Przychodnia, która nie jest podmiotem kluczowym ani ważnym, nie ma obowiązków zgłoszeniowych z KSC, ale 72 godziny na zgłoszenie do UODO obowiązują ją tak samo jak szpital. Szpital powiatowy z kilkusobowym działem IT nie przeanalizuje włamania sam: umowę z firmą od analizy powłamaniowej podpisuje się przed atakiem. Szpital specjalistyczny ma w sieci urządzenia medyczne i potrzebuje uzgodnionej listy, co wolno odłączyć. Sieć placówek ustala z góry, kto zgłasza incydent za każdy podmiot, i ćwiczy to na jednej lokalizacji. Kiedy ostatnio sprawdziliście, czy numery z tej kartki odbierają o trzeciej w nocy?