PORADNIK

Incydent w organizacji: pierwsze 72 godziny

Zgłoszenia według KSC, RODO i DORA, scenariusze i pomoc z zewnątrz

CyberKatalog.pl

Wydanie pierwsze
Wrzesień 2026

Wydawca: CyberKatalog.pl
Wydanie: pierwsze, wrzesień 2026
Stan prawny: 24 września 2026 r.
Format: Publikacja elektroniczna
Zdjęcie na okładce: Adam Borkowski, Unsplash (licencja Unsplash)

Publikacja jest dostępna nieodpłatnie na stronie CyberKatalog.pl na licencji Creative Commons Uznanie autorstwa - Bez Utworów Zależnych 4.0 Międzynarodowa (CC BY-ND 4.0).

O publikacji

Poradnik jest przeznaczony dla każdej organizacji w Polsce, która może albo musi zgłosić incydent bezpieczeństwa: dla działu IT, inspektora ochrony danych (IOD), zarządu, a w podrozdziale 3.1 także dla pracownika bez przygotowania technicznego, który kliknął w podejrzany link i nie wie, co zrobić dalej.

Jak korzystać z poradnika

Poradnik czyta się dwa razy: przed incydentem, żeby przygotować procedurę, listę kontaktów i podział odpowiedzialności, oraz w trakcie incydentu, żeby odnaleźć właściwy scenariusz, terminy i adresata zgłoszenia. Kartę do wydrukowania, powieszenia i uzupełnienia własnymi kontaktami zawiera załącznik A; ta sama karta jest osobnym plikiem PDF na stronie publikacji CyberKatalog.pl [1].

Metoda

Każde twierdzenie o obowiązku prawnym wskazuje akt i jednostkę redakcyjną, z której wynika, w brzmieniu ogłoszonym w Dzienniku Ustaw albo w Dzienniku Urzędowym Unii Europejskiej. Zalecenia postępowania pochodzą z publikacji instytucji publicznych, takich jak CERT Polska, NIST, CISA i Europejska Rada Ochrony Danych, a środki techniczne poradnik opisuje przez ich funkcję, bez nazw produktów i producentów.

Stan prawny

Poradnik uwzględnia stan prawny na 24 września 2026 r. Podstawą opisu zgłaszania incydentów jest nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa z 23 stycznia 2026 r., w mocy od 3 kwietnia 2026 r. [2] Nowelizacja daje okresy przejściowe na wdrożenie nowych obowiązków, w tym zgłaszania incydentów, ale obowiązków z RODO te okresy nie przesuwają. Daty, w których się kończą, podaje rozdział 1.

Zastrzeżenie

Poradnik opisuje obowiązki według brzmienia przepisów na dzień stanu prawnego i nie zastępuje porady prawnej w konkretnej sprawie.

Spis treści

1 Zegar zgłoszeń: jeden incydent, trzy zestawy przepisów **8**
1.1 Kogo obejmują KSC, RODO i DORA 8
1.2 Od czego liczy się termin 9
1.3 Ustawa o KSC 9
1.4 RODO 12
1.5 DORA 12
1.6 Jeden incydent, kilka zgłoszeń 13

2 Pierwsza godzina: kroki wspólne **15**
2.1 Kto decyduje 15
2.2 Dziennik zdarzeń 15
2.3 Zabezpieczenie śladów 15
2.4 Izolacja 16
2.5 Komunikacja poza zaatakowaną infrastrukturą 16
2.6 Wsparcie CSIRT 16
2.7 Czego nie robić 16

3 Phishing i kliknięty link **17**
3.1 Dla pracownika 17
3.2 Dla działu IT 17

4 Przejęcie konta **19**
4.1 Odebranie dostępu 19
4.2 Podszywanie się pod firmę 19

5 Ransomware **21**
5.1 Izolacja i pierwsze ustalenia 21
5.2 Kopie zapasowe 21
5.3 Zgłoszenie 21
5.4 Decyzja o okupie 22

6 Wyciek danych **23**
6.1 Moment stwierdzenia i ocena ryzyka 23
6.2 Zgłoszenie do Prezesa UODO 23
6.3 Zawiadomienie osób 23

7 Mapa instytucji **25**
7.1 Właściwość CSIRT MON, CSIRT NASK i CSIRT GOV 26
7.2 System S46 26
7.3 Naruszenie ochrony danych osobowych 27
7.4 Poważny incydent związany z ICT 27
7.5 Przestępstwo 27

8 Kto pomoże z zewnątrz **28**
8.1 Kiedy wezwać zewnętrzny zespół 28
8.2 O co zapytać dostawcę, zanim dojdzie do incydentu 28
8.3 Kategorie w katalogu 28

A Karta "Pierwsze 72 godziny" **30**

Bibliografia **32**

Spis rysunków

1.1 Kolejność zgłoszeń według KSC, RODO i DORA 10
1.2 Cztery pytania po wykryciu incydentu 14

Spis tabel

1.1 Trzy zegary zgłoszeń 11

7.1 Kto przyjmuje które zgłoszenie 25

Rozdział 1

Zegar zgłoszeń: jeden incydent, trzy zestawy przepisów

Jeden incydent bezpieczeństwa potrafi uruchomić kilka obowiązków zgłoszeniowych naraz, każdy z innym terminem, innym punktem startowym i innym adresatem. Ustawa o krajowym systemie cyberbezpieczeństwa (KSC), RODO i DORA nakładają te obowiązki na różne kategorie podmiotów, więc to, które z nich dotyczą danej organizacji, wynika z tego, kim ona jest: podmiotem kluczowym lub ważnym, podmiotem finansowym, administratorem albo podmiotem przetwarzającym dane osobowe.

1.1 Kogo obejmują KSC, RODO i DORA

Ustawa o KSC nakłada obowiązki zgłoszeniowe na podmioty kluczowe i podmioty ważne. Incydent to zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych (art. 2 pkt 5) [2]. Incydent poważny to incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub ważny, straty finansowe tego podmiotu albo wpływa na inne osoby przez wywołanie poważnej szkody materialnej lub niematerialnej (art. 2 pkt 7) [2]. Dla podmiotu publicznego usługą jest także realizowane przez niego zadanie publiczne (art. 2a) [2]. Kogo obejmuje ustawa i jakie obowiązki nakłada, zbiera przegląd ustawy o krajowym systemie cyberbezpieczeństwa [3], a pojęcie incydentu poza definicją ustawową opisuje hasło incydent bezpieczeństwa w słowniku CyberKatalog.pl [4].

RODO nakłada obowiązki zgłoszeniowe na każdego administratora danych osobowych i każdy podmiot przetwarzający, niezależnie od tego, czy podlegają ustawie o KSC. Naruszenie ochrony danych osobowych to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych (art. 4 pkt 12 RODO) [5]. Zakres rozporządzenia streszcza hasło GDPR (RODO) w słowniku CyberKatalog.pl [6].

DORA nakłada odrębne obowiązki na podmioty finansowe. Incydent związany z ICT to zdarzenie lub seria zdarzeń nieplanowanych przez podmiot finansowy, które zagrażają bezpieczeństwu sieci i systemów informatycznych i mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych lub usług, a poważny incydent związany

z ICT to taki o dużym negatywnym wpływie na sieci i systemy wspierające krytyczne lub istotne funkcje podmiotu (art. 3 pkt 8 i 10) [7]. Podmioty kluczowe i ważne z sektora bankowości i infrastruktury rynków finansowych nie stosują przepisów ustawy o KSC o zgłaszaniu poważnych incydentów (art. 8i ust. 1) i zgłaszają je na podstawie DORA. Ustawa o KSC wskazuje Komisję Nadzoru Finansowego jako właściwy organ w rozumieniu DORA (art. 2 pkt 14a) [2]. Rozporządzenie opisuje hasło DORA w słowniku CyberKatalog.pl [8].

Nowelizacja ustawy o KSC wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555, znaną jako NIS2 [9], którą szerzej opisuje hasło NIS2 w słowniku CyberKatalog.pl [10].

1.2 Od czego liczy się termin

Termin 72 h występuje w KSC, RODO i DORA, ale pierwszy dokument, jego termin i zdarzenie, od którego się go liczy, są w każdym inne. W ustawie o KSC zarówno wczesne ostrzeżenie, jak i zgłoszenie incydentu poważnego liczą się od momentu jego wykrycia (art. 11 ust. 1 pkt 4 i 4a) [2]. W RODO administrator liczy 72 h od stwierdzenia naruszenia (art. 33 ust. 1) [5]. W DORA wstępne powiadomienie liczy się od sklasyfikowania incydentu jako poważny, z górną granicą 24 h od chwili, w której podmiot dowiedział się o incydencie; gdy klasyfikacja zapada po tej granicy, obowiązuje tylko termin 4 h od niej (art. 5 ust. 1 lit. a i ust. 2 rozporządzenia 2025/301) [11]. **Wykrycie, stwierdzenie i sklasyfikowanie to trzy różne momenty tego samego zdarzenia**, a organizacja, która je pomyli, policzy termin od złej daty.

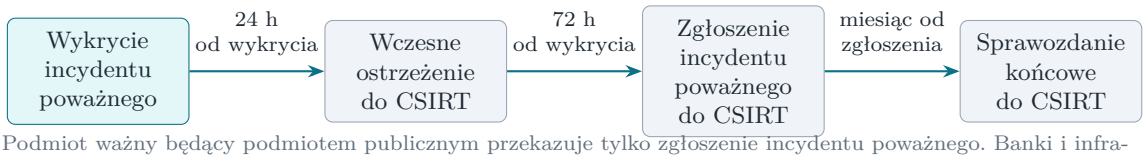
Rysunek 1.1 pokazuje kolejne dokumenty według KSC, RODO i DORA oraz terminy między nimi, przy czym zawiadomienie osób w RODO biegnie niezależnie od zgłoszenia do Prezesa UODO. Pełne zestawienie terminów, punktów odniesienia, adresatów i podstaw prawnych zawiera tabela 1.1.

1.3 Ustawa o KSC

Podmiot kluczowy lub ważny przekazuje wczesne ostrzeżenie o incydencie poważnym niezwłocznie, nie później niż w 24 h od jego wykrycia, do właściwego CSIRT sektorowego (art. 11 ust. 1 pkt 4) [2]. Zgłoszenie incydentu poważnego składa niezwłocznie, nie później niż w 72 h od wykrycia (art. 11 ust. 1 pkt 4a) [2]. Sprawozdanie okresowe składa na wniosek CSIRT sektorowego (art. 11 ust. 1 pkt 4b), a sprawozdanie końcowe nie później niż w miesiąc od dnia zgłoszenia (art. 11 ust. 1 pkt 4c) [2]. Gdy obsługa incydentu trwa dłużej, w terminie sprawozdania końcowego podmiot składa sprawozdanie z postępu, a sprawozdanie końcowe w miesiąc od zakończenia obsługi (art. 12b ust. 1 i 2) [2]. Sprawozdanie końcowe opisuje szczegółowo incydent, rodzaj zagrożenia lub jego przyczynę, zastosowane środki i skutki transgraniczne (art. 12a) [2]. Dostawca usług zaufania zgłasza incydent poważny w 24 h od wykrycia (art. 11 ust. 1a) [2]. Wszystkie te dokumenty przekazuje się przez system teleinformatyczny, o którym mowa w art. 46 ust. 1 ustawy (art. 11 ust. 2) [2]; dostęp do niego opisuje rozdział 7.

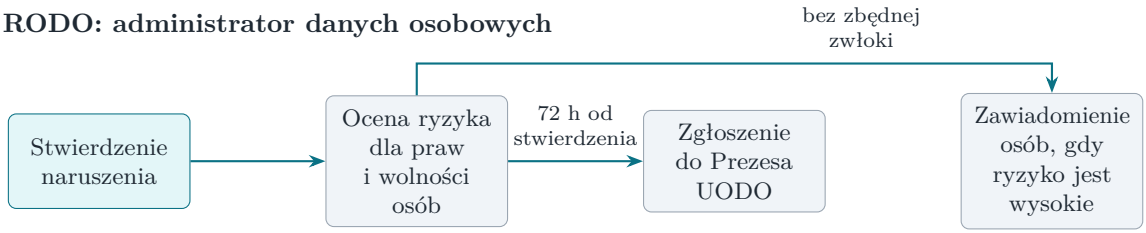
Wczesne ostrzeżenie zawiera dane podmiotu, osobę zgłaszającą i osobę do wyjaśnień, moment wystąpienia i wykrycia incydentu oraz czas jego trwania, informację, czy incydent wywołało działanie bezprawne lub działanie w złej wierze, jeśli da się to ocenić, i czy dotyczy on innych państw Unii Europejskiej (art. 12 ust. 1) [2]. Może też zawierać prośbę o wytyczne

Ustawa o KSC: podmiot kluczowy lub podmiot ważny



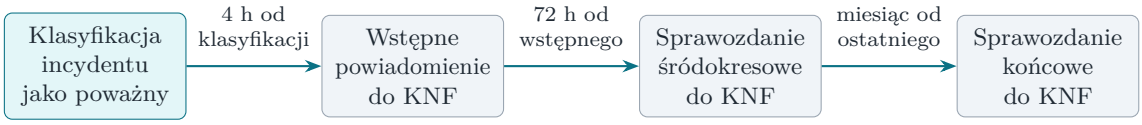
Podmiot ważny będący podmiotem publicznym przekazuje tylko zgłoszenie incydentu poważnego. Banki i infrastruktura rynków finansowych zgłaszają poważny incydent tylko według DORA (art. 8i).

RODO: administrator danych osobowych



Zgłoszenie do UODO nie jest wymagane, gdy ryzyko dla osób jest mało prawdopodobne. Zawiadomienie osób nie czeka na to zgłoszenie. Każde naruszenie trafia do dokumentacji.

DORA: podmiot finansowy



Wstępne powiadomienie idzie nie później niż 24 h od powzięcia wiadomości o incydencie. Gdy incydent zostaje sklasyfikowany jako poważny później, termin wynosi 4 h od klasyfikacji.

Rysunek 1.1: Pierwszy termin i zdarzenie, od którego się go liczy, są w każdym z trzech zestawów przepisów inne: 24 h od wykrycia incydentu poważnego (KSC), 72 h od stwierdzenia naruszenia (RODO) i 4 h od sklasyfikowania incydentu jako poważny, najpóźniej 24 h od powzięcia o nim wiadomości (DORA).

lub wsparcie techniczne; CSIRT sektorowy w 24 h przekazuje wtedy wytyczne albo udziela wsparcia, a przy incydencie wyczerpującym znamiona przestępstwa - także informację, jak zgłosić go organom ścigania (art. 12 ust. 2) [2]. Zgłoszenie 72-godzinne opisuje wpływ incydentu na usługę, w tym liczbę użytkowników, zasięg i wpływ na inne podmioty, przyczyny i przebieg zdarzenia oraz działania zapobiegawcze i naprawcze (art. 12 ust. 3) [2]. Podmiot przekazuje informacje znane mu w chwili zgłoszenia i uzupełnia je w trakcie obsługi incydentu (art. 12 ust. 5) [2].

Podmiot ważny będący podmiotem publicznym zgłasza wyłącznie incydent poważny, w 72 h od wykrycia, bez wczesnego ostrzeżenia i bez sprawozdań (art. 12c w związku z art. 11 ust. 1 pkt 4a) [2]. Podmiot kluczowy lub ważny informuje użytkowników swoich usług o incydencie poważnym, jeżeli ma on niekorzystny wpływ na świadczenie tych usług, a przy poważnym cyberzagrożeniu - o możliwych środkach zapobiegawczych (art. 11 ust. 2a i 2b) [2]. Informacje o innych incydentach, cyberzagrożeniach, wynikach szacowania ryzyka, podatnościach i potencjalnych zdarzeniach podmiot kluczowy lub ważny może przekazywać CSIRT dobrowolnie (art. 13 ust. 1) [2].

Progi, po przekroczeniu których incydent uznaje się za poważny, określa rozporządzenie Rady Ministrów, z wyłączeniem podmiotów, dla których progi określiła Komisja Europejska (art. 11 ust. 4) [2]. Komisja zrobiła to w rozporządzeniu wykonawczym (UE) 2024/2690 dla rejestrów nazw TLD i dostawców: usług DNS, usług chmurowych, usług ośrodka przetwarzania

Tabela 1.1: Trzy zegary zgłoszeń

Dokument	Termin	Liczony od	Adresat	Podstawa
Ustawa o KSC: podmiot kluczowy lub ważny spoza bankowości i infrastruktury rynków finansowych				
Wczesne ostrzeżenie	24 h	wykrycia incydentu poważnego	właściwy CSIRT, przez system S46	art. 11 ust. 1 pkt 4 i ust. 2
Zgłoszenie incydentu poważnego	72 h	wykrycia incydentu poważnego	właściwy CSIRT, przez system S46	art. 11 ust. 1 pkt 4a
Sprawozdanie końcowe	miesiąc	dnia zgłoszenia incydentu poważnego	właściwy CSIRT, przez system S46	art. 11 ust. 1 pkt 4c
RODO: administrator danych osobowych				
Zgłoszenie naruszenia	72 h, w miarę możliwości	stwierdzenia naruszenia	Prezes UODO	art. 33 ust. 1
Zawiadomienie osób, gdy ryzyko jest wysokie	bez zbędnej zwłoki	przepis nie wskazuje	osoby, których dane dotyczą	art. 34 ust. 1
RODO: podmiot przetwarzający				
Powiadomienie administratora	bez zbędnej zwłoki	stwierdzenia naruszenia	administrator	art. 33 ust. 2
DORA: podmiot finansowy				
Wstępne powiadomienie	4 h, najpóźniej 24 h	sklasyfikowania jako poważny; powzięcia wiadomości o incydencie	KNF	art. 19 ust. 4 DORA, art. 5 ust. 1 lit. a rozp. 2025/301
Sprawozdanie śródokresowe	72 h	przedłożenia wstępnego powiadomienia	KNF	art. 5 ust. 1 lit. b rozp. 2025/301
Sprawozdanie końcowe	miesiąc	ostatniego sprawozdania śródokresowego	KNF	art. 5 ust. 1 lit. c rozp. 2025/301

danych, sieci dostarczania treści, usług zarządzanych, usług zarządzanych w zakresie bezpieczeństwa, internetowych platform handlowych, wyszukiwarek internetowych, platform usług sieci społecznościowych i usług zaufania [12]. Do wydania nowego rozporządzenia obowiązuje dotychczasowe, najdłużej przez 12 miesięcy od wejścia w życie nowelizacji (art. 32 pkt 1 ustawy nowelizującej) [2]. Na dzień 24 września 2026 r. jest to rozporządzenie Rady Ministrów z 31 października 2018 r., które określa progi tylko dla sektorów dawnej ustawy: energii, transportu, bankowości i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną i jej dystrybucji oraz infrastruktury cyfrowej (§ 1 i załącznik) [13]. Dla sektorów dodanych nowelizacją progów w nim nie ma i zostaje sama definicja incydentu poważnego z art. 2 pkt 7.

Do czasu komunikatu o osiągnięciu przez właściwy CSIRT sektorowy zdolności operacyjnej podmioty zgłaszają incydenty poważne do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV (art. 44 ust. 1 i 2 ustawy nowelizującej). Wyjątkiem są sektory, w których sektorowy zespół cyberbezpieczeństwa powołano przed 2025 r., bo taki zespół jest już CSIRT sektorowym (art. 44 ust. 3 i art. 46 ustawy nowelizującej) [2]. Pełną mapę właściwości omawia rozdział 7.

Nowelizacja weszła w życie 3 kwietnia 2026 r. (art. 49 ustawy nowelizującej) [2]. Podmioty, które w dniu wejścia w życie nowelizacji spełniały przesłanki podmiotu kluczowego lub ważnego, wykonują obowiązki z rozdziału 3 ustawy, w tym zgłaszanie incydentów, w terminie 12 miesięcy od wejścia w życie nowelizacji, czyli do 3 kwietnia 2027 r. (art. 33 ust. 1 ustawy nowelizującej) [2]. Dawni operatorzy usług kluczowych przechodzą na zgłaszanie incydentów poważnych według nowych art. 11-12b w terminie 6 miesięcy od wejścia w życie nowelizacji, czyli do 3 października

2026 r. (art. 33 ust. 4 ustawy nowelizującej) [2]. Są to terminy na dostosowanie organizacji do nowych przepisów, ale **obowiązków z RODO nie przesuwają**. Kalendarz kolejnych terminów wdrożenia omawia artykuł o kalendarzu obowiązków cyberbezpieczeństwa [14].

1.4 RODO

Administrator zgłasza naruszenie ochrony danych osobowych organowi nadzorczemu bez zbędnej zwłoki, w miarę możliwości nie później niż w 72 h po jego stwierdzeniu, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych; do zgłoszenia złożonego po 72 h dołącza wyjaśnienie przyczyn opóźnienia (art. 33 ust. 1) [5]. Podmiot przetwarzający zgłasza naruszenie administratorowi bez zbędnej zwłoki (art. 33 ust. 2) [5]. Zgłoszenie opisuje co najmniej charakter naruszenia, w tym kategorie i przybliżoną liczbę osób i wpisów, których dotyczy, podaje dane inspektora ochrony danych lub innego punktu kontaktowego oraz opisuje możliwe konsekwencje i zastosowane lub proponowane środki (art. 33 ust. 3) [5]. Informacje, których nie da się podać od razu, administrator przekazuje sukcesywnie, a wszystkie naruszenia dokumentuje (art. 33 ust. 4 i 5) [5].

Przy wysokim ryzyku naruszenia praw lub wolności administrator bez zbędnej zwłoki zawiadamia o naruszeniu osobę, której dane dotyczą, jasnym i prostym językiem (art. 34 ust. 1 i 2) [5]. Trzy wyjątki zwalniają z tego obowiązku: zastosowanie szyfrowania lub podobnych środków uniemożliwiających odczyt danych, zastosowanie później środków eliminujących wysokie ryzyko oraz sytuację, w której zawiadomienie wymagałoby niewspółmiernie dużego wysiłku; w ostatnim przypadku administrator publikuje komunikat publiczny (art. 34 ust. 3) [5]. Organ nadzorczy może mimo to zażądać zawiadomienia osób (art. 34 ust. 4) [5]. W Polsce organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych (art. 34 ust. 1 i 2 ustawy o ochronie danych osobowych) [15].

1.5 DORA

Podmiot finansowy zgłasza poważny incydent związany z ICT właściwemu organowi w trzech etapach: wstępnym powiadomieniem, sprawozdaniem śródokresowym i sprawozdaniem końcowym (art. 19 ust. 1 i 4) [7]. Przy poważnym incydencie wpływającym na interesy finansowe klientów podmiot informuje ich bez zbędnej zwłoki (art. 19 ust. 3) [7].

Terminy określa rozporządzenie delegowane 2025/301. Wstępne powiadomienie idzie tak szybko, jak to możliwe, w ciągu 4 h od sklasyfikowania incydentu jako poważny i nie później niż 24 h od momentu, w którym podmiot dowiedział się o incydencie (art. 5 ust. 1 lit. a) [11]. Gdy podmiot sklasyfikuje incydent jako poważny dopiero po upływie 24 h od powzięcia o nim wiadomości, wstępne powiadomienie idzie w ciągu 4 h od tej klasyfikacji (art. 5 ust. 2) [11]. Sprawozdanie śródokresowe podmiot składa najpóźniej w 72 h od wstępnego powiadomienia, także wtedy, gdy stan incydentu się nie zmienił, a sprawozdanie końcowe nie później niż w miesiąc od sprawozdania śródokresowego lub od jego ostatniej aktualizacji (art. 5 ust. 1 lit. b i c) [11]. Gdy terminu nie da się dotrzymać, podmiot informuje o tym właściwy organ najpóźniej w tym terminie i wyjaśnia przyczyny opóźnienia (art. 5 ust. 3) [11]. Gdy termin wypada w weekend albo w dzień wolny od pracy, dokument wolno złożyć do

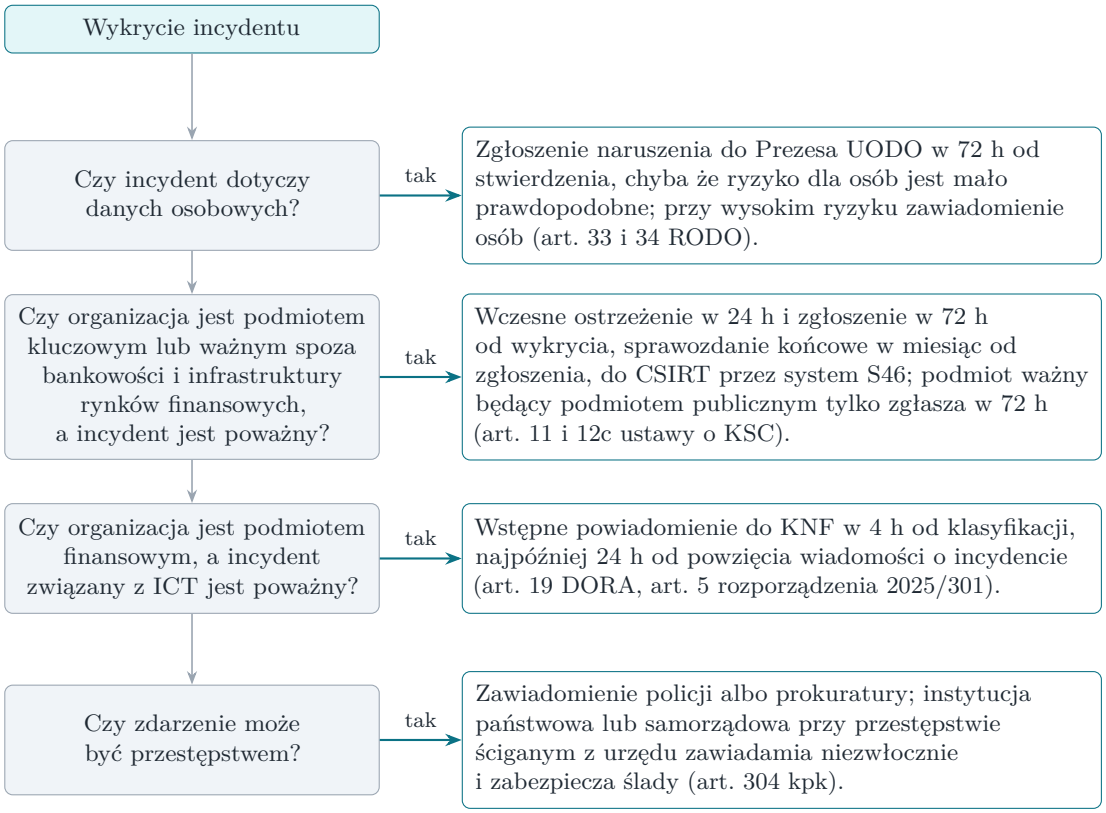
południa następnego dnia roboczego (art. 5 ust. 4) [11]. Instytucje kredytowe, kontrahenci centralni, operatorzy systemów obrotu i inne podmioty finansowe uznane za kluczowe lub ważne według NIS2 nie korzystają z tej ulgi przy wstępnym powiadomieniu i sprawozdaniu śródokresowym (art. 5 ust. 5), a właściwy organ może ją w tym zakresie wyłączyć także dla innych podmiotów znaczących dla sektora finansowego (art. 5 ust. 6) [11]. Kryteria klasyfikacji incydentów wymienia art. 18 ust. 1 DORA, a wraz z progami istotności doprecyzowuje je rozporządzenie delegowane Komisji (UE) 2024/1772 wydane na podstawie art. 18 ust. 3; o tym, kiedy incydent jest poważny, rozstrzyga art. 8 tego rozporządzenia [7, 16].

1.6 Jeden incydent, kilka zgłoszeń

Obowiązki z KSC, RODO i DORA nie wykluczają się nawzajem, z jednym wyjątkiem: banki i podmioty infrastruktury rynków finansowych zgłaszają poważny incydent tylko według DORA (art. 8i ust. 1 ustawy o KSC) [2]. Ten sam incydent może jednocześnie spełniać przesłanki incydentu poważnego z ustawy o KSC i naruszenia ochrony danych osobowych z RODO, jeśli podmiot kluczowy lub ważny przetwarza dane osobowe, a atak je narusza. Ransomware, który szyfruje bazę danych klientów podmiotu kluczowego, uruchamia oba zegary w tym samym momencie, ale od różnych zdarzeń: zegar KSC od wykrycia incydentu, zegar RODO od stwierdzenia naruszenia danych osobowych. **Organizacja składa wtedy dwa odrębne zgłoszenia, każde w swoim terminie**: incydentu poważnego do CSIRT i naruszenia ochrony danych osobowych do Prezesa UODO. Podmiot kluczowy lub ważny może złożyć oba w tym samym systemie teleinformatycznym, bo system z art. 46 ustawy o KSC służy także zgłaszaniu naruszeń z art. 33 RODO (art. 46 ust. 1 pkt 7) [2].

Cztery pytania ze schematu na rysunku 1.2 porządkują tę ocenę po wykryciu incydentu: czy dotyczy on danych osobowych, czy organizacja jest podmiotem kluczowym lub ważnym spoza bankowości i infrastruktury rynków finansowych z incydentem poważnym, czy jest podmiotem finansowym objętym DORA i czy zdarzenie może wyczerpywać znamiona przestępstwa.

Ostatnie pytanie dotyczy obowiązku, który biegnie obok KSC, RODO i DORA i wynika z kodeksu postępowania karnego: kto dowiedział się o przestępstwie ściganym z urzędu, ma społeczny obowiązek zawiadomić o tym prokuratora lub policję (art. 304 § 1 kodeksu postępowania karnego) [17]. Instytucja państwowa lub samorządowa, która w związku ze swoją działalnością dowiedziała się o takim przestępstwie, jest obowiązana niezwłocznie zawiadomić prokuratora lub policję i podjąć niezbędne czynności, żeby nie dopuścić do zatarcia śladów i dowodów, do czasu przybycia organu (art. 304 § 2 kodeksu postępowania karnego) [17].



Rysunek 1.2: Cztery pytania po wykryciu incydentu. Każde zadaje się niezależnie od odpowiedzi na poprzednie, więc kilka odpowiedzi "tak" oznacza kilka zgłoszeń.

Rozdział 2

Pierwsza godzina: kroki wspólne

Niezależnie od tego, czy chodzi o phishing, przejęcie konta, ransomware czy wyciek danych, pierwsza godzina zaczyna się od tych samych kroków. Wykonaj je, zanim ustalisz, który scenariusz z kolejnych rozdziałów pasuje do sytuacji.

2.1 Kto decyduje

O uruchomieniu procedury decyduje osoba wskazana przed incydentem. Wpisz ją na kartę z załącznika A. W podmiocie kluczowym lub ważnym za cyberbezpieczeństwo odpowiadają wewnętrzne struktury albo dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, z którym podmiot zawarł umowę (art. 14) [2], a taki dostawca świadczy między innymi obsługę incydentów (art. 2 pkt 4j) [2]. Umowa z nim powinna mówić, kto po jego stronie przejmuje incydent, a kto po stronie organizacji podejmuje decyzje i składa zgłoszenia.

2.2 Dziennik zdarzeń

Terminy z rozdziału 1 liczą się od wykrycia incydentu, od stwierdzenia naruszenia albo od sklasyfikowania incydentu jako poważny, dlatego zapisz godzinę każdego z tych momentów i ustalaj kolejność zdarzeń (RS.AN-03) [18]. Zapisuj też czynności reagowania: kto, co i kiedy zrobił (RS.AN-06) [18]. Wstępne ustalenia, czyli co się stało i jak to wykryto, udokumentuj od razu (s. 22) [19]. Dziennik zawiera dane wrażliwe, więc chroń go tak jak inne takie dane (RS.AN-06) [18]. Na tym dzienniku opiera się każde zgłoszenie z rozdziału 1.

2.3 Zabezpieczenie śladów

Zbieraj dane i metadane incydentu tak, żeby zachować ich integralność i pochodzenie (RS.AN-07) [18]. Wiele z nich pochodzi z dzienników systemów, które organizacja powinna prowadzić jeszcze przed incydentem (PR.PS-04) [18]. Nie usuwaj wiadomości phishingowych, zaszyfrowanych plików ani notatek z żądaniem okupu, bo CSIRT potrzebuje ich do analizy (rozdziały 3 i 5).

2.4 Izolacja

Ustal, które systemy zostały naruszone, i natychmiast je odizoluj (s. 21) [19]. **Urządzenie wyłączaj tylko wtedy, gdy nie da się go odłączyć od sieci**, bo wyłączenie niszczy ślady w pamięci ulotnej (s. 21, s. 7) [19, 20].

2.5 Komunikacja poza zaatakowaną infrastrukturą

Działania uzgadniaj kanałem niezależnym od zaatakowanych systemów, na przykład telefonicznie (s. 21) [19], bo poczta i komunikatory organizacji mogą być pod kontrolą atakującego.

2.6 Wsparcie CSIRT

Podmiot kluczowy lub ważny może już we wczesnym ostrzeżeniu poprosić CSIRT o wytyczne albo o wsparcie techniczne, a CSIRT przekazuje je w ciągu 24 h (art. 12 ust. 2) [2].

2.7 Czego nie robić

- Nie wyłączaj urządzeń, które da się odłączyć od sieci.
- Nie usuwaj wiadomości, plików ani dzienników, które mogą być dowodem.
- Nie uzgadniaj działań kanałami, które mogą być pod kontrolą atakującego.
- Nie odtwarzaj danych z kopii zapasowych, zanim ograniczysz dostęp atakującego (rozdział 5).
- Nie ustalaj w trakcie incydentu tego, co da się ustalić wcześniej: kto decyduje, kogo powiadomić i którym kanałem.

Rozdział 3

Phishing i kliknięty link

Phishing to podszywanie się pod zaufanego nadawcę, które ma skłonić odbiorcę do podania hasła lub kodu albo do wykonania przelewu [21]. Otwarcie linku zwykle niczego nie uruchamia, chyba że strona wykorzystuje niezałataną podatność przeglądarki albo systemu [21]. Zjawisko opisuje też hasło phishing w słowniku CyberKatalog.pl [22].

3.1 Dla pracownika

Jeśli skończyło się na otwarciu strony i niczego na niej nie wpisałeś ani nie pobrałeś, nie musisz zmieniać haseł. Zgłoś jednak wiadomość działowi IT, bo mogła trafić także do innych osób w organizacji. Jeśli na fałszywej stronie podałeś dane, działaj od razu [21]:

- nadaj nowe hasło w tej usłudze i w każdej innej, w której miałeś to samo hasło;
- od razu powiedz o tym działowi IT, który zabezpieczy konto według rozdziału 4;
- jeśli podałeś dane karty, dane logowania do bankowości albo kod z SMS-a lub zatwierdziłeś operację w aplikacji banku, od razu zadzwoń do banku.

Zgłoś zdarzenie działowi IT albo przełożonemu, nawet gdy nie masz pewności, czy dane trafiły do oszusta.

Jeśli pobrałeś lub otworzyłeś plik, zainstalowałeś aplikację albo wkleiłeś polecenie, które kazała skopiować strona, **odłącz komputer od sieci przewodowej i bezprzewodowej, nie wyłączaj go i od razu zadzwoń do działu IT** (podrozdział 2.4, s. 7) [20, 21].

Podejrzany SMS przekaż na numer 8080 w oryginalnej formie, bez wycinania odnośnika ani treści. Z jednego numeru można zgłosić najwyżej trzy wiadomości w ciągu 4 h, a w Polsce przesłanie jest bezpłatne [23]. Podejrzaną stronę albo e-mail zgłoś przez formularz incydent.cert.pl i dołącz wiadomość w oryginale, najlepiej jako plik EML lub MSG, bo zawiera on nagłówki techniczne potrzebne do analizy, których nie odczyta się ze zrzutu ekranu ani ze zwykłego przekazania [24]. Obie drogi opisuje narzędzie CyberKatalog.pl do zgłaszania phishingu [25].

3.2 Dla działu IT

Konta, które mogły zostać naruszone, zabezpiecz według procedury z rozdziału 4. Ustal, kto jeszcze dostał tę wiadomość, i sprawdź logowania tych osób. Powstrzymaj rozprzestrzenianie

się incydentu (RS.MI-01) [18]: usuń wiadomość z pozostałych skrzynek i zablokuj nadawcę oraz adres fałszywej strony w filtrach poczty i stron organizacji. Fałszywą domenę sprawdź na Liście Ostrzeżeń CERT Polska [26], a jeśli jej tam nie ma, zgłoś ją przez incydent.cert.pl [24]. Listę można też włączyć w serwerach DNS organizacji, na przykład jako strefę RPZ odświeżaną co 5 minut, żeby pracownicy nie otwierali domen, które CERT Polska już oznaczył [27].

Wiadomość phishingowa, która nie wyrządziła szkody, nie uruchamia obowiązku zgłoszenia z ustawy o KSC ani z RODO, choć podmiot kluczowy lub ważny może przekazać informację o niej CSIRT dobrowolnie (art. 13 ust. 1) [2]. Obowiązek pojawia się, gdy phishing doprowadził do naruszenia ochrony danych osobowych albo gdy u podmiotu kluczowego lub ważnego jego skutki spełniają przesłanki incydentu poważnego. Tę ocenę porządkuje schemat na rysunku 1.2, a konto przejęte w ten sposób opisuje rozdział 4.

Zgłoszenia i pomoc w tym scenariuszu

Jeśli phishing doprowadził do naruszenia ochrony danych osobowych, administrator zgłasza je Prezesowi UODO w 72 h od stwierdzenia, chyba że ryzyko dla osób jest mało prawdopodobne. Jeśli organizacja jest podmiotem kluczowym lub ważnym spoza bankowości i infrastruktury rynków finansowych, a skutki spełniają przesłanki incydentu poważnego, wysyła do właściwego CSIRT przez system S46 wczesne ostrzeżenie w 24 h i zgłoszenie w 72 h od wykrycia. Podmiot finansowy zgłasza poważny incydent związany z ICT do KNF według DORA. Zdarzenie, które może być przestępstwem, zgłasza się policji albo prokuraturze. Zegary opisuje rozdział 1. Firmy pomagające w analizie i reagowaniu zbiera kategoria Monitoring i SOC [28], a szkolące pracowników kategoria Szkolenia i Świadomość [29].

Rozdział 4

Przejęcie konta

Przejęcie konta to uzyskanie przez atakującego dostępu do skrzynki pocztowej albo innego konta organizacji bez wiedzy i zgody jego właściciela. Według CERT Polska najczęstsze przyczyny przejęcia skrzynki to phishing, ponowne użycie hasła, które wyciekło z innej usługi, i złośliwe oprogramowanie wykradające dane logowania i sesji [30].

4.1 Odebranie dostępu

Gdy ktoś obcy dostał się do skrzynki albo innego konta organizacji, odbierz mu dostęp w tej kolejności:

1. Sprawdź reguły skrzynki i ustawienia przekierowania poczty. Atakujący często ustawia automatyczne przekazywanie wiadomości na zewnętrzny adres, żeby dostawać także wiadomości do zmiany hasła [31].
2. Zmień hasło i zakończ wszystkie sesje konta. Sama zmiana hasła nie wystarczy, bo urządzenia, na których atakujący jest już zalogowany, zachowują dostęp, dopóki nie zakończysz ich sesji [30].
3. Odłącz od konta nieznane aplikacje i urządzenia oraz cofnij zgody udzielone aplikacjom, których nikt w organizacji nie rozpoznaje [21].
4. Uruchom uwierzytelnianie wieloskładnikowe, żeby do logowania nie wystarczało samo hasło [30].
5. Sprawdź konta, które odzyskuje się przez ten adres: każde z nich atakujący może przejąć funkcją przypominania hasła [30]. Przejrzyj też wiadomości wysłane z przejętej skrzynki do klientów i kontrahentów.

Gdy atakujący zmienił już hasło, konto odzyskuje się przez administratora usługi pocztowej, bo tylko on ma taką możliwość, a CERT Polska jej nie ma [30]. Zgłoś przejęcie właściwemu CSIRT, bo opis metody pozwala ostrzec innych użytkowników [30].

4.2 Podszywanie się pod firmę

Przestępcy podszywają się pod kontrahentów, dostawców, a nawet członków zarządu, żeby wyłudzić przelew albo dane firmy. Najczęstsze metody to fałszywe wiadomości e-mail i faktury

ze zmienionym numerem rachunku, typowe dla ataków typu Business Email Compromise; policja przywołuje te dane za raportem antyfraudowym BIK [32]. Wiadomość bywa wysłana z prawdziwej skrzynki firmy, do której oszust ma dostęp, albo z adresu łudząco podobnego, więc samo sprawdzenie adresu nadawcy nie wystarcza [33]. **Nietypowe albo pilne polecenie zapłaty i każdą zmianę numeru rachunku potwierdź innym kanałem**, na przykład telefonicznie albo na spotkaniu. Wprowadź też procedurę weryfikacji przelewów i zmian numerów rachunków, o co apelują Związek Banków Polskich i partnerzy kampanii "Bankowcy dla CyberEdukacji" [32].

Jeśli z przejętej skrzynki organizacji wysłano wiadomości do klientów albo kontrahentów, ostrzeż ich innym kanałem niż poczta. Jeśli przelew już wyszedł, pilnie skontaktuj się z bankiem, z którego go wysłano [34]. Potem zawiadom policję albo prokuraturę: osobiście w dowolnej jednostce albo pisemnie w jednostce właściwej dla miejsca zdarzenia [35].

Zgłoszenia i pomoc w tym scenariuszu

Jeśli atakujący miał dostęp do danych osobowych w przejętym koncie, to naruszenie ochrony danych: administrator zgłasza je Prezesowi UODO w 72 h od stwierdzenia, chyba że ryzyko dla osób jest mało prawdopodobne. Podmiot kluczowy lub ważny spoza bankowości i infrastruktury rynków finansowych, u którego skutki spełniają przesłanki incydentu poważnego, wysyła do właściwego CSIRT przez system S46 wczesne ostrzeżenie w 24 h i zgłoszenie w 72 h od wykrycia. Podmiot finansowy zgłasza poważny incydent związany z ICT do KNF według DORA. Wyłudzony przelew zgłasza się pilnie bankowi, a potem policji albo prokuraturze. Zegary opisuje rozdział 1. Firmy pomagające w analizie i reagowaniu zbiera kategoria Monitoring i SOC [28].

Rozdział 5

Ransomware

Ransomware to złośliwe oprogramowanie, którym przestępcy wymuszają okup: szyfruje pliki, odcina dostęp do systemów albo wyprowadza dane [24]. Mechanizm opisuje hasło ransomware w słowniku CyberKatalog.pl [36].

5.1 Izolacja i pierwsze ustalenia

Izolację opisuje podrozdział 2.4. Gdy zainfekowanych jest wiele systemów albo podsieci, odetnij sieć na poziomie przełącznika, bo odłączanie pojedynczych urządzeń w trakcie ataku bywa niewykonalne (s. 21) [19]. Zachowaj kopię zaszyfrowanych plików, bo narzędzie do ich odszyfrowania może pojawić się później (s. 7) [20].

Zanim uznasz dane za stracone, sprawdź, czy atak objął wszystkie pliki i czy dla tej rodziny ransomware istnieje ogólnodostępne narzędzie deszyfrujące [24]. Rodzinę pomaga ustalić serwis No More Ransom (s. 7-8) [20], inicjatywa holenderskiej policji i Europolu z partnerami prywatnymi, która ma pomóc ofiarom odzyskać dane bez płacenia okupu [37].

5.2 Kopie zapasowe

Zanim przywrócisz dane, ustal i usuń źródło infekcji: przeanalizuj dzienniki pod kątem nietypowych działań i połączeń, bo atakujący może wrócić tą samą drogą (s. 7) [20]. Szukaj też złośliwego oprogramowania, które poprzedziło szyfrowanie, bo odtworzenie systemów razem z nim ponawia włamanie (s. 22) [19]. Systemy odtwarzaj w czystej sieci, z czystych, przygotowanych wcześniej obrazów, zaczynając od najważniejszych (s. 22, s. 8) [19, 20].

5.3 Zgłoszenie

Zgłaszając ransomware do CSIRT NASK przez incydent.cert.pl albo na adres cert@cert.pl, dołącz co najmniej dwa zaszyfrowane pliki i notatkę z żądaniem okupu (s. 8) [20]. Podmiot kluczowy lub ważny z dostępem do systemu S46 zgłasza incydent poważny przez ten system [38]. Podmiot z właściwości CSIRT GOV albo CSIRT MON zgłasza się bezpośrednio do tego zespołu [24].

5.4 Decyzja o okupie

Decyzję o zapłacie okupu podejmuje zarząd albo kierownik jednostki. Inicjatywa No More Ransom zaleca, żeby nigdy nie płacić okupu [39], a autorzy przewodnika CISA, w tym FBI, również nie zalecają płacenia, bo okup nie gwarantuje odszyfrowania danych, usunięcia atakującego z systemów ani tego, że wykradzione dane nie zostaną opublikowane (s. 21) [19]. **Zapłata nie zmienia obowiązków zgłoszeniowych**, bo wynikają one z samego incydentu i naruszenia danych, a ich terminy biegną od wykrycia incydentu, stwierdzenia naruszenia albo sklasyfikowania incydentu jako poważny, bez względu na decyzję o okupie. Kiedy zapłata może naruszać prawo i jak oceniają ją instytucje publiczne, wyjaśnia artykuł CyberKatalog.pl o tym, czy płacić okup po ataku ransomware [40].

Zgłoszenia i pomoc w tym scenariuszu

Ransomware, które zaszyfrowało albo wykradło dane osobowe, jest naruszeniem ochrony danych: administrator zgłasza je Prezesowi UODO w 72 h od stwierdzenia, chyba że ryzyko dla osób jest mało prawdopodobne. Podmiot kluczowy lub ważny spoza bankowości i infrastruktury rynków finansowych, u którego skutki spełniają przesłanki incydentu poważnego, wysyła do właściwego CSIRT przez system S46 wczesne ostrzeżenie w 24 h i zgłoszenie w 72 h od wykrycia. Podmiot finansowy zgłasza poważny incydent związany z ICT do KNF według DORA. Zdarzenie, które może być przestępstwem, zgłasza się policji albo prokuraturze (art. 304 kpk) [17]. Zegary opisuje rozdział 1. Firmy pomagające w analizie i reagowaniu zbiera kategoria Monitoring i SOC [28], a zabezpieczające infrastrukturę kategoria Bezpieczeństwo Infrastruktury [41].

Rozdział 6

Wyciek danych

Wyciek danych to nieuprawnione ujawnienie danych albo nieuprawniony dostęp do nich. Gdy dotyczy danych osobowych, jest naruszeniem ochrony danych osobowych, które według RODO obejmuje także zniszczenie, utracenie i zmodyfikowanie danych (art. 4 pkt 12) [5].

6.1 Moment stwierdzenia i ocena ryzyka

Termin 72 h liczy się od stwierdzenia naruszenia (art. 33 ust. 1) [5], a to, kiedy administrator je stwierdza, wyjaśniają wytyczne Europejskiej Rady Ochrony Danych (s. 12-15) [42]. Od oceny ryzyka dla praw i wolności osób zależy, czy naruszenie trzeba zgłosić i czy trzeba zawiadomić osoby. Wytyczne opisują ją w rozdziale IV (s. 26-30) i **przy jakichkolwiek wątpliwościach zalecają zgłoszenie** (s. 30) [42].

Informacje, których administrator nie zna w chwili zgłoszenia, przekazuje sukcesywnie, a do zgłoszenia złożonego po 72 h dołącza wyjaśnienie przyczyn opóźnienia (art. 33 ust. 1 i 4) [5]. Oba przypadki omawiają wytyczne (s. 18, s. 19) [42]. Każde naruszenie, także niezgłoszone, administrator dokumentuje (art. 33 ust. 5) [5].

6.2 Zgłoszenie do Prezesa UODO

Naruszenie zgłasza się Prezesowi Urzędu Ochrony Danych Osobowych elektronicznie, przez formularz na platformie biznes.gov.pl [43]. Podmiot kluczowy lub ważny może złożyć to zgłoszenie w systemie S46, bo system z art. 46 ustawy o KSC służy także zgłaszaniu naruszeń z art. 33 RODO, a zgłoszenie przyjmuje Prezes UODO (art. 46 ust. 1 pkt 7 i ust. 2) [2, 44]. Podmiot przetwarzający nie ma obowiązku zgłoszenia do organu: bez zbędnej zwłoki powiadamia administratora (art. 33 ust. 2) [5].

6.3 Zawiadomienie osób

Przy wysokim ryzyku naruszenia praw lub wolności administrator bez zbędnej zwłoki zawiadamia osoby, których dane dotyczą, jasnym i prostym językiem, chyba że zachodzi jeden z wyjątków z art. 34 ust. 3 RODO opisanych w rozdziale 1 [5]. Zawiadomienie opisuje charakter naruszenia i podaje co najmniej dane kontaktowe inspektora ochrony danych, możliwe

konsekwencje oraz zastosowane lub proponowane środki, w tym to, co osoby mogą zrobić same (art. 34 ust. 2 w związku z art. 33 ust. 3 lit. b-d) [5]. Przy bezpośrednim zagrożeniu kradzieżą tożsamości albo ujawnieniu w internecie danych szczególnych kategorii administrator zawiadamia osoby bez zbędnej zwłoki, w wyjątkowych okolicznościach nawet przed zgłoszeniem do Prezesa UODO (s. 18, pkt 59) [42]. Nie wysyłaj zawiadomienia kanałem, który naruszenie przejęło, bo atakujący może się nim podszyć pod administratora (s. 25, pkt 92) [42]. Przypadek, w którym dane wyciekły u dostawcy oprogramowania, a zawiadomić pacjentów mają placówki jako administratorzy, opisuje artykuł CyberKatalog.pl o wycieku danych z MyDr [45].

Przy opisie tego, co osoby mogą zrobić same, pomagają materiały CyberKatalog.pl: przewodnik CyberKatalog.pl po wycieku danych [46] prowadzi przez zastrzeżenie numeru PESEL, sprawdzenie danych w serwisie bezpiecznedane.gov.pl i rozpoznawanie fałszywych stron podszywających się pod ten serwis. Zastrzeżenie numeru PESEL [47] jest bezpłatne i można je zrobić w serwisie albo aplikacji mObywatel lub w urzędzie gminy.

Zgłoszenia i pomoc w tym scenariuszu

Administrator zgłasza naruszenie Prezesowi UODO w 72 h od stwierdzenia, chyba że ryzyko dla osób jest mało prawdopodobne, przez biznes.gov.pl albo, w podmiocie kluczowym lub ważnym, przez system S46. Przy wysokim ryzyku zawiadamia też osoby, których dane dotyczą. Jeśli organizacja jest podmiotem kluczowym lub ważnym spoza bankowości i infrastruktury rynków finansowych, a skutki spełniają przesłanki incydentu poważnego, do właściwego CSIRT idą wczesne ostrzeżenie w 24 h i zgłoszenie w 72 h od wykrycia. Podmiot finansowy zgłasza poważny incydent związany z ICT do KNF według DORA. Zdarzenie, które może być przestępstwem, zgłasza się policji albo prokuraturze. Zegary opisuje rozdział 1. Firmy pomagające w ocenie ryzyka i dokumentowaniu naruszeń zbiera kategoria Ochrona Danych [48].

Rozdział 7

Mapa instytucji

Tabela 7.1 zestawia, co się zgłasza, kto zgłasza i którą drogą. Droga zgłoszenia incydentu poważnego zależy jeszcze od dwóch rzeczy: który zespół CSIRT jest właściwy dla organizacji i czy ma ona dostęp do systemu S46.

Tabela 7.1: Kto przyjmuje które zgłoszenie

Co zgłaszasz	Kto zgłasza	Dokąd i jak	Podstawa i źródło
Incydent poważny	podmiot kluczowy lub ważny spoza bankowości i infrastruktury rynków finansowych	właściwy CSIRT przez system S46, a bez dostępu do niego kanałem wskazanym przez ten CSIRT; do komunikatu o zdolności operacyjnej CSIRT sektorowego zgłoszenie trafia do CSIRT MON, CSIRT NASK albo CSIRT GOV, chyba że zespół sektorowy powołano przed 2025 r.	art. 11 ust. 2 ustawy o KSC, art. 44 i 46 ustawy nowelizującej [49]
Incydent w organizacji spoza ustawy o KSC, fałszywa strona internetowa	każda organizacja i osoba fizyczna	CSIRT NASK, formularz incydent.cert.pl	[27, 50]
Podejrzana wiadomość SMS	każdy odbiorca	CERT Polska, przekazanie wiadomości w oryginalnej formie na numer 8080	[23]
Naruszenie ochrony danych osobowych	administrator	Prezes UODO, formularz elektroniczny na biznes.gov.pl; podmiot kluczowy lub ważny także przez system S46	art. 33 RODO, art. 46 ust. 1 pkt 7 ustawy o KSC [43, 44]
Poważny incydent związany z ICT	podmiot finansowy	KNF, System do Obsługi Incydentów DORA (SOID) pod adresem csirt.knf.gov.pl; gdy system nie działa, e-mail incydenty.dora@knf.gov.pl na formularzach KNF	art. 19 DORA, art. 2 pkt 14a ustawy o KSC [51]
Przestępstwo	każdy, a instytucja państwowa lub samorządowa obowiązkowo przy przestępstwie ściganym z urzędu	policja albo prokuratura: osobiście w dowolnej jednostce, pisemnie (e-mail, faks, poczta) w jednostce właściwej dla miejsca zdarzenia	art. 304 kpk [35]

7.1 Właściwość CSIRT MON, CSIRT NASK i CSIRT GOV

Czym jest zespół CSIRT, wyjaśnia hasło CSIRT w słowniku CyberKatalog.pl [52]. Podział między trzy zespoły CSIRT poziomu krajowego wynika z art. 26 ust. 5-7 ustawy o KSC [2, 53]. CSIRT MON obsługuje podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane oraz przedsiębiorców realizujących zadania na rzecz Sił Zbrojnych (ust. 5). CSIRT GOV obsługuje między innymi jednostki podległe Prezesowi Rady Ministrów lub przez niego nadzorowane, Narodowy Bank Polski, Bank Gospodarstwa Krajowego, wskazane w ustawie jednostki sektora finansów publicznych i podmioty, których systemy objęte są wykazem infrastruktury krytycznej, a także incydenty w takich systemach u podmiotów z właściwości CSIRT NASK (ust. 7). CSIRT NASK obsługuje pozostałe podmioty, w tym podmioty kluczowe i ważne spoza właściwości dwóch pozostałych zespołów, oraz osoby fizyczne (ust. 6).

Podmiot, który podlega CSIRT GOV albo CSIRT MON, kieruje zgłoszenie wprost do tego zespołu [24], a zespół, do którego trafiło zgłoszenie spoza jego właściwości, niezwłocznie przekazuje je zespołowi właściwemu (art. 26 ust. 8) [53]. Do czasu komunikatu o osiągnięciu przez właściwy CSIRT sektorowy zdolności operacyjnej podmioty zgłaszają incydenty poważne do właściwego CSIRT MON, CSIRT NASK albo CSIRT GOV (art. 44 ust. 1 i 2 ustawy nowelizującej). Wyjątkiem są sektory, w których sektorowy zespół cyberbezpieczeństwa powołano przed 2025 r., bo taki zespół jest już CSIRT sektorowym (art. 44 ust. 3 i art. 46 ustawy nowelizującej) [2].

CSIRT GOV przyjmuje zgłoszenia przez system S46, przez formularz ze swojej strony przesłany e-mailem, a gdy droga elektroniczna jest niemożliwa, faksem [54].

7.2 System S46

Obowiązkowe zgłoszenia incydentów poważnych podmiot kluczowy albo ważny składa w systemie S46, jeśli ma do niego dostęp [24]. Dostęp przychodzi po wpisie do wykazu podmiotów kluczowych i ważnych, a do systemu loguje się przez Węzeł Krajowy [38]. Korzystanie z systemu podmioty rozpoczynają według harmonogramu ministra: strony porozumień o korzystaniu z S46 zawartych przed 3 kwietnia 2026 r. w terminie od 8 kwietnia 2026 r., pozostałe od 12 czerwca 2026 r., w obu przypadkach najpóźniej do 3 kwietnia 2027 r. (pkt 2) [55].

Wczesne ostrzeżenie to zgłoszenie z klasyfikacją "Poważny" i zaznaczonym polem "Wczesne ostrzeżenie", a zgłoszenie w 72 h powstaje przez uzupełnienie tego samego wpisu o pełny zakres danych [49]. **Termin dotrzymuje dopiero wysłanie**, bo zapisane zgłoszenie jest tylko kopią roboczą widoczną w podmiocie [38, 49]. Adresatów system ustawia sam, na podstawie wpisu w wykazie: właściwy CSIRT sektorowy i zespół CSIRT poziomu krajowego, a gdy podmiotowi nie przypisano CSIRT sektorowego, tylko ten drugi [49]. Bez dostępu do S46 zgłoszenie idzie kanałem zastępczym, który wskaże właściwy CSIRT. W CSIRT NASK jest nim formularz incydent.cert.pl, który najpierw pyta o dostęp do S46 [24]. Informacji niejawnych nie zgłasza się przez S46, tylko innym dopuszczonym kanałem komunikacji z zespołem CSIRT [49].

7.3 Naruszenie ochrony danych osobowych

Prezes UODO przyjmuje zgłoszenia naruszeń przez formularz na platformie biznes.gov.pl [43], a od podmiotów kluczowych i ważnych także przez system S46 (art. 46 ust. 1 pkt 7 i ust. 2 ustawy o KSC) [2, 44].

7.4 Poważny incydent związany z ICT

Podmiot finansowy zgłasza poważny incydent związany z ICT Komisji Nadzoru Finansowego przez System do Obsługi Incydentów DORA (SOID) pod adresem csirt.knf.gov.pl. Gdy zgłoszenie przez system nie jest możliwe, wysyła je e-mailem na adres incydenty.dora@knf.gov.pl na formularzach KNF, a po przywróceniu systemu rejestruje je w SOID [51].

7.5 Przestępstwo

Zawiadomienie o przestępstwie przyjmuje osobiście każda jednostka policji, a w godzinach pracy każda jednostka prokuratury; zgłoszenie złożone w jednostce niewłaściwej dla miejsca zdarzenia trafia do właściwej. Pisemne zawiadomienie wysyła się e-mailem, faksem lub pocztą do jednostki właściwej dla miejsca zdarzenia, która wzywa potem do jego ustnego uzupełnienia [35]. Warto dołączyć do niego to, co zabezpieczył dziennik incydentu: adresy stron, korespondencję w niezmienionej formie, numery rachunków i potwierdzenia przelewów [34]. W policji cyberprzestępczością zajmuje się Centralne Biuro Zwalczania Cyberprzestępczości [34].

Rozdział 8

Kto pomoże z zewnątrz

Podmiot kluczowy lub ważny może zamiast budowy własnych struktur odpowiedzialnych za cyberbezpieczeństwo zawrzeć umowę z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa (art. 14), a taki dostawca świadczy między innymi obsługę incydentów (art. 2 pkt 4j) [2]. Pomoc z zewnątrz przydaje się też organizacjom spoza ustawy, gdy incydent przerasta ich zespół.

8.1 Kiedy wezwać zewnętrzny zespół

Zewnętrzny zespół reagowania warto wezwać, gdy incydent obejmuje wiele systemów naraz, wymaga analizy śledczej albo dotyczy kont samego działu IT, na przykład konta administratora. **Wezwanie nie przesuwa terminów zgłoszeń**, więc dziennik zdarzeń z rozdziału 2 prowadzi się od pierwszej minuty, niezależnie od tego, kto przejmie obsługę.

8.2 O co zapytać dostawcę, zanim dojdzie do incydentu

- Kto po stronie dostawcy przyjmuje zgłoszenie i po jakim czasie zaczyna działać.
- Kto po stronie organizacji podejmuje decyzje w pierwszej godzinie i kto składa zgłoszenia do CSIRT, Prezesa UODO albo KNF.
- Jakie informacje dostawca przekaże na czas, żeby organizacja dotrzymała terminów 24 i 72 h.
- Jak dostawca zbiera i zabezpiecza dowody oraz dzienniki systemów, żeby zachować ich integralność (RS.AN-07, PR.PS-04) [18].
- Czy dostawca zna wymagania zgłoszeniowe, którym podlega organizacja: ustawę o KSC, RODO, a w sektorze finansowym także DORA.

8.3 Kategorie w katalogu

W katalogu CyberKatalog.pl firmy pomagające przed incydentem i po nim znajdziesz między innymi w kategoriach:

- Monitoring i SOC [28], w której mieści się reagowanie na incydenty;

- Ochrona Danych [48];
- GRC i Zgodność [56];
- Wdrożenie NIS2 i KSC [57];
- Wdrożenie DORA [58];
- Szkolenia i Świadomość [29];
- Bezpieczeństwo Infrastruktury [41];
- Bezpieczeństwo Chmury [59].

Katalog porządkuje firmy według kategorii usług i jest wobec nich neutralny: bez rankingu i bez rekomendacji. Kto w Polsce wdraża NIS2 i ustawę o KSC, opisuje artykuł CyberKatalog.pl o wykonawcach NIS2 i KSC [60].

Załącznik A

Karta "Pierwsze 72 godziny"

Karta na następnej stronie mieści na jednej stronie A4 to, czego zespół potrzebuje w pierwszych godzinach: siedem pierwszych kroków, zegar zgłoszeń według ustawy o KSC, RODO i DORA, drogi zgłoszeń do instytucji oraz pola na kontakty do osoby odpowiedzialnej za incydenty, działu IT, inspektora ochrony danych, zarządu, zewnętrznego zespołu reagowania, ubezpieczyciela i banku.

Wydrukuj kartę, wpisz kontakty przed incydentem i trzymaj ją tam, gdzie sięgną po nią osoby reagujące na incydenty. Kartę można też pobrać jako osobny plik PDF ze strony publikacji CyberKatalog.pl [1].

Pierwsze 72 godziny po incydencie

Terminy zgłoszeń, pierwsze kroki i kontakty

Najpierw

1. Zapisz datę i godzinę wykrycia oraz to, co widzisz, a potem chwilę stwierdzenia naruszenia danych osobowych i sklasyfikowania incydentu jako poważny. Od tych chwil biegną terminy zgłoszeń.
2. Odłącz zainfekowane urządzenia od sieci. Nie wyłączaj ich, jeśli da się je odłączyć, bo pamięć ulotna przechowuje ślady.
3. Zabezpiecz dowody: dzienniki systemów, wiadomości, zrzuty ekranu. Zapisuj każde podjęte działanie z godziną.
4. Uzgadniaj działania kanałem spoza zaatakowanej infrastruktury, na przykład telefonicznie.
5. Powiadom osoby z listy kontaktów niżej.
6. Sprawdź, czy incydent dotyczy danych osobowych, czy organizacja podlega ustawie o KSC albo DORA i czy zdarzenie może być przestępstwem. Każda odpowiedź "tak" to osobne zgłoszenie, ale banki i infrastruktura rynków finansowych zgłaszają poważny incydent tylko według DORA.
7. O okupie decyduje zarząd albo kierownik jednostki. Instytucje publiczne odradzają zapłatę, a narzędzia do odszyfrowania zbiera nomoreransom.org.

Kontakty

Osoba odpowiedzialna za incydenty

Dział IT

Inspektor ochrony danych

Zarząd lub kierownik jednostki

Zewnętrzny zespół reagowania

Ubezpieczyciel

Bank

Zegar zgłoszeń

Ustawa o KSC: incydent poważny

24 h od wykrycia	wczesne ostrzeżenie do CSIRT
72 h od wykrycia	zgłoszenie incydentu do CSIRT
miesiąc od zgłoszenia	sprawozdanie końcowe

Przez system S46. Podmiot ważny będący podmiotem publicznym przekazuje tylko zgłoszenie w 72 h. Banki i infrastruktura rynków finansowych zgłaszają tylko według DORA. Podmioty objęte nowelizacją stosują te terminy najpóźniej od 3 kwietnia 2027 r., dawni operatorzy usług kluczowych od 3 października 2026 r.

RODO: naruszenie ochrony danych

72 h od stwierdzenia	zgłoszenie do Prezesa UODO, chyba że ryzyko dla osób jest mało prawdopodobne
bez zbędnej zwłoki	zawiadomienie osób przy wysokim ryzyku

Każde naruszenie trafia do dokumentacji.

DORA: poważny incydent związany z ICT

4 h od klasyfikacji	wstępne powiadomienie do KNF, najpóźniej 24 h od powzięcia wiadomości
72 h od wstępnego	sprawozdanie śródokresowe
miesiąc od ostatniego	sprawozdanie końcowe

Podmioty finansowe. Przy klasyfikacji po 24 h wstępne powiadomienie idzie w 4 h od niej.

Przestępstwo

bez terminu	zawiadomienie policji albo prokuratury

Instytucje państwowe i samorządowe zawiadamiają niezwłocznie o przestępstwie ściganym z urzędu i zabezpieczają ślady.

Instytucje

Incydent poważny	system S46: właściwy CSIRT, adresata ustawia system
Naruszenie danych	Prezes UODO: biznes.gov.pl, podmioty KSC także S46
Incydent ICT w finansach	KNF: system SOID, csirt.knf.gov.pl
Organizacja spoza KSC, fałszywa strona	CSIRT NASK: incydent.cert.pl
Podejrzany SMS	przekaż w oryginale na numer 8080
Przestępstwo	policja albo prokuratura: osobiście w każdej jednostce

Zgłoszenie wysłane do niewłaściwego CSIRT trafia do właściwego.

Stan prawny na 24 września 2026 r. | CC BY-ND 4.0

Bibliografia

[1] CyberKatalog.pl. *Publikacje*. URL: https://cyberkatalog.pl/publikacje (dostęp 24 września 2026).

[2] *Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*. Dz.U. 2026 poz. 252. 2 marca 2026. URL: https://dziennikustaw.gov.pl/DU/2026/252 (dostęp 23 września 2026).

[3] CyberKatalog.pl. *Krajowy system cyberbezpieczeństwa*. Narzędzie: kto podlega ustawie i jakie ma obowiązki. URL: https://cyberkatalog.pl/narzedzia/krajowy-system-cyberbezpieczenstwa (dostęp 23 września 2026).

[4] CyberKatalog.pl. *Security Incident*. Hasło w słowniku cyberbezpieczeństwa. URL: https://cyberkatalog.pl/slownik/security-incident (dostęp 23 września 2026).

[5] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*. Dz.Urz. UE L 119 z 4.05.2016 ze zm. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/pol (dostęp 23 września 2026).

[6] CyberKatalog.pl. *GDPR*. Hasło w słowniku cyberbezpieczeństwa. URL: https://cyberkatalog.pl/slownik/gdpr (dostęp 23 września 2026).

[7] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (DORA)*. Dz.Urz. UE L 333 z 27.12.2022 ze zm. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/pol (dostęp 23 września 2026).

[8] CyberKatalog.pl. *DORA*. Hasło w słowniku cyberbezpieczeństwa. URL: https://cyberkatalog.pl/slownik/dora (dostęp 23 września 2026).

[9] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dyrektywa NIS 2)*. Dz.Urz. UE L 333 z 27.12.2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/pol (dostęp 23 września 2026).

[10] CyberKatalog.pl. *NIS2*. Hasło w słowniku cyberbezpieczeństwa. URL: https://cyberkatalog.pl/slownik/nis2 (dostęp 23 września 2026).

[11] *Rozporządzenie delegowane Komisji (UE) 2025/301 z dnia 23 października 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających treść i terminy przedłożenia wstępnego powiadomienia, sprawozdania śródokresowego i sprawozdania końcowego dotyczących poważnych incydentów związanych z ICT, a także treść dobrowolnego powiadomienia o znaczących cyberzagrożeniach.* Dz.Urz. UE L z 20.02.2025. URL: https://eur-lex.europa.eu/eli/reg_del/2025/301/oj/pol (dostęp 23 września 2026).

[12] *Rozporządzenie wykonawcze Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiające zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz dostawców usług zaufania.* Dz.Urz. UE L z 18.10.2024. URL: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/pol (dostęp 24 września 2026).

[13] *Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny.* Dz.U. 2018 poz. 2180. URL: https://dziennikustaw.gov.pl/DU/2018/2180 (dostęp 24 września 2026).

[14] CyberKatalog.pl. *Kalendarz obowiązków cyberbezpieczeństwa: NIS2, KSC, CRA i DORA.* Artykuł. URL: https://cyberkatalog.pl/aktualnosci/artykuly/kalendarz-obowiazkow-cyberbezpieczenstwa (dostęp 23 września 2026).

[15] *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, tekst jednolity.* Dz.U. 2019 poz. 1781 ze zm. URL: https://dziennikustaw.gov.pl/DU/2019/1781 (dostęp 23 września 2026).

[16] *Rozporządzenie delegowane Komisji (UE) 2024/1772 z dnia 13 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających kryteria klasyfikacji incydentów związanych z ICT i cyberzagrożeń, progi istotności i szczegółowe informacje dotyczące zgłaszania poważnych incydentów.* Dz.Urz. UE L z 25.06.2024. URL: https://eur-lex.europa.eu/eli/reg_del/2024/1772/oj/pol (dostęp 24 września 2026).

[17] *Ustawa z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego, tekst jednolity.* Dz.U. 2026 poz. 490 ze zm. URL: https://dziennikustaw.gov.pl/DU/2026/490 (dostęp 23 września 2026).

[18] Alex Nelson, Sanjay Rekhi, Murugiah Souppaya i Karen Scarfone. *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.* NIST Special Publication 800-61 Rev. 3. National Institute of Standards and Technology, kwiecień 2025. DOI: 10.6028/NIST.SP.800-61r3. URL: https://web.archive.org/web/20260828122510/https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf (dostęp 23 września 2026).

[19] Cybersecurity and Infrastructure Security Agency, Multi-State Information Sharing and Analysis Center, National Security Agency i Federal Bureau of Investigation. *#StopRansomware Guide*. Version 3.0. Październik 2023. URL: https://web.archive.org/web/20260823184717/https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf (dostęp 23 września 2026).

[20] CERT Polska. *Poradnik ransomware*. URL: https://web.archive.org/web/20260801132345/https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf (dostęp 23 września 2026).

[21] CERT Polska. *Phishing: jak rozpoznać oszustwo i nie dać się nabrać*. Baza wiedzy CERT Polska. 2 września 2026. URL: https://web.archive.org/web/20260906104219/https://wiedza.cert.pl/bezpieczenstwo-osobiste/rozpoznanie-phishingu/ (dostęp 23 września 2026).

[22] CyberKatalog.pl. *Phishing*. Hasło w słowniku cyberbezpieczeństwa. URL: https://cyberkatalog.pl/slownik/phishing (dostęp 23 września 2026).

[23] Ministerstwo Cyfryzacji. *Dostałeś niepokojący sms albo email? Zgłoś go do CERT Polska (CSIRT NASK)*. Baza wiedzy gov.pl. URL: https://web.archive.org/web/20260917070658/https://www.gov.pl/web/baza-wiedzy/dostales-niepokojacy-sms-albo-email-zglos-go-do-cert-polska-csirt-nask (dostęp 23 września 2026).

[24] CERT Polska. *Zgłaszanie incydentów przez formularz na stronie incydent.cert.pl*. Baza wiedzy CERT Polska. 2 września 2026. URL: https://web.archive.org/web/20260906104149/https://wiedza.cert.pl/obsluga-incydentow/zgloszenie/incydent-cert-pl/ (dostęp 23 września 2026).

[25] CyberKatalog.pl. *Zgłoś incydent*. Narzędzie. URL: https://cyberkatalog.pl/narzedzia/zglos-incydent (dostęp 23 września 2026).

[26] CyberKatalog.pl. *Lista ostrzeżeń przed niebezpiecznymi stronami*. Narzędzie. URL: https://cyberkatalog.pl/narzedzia/lista-ostrzezen (dostęp 23 września 2026).

[27] CERT Polska. *Lista Ostrzeżeń przed niebezpiecznymi stronami*. URL: https://web.archive.org/web/20260902133049/https://cert.pl/lista-ostrzezen/ (dostęp 23 września 2026).

[28] CyberKatalog.pl. *Monitoring i SOC*. Kategoria katalogu firm. URL: https://cyberkatalog.pl/kategoria/monitoring-i-soc (dostęp 23 września 2026).

[29] CyberKatalog.pl. *Szkolenia i Świadomość*. Kategoria katalogu firm. URL: https://cyberkatalog.pl/kategoria/szkolenia-i-swiadomosc (dostęp 23 września 2026).

[30] CERT Polska. *Przejęta skrzynka pocztowa*. Baza wiedzy CERT Polska, ścieżki postępowania. 2 września 2026. URL: https://web.archive.org/web/20260906104313/https://wiedza.cert.pl/sciezki-postepowania/przejeta-skrzynka-pocztowa/ (dostęp 23 września 2026).

[31] National Cyber Security Centre. *Recovering a hacked account*. 24 sierpnia 2022. URL: https://web.archive.org/web/20260924114906/https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account (dostęp 24 września 2026).

[32] Policja. *Bankowcy dla CyberEdukacji: uważaj na oszustwo na "maila firmowego"*. 26 marca 2026. URL: https://web.archive.org/web/20260510171041/https://www.policja.pl/pol/aktualnosci/275067,Bankowcy-dla-CyberEdukacji-uwazaj-na-oszustwo-na-quotmaila-firmowego.html (dostęp 23 września 2026).

[33] Policja. *Uwaga na oszustwo na podmianę numeru rachunku bankowego*. 21 sierpnia 2019. URL: https://web.archive.org/web/20251016100742/https://policja.pl/pol/aktualnosci/177772,Uwaga-na-oszustwo-na-podmiane-numeru-rachunku-bankowego.html (dostęp 23 września 2026).

[34] Centralne Biuro Zwalczania Cyberprzestępczości. *Zgłoś cyberoszustwo*. URL: https://web.archive.org/web/20260904083818/https://cbzc.policja.gov.pl/bzc/zglos-cyberprzestepstwo/464,Zglos-cyberoszustwo.html (dostęp 23 września 2026).

[35] Ministerstwo Spraw Wewnętrznych i Administracji. *Zgłoś przestępstwo*. Serwis gov.pl. URL: https://web.archive.org/web/20260924061556/https://www.gov.pl/web/gov/zglos-przestepstwo (dostęp 24 września 2026).

[36] CyberKatalog.pl. *Ransomware*. Hasło w słowniku cyberbezpieczeństwa. URL: https://cyberkatalog.pl/slownik/ransomware (dostęp 23 września 2026).

[37] No More Ransom. *O Projekcie*. URL: https://web.archive.org/web/20260115094825/https://www.nomoreransom.org/pl/about-the-project.html (dostęp 23 września 2026).

[38] CERT Polska. *Zgłaszanie incydentu z użyciem systemu S46*. Baza wiedzy CERT Polska. 2 września 2026. URL: https://web.archive.org/web/20260906104150/https://wiedza.cert.pl/obsluga-incydentow/zgloszenie/s46/ (dostęp 23 września 2026).

[39] No More Ransom. *No More Ransom*. Inicjatywa policji holenderskiej, Europolu i partnerów. URL: https://web.archive.org/web/20260513095721/https://www.nomoreransom.org/pl/index.html (dostęp 23 września 2026).

[40] CyberKatalog.pl. *Czy płacić okup po ataku ransomware*. Artykuł. URL: https://cyberkatalog.pl/aktualnosci/artykuly/okup-ransomware-czy-placic (dostęp 7 października 2026).

[41] CyberKatalog.pl. *Bezpieczeństwo Infrastruktury*. Kategoria katalogu firm. URL: https://cyberkatalog.pl/kategoria/bezpieczenstwo-infrastruktury (dostęp 23 września 2026).

[42] Europejska Rada Ochrony Danych. *Wytyczne 9/2022 dotyczące zgłaszania naruszenia ochrony danych osobowych na podstawie RODO*. Wersja 2.0. 28 marca 2023. URL: https://web.archive.org/web/20251215025752/https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202209_personal_data_breach_notification_v2.0_pl_0.pdf (dostęp 23 września 2026).

[43] Urząd Ochrony Danych Osobowych. *Zgłoszenie naruszenia ochrony danych*. 9 kwietnia 2026. URL: https://web.archive.org/web/20260901151405/https://uodo.gov.pl/pl/492/2278 (dostęp 23 września 2026).

[44] Ministerstwo Cyfryzacji. *Zgłoszenie naruszenia ochrony danych osobowych*. Serwis System S46. URL: https://web.archive.org/web/20260924061159/https://www.gov.pl/web/system-s46/zgloszenie-naruszenia-ochrony-danych-osobowych (dostęp 24 września 2026).

[45] CyberKatalog.pl. *Wyciek danych z MyDr - jakie dane wyciekły i co teraz zrobić*. Artykuł. URL: https://cyberkatalog.pl/aktualnosci/artykuly/wyciek-danych-mydr-sierpien-2026 (dostęp 24 września 2026).

[46] CyberKatalog.pl. *Wyciek danych*. Narzędzie. URL: https://cyberkatalog.pl/narzedzia/wyciek-danych (dostęp 23 września 2026).

[47] CyberKatalog.pl. *Zastrzeżenie numeru PESEL*. Narzędzie. URL: https://cyberkatalog.pl/narzedzia/zastrzez-pesel (dostęp 23 września 2026).

[48] CyberKatalog.pl. *Ochrona Danych*. Kategoria katalogu firm. URL: https://cyberkatalog.pl/kategoria/ochrona-danych (dostęp 23 września 2026).

[49] Ministerstwo Cyfryzacji. *Zgłoszenie incydentu*. Serwis System S46. URL: https://web.archive.org/web/20260924061123/https://www.gov.pl/web/system-s46/zgloszenie-incydentu (dostęp 24 września 2026).

[50] CERT Polska. *Zgłoś incydent*. Formularz zgłoszeń do CSIRT NASK. URL: https://web.archive.org/web/20260917095742/https://incydent.cert.pl/ (dostęp 23 września 2026).

[51] Komisja Nadzoru Finansowego. *Incydenty DORA*. 13 stycznia 2025. URL: https://web.archive.org/web/20260924061330/https://www.knf.gov.pl/dla_rynku/dora/incydenty_dora (dostęp 24 września 2026).

[52] CyberKatalog.pl. *CSIRT*. Hasło w słowniku cyberbezpieczeństwa. URL: https://cyberkatalog.pl/slownik/csirt (dostęp 23 września 2026).

[53] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, tekst jednolity*. Dz.U. 2026 poz. 20 ze zm. URL: https://dziennikustaw.gov.pl/DU/2026/20 (dostęp 23 września 2026).

[54] CSIRT GOV. *Zgłoszenie incydentu do CSIRT GOV*. URL: https://web.archive.org/web/20260910151604/https://csirt.gov.pl/cer/zgloszenie-incydentu/16,Zgloszenie-incydentu-do-CSIRT-GOV.html (dostęp 23 września 2026).

[55] Minister Cyfryzacji. *Komunikat Ministra Cyfryzacji z dnia 8 kwietnia 2026 r. w sprawie harmonogramu złożenia wniosków o wpis do wykazu podmiotów kluczowych i podmiotów ważnych oraz rozpoczęcia korzystania z systemu teleinformatycznego przez podmioty kluczowe lub podmioty ważne*. Dz. Urz. Min. Cyfr. 2026 poz. 7. 8 kwietnia 2026. URL: https://web.archive.org/web/20260501125526/https://www.gov.pl/attachment/a3b63395-503b-426c-9913-6d0b6d3c205d (dostęp 24 września 2026).

[56] CyberKatalog.pl. *GRC i Zgodność*. Kategoria katalogu firm. URL: https://cyberkatalog.pl/kategoria/grc-i-zgodnosc (dostęp 23 września 2026).

[57] CyberKatalog.pl. *Wdrożenie NIS2 i KSC*. Strona katalogu firm. URL: https://cyberkatalog.pl/kategoria/nis2 (dostęp 23 września 2026).

[58] CyberKatalog.pl. *Wdrożenie DORA*. Strona katalogu firm. URL: https://cyberkatalog.pl/kategoria/dora (dostęp 23 września 2026).

[59] CyberKatalog.pl. *Bezpieczeństwo Chmury*. Kategoria katalogu firm. URL: https://cyberkatalog.pl/kategoria/bezpieczenstwo-chmury (dostęp 23 września 2026).

[60] CyberKatalog.pl. *Kto w Polsce wdroży NIS2 i ustawę o KSC - lista wykonawców*. Artykuł. URL: https://cyberkatalog.pl/aktualnosci/artykuly/kto-wdrozy-nis2-i-ustawe-o-ksc (dostęp 23 września 2026).