

Cyberbezpieczeństwo i NIS2 • Moduł I

NIS2 i nowelizacja KSC – wymagania, obowiązki i odpowiedzialność

Szkolenie otwarte online · 18.09.2026, 9:00–15:00

Organizator: Platforma Wiedzy

Prowadzący: **Paweł Maliszewski**
Perfectinfo Sp. z o.o.



O prowadzącym



Paweł Maliszewski

Prezes Zarządu Perfectinfo Sp. z o.o.

Ekspert ds. cyberbezpieczeństwa, ochrony danych osobowych i wdrażania SZBI zgodnych z ISO 27001. Od 2006 roku realizuje projekty z zakresu ochrony danych i bezpieczeństwa informacji.

Projekty doradcze i wdrożeniowe m.in. dla: Komisji Nadzoru Finansowego, Przedsiębiorstwa Państwowego „Porty Lotnicze” oraz Networks! (T-Mobile/Orange).

Praktyka w postępowaniach kontrolnych przed UODO.
Wykształcenie: Wojskowa Akademia Techniczna w Warszawie.

- ❑ **Na szkoleniu:** przepisy z numerami artykułów, prawdziwe incydenty ze źródłami, konkretne zabezpieczenia i praktyczne Checklisty.

Dlaczego Perfectinfo

15+

lat doświadczenia
na rynku, od 2010 r.

80+

postępowań
przed UODO i NIK — 0 zł kar dla naszych klientów

TOP 5 firm cyberbezpieczeństwa wg Business Insider 2026

Interdyscyplinarny zespół: prawnicy + inżynierowie (CISSP, OSCP, CIPP-E, ISO 27001 LA, BCM)



200+

stałych klientów
700+ kompleksowych wdrożeń

3h

czas reakcji
średni (umowny do 10h roboczych)

Agenda dnia i zasady czatu

01

9:00–10:30 • Moduł I

NIS2 i nowelizacja KSC – wymagania, zakres obowiązków i odpowiedzialność

02

10:30–10:45 • Przerwa

03

10:45–12:15 • Moduł II

Jak przygotować organizację do wymagań NIS2 i KSC

04

12:15–12:45 • Przerwa obiadowa

05

12:45–15:00 • Moduł III

Incydenty, pracownicy i współczesne zagrożenia (krótka przerwa ok. 13:45)

Zasady czatu

Na Ćwiczenia odpowiadają Państwo na czacie Zoom: literą **A**, **B** lub **C** albo liczbą.

Pytania można wpisywać na czacie w dowolnym momencie. Odpowiadam na bieżąco lub przed przerwą.

W programie dnia

- **8** Historii prawdziwych incydentów (każda z Anatomią ataku: wektor i zabezpieczenia)
- **7** Ciekawostek
- **6** Ćwiczeń i Studium przypadku „pierwsze 60 minut”

Checklistę zarządu i Checklistę pracownika otrzymają Państwo od Organizatora.

Hook: ankieta wśród członków zarządów i CERT Polska 2025

Ankieta Blackpartners wśród 1 356 członków zarządów (sierpień 2026)

57%

nie potwierdziło

analizą prawną, czy ich organizacja podlega ustawie o KSC

38%

wie o terminie

rejestracji w wykazie podmiotów kluczowych i ważnych (termin: 3.10.2026)

CERT Polska w 2025 r.

658K

zgłoszeń (+10%)

ponad 1 800 dziennie

260K

incydentów (+152%)

z czego 97% to oszustwa

179

ataków ransomware

wzrost o +21%

Pytanie na start: czy Państwa organizacja ma już analizę, czy podlega ustawie – i kto w zarządzie ją zna?

Źródła: CRN.pl, 9.09.2026: badanie Blackpartners, VIII 2026; CERT Polska, Raport roczny 2025 (8.04.2026)

Najczęstsze zagrożenia dla firm i administracji

Phishing

60% wektorów wejścia w incydentach w UE, a wykorzystanie podatności – 21,3% (ENISA). CERT Polska obsłużył w 2025 r. 78 391 incydentów phishingu, w tym 28 462 pod szyldem OLX i 22 513 pod szyldem Allegro.

Ataki na tożsamość

Ponad 97% ataków na tożsamość to ataki na hasła (Microsoft).

Ransomware i wymuszenia

Ransomware w 48% naruszeń (Verizon). Co najmniej 52% incydentów o znanym motywie to wymuszenia lub ransomware (Microsoft).

Dostawcy

Udział stron trzecich w naruszeniach sięga 48%, o 60% więcej niż rok wcześniej (Verizon).

AI po stronie przestępców

Według danych przytaczanych przez ENISA na początku 2025 r. kampanie phishingowe wspierane przez AI miały stanowić ponad 80% obserwowanej socjotechniki na świecie.



Administracja publiczna jest najczęściej atakowanym sektorem w UE: 38,2% analizowanych incydentów (ENISA, VII 2024 – VI 2025).



Firmy: średni koszt naruszenia danych to 4,44 mln USD, a w ochronie zdrowia 7,42 mln USD (IBM).

Źródła: ENISA Threat Landscape 2025 (1.10.2025); CERT Polska, Raport roczny 2025 (8.04.2026); Microsoft Digital Defense Report 2025 (16.10.2025); Verizon DBIR 2026 (19.05.2026); IBM Cost of a Data Breach 2025 (30.07.2025)

Jak przestępcy wchodzą do organizacji i gdzie przerwać atak

Jak wchodzą (Verizon, dane z okresu X 2024 – XI 2025)

Pierwszy raz w historii raportu najczęstszym wektorem wejścia jest **wykorzystanie podatności** – 31% naruszeń ze znanym wektorem, a w Europie, na Bliskim Wschodzie i w Afryce 47%. W pełni załatano tylko 26% krytycznych podatności z katalogu CISA KEV; mediana – 43 dni.

W Polsce (CERT Polska, 2025 r.)

W znacznej większości ataków ransomware z ustalonym wektorem przestępcy weszli przez usługi dostępu zdalnego bez uwierzytelniania dwuskładnikowego. W 46 incydentach ofiara miała pulpit zdalny (RDP) dostępny z internetu, a w dwóch hasło przełamano i zaszyfrowano dane w czasie krótszym niż 2 tygodnie od jego wystawienia.

Ubezpieczyciel At-Bay (roszczenia z 2025 r.)

VPN w 73% ataków ransomware ze znanym wektorem.



Czas gra na korzyść przestępcy (Mandiant, 2025 r.): mediana obecności w sieci – 14 dni; od uzyskania dostępu do przekazania go kolejnej grupie – 22 sekundy.

Etap ataku	Co robi przestępca	Co go zatrzymuje
1. Wejście	podatne urządzenie brzegowe, VPN lub RDP bez drugiego składnika	łatki według ryzyka, MFA na każdym dostępie zdalnym
2. Przejęcie uprawnień	konta administratorów, Active Directory	osobne konta administratorów, model warstwowy
3. Kopie zapasowe	szuka serwerów kopii i wirtualizatorów; kopie na NAS kasuje	kopia offline lub niezmiennalna
4. Kradzież i szyfrowanie	wynosi dane, szyfruje systemy, szantażuje	monitorowanie, EDR, przeciwiczony plan reakcji

Źródła: Verizon DBIR 2026 (19.05.2026); CERT Polska, Raport roczny 2025 (8.04.2026); At-Bay 2026 InsurSec Report (IV 2026); Mandiant M-Trends 2026 (23.03.2026)

Historia: Szpital Wojewódzki w Szczecinie

Co się stało

W nocy z 7 na 8 marca 2026 r. przestępcy zaszyfrowali część danych Samodzielnego Publicznego Wojewódzkiego Szpitala Zespólnego w Szczecinie i zażądali kilku milionów dolarów za przywrócenie dostępu.

Jak do tego doszło

Atak ransomware. W komunikatach szpitala i prokuratury nie podano, jak przestępcy dostali się do sieci. Śledztwo nadzoruje Prokurator Okręgowy w Szczecinie, m.in. w sprawie sprowadzenia niebezpieczeństwa dla życia lub zdrowia ludzi.

Skutki

- Szpital przeszedł na pracę „na papierze”; laboratorium centralne i diagnostyka obrazowa badały tylko pacjentów szpitalnych.
- Szpital zawiadomił o wysokim prawdopodobieństwie przejęcia danych osobowych, m.in. pacjentów i pracowników, w tym numerów PESEL i danych o zdrowiu.
- Żołnierze WOT od 12.03 do 10.04.2026 wspierali szpital m.in. przy ponad 1 000 stacji roboczych, ponad 140 resetach haseł i reinstalacjach systemów.

Lekcja dla Państwa

Ciągłość działania to przeciwieństwo praca bez systemów: procedury papierowe, kopie zapasowe, z których da się odtworzyć dane, i lista kontaktów kryzysowych. Jeden incydent uruchamia jednocześnie obowiązki wobec CSIRT i UODO.

Źródła: komunikaty SPWSZ w Szczecinie (8.03 i 11.03.2026); Prokuratura Okręgowa w Szczecinie (gov.pl, 11.03.2026); Rynek Zdrowia (11.03.2026); Wojska Obrony Terytorialnej (14.05.2026)

Anatomia ataku: ransomware w szpitalu

Wektor ataku

Szpital ani prokuratura nie ujawniły do dziś, jak przestępcy weszli do sieci. CERT Polska o polskich atakach ransomware z 2025 r.: „w znacznej większości zdarzeń” – tam, gdzie były logi – doszło do „nieuprawnionego dostępu poprzez usługi dostępu zdalnego, które nie były zabezpieczone dwuskładnikowym uwierzytelnieniem”; w 46 incydentach ofiara miała pulpit zdalny (RDP) dostępny z internetu. Dane logowania przestępcy zdobywają przez phishing, wycieki, infostealery albo zgadywanie. To typowy wektor, nie ustalenie w sprawie szpitala.

Dlaczego się udało

Technicznie: ataki są rozłożone nawet na kilka tygodni; przestępcy szukają najwyższych uprawnień, serwerów kopii zapasowych i wirtualizatorów – kopie na NAS reinicjalizują, migawki maszyn wirtualnych usuwają (CERT Polska). W szpitalu trzeba było przeinstalować systemy na ponad 1 000 stacji i zresetować ponad 140 haseł – skala wskazuje na przejęcie uprawnień w całej domenie.

Organizacyjnie: wiele ofiar nie ma centralnego kolektora logów, więc logi „sięgają zaledwie kilku dni wstecz” i wektora nie da się ustalić; powrót do pełnej sprawności rozpisano na miesiące, a dokumentację papierową trzeba zdigitalizować.

Jak temu zaradzić

Zabezpieczenia: MFA „we wszystkich usługach umożliwiających zdalny dostęp” (CERT Polska), RDP niedostępny z internetu, EDR na stacjach i serwerach, osobne konta administratorów, kopie odłączone od domeny i testowane, centralne logi z retencją liczoną w miesiącach.

Procedury: przeciwiczony tryb papierowy dla rejestracji, laboratorium i diagnostyki; plan odtworzenia z kolejnością systemów krytycznych; lista kontaktów: CSIRT, UODO, prokuratura, zewnętrzny zespół reagowania; podmiot leczniczy z zał. nr 1 do ustawy o KSC – zgłoszenie do CSIRT w 24 h i 72 h oraz do UODO w 72 h od stwierdzenia naruszenia.

Źródła: CERT Polska, Raport roczny 2025 (8.04.2026); Wojska Obrony Terytorialnej (14.05.2026); Rynek Zdrowia (7.04.2026); ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); RODO (rozporządzenie 2016/679)

Historia: Marks & Spencer i Co-op

Co się stało

Marks & Spencer: atak rozpoczął się 17.04.2025. M&S wskazało grupę ransomware DragonForce jako potencjalnego sprawcę. Wstrzymano zamówienia online, click and collect i zamawianie w sklepach.

Co-op: w kwietniu 2025 r. przestępcy wykradli dane wszystkich 6,5 mln członków spółdzielni: imiona i nazwiska, adresy i dane kontaktowe.

Jak do tego doszło

Marks & Spencer: przewodniczący rady dyrektorów przed brytyjskim parlamentem: wejście nastąpiło przez socjotechnikę – podszycie się pod osobę z użyciem jej danych – z udziałem firmy zewnętrznej.

Co-op: dyrektor ds. cyfrowych przed komisją Izby Gmin: przestępcy podszyli się pod pracownika i poprawnie odpowiedzieli na pytania kontrolne, uzyskując reset konta; ok. godzinę później zaczęli go używać w złych celach – zespół Co-op wykrył to, ograniczył konto i nie dopuścił do uruchomienia ransomware.

Źródła: M&S, wyniki półroczne (5.11.2025); CNBC, wyniki roczne M&S (21.05.2025); BleepingComputer (8.07.2025); Izba Gmin, Business and Trade Sub-Committee: zeznania M&S i Co-op (8.07.2025); TechCrunch (16.07.2025); Co-op, wyniki półroczne (25.09.2025); Talking Retail (26.03.2026)

Skutki

Marks & Spencer: ok. £300 mln wpływu na zysk operacyjny roku 2025/26. W I półroczu sprzedaż online w segmencie odzieży, domu i kosmetyków spadła o 42,9%, koszty incydentu wyniosły £101,6 mln, a wypłata z ubezpieczenia – £100 mln.

Co-op: w 2025 r. £285 mln utraconej sprzedaży i £107 mln wpływu na zysk; ograniczona dostępność towaru w sklepach i brak ubezpieczenia od ryzyk cybernetycznych.

Lekcja dla Państwa

- Weryfikacja tożsamości osoby, która prosi o dostęp, to zabezpieczenie, a nie formalność – także wobec pracowników dostawców.
- Szybka decyzja o odcięciu systemów ogranicza szkody, ale nie cofa kradzieży danych.
- Ubezpieczenie przenosi część kosztów, pod warunkiem że polisa istnieje, zanim dojdzie do ataku.

Anatomia ataku: podszycie się pod pracownika w handlu

Wektor ataku

Podszycie się pod pracownika i prośba o reset dostępu. Przewodniczący rady M&S przed komisją Izby Gmin (8.07.2025): to była „sophisticated impersonation” — przestępcy „appeared as an individual, with their details”, a w punkcie wejścia brała udział firma zewnętrzna. Dyrektor ds. cyfrowych Co-op: przestępcy podszyli się pod pracownika i „successfully answer a number of security questions to get their account reset”; ok. godzinę później zaczęli używać konta w złych celach.

Dlaczego się udało

Technicznie: MFA nie chroni, gdy sam proces resetu hasła i drugiego składnika da się przejść na telefon; pytania kontrolne (data urodzenia, adres, numer pracownika) są do zdobycia w wyciekach i mediach społecznościowych. M&S: „we do have legacy systems”.

Organizacyjnie: 50 tys. osób pracujących na systemach M&S — pracownicy, kontraktorzy, outsourcing: „the attacker (...) has only to be lucky once”. Wykrycie w M&S 19.04, dwa dni po wejściu 17.04. Co-op wykryło nietypowe działanie konta w ok. godzinę, ograniczyło je i nie dopuściło do ransomware — różnica między dwoma wynikami to czas wykrycia i reakcji.

Jak temu zaradzić

Zabezpieczenia (zalecenia NCSC UK, maj 2025): MFA „deployed comprehensively”; monitoring nadużyć kont, np. „risky logins” w Microsoft Entra ID Protection; szczególna uwaga na konta Domain Admin, Enterprise Admin i Cloud Admin; SOC wykrywający logowania „from atypical sources such as VPNs services in residential ranges”.

Procedury: „review helpdesk password reset processes, including how the helpdesk authenticates staff members credentials before resetting passwords, especially those with escalated privileges” — w praktyce: oddzwonienie na numer z kadr, potwierdzenie przez przełożonego, weryfikacja wideo dla kont uprzywilejowanych, zakaz resetu MFA „na telefon”; te same zasady w umowie z zewnętrznym wsparciem IT; ćwiczony scenariusz „przejęte konto”.

Źródła: Izba Gmin, Business and Trade Sub-Committee: zeznania M&S i Co-op (8.07.2025); NCSC UK: Incidents impacting retailers – recommendations from the NCSC (V 2025)

Hakerzy w polskich wodociągach



- **2025 r.:** hakerzy atakowali systemy sterowania stacji uzdatniania wody w małych gminach — m.in. w Tolkmicku, Małdytach i Sierakowie (pierwsza połowa 2025 r.), w Szczycinie (maj 2025 r.) i Jabłonie Lackiej (wrzesień 2025 r.).
- W jednym z incydentów opisanych przez CERT Polska (bez nazwy gminy) hakerzy zmienili ustawienia pomp, co doprowadziło do wyczerpania wody w zbiorniku: ok. 2,5 tys. mieszkańców nie miało wody przez ok. 6 godzin.
- ABW: zaatakowane obiekty miały zasoby IT dostępne z internetu, w tym panele HMI sterujące procesami technologicznymi.
- **Sierpień 2026:** Prokuratura Okręgowa w Białymstoku — zarzuty dla dwóch obywateli Rosji za 17 cyberataków w Polsce, w tym 7 na obiekty wodno-kanalizacyjne. Obaj przebywają w Rosji.

❏ **Lekcja dla Państwa:** mała gmina i mały zakład też są celem. Panel sterowania nie powinien być dostępny z internetu, a dostęp serwisowy wymaga silnego uwierzytelnienia.

Źródła: CERT Polska, Raport roczny 2025 (8.04.2026); CyberDefence24: ABW o atakach na wodociągi (8.10.2025); CyberDefence24: zarzuty prokuratury (10.08.2026)

NIS2 i KSC: oś czasu i terminy

Data	Co się dzieje	Podstawa
14.12.2022 · 17.10.2024	przyjęcie dyrektywy NIS2; termin jej wdrożenia w państwach członkowskich	dyrektywa NIS2 (2022/2555)
3.04.2026	nowelizacja ustawy o KSC w mocy (ustawa z 23.01.2026, Dz.U. 2026 poz. 252)	art. 49 nowelizacji
7.05–3.10.2026	wniosek o wpis do wykazu podmiotów kluczowych i ważnych (S46); nie dotyczy podmiotów wpisanych z urzędu	art. 33 ust. 3 nowelizacji; komunikat MC, Dz. Urz. Min. Cyfr. 2026 poz. 7
3.04.2027	obowiązki z rozdziału 3: SZBI, dokumentacja, osoby do kontaktu, zgłaszanie incydentów, struktury lub umowa z MSSP	art. 33 ust. 1 nowelizacji
3.04.2028	pierwszy audyt podmiotu kluczowego; koniec odroczenia kar za większość obowiązków	art. 33 ust. 2 i art. 35 nowelizacji

- **Podmiot, który spełni przesłanki później:** wniosek o wpis w 6 miesięcy, obowiązki w 12 miesięcy, pierwszy audyt podmiotu kluczowego w 24 miesiące – od dnia spełnienia przesłanek (art. 7c ust. 1, art. 16 KSC).
- **Brak wniosku w terminie:** wpis z urzędu (art. 7j) i możliwa kara (art. 73 ust. 1a pkt 1), nakładana po 3.04.2028. Kara do 100 mln zł z art. 73 ust. 5 nie jest objęta odroczeniem z art. 35 nowelizacji.
- **Sprawa K 19/26:** wniosek Prezydenta wpłynął do Trybunału Konstytucyjnego 21.07.2026. Obejmuje przepisy o dostawcy wysokiego ryzyka (art. 67b, 67c, 67e KSC), poleceniu zabezpieczającym (art. 67g KSC) i definicje z art. 2 pkt 11k–11m. Wniosek nie dotyczy kar ani katalogu sektorów. Stan na 17.09.2026: brak terminu rozprawy i rozstrzygnięcia – obowiązki i terminy bieżąco niezależnie.

Źródła: dyrektywa NIS2 (2022/2555); ustawa z 23.01.2026 o zmianie ustawy o KSC (Dz.U. 2026 poz. 252); ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); komunikat MC z 8.04.2026 (Dz. Urz. Min. Cyfr. 2026 poz. 7); Ministerstwo Cyfryzacji (3.09.2026); Trybunał Konstytucyjny, sprawa K 19/26 (stan 17.09.2026)

Podmioty kluczowe i ważne

Status ustala się w trzech krokach (art. 5 KSC)

1 Sektor lub rodzaj podmiotu

Czy organizacja faktycznie prowadzi działalność z zał. nr 1 (sektory kluczowe) albo zał. nr 2 (sektory ważne)? PKD przeważające nie rozstrzyga.

2 Wielkość

Według unijnej definicji MŚP – pracownicy (RJR), obrót i suma bilansowa, z przedsiębiorstwami powiązanymi i partnerskimi (art. 5 ust. 3).

3 Przypadki niezależne od wielkości

M.in. podmiot krytyczny, kwalifikowany dostawca usług zaufania, dostawca usług DNS, podmiot publiczny z zał. nr 1 (art. 5 ust. 1 pkt 4).

- ☐ **Analogia:** jak kategoria prawa jazdy – decyduje rodzaj pojazdu (sektor) i jego masa (wielkość), a nie napis na naczepie (PKD).

Wielkość organizacji	Sektor z zał. nr 1	Sektor z zał. nr 2
duża (co najmniej 250 osób albo obrót ponad 50 mln EUR i bilans ponad 43 mln EUR)	kluczowy (art. 5 ust. 1 pkt 1)	ważny (art. 5 ust. 2 pkt 2)
średnia (50–249 osób albo obrót i bilans ponad 10 mln EUR)	ważny (art. 5 ust. 2 pkt 1)	ważny (art. 5 ust. 2 pkt 2)
mała i mikro	nie podlega, chyba że zachodzi przypadek niezależny od wielkości	nie podlega, chyba że zachodzi przypadek niezależny od wielkości

Samorządowe jednostki budżetowe i zakłady budżetowe, instytucje kultury i spółki komunalne realizujące zadania publiczne z wykorzystaniem systemów informacyjnych są podmiotami ważnymi, jeśli nie są kluczowymi (art. 5 ust. 2 pkt 8) – urząd gminy od 50 etatów jest kluczowy.

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); zał. I do rozporządzenia Komisji (UE) nr 651/2014

Ćwiczenie 1: kluczowy, ważny czy nie podlega?

Prosimy wpisać na czacie trzy odpowiedzi, np. „1A 2C 3B”.

1	2	3
Gmina Zielonów Gmina wiejska, 8 tys. mieszkańców. Urząd Gminy zatrudnia na 1.01.2026 52 osoby na umowę o pracę (w przeliczeniu na pełne etaty).	FoliaPak sp. z o.o. Wyłacza folie i worki z kupowanego granulatu polietylenu (PKD 22.22.Z). 120 pracowników, obrót ok. 14 mln EUR, brak przedsiębiorstw powiązanych i partnerskich.	Przychodnia Medica Plus sp. z o.o. Podmiot leczniczy, podstawowa i ambulatoryjna opieka zdrowotna. 60 pracowników na pełnych etatach, przychód ok. 4,7 mln EUR, brak powiązań.

✓ Klucz odpowiedzi: 1 – A, 2 – B, 3 – B

Gmina: urząd gminy zatrudniający co najmniej 50 osób jest podmiotem kluczowym niezależnie od wielkości – art. 5 ust. 1 pkt 4 lit. d i zał. nr 1. FoliaPak: sektor chemikaliów z zał. nr 2; średnie przedsiębiorstwo – art. 5 ust. 2 pkt 2. Przychodnia: sektor ochrony zdrowia z zał. nr 1; średnie przedsiębiorstwo – art. 5 ust. 2 pkt 1. FoliaPak: kwalifikacja według uzasadnienia projektu ustawy; część doktryny kwestionuje tak szeroką wykładnię. **Wniosek:** o statusie decydują załącznik, wielkość i faktyczna działalność – nie PKD, nie liczba mieszkańców i nie nazwa branży.

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); zał. I do rozporządzenia Komisji (UE) nr 651/2014; rozporządzenie REACH (WE) nr 1907/2006, art. 3 pkt 3; uzasadnienie projektu nowelizacji KSC (druk sejmowy nr 1955)

Najważniejsze obowiązki



Wpis do wykazu

Wniosek w ciągu 6 miesięcy od spełnienia przesłanek, zmiany danych w ciągu 14 dni (art. 7c ust. 1 i 3). Brak wniosku: wpis z urzędu (art. 7j).



Dokumentacja

Normatywna i operacyjna, pod nadzorem, przechowywana co najmniej 2 lata od wycofania (art. 10).



Audyt

Podmiot kluczowy co najmniej raz na 3 lata (art. 15 ust. 1); podmiot ważny na nakaz organu, np. po incydencie poważnym (art. 15 ust. 1b).



SZBI

Systematyczne szacowanie ryzyka i środki proporcjonalne do ryzyka, m.in. polityki, ciągłość działania, łańcuch dostaw, kontrola dostępu, zarządzanie aktywami, uwierzytelnianie wieloskładnikowe „w stosownych przypadkach” (art. 8 ust. 1). Podmiot ważny publiczny: uproszczony SZBI z zał. nr 4 (art. 8 ust. 3).



Ludzie

Co najmniej 2 osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa, a 1 w mikro- i małym przedsiębiorstwie oraz w podmiocie ważnym publicznym (art. 9), informacja z KRK przed dopuszczeniem do zadań (art. 8f), coroczne szkolenie kierownika (art. 8e).



Incydenty

Obsługa incydentów, wczesne ostrzeżenie w 24 h i zgłoszenie w 72 h od wykrycia incydentu poważnego, sprawozdanie końcowe w ciągu miesiąca od zgłoszenia (art. 11–12c).



Zasoby

Wewnętrzne struktury albo umowa z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa (art. 14).



Analogia: SZBI to nie segregator na półce, tylko układ hamulcowy — działa na co dzień, jest testowany i serwisowany.

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252)

Powiązane regulacje: RODO, ISO 27001/27002, KRI, CER i DORA

Regulacja	Związek z ustawą o KSC	Na co uważać
RODO	jeden incydent, dwa zgłoszenia: do CSIRT w 24 h i 72 h od wykrycia incydentu poważnego (art. 11 KSC), do UODO w miarę możliwości w 72 h po stwierdzeniu naruszenia (art. 33 RODO)	przy wysokim ryzyku zawiadomienie osób (art. 34 RODO); po prawomocnej karze UODO za ten sam czyn organ KSC poprzestaje na pouczeniu (art. 76c KSC)
ISO/IEC 27001 i 27002	rama systemu zarządzania i katalog zabezpieczeń – pomagają zbudować SZBI z art. 8 KSC	ustawa o KSC nie przewiduje domniemania zgodności dla organizacji z certyfikatem
KRI (Dz.U. 2024 poz. 773)	SZBI podmiotów realizujących zadania publiczne w § 19, z domniemaniem przy SZBI opartym na PN-ISO/IEC 27001	rozporządzenie traci moc 23.02.2027; projekt nowego KRI (RD313) przewiduje usunięcie wymagań SZBI jako uregulowanych w ustawie o KSC
CER (Dz.U. 2026 poz. 815, od 4.07.2026)	podmiot krytyczny jest podmiotem kluczowym niezależnie od wielkości (art. 5 ust. 1 pkt 4 lit. c KSC)	ocena ryzyka co najmniej raz na 2 lata, zgłoszenie incydentu istotnego w 24 h, audyt co najmniej raz na 3 lata; kary pieniężne do 200 000 zł (art. 6zzr)
DORA (2022/2554, stosowane od 17.01.2025, nadzór KNF)	akt sektorowy wobec NIS2 (art. 4 NIS2)	bankowość i infrastruktura rynków finansowych: bez przepisów KSC o SZBI i zgłaszaniu poważnych incydentów, z wyjątkami; art. 8c–8f KSC stosuje się odpowiednio (art. 8i KSC)

 **Spójny system compliance:** jeden rejestr aktywów, jedna analiza ryzyka i jedna procedura incydentów. Stan prawny na wrzesień 2026.

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); RODO (rozporządzenie 2016/679); rozporządzenie RM w sprawie KRI (Dz.U. 2024 poz. 773); projekt nowego KRI, RD313 (wersja z 29.07.2026); ustawa z 29.05.2026 o zmianie ustawy o zarządzaniu kryzysowym (Dz.U. 2026 poz. 815); rozporządzenie DORA (2022/2554); ustawa z 25.06.2025 (Dz.U. 2025 poz. 1069); dyrektywa NIS2 (2022/2555)

Obowiązki zarządu: decyzje, zatwierdzanie i nadzór

Kto jest kierownikiem?

Kierownik jednostki w rozumieniu ustawy o rachunkowości – w spółce zarząd, w jednostce sektora finansów publicznych kierownik tej jednostki (art. 2 pkt 8a KSC).

Kierownik podmiotu kluczowego lub ważnego (art. 8d KSC)

1. podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania, przeglądu i nadzoru SZBI;
2. planuje adekwatne środki finansowe na cyberbezpieczeństwo;
3. przydziela zadania z zakresu cyberbezpieczeństwa i nadzoruje ich wykonanie;
4. zapewnia, że personel zna obowiązki i wewnętrzne regulacje;
5. zapewnia zgodność działania podmiotu z przepisami i regulacjami wewnętrznymi.

Szkolenie i odpowiedzialność

Szkolenie: raz w roku kalendarzowym, udokumentowane – także dla osoby, której powierzono obowiązki kierownika (art. 8e). **Odpowiedzialność (art. 8c):** w zarządzie wieloosobowym bez wskazanej osoby odpowiadają wszyscy członkowie; powierzenie obowiązków innej osobie nie zwalnia kierownika.

Zatwierdzanie i nadzór

Dyrektywa NIS2 wymaga, aby organy zarządzające „zatwierdzały środki zarządzania ryzykiem w cyberbezpieczeństwie (...), nadzorowały ich wdrażanie i mogły być pociągnięte do odpowiedzialności” (art. 20 ust. 1 NIS2). Ustawa o KSC nie używa słowa „zatwierdza”; odpowiednikami są decyzje w zakresie SZBI oraz przydział zadań i nadzór nad ich wykonaniem (art. 8d pkt 1 i 3).

☐ **Ślad decyzji** (dobra praktyka): uchwały, zapisane akceptacje ryzyka i regularne raporty dla zarządu. Organ nadzoru może wystąpić o dowody realizacji wymogów SZBI (art. 53 ust. 2 pkt 6 KSC).

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); dyrektywa NIS2 (2022/2555)

O co zarząd ma pytać IT: 10 pytań

Pytania 1–6: irlandzkie NCSC (wytyczne dla zarządów podmiotów NIS2), 7–10: brytyjskie NCSC. Sygnały ostrzegawcze to przykłady z praktyki audytowej.

Pytanie zarządu	Sygnał ostrzegawczy w odpowiedzi
1. Jakie są nasze krytyczne aktywa i systemy?	„wszystko jest ważne” albo brak rejestru z właścicielami
2. Jakie ryzyka cyber mogą zakłócić nasze usługi?	lista zagrożeń bez skutków dla procesów i bez decyzji zarządu
3. Jak zarządzamy ryzykiem dostawców?	dostawca serwisuje systemy przez wspólne konto bez MFA
4. Jak porównujemy nasz poziom bezpieczeństwa?	„nie było incydentu, więc jest dobrze”
5. Kiedy był ostatni test lub ćwiczenie?	„nigdy” albo raport z testu bez planu naprawczego
6. Jak jesteśmy przygotowani do wykrycia incydentu i reakcji?	MFA „na większości” dostępów zdalnych; nikt nie odbiera alertów w nocy i w weekend
7. Czy mamy plan reagowania na incydent i czy go ćwiczymy?	plan tylko w pliku na serwerze, który też może zostać zaszyfrowany
8. Czy każdy członek zarządu wie, czego się od niego oczekuje podczas incydentu?	„to sprawa działu IT”
9. Czy incydenty cyber uwzględniono w planach ciągłości działania i odtworzenia?	plan zakłada awarię jednego serwera, a nie utratę wszystkich systemów naraz
10. Czy wiemy, gdzie szukać pomocy w razie incydentu?	brak kontaktu do CSIRT i do firmy reagującej na incydenty

 **Rytm nadzoru** (brytyjski Cyber Governance Code of Practice, dobrowolny): ćwiczenie planu reagowania co najmniej raz w roku i formalny raport dla zarządu co najmniej raz na kwartał – z ustalonymi wskaźnikami i tolerancjami.

Źródła: NCSC Ireland: Guidance on Cyber Governance for Management Board Members in NIS2 entities (2026); NCSC UK: Cyber Security Toolkit for Boards (2025); DSIT i NCSC UK: Cyber Governance Code of Practice (8.04.2025)

Sankcje

Kto	Górna granica kary	Podstawa
Podmiot kluczowy	10 mln EUR lub 2% przychodów, przy czym stosuje się kwotę wyższą; min. 20 000 zł	art. 73 ust. 3 KSC
Podmiot ważny	7 mln EUR lub 1,4% przychodów; min. 15 000 zł	art. 73 ust. 4 KSC
Podmiot kluczowy lub ważny – naruszenie powodujące bezpośrednie i poważne cyberzagrożenie albo zagrożenie poważną szkodą majątkową lub poważnymi utrudnieniami w usługach	100 mln zł	art. 73 ust. 5 KSC
Okresowa kara za zwłokę w wykonaniu decyzji organu	500–100 000 zł za każdy dzień	art. 76b KSC

Od kiedy?

Ministerstwo Cyfryzacji: „w przypadku większości obowiązków” kary mogą być nakładane dopiero po 3.04.2028: art. 35 nowelizacji odracza kary z art. 73 ust. 1–4, art. 73a–73c i art. 76b. **Kara do 100 mln zł z art. 73 ust. 5 nie jest odroczona.**

Zakaz pełnienia funkcji zarządczych przez kierownika do czasu usunięcia uchybień – wyłącznie w podmiocie kluczowym, po niewykonaniu nakazu lub decyzji organu, nie w podmiotach publicznych (art. 53 ust. 9 pkt 6 i ust. 10).

- Art. 73 ust. 4 KSC nie zawiera klauzuli kwoty wyższej, którą przewiduje art. 34 ust. 5 NIS2.
- Organ może odstąpić od kary, gdy waga naruszenia jest znikoma, a naruszenie zaprzestane lub szkoda naprawiona (art. 76a ust. 9).
- Wniosek Prezydenta do TK (K 19/26) nie obejmuje kar.

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); ustawa z 23.01.2026 o zmianie ustawy o KSC (Dz.U. 2026 poz. 252); Ministerstwo Cyfryzacji (2.04.2026); dyrektywa NIS2 (2022/2555); Trybunał Konstytucyjny, sprawa K 19/26 (stan 17.09.2026)

Osobista odpowiedzialność kierownika

Kara pieniężna dla kierownika (art. 73a KSC)

Za niewykonanie 14 grup obowiązków, m.in. SZBI (art. 8), decyzji i nadzoru (art. 8d), corocznego szkolenia (art. 8e), zgłaszania incydentów (art. 11) i audytu (art. 15) – „jeżeli przemawia za tym czas, zakres lub charakter naruszenia” (ust. 1).

Także za zaniechanie jednorazowe (ust. 2) i niezależnie od kary dla podmiotu (ust. 3). Nakładana po raz pierwszy po 3.04.2028 (art. 35 nowelizacji).

Do 300%

wynagrodzenia (ekwiwalent za urlop) – podmiot prywatny (ust. 4)

Poza ustawą o KSC

Członek zarządu odpowiada wobec spółki za szkodę wyrządzoną działaniem lub zaniechaniem sprzecznym z prawem, chyba że nie ponosi winy (art. 293 § 1 KSH w sp. z o.o., art. 483 § 1 KSH w S.A.).

Zarząd wieloosobowy bez wskazanej osoby odpowiedzialnej: odpowiadają wszyscy członkowie (art. 8c ust. 2 KSC).



Lekcja: osobista odpowiedzialność nie kończy się na podpisaniu umowy z dostawcą – kierownik odpowiada także za obowiązki powierzone innym (art. 8c ust. 3 KSC).

Do 100%

wynagrodzenia – podmiot publiczny; 300% gdy podlega z innego sektora (ust. 5)

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); ustawa z 23.01.2026 o zmianie ustawy o KSC (Dz.U. 2026 poz. 252); Kodeks spółek handlowych

Za co karzą nadzorcy: brak podstawowych zabezpieczeń

Capita (Wielka Brytania) — kary ICO łącznie 14 mln GBP (15.10.2025)

22.03.2023 pracownik nieumyślnie pobrał złośliwy plik. Alert wysokiego priorytetu pojawił się w ciągu 10 minut, ale urządzenie odizolowano dopiero po 58 godzinach, przy wewnętrznym celu 1 godziny.

29–30.03.2023 przestępcy wynieśli prawie 1 TB danych, 31.03 uruchomili ransomware. Skradziono dane 6,6 mln osób.

Ustalenia ICO: zespół SOC miał za mało ludzi i co najmniej przez 6 miesięcy przed incydem nie mieścił się w docelowych czasach reakcji; brak modelu warstwowego kont administratorów zgłaszano co najmniej 3 razy bez naprawy; wyniki testów penetracyjnych zostawały w jednostkach biznesowych.

Advanced (Wielka Brytania) — kara ICO 3 076 320 GBP (27.03.2025)

Ransomware w sierpniu 2022 r. przez konto klienta bez MFA; zakłócenia m.in. infolinii medycznej NHS 111; dane 79 404 osób.

Ustalenia ICO: luki we wdrożeniu MFA, brak pełnego skanowania podatności i niewystarczające zarządzanie łatkami. Komisarz ICO: MFA było wdrożone na wielu systemach, ale brak pełnego pokrycia pozwolił przestępcom wejść.



Lekcja dla zarządu: nadzorca sprawdza, czy zabezpieczenie działało i czy znane ryzyko zostało usunięte — nie tylko, czy istnieje polityka. Organ nadzoru według ustawy o KSC także może żądać dowodów realizacji wymogów SZBI (art. 53 ust. 2 pkt 6 KSC).

Źródła: ICO, komunikat z 15.10.2025 (Capita); ICO, komunikat z 27.03.2025 (Advanced); ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252)

Historia: główna księgowa PZDW i CSO Ubera

Co się stało

Podlaski Zarząd Dróg Wojewódzkich, wiosna 2015: główna księgowa przełała ponad 3,7 mln zł na konto oszustów, przekonana, że płaci wykonawcy drogi.

Uber, 2016: przestępcy wykradli ok. 57 mln rekordów pasażerów i kierowców, a szef bezpieczeństwa (CSO) Joe Sullivan nie ujawnił incydentu.

Jak do tego doszło

PZDW: mężczyzna podający się za pracownika firmy Unibep zadzwonił z informacją o zmianie rachunku, potem przysłał e-mail ze skanem oświadczenia i nowym numerem konta. Poszły dwa przelewy: blisko 640 tys. zł i ponad 3,1 mln zł.

Uber: trwało już postępowanie FTC w sprawie wcześniejszego wycieku z 2014 r. Hakerom zapłacono 100 tys. USD w ramach programu bug bounty w zamian za podpisanie umowy o poufności i usunięcie danych. FTC o nowym wycieku nie poinformowano.

Skutki

PZDW: pieniądze szybko wyprowadzono za granicę. W 2018 r. księgowa została prawomocnie skazana za nieumyślne niedopełnienie obowiązków służbowych na 8 tys. zł grzywny.

Uber: w październiku 2022 r. ława przysięgłych uznała Sullivana winnym utrudniania postępowania FTC i ukrywania przestępstwa. Kara: 3 lata dozoru (probation) i 50 tys. USD grzywny; apelacja utrzymała wyrok 13.03.2025.

Lekcja dla Państwa

- Osobista odpowiedzialność nie dotyczy tylko prezesa: także osoby, która zleca przelew, i osoby, która decyduje o ukryciu incydentu.
- Weryfikacja zmiany rachunku drugim kanałem i jawne zgłaszanie incydentów chronią organizację i ludzi.

Źródła: TVN24 Białystok (7.10.2025); Gazeta Współczesna (26.04.2018); Radio Białystok (26.04.2018); U.S. Court of Appeals for the Ninth Circuit, No. 23-927 (13.03.2025); U.S. Department of Justice (2022, 2023)

Anatomia ataku: fałszywy kontrahent i ukryty wyciek

Wektor ataku

PZDW (2015): telefon „od pracownika wykonawcy” o zmianie rachunku, potem e-mail ze skanem „oświadczenia o zmianie rachunku” z prawdziwymi NIP, REGON i KRS firmy.

Uber (2016) – skarga FTC: przestępcy zalogowali się hasłami z wcześniejszych wycieków na osobiste konta inżynierów w GitHub, w prywatnym repozytorium znaleźli klucz dostępowy do chmury Amazon S3 „in plain text in code” i pobrali 16 plików z niezaszyfrowanymi danymi – m.in. ok. 25,6 mln nazwisk i adresów e-mail oraz 607 tys. numerów praw jazdy.

Dlaczego się udało

Technicznie: Uber – brak MFA na kontach GitHub, brak zakazu powtarzania haseł, sekret w kodzie, kopie bazy bez szyfrowania; w 2014 r. ten sam wektor: klucz w publicznym repozytorium. FTC: zabezpieczenia były możliwe „through relatively low-cost measures”.

Organizacyjnie: PZDW – dyrektor zeznał, że praktyką było czekanie na oryginał dokumentu, a zmianę wprowadzono na podstawie skanu z e-maila; obieg z pięcioma podpisami nie zawierał potwierdzenia u wykonawcy. Uber – szef bezpieczeństwa uznał wymuszenie za zgłoszenie „bug bounty”, zapłacił 100 tys. USD za podpisanie NDA i nie poinformował FTC, która prowadziła już postępowanie po wycieku z 2014 r.

Jak temu zaradzić

Zabezpieczenia: MFA na repozytoriach kodu i kontach chmury, skanowanie kodu pod kątem sekretów, rotacja kluczy, szyfrowanie danych i kopii, konta o minimalnych uprawnieniach; w księgowości – dane rachunków kontrahentów zmienia jedna rola z historią zmian, system sprawdza rachunek w wykazie podatników VAT.

Procedury: zmiana rachunku tylko po oddzwonieniu na numer z umowy i na podstawie oryginału, „cztery oczy” dla danych płatniczych; procedura zgłaszania incydentów z udziałem prawnika i zarządu – ukrycie incydentu zmieniło wyciek w sprawę karną, a ugoda z FTC objęła program prywatności i zewnętrzne audyty przekazywane regulatorowi.

Źródła: PortalSamorządowy (11.07.2017); TVN24 Białystok (7.10.2025); MiastoBiałystok.pl (14.05.2026); FTC: Revised Complaint, Uber Technologies, C-4662 (25.10.2018); FTC, komunikat z 12.04.2018; U.S. Court of Appeals for the Ninth Circuit, No. 23-927 (13.03.2025)

Literówka w Bangladesh Bank



Luty 2016

Przestępcy wykradli dane uwierzytniające Bangladesh Bank do zleceń płatniczych i wysłali do Rezerwy Federalnej w Nowym Jorku kilkadziesiąt zleceń przelewów z rachunków banku.

- Cztery zlecenia na ok. **81 mln USD** trafiły na Filipiny.
- W zleceniu na 20 mln USD dla rzekomej organizacji pozarządowej ze Sri Lanki była literówka: „**Shalika Fandation**” zamiast „Foundation”.
- Deutsche Bank poprosił Bangladesh Bank o wyjaśnienia i kolejne transakcje zablokowano. Zatrzymano **850–870 mln USD**.

❏ **Lekcja dla Państwa:** tym razem przestępców zatrzymała literówka i czujność banku pośredniczącego. Mechanizmy kontrolne – drugi zatwierdzający, weryfikacja odbiorcy, alarm przy nietypowych zleceniach – mają działać z założenia, a nie przypadkiem. Zarząd ich nie obsługuje, ale je zatwierdza i nadzoruje.

Źródła: OCCRP za Reuters (12.03.2016); NBC News za Reuters (III 2016)

Podstawowe zabezpieczenia, które działają, i darmowe wsparcie

Podstawy działają

Wielka Brytania: organizacje z certyfikatem Cyber Essentials (5 podstawowych zabezpieczeń) o **92% rzadziej** zgłaszają szkodę z polisy cyber – według danych ubezpieczyciela, który dołącza polisę do certyfikatu (NCSC).

CIS: 56 podstawowych zabezpieczeń z grupy IG1 chroni przed **78% technik** stosowanych w atakach ransomware (model CIS).

Zakupy to jeszcze nie odporność — NIK o programie „Cyberbezpieczny Samorząd” (21.07.2026)

- ok. 1,5 mld zł dla 2 807 gmin, powiatów i województw, z czego 80% na sprzęt, oprogramowanie i usługi wdrożeniowe;
- program nie wymagał audytów ani przed dofinansowaniem, ani po zakończeniu prac, a wskaźniki liczyły zakupy i przeszkolone osoby — nie wiadomo, czy urzędy są odporniejsze;
- w ponad połowie skontrolowanych urzędów nie wdrożono SZBI.

Bezpłatne wsparcie CERT Polska

moje.cert.pl

Skanowanie domen i sieci (system Artemis), powiadomienia o wyciekach danych kont w domenie i o podatnościach. Przykład: w styczniu 2025 r. CERT Polska powiadomił administratorów 240 podatnych urządzeń FortiOS; na koniec grudnia 2025 r. zostało 35.

Lista Ostrzeżeń

Domeny wydłużające dane, które można blokować we własnym DNS; w 2025 r. ok. 141,1 mln zablokowanych wejść.

- ❑ **Dla budżetu:** najpierw podstawowe zabezpieczenia i sprawdzenie ich skuteczności, potem kolejne zakupy.

Źródła: NCSC UK: A decade of Cyber Essentials (15.11.2024); CIS Community Defense Model v2.0 (29.09.2021); NIK, komunikat z 21.07.2026: Cyberbezpieczny Samorząd; CERT Polska, Raport roczny 2025 (8.04.2026); CERT Polska: moje.cert.pl i Lista Ostrzeżeń

Checklista zarządu 1/2

Nadzór nad systemem bezpieczeństwa · art. 8c, 8d, 8f, 9 KSC; art. 20 NIS2

- ☐ Zarząd decyduje o SZBI i go nadzoruje
- ☐ Zadania przydzielone i nadzorowane
- ☐ Wskazana osoba odpowiedzialna w zarządzie
- ☐ Dwie osoby do kontaktu
- ☐ Informacja z KRK przed dopuszczeniem

Polityki i procedury bezpieczeństwa · art. 8 ust. 1 pkt 2, art. 10 KSC

- ☐ Polityki bezpieczeństwa i szacowania ryzyka
- ☐ Plany ciągłości i odtworzenia
- ☐ Dokumentacja pod nadzorem

Szkolenia i podnoszenie świadomości · art. 8 ust. 1 pkt 2, art. 8d, 8e KSC; art. 20 NIS2

- ☐ Coroczne szkolenie zarządu
- ☐ Personel zna obowiązki i regulacje
- ☐ Edukacja i cyberhigiena

Zasoby i budżet przeznaczony na bezpieczeństwo · art. 8d pkt 2, art. 14 KSC

- ☐ Budżet na cyberbezpieczeństwo
- ☐ Własny zespół lub MSSP

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); RODO (rozporządzenie 2016/679); dyrektywa NIS2 (2022/2555); pełna podstawa prawna każdej pozycji: Checklista zarządu (PDF)

Checklista zarządu 2/2

Zarządzanie ryzykiem · art. 8 ust. 1–2 KSC

- ☐ Systematyczne szacowanie ryzyka
- ☐ Zinwentaryzowane aktywa
- ☐ Ryzyko dostawców ICT
- ☐ Podatności i aktualizacje

Obowiązki związane ze zgłaszaniem incydentów · art. 11–12c KSC; art. 33–34 RODO

- ☐ Procedura obsługi incydentów
- ☐ Terminy 24 h / 72 h / miesiąc
- ☐ Kanał S46 i właściwy CSIRT
- ☐ Naruszenia danych osobowych

Przygotowanie organizacji do kontroli i audytów · art. 5, 7c, 15, 53 KSC

- ☐ Ustalony status organizacji
- ☐ Wniosek o wpis do wykazu
- ☐ Dowody na żądanie organu
- ☐ Audyt podmiotu kluczowego

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); RODO (rozporządzenie 2016/679); dyrektywa NIS2 (2022/2555); pełna podstawa prawna każdej pozycji: Checklista zarządu (PDF)

Ćwiczenie 2: samoocena w 7 pytaniach

Prosimy odpowiedzieć w myślach **TAK** albo **NIE** na każde pytanie w odniesieniu do Państwa organizacji.

1	Zarząd decyduje o SZBI i go nadzoruje Czy zarząd podjął decyzje o wdrożeniu SZBI i sposobie jego nadzoru?
2	Polityki bezpieczeństwa i szacowania ryzyka Czy organizacja ma przyjęte polityki bezpieczeństwa systemu informacyjnego i szacowania ryzyka?
3	Coroczne szkolenie zarządu Czy członkowie zarządu przechodzą udokumentowane szkolenie z cyberbezpieczeństwa raz w roku?
4	Budżet na cyberbezpieczeństwo Czy w budżecie zaplanowano środki na obowiązki wynikające z ustawy o KSC?
5	Systematyczne szacowanie ryzyka Czy organizacja systematycznie szacuje ryzyko wystąpienia incydentu?
6	Terminy 24 h / 72 h / miesiąc Czy wiadomo, kto i w jakich terminach zgłasza incydent poważny do CSIRT?
7	Wniosek o wpis do wykazu Czy organizacja złożyła wniosek o wpis do wykazu albo potwierdziła wpis z urzędu?
6–7 TAK Dobra baza — warto sprawdzić, czy mają Państwo na to dowody.	
3–5 TAK Prace w toku — priorytety wyznaczają terminy 3.10.2026 i 3.04.2027.	
0–2 TAK Czas zacząć od ustalenia statusu i szacowania ryzyka.	

Pełna lista 25 pozycji z podstawą prawną: Checklista zarządu od Organizatora.

Źródła: Checklista zarządu (PDF)

Podsumowanie Modułu I i przerwa

Najważniejsze z Modułu I



Jak atakują

Najczęściej przez podatne urządzenia brzegowe i dostęp zdalny bez MFA; podstawowe zabezpieczenia zatrzymują większość technik ransomware.



Status podmiotu

Wynika z załącznika do ustawy, wielkości i faktycznej działalności — nie z samego PKD (art. 5 KSC).



Odpowiedzialność

Kierownik odpowiada za obowiązki z ustawy o KSC także wtedy, gdy je powierzy (art. 8c ust. 1 i 3), a nadzorcy sprawdzają, czy zabezpieczenia działały.



Terminy i kary

3.10.2026 wniosek o wpis · 3.04.2027 obowiązki z rozdziału 3 · 3.04.2028 pierwszy audyt podmiotu kluczowego; kary za większość obowiązków po 3.04.2028, ale kara do 100 mln zł z art. 73 ust. 5 KSC nie jest odroczone.



Plan działania

10 pytań zarządu do IT i Checklista zarządu — 25 pozycji w 7 obszarach, każda z podstawą prawną.



Przerwa 10:30–10:45

Po przerwie, 10:45–12:15: Moduł II — Jak przygotować organizację do wymagań NIS2 i KSC.

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); art. 33 i 35 nowelizacji; Verizon DBIR 2026 (19.05.2026); CERT Polska, Raport roczny 2025 (8.04.2026)