

SZKOLENIE JEDNODNIOWE



NIS2 / UoKSC w praktyce

Praktyczne wdrożenie wymagań Krajowego Systemu Cyberbezpieczeństwa

Rejestracja i S46

Art. 8 – 10 środków

SZBI / ISO 27001

Analiza ryzyka

Analiza luk

Incydenty i CSIRT

Dostawcy ICT

BCP / DR

Audyt KSC

8 godzin dydaktycznych · 5 modułów · 6 ćwiczeń praktycznych · pre-test i post-test · zaświadczenie i certyfikat

LT MASTERY Szkolenia dla Biznesu Piotr Szymczyk · marka LegacyTurn · Dostawca Usług BUR ID 204299

Stan prawny: nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. 2026 poz. 252) – obowiązuje od 3 kwietnia 2026 r.

Prowadzący:

Piotr Szymczyk – konsultant i audytor zgodności regulacyjnej cyberbezpieczeństwa

- Założyciel Grupy LT Mastery / LegacyTurn; specjalizacja: UoKSC, NIS2, DORA, CRA, AI Act
- Audytor wiodący ISO/IEC 27001 (Lead Auditor)
- Autor książki „UoKSC i NIS2 w Praktyce” (ISBN 978-83-981562-0-2) – pierwszej polskiej publikacji o praktycznym wdrożeniu ustawy
- Certyfikowany trener ICVC-SURE, AgilePM Practitioner, Maxwell Leadership Certified Coach & Trainer
- Praktyk wdrożeń SZBI w środowiskach IT oraz OT/ICS
- Prowadzi audyty zgodności i przygotowuje organizacje do audytu ustawowego z art. 15 UoKSC



Zasady pracy na szkoleniu

- Pytania zadajemy na bieżąco – nie czekamy do końca
- Pytania spoza wątku trafiają na „parking” i wracają w bloku FAQ
- Każdy moduł kończy ćwiczenie na własnej organizacji
- Wszystkie szablony zostają u uczestnika po szkoleniu

Ten dzień wypełnia obowiązek z art. 8e UoKSC

- Osoby kierujące podmiotem kluczowym lub ważnym mają obowiązek regularnego udziału w szkoleniach z cyberbezpieczeństwa – minimum raz w roku
- Zachowaj zaświadczenie i listę obecności – to dowód dla audytora

Agenda dnia – 5 modułów i sesja końcowa

Godzina dydaktyczna = 45 minut. 8 godzin dydaktycznych = $8 \times 45 \text{ min} = 360 \text{ minut zajęć}$. Szkolenie realizuje obowiązek ustawowy z art. 8e UoKSC.

1

Zakres, rejestracja i S46 · 09:00 – 10:15 · 1,5 godz. dyd.

Studium przypadku „Czarny Grudzień 2025”, zakres podmiotowy, samoidentyfikacja i wnioski o wpis w systemie S46.

2

Obowiązki, odpowiedzialność, nadzór · 10:30 – 11:45 · 1,5 godz. dyd.

10 obszarów środków bezpieczeństwa z art. 8, odpowiedzialność kierownictwa (art. 73a), kary, nadzór i podział ról.

3

SZBI, ISO 27001, ryzyko i analiza luk · 12:00 – 13:30 · 2 godz. dyd.

Moduł rozszerzony ze względu na kluczowy charakter SZBI i analizy ryzyka. Mapowanie na ISO 27001:2022, metodyka analizy luk.

4

Środki techniczne, incydenty i CSIRT · 14:15 – 15:30 · 1,5 godz. dyd.

MFA, szyfrowanie, monitoring 24/7, SIEM i SOC, podatności; incydenty i zgłoszenia wg art. 11–12a UoKSC.

5

Dostawcy, ciągłość działania, audyt i plan · 15:40 – 16:30 · 1 godz. dyd.

Dostawcy ICT i chmura, BCP/DR i testy, audyt z art. 15, indywidualny plan wdrożenia na 90 dni.

6

Sesja końcowa: Q&A i post-test · 16:30 – 17:00 · 0,5 godz. dyd.

Pytania zaparkowane w trakcie dnia, post-test, omówienie wyników i Ankieta.

Przerwy: 10:15–10:30 · 11:45–12:00 · 13:30–14:15 (obiadowa) · 15:30–15:40. Łącznie 85 minut, nie wliczane do 8 godzin dydaktycznych.

Efekty uczenia się i sposób ich weryfikacji

Efekty zapisane zgodnie ze standardem karty usługi w Bazie Usług Rozwojowych.

Nr	Po ukończeniu szkolenia uczestnik...	Kryterium weryfikacji
1	Ustala samodzielnie, czy i w jakiej kategorii (Podmiot Kluczowy / Ważny / Uznany) jego organizacja podlega UoKSC	Ćwiczenie 1 – wypełniony formularz samoidentyfikacji; post-test
2	Wymienia 10 obszarów środków bezpieczeństwa z art. 8 UoKSC i przypisuje je do ról w organizacji	Ćwiczenie 2 – macierz RACI; post-test
3	Przeprowadza analizę ryzyka zgodną z ISO 27005 i prowadzi rejestr ryzyk	Ćwiczenie 3 – wypełniony rejestr ryzyk
4	Przeprowadza analizę luk wobec wymagań UoKSC i priorytetyzuje luki krytyczne	Ćwiczenie 4 – wypełniona checklista gap analysis
5	Klasyfikuje incydent i sporządza zgłoszenie do właściwego CSIRT w terminach 24 h / 72 h / 1 miesiąc	Ćwiczenie 5 – symulacja „pierwsze 24 godziny”; post-test
6	Formułuje wymagania bezpieczeństwa wobec dostawców ICT oraz ocenia kompletność planu ciągłości działania	Post-test; dyskusja moderowana
7	Przygotowuje organizację do audytu KSC i kompletuje wymagane dowody	Ćwiczenie 6 – mapa drogowa 90 dni; post-test
8	Opracowuje własny plan wdrożenia na najbliższe 90 dni	Ćwiczenie 6 – wypełniony arkusz planu

Walidacja: pre-test na starcie (10 pytań) i post-test w sesji końcowej (20 pytań). Zaliczenie od 60 % poprawnych odpowiedzi. Wynik post-testu jest odnotowany w dokumentacji usługi zgodnie ze standardem Bazy Usług Rozwojowych, a przyrost wiedzy raportowany uczestnikowi.

Jak pracujemy – 6 ćwiczeń i pakiet materiałów

Wszystkie sześć ćwiczeń opiera się na jednym studium przypadku – ataku na polską energetykę z grudnia 2025 – a wnioski uczestnik przenosi na własną organizację.

Ćw. 1 Samoidentyfikacja

Ustalenie statusu PK / PW / poza zakresem na formularzu roboczym – sektor, size-cap, kody PKD, podmioty powiązane.

Ćw. 2 Macierz RACI

Kto w NOVENERGII powinien odpowiadać za każdy z 10 obszarów art. 8 – i który brak właściciela doprowadził do grudniowego incydentu.

Ćw. 3 Rejestr ryzyk

Analiza ryzyka dla infrastruktury NOVENERGII: aktywo – zagrożenie – podatność – $P \times S$ – postępowanie – właściciel i termin.

Ćw. 4 Analiza luk

Checklista wymagań UoKSC wypełniona dla stanu NOVENERGII sprzed ataku – wskazanie 5 luk krytycznych i ich wyceny.

Ćw. 5 Pierwsze 24 godziny

Powtórzenie poranka 29 grudnia 2025 wykonane prawidłowo: klasyfikacja, decyzja o zgłoszeniu, formularz wczesnego ostrzeżenia w terminie 24 h.

Ćw. 6 Plan na 90 dni

Plan naprawczy dla NOVENERGII, a następnie przeniesienie tej samej struktury na własną organizację uczestnika.

Pakiet materiałów – zostaje u uczestnika

- Prezentacja szkoleniowa (PDF)
- Kompendium wiedzy NIS2 / UoKSC / SZBI / ISO 27001
- Checklista audytowa NIS2/UoKSC dla PK i PW (XLSX)
- Roadmapa wdrożenia UoKSC z osią czasu (XLSX)
- Spis dokumentów wymaganych do audytu zgodności (XLSX)
- Matryca kryteriów incydentu poważnego wg 2024/2690 (XLSX)

Szablony robocze do ćwiczeń

- Karta scenariusza NOVENERGIA OZE + formularz samoidentyfikacji PK / PW
- Macierz RACI dla 10 obszarów art. 8
- Arkusz analizy ryzyka cybernetycznego (dane z case'u)
- Formularz zgłoszenia incydentu 24 h / 72 h
- Ankieta oceny dostawcy ICT + klauzule umowne
- Arkusz planu wdrożenia na 90 dni

Pre-test – diagnoza wejściowa

10 pytań · 8 minut · wynik zna tylko uczestnik i prowadzący – to punkt odniesienia, nie ocena.

Pytania pre-testu

- 1. Od kiedy obowiązuje znowelizowana ustawa o KSC?
- 2. Co decyduje o zakwalifikowaniu podmiotu jako kluczowy lub ważny?
- 3. Do kiedy należy złożyć wniosek o wpis do wykazu PK/PW?
- 4. Do czego służy system S46?
- 5. Ile obszarów środków zarządzania ryzykiem wskazuje art. 8 UoKSC?
- 6. W jakim terminie zgłasza się wczesne ostrzeżenie o poważnym incydencie?
- 7. Kto odpowiada osobiście za niewykonanie obowiązków ustawowych?
- 8. Jak często musi być aktualizowany rejestr ryzyk?
- 9. Co oznacza zasada 3-2-1 w kontekście kopii zapasowych?
- 10. W jakim terminie Podmiot Kluczowy przeprowadza pierwszy audyt KSC?

Po co robimy pre-test

- Ustala punkt wyjścia – ten sam zestaw zagadnień wraca w post-teście
- Pozwala prowadzącemu dostosować tempo i głębokość poszczególnych modułów
- Daje mierzalny przyrost wiedzy; wynik post-testu jest odnotowywany w dokumentacji usługi zgodnie ze standardem BUR

Zasady

- Nie korzystamy z materiałów ani wyszukiwarki
- Nie ma punktów ujemnych – „nie wiem” jest poprawną odpowiedzią
- Wyniki nie są nikomu udostępniane poza uczestnikiem
- Do każdego pytania wracamy w trakcie dnia – zapisz numery tych, przy których się zawahałeś

Wynik pre-testu: zapisz go – na końcu dnia porównamy go z post-testem i policzymy przyrost wiedzy.

Zakres, rejestracja i S46

09:00 – 10:15 · 1,5 godz. dyd.

- ✓ Dlaczego powstała NIS2 – realny incydent w polskiej infrastrukturze i krajobraz zagrożeń 2025
- ✓ Od dyrektywy NIS1 do NIS2 i nowelizacji ustawy o KSC – co zmienia się w praktyce
- ✓ Ujednolicona oś czasu 2026–2028: wszystkie terminy ustawowe w jednym miejscu
- ✓ Zakres podmiotowy: podmiot kluczowy, ważny i uznany; 18 sektorów; reguła size-cap (kryterium wielkości przedsiębiorstwa)
- ✓ Drzewo decyzyjne – czy moja organizacja podlega pod UoKSC (Ćwiczenie 1)
- ✓ System S46 / wykaz-ksc.gov.pl – rejestracja krok po kroku i 18 kategorii danych

Studium przypadku: 29 grudnia 2025 – atak na polską energetykę

MODUŁ 1

Źródło: „Raport z incydentu w sektorze energii 29.12”, CERT Polska. Wszystkie fakty na tym i kolejnym slajdzie pochodzą z raportu.

Skala i cel

Skoordynowane ataki w godzinach porannych i popołudniowych 29.12.2025, w okresie mrozów i zamieci przed Nowym Rokiem. Co najmniej 30 farm wiatrowych i fotowoltaicznych, duża elektrociepłownia zasilająca w ciepło blisko pół miliona odbiorców oraz przedsiębiorstwo produkcyjne.

Charakter ataku

Cel wyłącznie destrukcyjny – bez żądania okupu i bez kradzieży dla zysku. CERT Polska porównuje go do celowych podpaleń. Wszystkie ataki wykonał ten sam atakujący.

Wektor wejścia – ten sam wszędzie

Urządzenie brzegowe Fortigate pełniące funkcję koncentratora VPN i zapory. Interfejs VPN dostępny z Internetu, logowanie na konta zdefiniowane lokalnie, bez uwierzytelniania wieloskładnikowego. Część urządzeń była w przeszłości przez długi czas podatna, w tym na zdalne wykonanie kodu.

Dlaczego jeden obiekt otworzył trzydzieści

Powszechną praktyką w branży jest używanie tych samych kont i haseł w wielu obiektach. Przejęcie jednego konta pozwoliło znaleźć kolejne urządzenia, w których było użyte.

Skutek – i czego NIE było

- Zerwanie komunikacji obiektów z operatorem sieci dystrybucyjnej i utrata zdalnego sterowania
- Brak wpływu na bieżącą produkcję energii i na stabilność krajowego systemu elektroenergetycznego
- Poziom uzyskanych dostępów stwarzał ryzyko spowodowania przestoju produkcji

Atrybuty

- Infrastruktura pokrywa się z klastrem znanym jako Static Tundra / Berserk Bear / Ghost Blizzard / Dragonfly
- To pierwsza publicznie opisana aktywność destrukcyjna przypisywana temu klastrowi
- Wykorzystano przejęte serwery VPS i przejęte routery jako infrastrukturę anonimizującą

Wniosek: żaden z użytych mechanizmów nie był wyrafinowany. Domyślne poświadczenia, brak uwierzytelniania wieloskładnikowego, nieaktualne urządzenia brzegowe i współdzielone hasła. Każdy z nich jest wprost adresowany przez art. 8 UoKSC.

Jak wyglądał atak na farmę OZE – krok po kroku

MODUŁ 1

Architektura Głównego Punktu Odbioru i kolejne urządzenia niszczone w kolejności rosnącej po adresie IP.

1

Wejście przez Fortigate

Logowanie do interfejsu SSL-VPN dostępnego z Internetu, na konto lokalne bez MFA. Atakujący uzyskał uprawnienia administratora urządzenia, co pozwoliło pozyskać poświadczenia konta VPN z dostępem do wszystkich podsięci – wydzielone VLAN-y nie stanowiły przeszkody.

2

Sterownik RTU Hitachi RTU560

Logowanie do interfejsu webowego na wbudowane konto „Default” z domyślnym hasłem. Wgranie uszkodzonego firmware (240 bajtów 0xFF w miejscu startu programu) → nieskończona pętla restartu. Funkcja secure update była dostępna, ale na żadnym urządzeniu nie została włączona.

3

Sterownik RTU Mikronika

Logowanie przez SSH na konto root z domyślnymi poświadczeniami i usunięcie wszystkich plików systemowych. Cztery dni wcześniej, 25.12, na tych obiektach odnotowano skanowanie sieci i próby logowania.

4

Sterowniki zabezpieczeń Hitachi Relion 650

Domyślnie włączona usługa FTP i wbudowane konto z domyślnym hasłem – usunięcie plików systemowych i trwałe wyłączenie urządzenia. Wdrożenie zgodne z zaleceniami producenta zablokowałoby to konto automatycznie.

5

Komputer HMI (Windows 10)

8.12 – dostęp przez pulpit zdalny na konto lokalnego administratora z hasłem ustawionym przy wdrożeniu, zmiany konfiguracji przez PowerShell (udziały administracyjne, reguła zapory na porcie 445), rekonesans przy użyciu Impacket. 29.12 rano – uruchomienie wipera DynoWiper. Tam, gdzie hasło było inne, próby były nieskuteczne i HMI ocalało.

6

Serwery portów szeregowych Moxa NPort

Domyślny login i hasło w interfejsie webowym – przywrócenie do ustawień fabrycznych, zmiana hasła i ustawienie adresu IP na nieosiągalny (127.0.0.1), aby opóźnić przywrócenie sprawności.

7

Zacieranie śladów

Wszystkie urządzenia Fortigate przywrócono do ustawień fabrycznych. Z żadnego z zaatakowanych urządzeń nie udało się odzyskać pełnych logów.

Od incydentu do obowiązku ustawowego

MODUŁ 1

Sześć mechanizmów z 29 grudnia i przepis, który każdy z nich adresuje.

Braki zidentyfikowane w analizie po incydencie	Wymóg UoKSC / NIS2	Gdzie omawiamy na szkoleniu
Brak MFA na dostępie zdalnym	Art. 8 – obszar 6: zarządzanie tożsamością i dostępem, uwierzytelnianie wieloskładnikowe	Moduł 4 – minimalny standard techniczny
Domyślne poświadczenia w urządzeniach OT	Art. 8 – obszar 6 oraz obszar 2: bezpieczeństwo nabywania i wdrażania systemów	Moduł 4 – IAM/PAM; Moduł 5 – odbiór wdrożeń od integratora
Współdzielone konta w wielu obiektach	Art. 8 – obszar 5: bezpieczeństwo łańcucha dostaw ICT; nadzór nad dostępem serwisowym	Moduł 5 – ocena dostawców i klauzule umowne
Nieaktualne urządzenia brzegowe	Art. 8 – obsługa podatności i ich ujawnianie; zbieranie informacji o podatnościach	Moduł 4 – zarządzanie podatnościami, SLA patchowania
Brak monitorowania w trybie ciągłym	Art. 8 – objęcie systemu informacyjnego systemem monitorowania w trybie ciągłym	Moduł 4 – monitoring 24/7, SIEM i SOC
Utrata logów po ataku	Art. 8 – logowanie i retencja; art. 12a – sprawozdanie końcowe wymaga chronologii	Moduł 4 – centralne logowanie, retencja 12 miesięcy

Zapamiętaj: organ nadzoru nie pyta „czy mieliście incydent”. Pyta „czy mieliście wdrożone środki, które temu incydentowi miały zapobiec, i czy potraficie to udowodnić”. To jest cała różnica między incydemtem a naruszeniem ustawy.

Karta scenariusza – NOVENERGIA OZE sp. z o.o.

MODUŁ 1

Spółka fikcyjna, ale architektura, podatności i przebieg ataku odwzorowują raport CERT Polska z 29.12.2025. Na niej wykonamy wszystkie sześć ćwiczeń.

Profil podmiotu

- Siedziba: Płock; działalność od 2014 r.
- Wytwarzanie energii z OZE: 5 farm fotowoltaicznych i 1 farma wiatrowa, łącznie 180 MW
- Sprzedaż energii oraz usługi utrzymania farm dla podmiotów trzecich
- Kody PKD: 35.11.Z wytwarzanie energii elektrycznej · 35.14.Z handel energią · 33.14.Z naprawa urządzeń elektrycznych · 62.09.Z usługi ICT

Dane do reguły wielkości

- Spółka: 168 etatów, obrót 41 mln EUR
- NOVENERGIA Serwis sp. z o.o. (100 % udziałów): 74 etaty
- NOVENERGIA Trading sp. z o.o. (100 % udziałów): 23 etaty
- Razem grupa: 265 etatów, obrót 63 mln EUR, suma bilansowa 58 mln EUR
- Sama spółka wygląda na średnie przedsiębiorstwo – grupa już nie

Architektura IT / OT

- Sieć biurowa IT: Active Directory, poczta w chmurze
- GPO: sterownik RTU Hitachi RTU560, HMI na Windows 10, sterowniki zabezpieczeń Relion 650, serwery portów Moxa NPort
- Fortigate jako koncentrator VPN i zaporą; interfejs VPN dostępny z Internetu, konta lokalne bez MFA
- Te same konta serwisowe integratora na wszystkich sześciu obiektach
- Kopie zapasowe na serwerze NAS w tej samej domenie

Stan zgodności na 1 grudnia 2025 r.

- Brak wniosku o wpis do wykazu podmiotów kluczowych i ważnych
- Polityka bezpieczeństwa informacji z 2019 r., nigdy nieaktualizowana
- Brak analizy ryzyka i rejestru ryzyk
- Brak MFA na dostępie zdalnym i na kontach administracyjnych
- Monitoring 8x5 realizowany przez dwuosobowy zespół IT
- Ostatni test odtworzenia z kopii zapasowej: marzec 2023 r.
- Domyślne poświadczenia na RTU, Relion i Moxa – nigdy niezmienione po wdrożeniu

Do czego użyjemy tej karty

- Ćwiczenie 1 – ustalenie statusu podmiotu i kategorii
- Ćwiczenie 2 – przypisanie odpowiedzialności za 10 obszarów art. 8
- Ćwiczenie 3 – rejestr ryzyk dla tej infrastruktury
- Ćwiczenie 4 – analiza luk wobec stanu z 1 grudnia 2025 r.
- Ćwiczenie 5 – pierwsze 24 godziny od 29 grudnia wykonane prawidłowo
- Ćwiczenie 6 – plan naprawczy na 90 dni, przenoszony na własną organizację

Krajobraz zagrożeń 2025 – TOP 10

MODUŁ 1

Źródła: ENISA Threat Landscape 2025, raporty CERT Polska. Zagrożenia oznaczone jako krytyczne bezpośrednio dotyczą podmiotów kluczowych i ważnych.

1 Ransomware 3.0

Podwójne i potrójne wymuszenie połączone z destrukcją danych.

KRYTYCZNY

2 Ataki na tożsamość

Kradzież sesji i tokenów, obchodzenie MFA, przejęcia kont.

KRYTYCZNY

3 Phishing z użyciem AI

Deepfake głosu i wideo, spersonalizowany spear phishing.

WYSOKI

4 Ataki na łańcuch dostaw

Dostawcy ICT, SaaS, MSP, złośliwe aktualizacje oprogramowania.

KRYTYCZNY

5 Podatności zero-day

Masowe skanowanie internetu i automatyczna eksploatacja CVE.

WYSOKI

6 Błędy konfiguracji chmury

Otwarte zasoby, błędy IAM, przejęcia kont w usługach chmurowych.

WYSOKI

7 DDoS na usługi krytyczne

Ataki wolumetryczne na infrastrukturę publiczną i usługi kluczowe.

WYSOKI

8 Zagrożenie wewnętrzne

Świadome i nieświadome działania pracowników i podwykonawców.

ŚREDNI

9 Ataki na OT / ICS

Infrastruktura krytyczna i OZE – incydent w Polsce, grudzień 2025.

KRYTYCZNY

10 Wycieki z SaaS

Shadow IT, brak kontroli udostępnień, brak CASB.

ŚREDNI

Praktyczne zastosowanie: ta lista jest dobrym punktem wyjścia do katalogu zagrożeń w analizie ryzyka (Moduł 3, Ćwiczenie 3) – zamiast wymyślać zagrożenia od zera.

Od NIS1 do NIS2 – co się zmieniło

MODUŁ 1

Dyrektywa NIS1 (2016) – ograniczenia

- Wąski zakres podmiotowy – objęła relatywnie nieliczne sektory (7 sektorów)
- Brak harmonizacji wdrożenia między państwami członkowskimi
- Niewystarczające mechanizmy egzekwowania
- Brak przepisów o odpowiedzialności kierownictwa
- Brak wymagań wobec łańcucha dostaw
- Kary symboliczne, w praktyce rzadko stosowane

Dyrektywa NIS2 (UE 2022/2555) – rozszerzenie

- 18 sektorów zamiast pierwotnych: 7, w podziale na kluczowe i ważne (PK / PW)
- Jednolity katalog 10 obszarów środków zarządzania ryzykiem (art. 21)
- Obowiązkowe zarządzanie ryzykiem dostawców ICT
- Kary administracyjne na poziomie porównywalnym z RODO
- Osobista odpowiedzialność kierownictwa – zmiana modelu odpowiedzialności
- Ścisłe terminy zgłaszania incydentów: 24 h / 72 h / do 1 miesiąca
- Obowiązkowe szkolenia dla kadry zarządzającej, nie tylko dla IT

Przesunięcie paradygmatu: z „mamy dokumenty” na „umiemy zarządzać ryzykiem i potrafimy to wykazać”. Dokumentacja bez operacyjności i operacyjność bez dokumentacji to w obu przypadkach niezgodność.

Implementacja w Polsce – ścieżka legislacyjna nowelizacji UoKSC

MODUŁ 1

Ujednolicony stan faktyczny – ten sam opis obowiązuje we wszystkich materiałach szkoleniowych.

1

Ustawa z 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa

Implementacja dyrektywy NIS2 do prawa polskiego.

2

19 lutego 2026 – podpis Prezydenta RP

Jednocześnie skierowanie wybranych przepisów do Trybunału Konstytucyjnego w trybie kontroli następczej.

3

2 marca 2026 – ogłoszenie w Dzienniku Ustaw (Dz.U. 2026 poz. 252)

Podstawowa sygnatura, do której odwołujemy się w całym szkoleniu.

4

3 kwietnia 2026 – wejście w życie

Start obowiązków dla podmiotów kluczowych i ważnych; nadzór aktywny.

Czy ustawa obowiązuje mimo wniosku do TK?

- Tak. Skierowanie do Trybunału w trybie następczym nie wstrzymuje wejścia w życie ustawy
- Ewentualne stwierdzenie niekonstytucyjności dotyczyłoby wyłącznie zakwestionowanych przepisów

Zastrzeżenia skierowane do TK

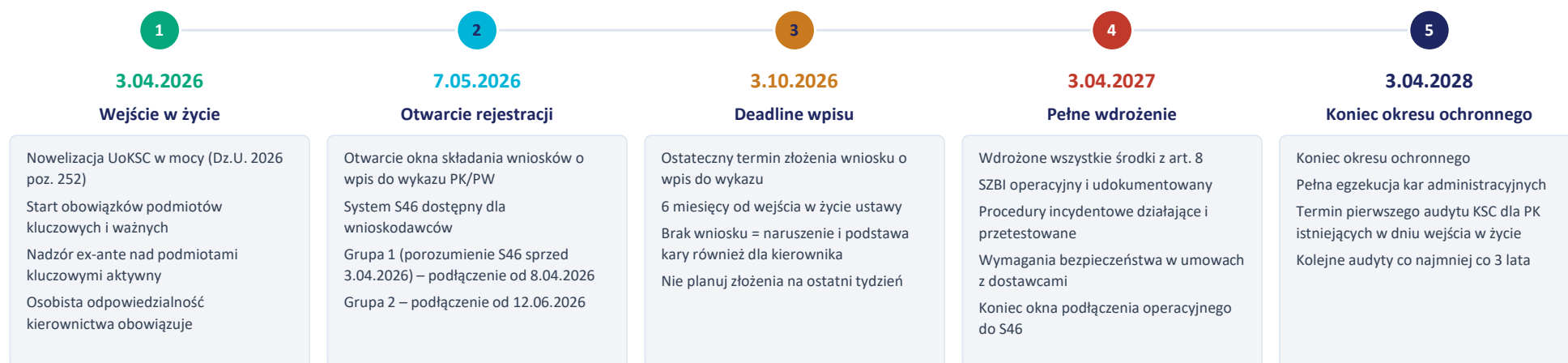
- Objęcie ustawą 18 branż gospodarki w podziale na podmioty kluczowe i ważne
- Mechanizm uznawania dostawców wysokiego ryzyka
- Zakres uprawnień organów nadzoru

Konsekwencja praktyczna: terminy będą niezależnie od postępowania przed Trybunałem. Wstrzymywanie wdrożenia w oczekiwaniu na wyrok jest ryzykiem, nie strategią.

Oś czasu 2026–2028 – jedno źródło terminów

MODUŁ 1

Wszystkie terminy w tej prezentacji, kompendium i materiałach uczestnika odwołują się do tej osi.



Uwaga do audytu (art. 15): dla podmiotów kluczowych wpisanych po wejściu w życie ustawy 24-miesięczny termin biegnie od daty wpisu do wykazu; dla podmiotów uznanych decyzją – od jej doręczenia. 3.04.2028 dotyczy PK istniejących w dniu wejścia w życie nowelizacji.

NIS2 / UoKSC w ekosystemie regulacji – z czym się styka

Najczęstsze pytanie z sali: „a jak to się ma do RODO / DORA / ISO?”.

Regulacja	Czego dotyczy	Relacja do UoKSC
RODO (2016/679)	Ochrona danych osobowych	Zbiory obowiązków się przecinają, ale nie pokrywają. Jeden incydent może wymagać zgłoszenia do CSIRT (24 h) i do UODO (72 h) – to dwa niezależne obowiązki.
DORA (2022/2554)	Odporność operacyjna sektora finansowego	Dla podmiotów finansowych DORA jest lex specialis – ma pierwszeństwo w zakresie, który reguluje. UoKSC stosuje się w pozostałym zakresie.
CRA (2024/2847)	Cyberodporność produktów z elementami cyfrowymi	UoKSC dotyczy organizacji, CRA – produktu. Producent podlegający obu regulacjom może wykorzystać dokumentację SZBI w dokumentacji technicznej produktu.
AI Act (2024/1689)	Systemy sztucznej inteligencji	Systemy AI wysokiego ryzyka mają własne wymagania w zakresie cyberbezpieczeństwa i odporności – uwzględnij je w analizie ryzyka.
ISO/IEC 27001:2022	System zarządzania bezpieczeństwem informacji	Nie jest obowiązkowa, ale stanowi naturalną ramę wdrożeniową. Szczegółowe mapowanie omawiamy w Module 3.
Regulacje sektorowe	URE, UKE, KNF, GIS, ULC i inne	Organ sektorowy jest właściwy dla nadzoru i dla zgłoszeń. Ustal swój organ przed pierwszym incydentem, nie w jego trakcie.

Zakres podmiotowy – trzy kategorie podmiotów

MODUŁ 1

PODMIOT KLUCZOWY

art. 5 ust. 1 UoKSC

Sektor z Załącznika nr 1 (wysoka krytyczność)
Duże przedsiębiorstwo wg reguły size-cap
Nadzór ex-ante – kontrola prewencyjna w każdej chwili
Obowiązkowy audyt KSC co 3 lata
Kara do 10 mln EUR lub 2 % przychodu

PODMIOT WAŻNY

art. 5 ust. 2 UoKSC

Sektor z Załącznika nr 1 lub 2, poniżej progu PK
Średnie przedsiębiorstwo wg reguły size-cap
Nadzór ex-post – kontrola po incydencie lub skardze
Audyt po incydencie / zgłoszeniu, nie prewencyjnie
Kara do 7 mln EUR lub 1,4 % przychodu

PODMIOT UZNANY

art. 7 UoKSC

Uznanie decyzją organu mimo niespełnienia kryteriów wielkościowych
Przesłanka: istotny wpływ na bezpieczeństwo lub ciągłość usług
Typowo: jedyny dostawca usługi krytycznej w kraju
Nie składa wniosku o wpis – wpis następuje z urzędu, na podstawie decyzji organu
Terminy biegną od dnia doręczenia decyzji

Zakres obowiązków merytorycznych jest w praktyce ten sam

- Katalog 10 obszarów środków bezpieczeństwa z art. 8 obowiązuje jednakowo podmioty kluczowe i ważne – różnica leży w intensywności nadzoru, obowiązku audytu i wysokości kar
- Nie buduj więc „lżejszego SZBI dla PW” – buduj SZBI proporcjonalny do własnego ryzyka, tak samo udokumentowany

18 sektorów objętych regulacją – 11 + 7

MODUŁ 1

Kwalifikacja wynika z faktycznie prowadzonej działalności, nie wyłącznie z brzmienia wpisu w rejestrze.

Załącznik nr 1 – sektory wysokiej krytyczności (11)

1. Energetyka – elektroenergetyka, ciepłownictwo i chłodnictwo, ropa naftowa, gaz, wodór
2. Transport – lotniczy, kolejowy, wodny, drogowy
3. Bankowość
4. Infrastruktura rynków finansowych
5. Opieka zdrowotna
6. Woda pitna
7. Ścieki
8. Infrastruktura cyfrowa – DNS, rejestry TLD, punkty wymiany ruchu, chmura, centra danych, CDN, usługi zaufania, łączność elektroniczna
9. Zarządzanie usługami ICT (B2B) – dostawcy usług zarządzanych MSP i MSSP
10. Podmioty administracji publicznej
11. Przestrzeń kosmiczna

Załącznik nr 2 – pozostałe sektory krytyczne (7)

1. Usługi pocztowe i kurierskie
2. Gospodarowanie odpadami
3. Produkcja, wytwarzanie i dystrybucja chemikaliów
4. Produkcja, przetwarzanie i dystrybucja żywności
5. Produkcja – wyroby medyczne, komputery i elektronika, urządzenia elektryczne, maszyny, pojazdy, pozostały sprzęt transportowy
6. Dostawcy usług cyfrowych – platformy handlowe, wyszukiwarki, sieci społecznościowe
7. Badania naukowe

Pułapka praktyczna: sprawdź wszystkie kody PKD zarejestrowane w KRS, nie tylko przeważający. Jeżeli choćby jeden obszar działalności mieści się w sektorze z Załącznika nr 1, cały podmiot może zostać zakwalifikowany jako kluczowy. NOVENERGIA z naszego scenariusza ma cztery kody PKD – i to czwarty z nich zmienia wynik.

Reguła wielkości przedsiębiorstwa (size-cap) – jak ją liczyć

MODUŁ 1

Kryteria wielkościowe wg rozporządzenia Komisji (UE) nr 651/2014.

Kategoria	Zatrudnienie	Obrót roczny / suma bilansowa	Skutek dla UoKSC
Duże przedsiębiorstwo	≥ 250 osób	obróć > 50 mln EUR lub bilans > 43 mln EUR	Sektor z Zał. 1 → podmiot kluczowy
Średnie przedsiębiorstwo	50 – 249 osób	obróć 10 – 50 mln EUR lub bilans 10 – 43 mln EUR	Podmiot ważny (lub kluczowy zależnie od sektora)
Małe i mikro	< 50 osób	obróć i bilans ≤ 10 mln EUR	Co do zasady poza zakresem – z wyjątkami obok

Jak liczyć – trzy zasady, o których się zapomina

- Progi są alternatywne: wystarczy przekroczenie zatrudnienia LUB obrotu LUB sumy bilansowej
- Wartości liczy się łącznie z podmiotami powiązanymi i partnerskimi zgodnie z rozporządzeniem 651/2014 – grupa kapitałowa wygląda na papierze jak zbiór małych spółek, ale po zsumowaniu progi przekracza
- Zatrudnienie liczone jako ekwiwalent pełnych etatów, z uwzględnieniem umów zlecenia
- Wartości obrotu i sumy bilansowej wyrażone są w euro – przeliczenia dokonuje się według kursu ogłaszanego przez Narodowy Bank Polski

Kiedy mały podmiot i tak podlega ustawie

- Jest jedynym dostawcą usługi krytycznej w kraju
- Świadczy usługi dla podmiotu kluczowego lub ważnego i jego zakłócenie przenosi się na usługę kluczową
- Został uznany decyzją organu na podstawie art. 7
- Działa w sektorze, dla którego ustawa nie stosuje progów wielkościowych (m.in. część infrastruktury cyfrowej i administracja publiczna)

Dzień referencyjny: wielkość oceniamy na podstawie ostatniego zatwierdzonego roku obrotowego. Utrata lub przekroczenie progu wpływa na status dopiero, gdy utrzymuje się przez dwa kolejne okresy obrachunkowe.

Drzewo decyzyjne – czy moja organizacja podlega pod UoKSC?

MODUŁ 1

1

Czy działasz w jednym z 18 sektorów z Załącznika nr 1 lub nr 2?

Sprawdź wszystkie kody PKD w KRS oraz faktycznie prowadzone procesy biznesowe, nie tylko przeważającą działalność.

TAK → krok 2

NIE → poza zakresem (zweryfikuj z prawnikiem)

2

Czy spełniasz kryterium size-cap – jesteś dużym albo średnim przedsiębiorstwem?

Licz łącznie z podmiotami powiązanymi i partnerskimi wg rozporządzenia 651/2014.

TAK → krok 3

NIE → sprawdź wyjątki dla małych podmiotów

3

Czy działasz w sektorze z Załącznika nr 1 jako duże przedsiębiorstwo?

To rozstrzyga o przypisaniu do kategorii kluczowej albo ważnej.

TAK → PODMIOT KLUCZOWY

NIE → PODMIOT WAŻNY

4

Czy otrzymałeś decyzję organu o uznaniu za podmiot kluczowy lub ważny?

Sprawdź korespondencję urzędową i skrzynkę do doręczeń elektronicznych.

TAK → terminy biegną od doręczenia

NIE → składasz wniosek 7.05 – 3.10.2026

Udokumentuj wynik: niezależnie od rezultatu sporządź notatkę z uzasadnieniem i przedstaw ją zarządowi do akceptacji. Także wynik negatywny wymaga dowodu – organ może zapytać, na jakiej podstawie uznaliście, że ustawa Was nie dotyczy.

Ćwiczenie 1 – samoidentyfikacja na przykładzie NOVENERGII

MODUŁ 1

12 minut pracy + 5 minut omówienia. Szablony: karta scenariusza NOVENERGIA OZE oraz formularz samoidentyfikacji PK / PW.

1

Sektor

Przejdź cztery kody PKD z karty scenariusza i wskaż, które z nich mieszczą się w Załączniku nr 1 lub nr 2. Zapisz sektor i podsektor.

2

Wielkość

Policz zatrudnienie i obrót najpierw dla samej spółki, a następnie łącznie z dwiema spółkami zależnymi. Zapisz obie wartości.

3

Kategoria

Przejdź drzewo decyzyjne z poprzedniego slajdu i wskaż wynik: podmiot kluczowy, ważny czy poza zakresem.

4

Uzasadnienie

Zapisz jednym akapitem, dlaczego taki wynik – tak, jakbyś przedstawiał go zarządowi do akceptacji.

5

Twoja organizacja

Powtórz kroki 1–4 dla własnego podmiotu. To jest pierwszy dokument Twojej dokumentacji zgodności.

Ćwiczenie 1 – samoidentyfikacja na przykładzie NOVENERGII

MODUŁ 1

12 minut pracy + 5 minut omówienia. Szablony: karta scenariusza NOVENERGIA OZE oraz formularz samoidentyfikacji PK / PW.

1

Sektor

Przejdź cztery kody PKD z karty scenariusza i wskaż, które z nich mieszczą się w Załączniku nr 1 lub nr 2. Zapisz sektor i podsektor.

2

Wielkość

Policz zatrudnienie i obrót najpierw dla samej spółki, a następnie łącznie z dwiema spółkami zależnymi. Zapisz obie wartości.

3

Kategoria

Przejdź drzewo decyzyjne z poprzedniego slajdu i wskaż wynik: podmiot kluczowy, ważny czy poza zakresem.

4

Uzasadnienie

Zapisz jednym akapitem, dlaczego taki wynik – tak, jakbyś przedstawiał go zarządowi do akceptacji.

5

Twoja organizacja

Powtórz kroki 1–4 dla własnego podmiotu. To jest pierwszy dokument Twojej dokumentacji zgodności.

Pułapki wbudowane w scenariusz

- Przeważający PKD 35.11.Z sam w sobie prowadzi do sektora Energetyka z Załącznika nr 1
- Kod 62.09.Z wskazuje na usługi ICT – trzeba sprawdzić, czy spółka nie świadczy ich jako usług zarządzanych
- Sama spółka mieści się w progach średniego przedsiębiorstwa; po zsumowaniu z podmiotami zależnymi przekracza próg 250 etatów i 50 mln EUR
- Wynik zmienia się z podmiotu ważnego na kluczowy – a wraz z nim tryb nadzoru, obowiązek audytu i wysokość kar

Wynik, do którego dochodzimy: NOVENERGIA OZE to podmiot kluczowy – sektor Energetyka z Załącznika nr 1 oraz duże przedsiębiorstwo po zsumowaniu wartości grupy zgodnie z rozporządzeniem 651/2014. Konsekwencje: nadzór ex-ante, obowiązkowy audyt bezpieczeństwa co najmniej co 3 lata i kara do 10 mln EUR lub 2 % przychodu.

Nie podlegasz ustawie? Klient i tak Cię rozliczy

MODUŁ 1

Rozszerzony krąg oddziaływania regulacji poprzez łańcuch dostaw.

Podmiot kluczowy lub ważny odpowiada za swój łańcuch dostaw

Art. 8 UoKSC oraz art. 21 ust. 2 lit. d NIS2 nakładają obowiązek oceny ryzyka dostawców i wprowadzenia wymagań bezpieczeństwa do umów.

Wymagania egzekwowane w dół łańcucha dostaw umową, nie ustawą

Dostawca nie jest kontrolowany przez organ nadzoru, ale przez swojego klienta – ankietą bezpieczeństwa, klauzulą umowną i prawem do audytu.

Presja rynkowa działa szybciej niż kontrola

Pierwsze pytania o zgodność przychodzą nie od organu, lecz z działu zakupów kontrahenta – zwykle w formie ankiety przy odnowieniu umowy.

To ryzyko biznesowe, nie tylko regulacyjne

Brak odpowiedzi na ankietę bezpieczeństwa albo brak podstawowych zabezpieczeń może oznaczać utratę kontraktu, zanim pojawi się jakakolwiek kara.

Minimalny zestaw, o który zapyta Cię klient

- Kto u Was odpowiada za bezpieczeństwo informacji
- Czy macie politykę bezpieczeństwa informacji i kiedy była aktualizowana
- Czy prowadzicie analizę ryzyka i rejestr ryzyk
- Czy macie procedurę zgłaszania incydentów i w jakim czasie nas powiadomicie
- Czy stosujecie MFA i jak zarządzacie dostępem uprzywilejowanym
- Czy testujecie odtwarzanie z kopii zapasowych
- Czy posiadacie certyfikat ISO 27001 lub równoważny

System S46 – portal wykaz-ksc.gov.pl

MODUŁ 1

Jedynе oficjalne miejsce składania wniosków i komunikacji z organami Krajowego Systemu Cyberbezpieczeństwa.

Czym jest S46

- System teleinformatyczny prowadzony przez Ministerstwo Cyfryzacji do wymiany informacji z organami KSC
- Adres: wykaz-ksc.gov.pl
- Uwierzytelnianie: profil zaufany, e-dowód lub kwalifikowany podpis elektroniczny

Co składa się przez S46

- Wniosek o wpis do wykazu podmiotów kluczowych i ważnych
- Zgłoszenia poważnych incydentów (24 h / 72 h / raport końcowy do 1 miesiąca)
- Aktualizacje danych podmiotu
- Korespondencję formalną z organami nadzoru

Cztery decyzje do podjęcia zanim usiądziesz do wniosku

- Kto jest administratorem konta S46 – wniosek wymaga podania numeru PESEL tej osoby
- Kto jest osobą (osobami) do kontaktu z podmiotami KSC – minimum dwie osoby; dla mikro i małych podmiotów wystarczy jedna
- Kto podpisuje wniosek w imieniu podmiotu i czy dysponuje ważnym podpisem
- Jak obsługujecie powiadomienia z S46 poza godzinami pracy – incydent nie czeka do poniedziałku

Obowiązek ciągły: dane w wykazie muszą pozostawać aktualne. Zmiana adresu, struktury, zakresu usług albo osób kontaktowych wymaga aktualizacji wniosku – to nie jest czynność jednorazowa.

Wniosek o wpis – 18 kategorii danych (art. 7 ust. 2 pkt 1–18 UoKSC)

MODUŁ 1

Zbierz te dane zanim otworzysz formularz – kompletowanie ich w trakcie wypełniania jest najczęstszą przyczyną opóźnień.

Dane podstawowe i rejestrowe (1–9)

Część danych podstawowych system pobiera automatycznie z rejestrów publicznych (KRS, REGON) – zweryfikuj ich aktualność przed wystaniem wniosku

1. Nazwa (firma) podmiotu
2. Adres siedziby
3. Adres do korespondencji
4. Adres do doręczeń elektronicznych (ADE), jeżeli istnieje
5. Adres e-mail podmiotu
6. Numer NIP
7. Numer REGON
8. Numer w rejestrze działalności regulowanej, jeżeli dotyczy
9. Sektor, podsektor i rodzaj podmiotu zgodnie z Załącznikiem nr 1 lub nr 2

Dane techniczne, osobowe i uzupełniające (10–18)

10. Zakresy publicznych adresów IP wykorzystywanych w sposób ciągły
11. Zakresy domen internetowych wykorzystywanych w sposób ciągły
12. Dane osób kontaktowych – imię, nazwisko, telefon i e-mail służbowy
13. PESEL administratora konta w systemie S46
14. Deklaracja wielkości przedsiębiorstwa wg rozporządzenia 651/2014
15. Informacja o działalności w innych państwach UE
16. Szacunkowa liczba użytkowników usług w Polsce
17. Szacunkowa liczba użytkowników usług w UE
18. Dane dotyczące usług MSSP, jeżeli podmiot z nich korzysta

Wskazówka: pozycje 16 i 17 dotyczą przede wszystkim podmiotów infrastruktury cyfrowej. Nie zgaduj – jeżeli nie prowadzisz takiej działalności, opisz to zgodnie ze stanem faktycznym.

Zakresy adresów IP i domen – skąd wziąć te dane

MODUŁ 1

Najczęstszy punkt zatrzymania przy wypełnianiu wniosku.

Publiczne adresy IP wykorzystywane w sposób ciągły

- Co podać: adresy publiczne używane w usługach teleinformatycznych objętych KSC
- Formaty: pojedynczy adres (195.12.34.56), zakres CIDR (195.12.34.0/24), kilka zakresów, także IPv6 (2a02:25a0:abcd::/48)
- Gdzie znaleźć: administrator sieci lub dostawca usług IT
- Dokumentacja od operatora (umowa, protokół przekazania adresacji)
- Konfiguracja firewalli, routerów i serwerów brzegowych
- Panel usług chmurowych – Azure, AWS, Google Cloud

Zakresy nazw domenowych (FQDN)

- Co podać: domeny i subdomeny wykorzystywane w usługach teleinformatycznych podmiotu
- Domena główna: twojafirma.pl
- Subdomeny: vpn.twojafirma.pl, mail.twojafirma.pl, portal.twojafirma.pl
- Domeny usług chmurowych: twojafirma.sharepoint.com i podobne
- Gdzie znaleźć: administrator DNS, panel rejestratora domen, konfiguracja serwerów i usług

Efekt uboczny, który warto wykorzystać: zebranie tych danych to w praktyce pierwszy krok inwentaryzacji aktywów, wymaganej później w analizie ryzyka. Nie traktuj tego jak formalności – zapisz wynik w rejestrze aktywów.

Zakresy IP i domen: nie podlegają odpowiedzialności karnej za niepełne / błędne dane (wyjątek w ustawie).

Rejestracja krok po kroku – od ustalenia statusu do uruchomienia obowiązków

MODUŁ 1

1 Ustal status

Analiza sektora, size-cap i kodów PKD.
Udokumentuj wynik notatką i uzyskaj akceptację zarządu.

2 Wyznacz właściciela

CISO, dyrektor IT lub compliance jako właściciel procesu KSC oraz minimum dwie osoby do kontaktu z podmiotami KSC.

3 Przygotuj dostęp

Konto na wykaz-ksc.gov.pl, uwierzytelnianie profilem zaufanym, e-dowodem lub podpisem kwalifikowanym. Sprawdź to wcześniej.

4 Zbierz dane

18 kategorii z art. 7 ust. 2: dane rejestrowe, opis usług, zakresy IP i domen, osoby kontaktowe, PESEL administratora konta.

5 Złóż wniosek

Wyłącznie elektronicznie, w oknie 7.05 – 3.10.2026. Zachowaj potwierdzenie w PDF i numer sprawy.

6 Odbierz wpis

Zweryfikuj dane w wykazie. Poinformuj zarząd, IT i compliance o formalnym statusie podmiotu.

7 Skonfiguruj S46

Konta użytkowników, minimalne uprawnienia, procedura obsługi powiadomień także poza godzinami pracy.

8 Uruchom obowiązki

Od wpisu masz czas do 3.04.2027 na pełne wdrożenie środków z art. 8 – patrz moduły 2–5.

Rezerwa czasowa: problemy z podpisem kwalifikowanym, pełnomocnictwem lub kompletowaniem danych technicznych potrafią zająć kilka tygodni. Nie planuj złożenia wniosku na ostatni tydzień września.

Harmonogram rejestracji i korzystania z S46

MODUŁ 1

1

3 kwietnia 2026 – start obowiązków

Wejście w życie nowelizacji. Nadzór nad podmiotami kluczowymi aktywny w trybie ex-ante. Komunikat Ministra Cyfryzacji określa harmonogram podłączeń do S46.

2

7 maja 2026 – otwarcie okna wniosków

Od tego dnia można składać wnioski o wpis do wykazu podmiotów kluczowych i ważnych.

3

8 kwietnia 2026 – 3 kwietnia 2027: Grupa 1

Podmioty, które zawarły porozumienie o korzystaniu z S46 przed 3 kwietnia 2026 – wcześniejsze okno podłączenia operacyjnego.

4

12 czerwca 2026 – 3 kwietnia 2027: Grupa 2

Pozostałe podmioty, bez wcześniejszego porozumienia. Podłączenie operacyjne do S46 w tym oknie.

5

3 października 2026 – termin ostateczny

Ostatni dzień na złożenie wniosku o wpis do wykazu. Po tym terminie brak wpisu stanowi naruszenie i podstawę kary, także dla kierownika.

Rozróżnij dwie rzeczy: termin złożenia wniosku o wpis (do 3.10.2026) i okno operacyjnego podłączenia do S46 (do 3.04.2027) to dwa różne obowiązki o różnych terminach.

Moduł 1 — podsumowanie

MODUŁ 1

Zakres, rejestracja i S46

Ustawa obowiązuje od 3 kwietnia 2026 r. i terminy będą niezależnie od postępowania przed Trybunałem Konstytucyjnym

Dz.U. 2026 poz. 252. Wniosek do TK w trybie następczym nie wstrzymuje wejścia w życie.

Status ustalasz sam – i musisz umieć go uzasadnić

Sektor z Załącznika nr 1 lub 2, reguła size-cap (kryterium wielkości przedsiębiorstwa) wg 651/2014 liczona łącznie z podmiotami powiązanymi, wszystkie kody PKD. Wynik – także nieklasyfikujący do PK/PW – dokumentujesz notatką z akceptacją zarządu.

Wniosek o wpis do wykazu składasz w S46 w oknie 7.05 – 3.10.2026

18 kategorii danych z art. 7 ust. 2, w tym zakresy IP i domen oraz PESEL administratora konta. Dostęp i podpis przygotuj z wyprzedzeniem.

Jeżeli nie podlegasz ustawie, i tak zapyta Cię o zgodność Twój klient

Wymagania wpływają w dół łańcucha dostaw umową i ankietą bezpieczeństwa, zwykle szybciej niż kontrola organu.

Incydent z grudnia 2025 pokazał, że wszystkie cztery przyczyny były organizacyjne

Patch management, segmentacja, monitoring i przetestowane procedury – każdy z tych punktów to konkretny obowiązek z art. 8.

Przechodzimy dalej: w module 2 przechodzimy od „czy mnie dotyczy” do „co konkretnie muszę zrobić i kto za to osobiście odpowiada”.

Obowiązki, odpowiedzialność, nadzór

10:30 – 11:45 · 1,5 godz. dyd.

- ✓ 10 obszarów obowiązkowych środków bezpieczeństwa – art. 8 UoKSC / art. 21 NIS2
- ✓ Osobista odpowiedzialność kierownictwa – art. 73a i realne konsekwencje majątkowe
- ✓ Obowiązkowe roczne szkolenie kierownictwa (art. 8e) i wymóg niekaralności (art. 8f)
- ✓ Kary administracyjne dla podmiotów – progi, minima i okres ochronny do 3.04.2028
- ✓ Organy nadzoru: kto kontroluje, czego żąda i czym różni się nadzór ex-ante od ex-post
- ✓ Podział ról w organizacji i macierz odpowiedzialności (Ćwiczenie 2)

10 obszarów środków – art. 8 UoKSC / art. 21 NIS2 (1/2)

MODUŁ 2

To jest katalog, według którego kontroluje organ nadzoru i według którego budujemy analizę luk w Module 3.

1 Polityki i szacowanie ryzyka

Polityka bezpieczeństwa informacji, systematyczne szacowanie ryzyka, tematyczne polityki szczegółowe, kryteria akceptacji ryzyka zatwierdzone przez zarząd.

2 Bezpieczeństwo nabywania i rozwoju

Bezpieczny cykl wytwarzania oprogramowania, testy bezpieczeństwa systemów, wymagania bezpieczeństwa w procesach zakupowych ICT.

3 Bezpieczeństwo fizyczne i środowiskowe

Ochrona pomieszczeń i infrastruktury, kontrola dostępu fizycznego, zabezpieczenia środowiskowe (zasilanie, chłodzenie, ppoż.).

4 Bezpieczeństwo zasobów ludzkich

Weryfikacja pracowników, szkolenia i budowanie świadomości, zasady offboardingu, odbieranie uprawnień przy odejściu.

5 Bezpieczeństwo łańcucha dostaw ICT

Ocena ryzyka dostawców i podwykonawców, wymagania bezpieczeństwa w umowach, monitorowanie zgodności dostawców.

6 Zarządzanie tożsamością i dostępem

Zarządzanie kontami i uprawnieniami, uwierzytelnianie wieloskładnikowe, zasada minimalnych uprawnień, dostęp uprzywilejowany (PAM).

Zmiana wobec dotychczasowej narracji: wcześniejsze materiały grupowały obowiązki w siedem obszarów rozdziału 3 ustawy. Punktem odniesienia dla kontroli jest katalog 10 środków – i tego katalogu używamy w całym szkoleniu.

10 obszarów środków – art. 8 UoKSC / art. 21 NIS2 (2/2)

MODUŁ 2

7

Kryptografia i szyfrowanie

Polityka kryptograficzna, szyfrowanie danych w spoczynku i w transmisji, zarządzanie kluczami i certyfikatami.

8

Monitorowanie i reagowanie

Logowanie zdarzeń, korelacja (SIEM), monitorowanie w trybie ciągłym, procedury reagowania na incydenty.

9

Ciągłość działania i odtwarzanie

Plany ciągłości działania i odtwarzania po awarii, kopie zapasowe, zarządzanie kryzysowe, testy planów.

10

Zarządzanie incydentami

Wykrywanie, klasyfikacja, obsługa, zgłaszanie do CSIRT i analiza poincydentalna z działaniami doskonalącymi.

Dotychczasowy podział na 7 obszarów rozdziału 3	Odpowiada środkom z art. 8 UoKSC
System Zarządzania Bezpieczeństwem Informacji	Obszar 1 – polityki; spina wszystkie pozostałe obszary
Systematyczne szacowanie ryzyka	Obszar 1 – szacowanie ryzyka
Środki techniczne i organizacyjne	Obszary 2, 3, 6, 7, 8 – nabywanie, fizyczne, IAM, kryptografia, monitoring
Zarządzanie incydentami i zgłaszanie	Obszary 8 i 10 – monitorowanie, reagowanie, zgłoszenia do CSIRT
Dokumentacja (art. 10 ust. 1)	Dowód wdrożenia wszystkich dziesięciu obszarów
Szkolenia i świadomość	Obszar 4 – zasoby ludzkie; dodatkowo art. 8e dla kierownictwa
Osoba odpowiedzialna / punkt kontaktowy	Wymóg organizacyjny warunkujący działanie obszarów 8 i 10

Odpowiedzialność osobista kierownictwa – art. 73a UoKSC

MODUŁ 2

Najważniejsza zmiana ustrojowa NIS2: sankcja dotyka konkretnej osoby, nie tylko organizacji.

Kto jest kierownikiem w rozumieniu ustawy

Zarząd spółki, prezes, dyrektor generalny, a także likwidator i syndyk – każda osoba faktycznie prowadząca bieżące sprawy podmiotu.

Kara pieniężna nakładana na osobę fizyczną

Do 300 % miesięcznego wynagrodzenia kierownika w podmiotach prywatnych; do 100 % w podmiotach publicznych.

Kara osobista jest niezależna od kary dla podmiotu

Obie mogą zostać nałożone jednocześnie, w odrębnych postępowaniach. Jedna nie konsumuje drugiej.

Powierzenie obowiązków nie zwalnia z odpowiedzialności

Kierownik może powierzyć wykonanie obowiązku innej osobie, ale nadal odpowiada za wynik – w tym za jednorazowe zaniechania.

Odpowiedzialność obejmuje także zatwierdzanie polityk i nadzór nad SZBI

To nie jest wyłącznie odpowiedzialność za skutek incydentu. Kierownik odpowiada za zatwierdzenie polityk bezpieczeństwa, zatwierdzenie ryzyk akceptowanych oraz za bieżący nadzór nad funkcjonowaniem systemu zarządzania bezpieczeństwem informacji.

Za co konkretnie odpowiada kierownik

- Brak wpisu do wykazu podmiotów kluczowych i ważnych
- Brak wdrożonego SZBI
- Brak szkoleń z cyberbezpieczeństwa
- Brak zgłoszenia poważnego incydentu
- Niezapewnienie audytu w terminie

Jedyna skuteczna ochrona

- Faktyczne wdrożenie obowiązków z art. 8 i art. 73a
- Udokumentowanie tego wdrożenia – bez dowodu wdrożenie nie istnieje
- Sprawdź polisę D&O: wiele standardowych polis wyłącza kary administracyjne

Konsekwencja majątkowa: niezapłacona kara podlega egzekucji z majątku osobistego. Pokrycie kary przez spółkę stanowi przychód kierownika i podlega opodatkowaniu – nie jest to sposób na uniknięcie skutku.

Katalog obowiązków kierownika – co konkretnie musi zrobić

MODUŁ 2

Rejestracja i wpis

- Dopilnować wpisu do wykazu PK/PW w terminie (S46)
- Wyznaczyć minimum dwie osoby do kontaktu z podmiotami KSC; w mikro i małych podmiotach wystarczy jedna

SZBI i bezpieczeństwo

- Zatwierdzić SZBI i nadzorować jego wdrożenie (art. 8)
- Zapewnić szkolenia z cyberbezpieczeństwa dla siebie i personelu – minimum raz w roku

Incydenty i zgłoszenia

- Wdrożyć procedury zgłaszania incydentów do CSIRT
- Zapewnić użytkownikom usługi możliwość zgłaszania cyberzagrożeń i podatności

Audyt i kontrola

- Zapewnić przeprowadzenie audytu bezpieczeństwa w terminie ustawowym
- Zapewnić weryfikację personelu realizującego zadania z zakresu cyberbezpieczeństwa
- Zapewnić aktualność danych podmiotu w wykazie

Dowody, których zażąda organ

- Uchwała lub decyzja zatwierdzająca politykę bezpieczeństwa informacji
- Protokoły przeglądu zarządzania z podpisami
- Lista obecności i zaświadczenie ze szkolenia kierownictwa
- Potwierdzenie złożenia wniosku w S46 (PDF i numer sprawy)

Praktyczna rada: zbuduj jeden folder „dowody kierownika” i trzymaj w nim komplet powyższych dokumentów. W czasie kontroli nie będzie czasu na ich odtwarzanie.

Szkolenie kierownictwa (art. 8e) i wymóg niekaralności (art. 8f)

MODUŁ 2

Dwa obowiązki, które najczęściej umykają, bo nie leżą po stronie działu IT.

Art. 8e – obowiązkowe szkolenie kierownictwa

- Osoby kierujące podmiotem kluczowym lub ważnym muszą regularnie uczestniczyć w szkoleniach z cyberbezpieczeństwa
- Częstotliwość: minimum raz w roku; szkolenie musi być udokumentowane
- Zakres: zarządzanie ryzykiem, polityki bezpieczeństwa, zgłaszanie incydentów, SZBI, rola kierownictwa
- Udziału nie można delegować – kierownik uczestniczy osobiście
- Dowód: lista obecności, zaświadczenie lub protokół szkolenia
- Ten dzień szkoleniowy wypełnia ten obowiązek – zachowaj dokumentację uczestnictwa

Art. 8f – niekaralność personelu bezpieczeństwa

- Nowy obowiązek: weryfikacja niekaralności osób realizujących zadania z art. 8 i art. 11
- Dotyczy zarówno pracowników własnych, jak i personelu dostawców realizującego te zadania
- Wymaga zmiany procesu rekrutacyjnego i onboardingowego po stronie HR
- Ustal: kto zbiera zaświadczenia, jak długo je przechowujecie i jak często odnawiacie weryfikację
- Zaplanuj podstawę prawną przetwarzania tych danych wspólnie z IOD

Dlaczego to jest ryzyko: oba obowiązki należą do HR i zarządu, a projekty wdrożeniowe prowadzi zwykle IT. To klasyczna luka organizacyjna – obowiązek istnieje, ale nikt nie czuje się jego właścicielem. Przypisz go imiennie jeszcze dziś.

Kary administracyjne dla podmiotów – art. 73 UoKSC

MODUŁ 2

**10 mln EUR
lub 2 %**

Podmiot kluczowy

Kara wyższa z dwóch: 10 000 000 EUR albo 2 %
przychodu z działalności gospodarczej za rok
poprzedni

Minimum: 20 000 zł

**7 mln EUR
lub 1,4 %**

Podmiot ważny

Kara wyższa z dwóch: 7 000 000 EUR albo 1,4 %
przychodu z działalności gospodarczej za rok
poprzedni

Minimum: 15 000 zł

do 100 mln zł

Kara kwalifikowana

Przy bezpośrednim i poważnym cyberzagrożeniu
dla obronności, bezpieczeństwa państwa,
porządku publicznego lub życia i zdrowia ludzi

do 3.04.2028

Okres ochronny

Kary pieniężne mogą być nakładane po upływie
2 lat od wejścia w życie ustawy – nadzór i
kontrole działają jednak od 3.04.2026

Uwaga interpretacyjna: okres ochronny nie oznacza, że można zaniechać wdrożenia. Po jego upływie kara może objąć cały okres niedostosowania, także miesiące między 12 a 24 miesiącem obowiązywania ustawy. Wyjątkiem objętym karą od początku jest bezpośrednie i poważne cyberzagrożenie oraz brak działań w celu jego unikania.

Za co najczęściej grozi kara – katalog naruszeń z art. 73

- Brak uzupełnienia lub korekty danych w wykazie mimo wezwania · brak systematycznego szacowania ryzyka · brak wdrożonego SZBI · brak zgłoszenia poważnego incydentu w terminie · brak przeprowadzenia audytu · niewykonanie zaleceń pokontrolnych · utrudnianie czynności kontrolnych

Jak wygląda postępowanie w sprawie kary dla kierownika

MODUŁ 2

1

Postępowanie administracyjne, nie karne

Prowadzi je organ właściwy do spraw cyberbezpieczeństwa. To kara administracyjna – nie postępowanie karne ani sądowe.

2

Dwa niezależne postępowania

Kara dla kierownika nie zwalnia podmiotu z kary z art. 73 i odwrotnie. Oba postępowania toczą się odrębnie.

3

Środki odwoławcze

Wniosek o ponowne rozpatrzenie sprawy, a następnie skarga do Wojewódzkiego Sądu Administracyjnego.

4

Płatność i egzekucja

Standardowo 30 dni od uprawomocnienia decyzji. Niezapłacona kara podlega egzekucji z majątku osobistego kierownika.

5

Kara nie jest jednorazowa

Organ może nakładać kolejne kary za utrzymujący się stan niezgodności – dopóki obowiązek nie zostanie wykonany.

Do sprawdzenia w tym tygodniu: zapytaj brokera, czy polisa D&O Twojej organizacji obejmuje kary administracyjne nakładane na członków organu zarządzającego. W wielu standardowych polisach są one wprost wyłączone.

Organy nadzoru – kto kontroluje i czego może żądać

MODUŁ 2

Struktura nadzoru

- Minister właściwy do spraw informatyzacji – organ koordynujący, nadzór ogólny nad krajowym systemem cyberbezpieczeństwa
- Organy właściwe sektorowo – m.in. Prezes URE (energia), Prezes UKE (telekomunikacja), KNF (finanse), GIS (zdrowie), ULC (lotnictwo)
- Ustal swój organ sektorowy zanim wystąpi pierwszy incydent

Podmiot kluczowy – nadzór ex-ante

- Organ może przeprowadzić kontrolę prewencyjnie, w każdej chwili, bez wystąpienia incydentu
- Kontrola planowa jest normą, nie wyjątkiem
- Obowiązkowy audyt bezpieczeństwa co najmniej co 3 lata

Czego może żądać organ w toku kontroli

- Dokumentacji: polityk, analiz ryzyka, protokołów testów, rejestrów
- Dostępu do pomieszczeń, systemów i urządzeń
- Wyjaśnień ustnych i pisemnych od pracowników
- Logów i dowodów działania zabezpieczeń
- Wydania zaleceń pokontrolnych z terminem wykonania

Podmiot ważny – nadzór ex-post

- Kontrola zasadniczo po incydencie, zgłoszeniu, skardze lub informacji o naruszeniu
- Brak obowiązku audytu prewencyjnego
- To nie oznacza mniejszego zakresu obowiązków – wyłącznie inny moment weryfikacji

Podział ról – kto co robi w organizacji

MODUŁ 2

Bez imiennego przypisania obowiązków istnieje na papierze, ale nie ma właściciela.

Zarząd / kierownik podmiotu

- Zatwierdzenie polityk SZBI
- Zapewnienie budżetu i zasobów
- Nadzór nad realizacją obowiązków
- Osobisty udział w szkoleniu (art. 8e)
- Odpowiedzialność za wniosek w S46

CISO / osoba wyznaczona

- Właściciel procesu KSC i konta S46
- Koordynacja wdrożenia SZBI
- Prowadzenie analizy ryzyka
- Kontakt z CSIRT i organem nadzoru
- Raportowanie do zarządu – min. kwartalnie

Compliance / audyt wewnętrzny

- Monitorowanie zgodności z wymaganiami
- Przeglądy dokumentacji SZBI
- Koordynacja audytu KSC
- Nadzór nad wersjonowaniem polityk
- Niezależność od obszaru audytowanego

IT / OT

- Wdrożenie środków technicznych: MFA, SIEM, EDR, segmentacja
- Zarządzanie podatnościami i patch management
- Plany i testy techniczne BCP/DR
- Utrzymanie inwentaryzacji aktywów

HR i dział prawny / dział zakupów

- Szkolenia pracowników i budowanie świadomości
- Weryfikacja niekaralności personelu (art. 8f)
- Klauzule bezpieczeństwa w umowach z dostawcami
- Zarządzanie łańcuchem dostaw
- Onboarding i offboarding – nadanie i odebranie dostępów (wniosek/sygnał do IT)

Zasada rozdzielności: IT odpowiada za działanie systemów, bezpieczeństwo informacji – za ich ochronę. Połączenie obu ról w jednej osobie jest konfliktem interesów i standardowym ustaleniem audytowym.

Ćwiczenie 2 – macierz RACI dla NOVENERGII

MODUŁ 2

12 minut pracy + 5 minut omówienia. Szablon: macierz RACI dla 10 obszarów art. 8. Punkt wyjścia: karta scenariusza.

Obszar art. 8 UoKSC	Zarząd	CISO	IT / OT	Compliance	HR / Legal	Stan w NOVENERGII przed atakiem
1. Polityki i szacowanie ryzyka						
2. Nabywanie i rozwój systemów						
3. Bezpieczeństwo fizyczne						
4. Zasoby ludzkie						
5. Łańcuch dostaw ICT						
6. Tożsamość i dostęp						
7. Kryptografia						
8. Monitorowanie i reagowanie						
9. Ciągłość działania						
10. Zarządzanie incydentami						

Zadanie: wskaż jedno uchybienie per obszar, w którym brak właściciela bezpośrednio doprowadził do incydentu z 29 grudnia. Następnie powtórz macierz dla własnej organizacji, wpisując imiona i nazwiska. **LEGENDA:** R – wykonuje, A – odpowiada i rozlicza, C – konsultowany, I – informowany.

TEST POPRAWNOŚCI: każdy wiersz ma dokładnie jedno „A”, przypisane osobie, nie działowi. Wiersz bez „A” to luka, którą wykorzystał napastnik.

Ćwiczenie 2 – macierz RACI dla NOVENERGII

MODUŁ 2

12 minut pracy + 5 minut omówienia. Szablon: macierz RACI dla 10 obszarów art. 8. Punkt wyjścia: karta scenariusza.

Obszar art. 8 UoKSC	Zarząd	CISO	IT / OT	Compliance	HR / Legal	Stan w NOVENERGII przed atakiem
1. Polityki i szacowanie ryzyka	A	R	C	C	I	Polityka z 2019 r., brak analizy ryzyka
2. Nabywanie i rozwój systemów	I	A	R	C	C	Brak wymagań bezpieczeństwa w zakupach
3. Bezpieczeństwo fizyczne	I	A	R	I	C	Wdrożone – kontrola dostępu na farmach
4. Zasoby ludzkie	A	C	I	C	R	Szkolenia tylko dla nowych pracowników
5. Łańcuch dostaw ICT	A	R	C	C	R	Brak rejestru dostawców i klauzul
6. Tożsamość i dostęp	I	A	R	C	C	Brak MFA, konta serwisowe integratora bezterminowe
7. Kryptografia	I	A	R	I	I	Częściowo – TLS na portalu klienta
8. Monitorowanie i reagowanie	I	A	R	C	I	Monitoring 8x5, brak obsługi alertów nocą
9. Ciągłość działania	A	C	R	C	I	Plan istnieje, ostatni test w 2023 r.
10. Zarządzanie incydentami	A	R	R	C	I	Procedura na papierze, nigdy nieprzećwiczona

Zadanie: wpisz w kolumny konkretne role z NOVENERGII, a następnie wskaż jeden obszar, w którym brak właściciela bezpośrednio doprowadził do incydentu z 29 grudnia. Na koniec powtórz macierz dla własnej organizacji, wpisując imiona i nazwiska. · LEGENDA: R – wykonuje, A – odpowiada i rozlicza, C – konsultowany, I – informowany. · TEST POPRAWNOŚCI: każdy wiersz ma dokładnie jedno „A”, przypisane osobie, nie działowi. Wiersz bez „A” to luka, którą wykorzystał napastnik.

Moduł 2 — podsumowanie

MODUŁ 2

Obowiązki, odpowiedzialność, nadzór

Punktem odniesienia jest katalog 10 obszarów środków bezpieczeństwa z art. 8 UoKSC / art. 21 NIS2

Ten sam katalog wykorzystamy jako listę kontrolną analizy luk w Module 3 i jako zakres audytu w Module 5.

Kierownik podmiotu odpowiada osobiście – do 300 % miesięcznego wynagrodzenia

Powierzenie obowiązków innej osobie nie zwalnia z odpowiedzialności za wynik. Kara osobista i kara dla podmiotu są niezależne.

Kary dla podmiotu: 10 mln EUR lub 2 % (PK) i 7 mln EUR lub 1,4 % (PW), z minimami 20 000 i 15 000 zł

Okres ochronny do 3.04.2028 odracza nakładanie kar, ale nie odracza obowiązków – kara może objąć cały okres niedostosowania.

Dwa obowiązki poza IT: roczne szkolenie kierownictwa (art. 8e) i weryfikacja niekaralności (art. 8f)

Oba należą do zarządu i HR. To najczęstsza luka organizacyjna – obowiązek bez właściciela.

Podmiot kluczowy podlega nadzorowi ex-ante, podmiot ważny ex-post – zakres obowiązków jest ten sam

Różnica dotyczy momentu i trybu kontroli oraz obowiązku audytu, nie katalogu wymagań.

Przechodzimy dalej: w module 3 budujemy fundament: SZBI, mapowanie na ISO 27001, analizę ryzyka i analizę luk.

SZBI, ISO 27001, ryzyko i analiza luk

12:00 – 13:30 · 2 godz. dyd.

- ✓ SZBI jako system procesowy – czym jest, czym nie jest i ile trwa jego wdrożenie
- ✓ Cykl PDCA jako mechanizm zapewniający wymaganą przez ustawę systematyczność
- ✓ ISO/IEC 27001:2022 jako rama wdrożeniowa – klauzule 4–10 i 93 kontrole Załącznika A
- ✓ Tabela mapowania: 10 obszarów art. 8 UoKSC → konkretne kontrole ISO 27001:2022
- ✓ Dokumentacja SZBI – trzy poziomy, katalog dokumentów i zasady nadzoru nad nimi
- ✓ Analiza ryzyka w 6 krokach (Ćwiczenie 3) oraz metodyka analizy luk (Ćwiczenie 4)

Czym jest SZBI

- Zintegrowany system polityk, procedur, procesów i narzędzi zapewniający bezpieczeństwo informacji w organizacji
- Obowiązek wdrożenia wynika wprost z art. 8 ust. 1 UoKSC – to twardy wymóg prawny, nie zalecenie dobrej praktyki
- Musi obejmować bezpieczeństwo informacji w szerokim rozumieniu, a w podmiotach z infrastrukturą przemysłową- także środowiska OT

Czym SZBI nie jest

- Zestawem dokumentów kupionym od doradcy i odłożonym na półkę
- Systemem informatycznym ani narzędziem technologicznym
- Jednorazowym projektem z datą zakończenia
- Zadaniem wyłącznie działu IT

Kluczowe elementy SZBI wg art. 8

- Szacowanie ryzyka i zarządzanie ryzykiem – obowiązkowe i dokumentowane
- Środki techniczne i organizacyjne proporcjonalne do ryzyka
- Polityka bezpieczeństwa informacji i polityki tematyczne
- Procesy zarządzania incydentami, zmianą i ciągłością działania

Realny czas wdrożenia

- Od zera do operacyjnego SZBI: około 7–8 miesięcy dla organizacji średniej wielkości
- Termin pełnego wdrożenia to 3.04.2027 – licząc wstecz, projekt powinien ruszyć najpóźniej w połowie 2026 r.

Zasada kluczowa: posiadanie polityk nie oznacza zgodności. Realizacja procesów bez dokumentacji też nie oznacza zgodności. Wymagane są oba elementy jednocześnie.

Cykl PDCA – silnik systematyczności wymaganej przez ustawę

MODUŁ 3

Art. 8 wymaga, by SZBI był systematyczny. PDCA jest sprawdzonym mechanizmem zapewniającym tę systematyczność.

P

Plan – planuj

Definiowanie aktywów, szacowanie ryzyka, ustalenie polityk i celów bezpieczeństwa, kryteria akceptacji ryzyka, plan postępowania z ryzykiem.

D

Do – wykonaj

Wdrożenie polityk, procedur oraz środków technicznych i organizacyjnych; szkolenia i budowanie świadomości.

C

Check – sprawdź

Monitorowanie i pomiar, audyty wewnętrzne, analiza wskaźników, przegląd zarządzania.

A

Act – działaj

Działania korygujące i doskonalące na podstawie wyników monitorowania, audytów i wniosków po incydentach.

Co to znaczy w praktyce

- ISO/IEC 27001:2022 nie narzuca PDCA wprost, ale struktura klauzul 4–10 i wymóg ciągłego doskonalenia (kl. 10.2) odzwierciedlają ten cykl
- Cykl nie kończy się nigdy – po fazie Act wracamy do Plan z wnioskami z poprzedniej iteracji

Minimalny roczny rytm SZBI

- Przegląd i aktualizacja analizy ryzyka – raz w roku, po incydencie / istotnych zmianach
- Audyt wewnętrzny – raz w roku
- Przegląd zarządzania – raz w roku, protokołowany
- Test planu ciągłości działania – raz w roku
- Szkolenie kierownictwa i pracowników – raz w roku

ISO/IEC 27001:2022 jako rama wdrożeniowa

MODUŁ 3

Norma nie jest obowiązkowa, ale daje gotową strukturę, listy kontrolne i uznaną metodykę.

Wymagania normy

- Zakres normy
- Powołanie normatywne
- Terminy i Definicje

Załącznik A – 93 kontrole w 4 tematach

- Kontrole organizacyjne – 37
- Kontrole dotyczące osób – 8
- Kontrole fizyczne – 14
- Kontrole technologiczne – 34

Klauzule 4–10 – wymagania systemu zarządzania

- Klauzula 4 – Kontekst organizacji: analiza otoczenia, potrzeby stron zainteresowanych, zakres SZBI
- Klauzula 5 – Przywództwo: zaangażowanie kierownictwa, polityka, role i odpowiedzialności
- Klauzula 6 – Planowanie: szacowanie i postępowanie z ryzykiem, cele bezpieczeństwa, Deklaracja Stosowania
- Klauzula 7 – Wsparcie: zasoby, kompetencje, świadomość, komunikacja, udokumentowana informacja
- Klauzula 8 – Działania operacyjne: realizacja planów, przeprowadzanie ocen ryzyka
- Klauzula 9 – Ocena efektów: monitorowanie i pomiar, audyt wewnętrzny, przegląd zarządzania
- Klauzula 10 – Doskonalenie: niezgodności, działania korygujące, ciągłe doskonalenie

Normy wspierające

- ISO 31000 – zarządzanie ryzykiem (rama ogólna)
- ISO/IEC 27005 – ryzyko w bezpieczeństwie informacji
- ISO 22301 – ciągłość działania
- ISA/IEC 62443 – bezpieczeństwo systemów przemysłowych (OT/ICS)
- NIST SP 800-30 – metodyka operacyjna oceny ryzyka

Mapowanie: 10 obszarów art. 8 UoKSC → kontrole ISO 27001:2022

MODUŁ 3

To zestawienie zastępuje dotychczasowe szacunkowe „około 90 % pokrycia” konkretnym przyporządkowaniem.

Obszar art. 8 UoKSC / art. 21 NIS2	Kontrole i klauzule ISO/IEC 27001:2022	Dowód wdrożenia
1. Polityki i szacowanie ryzyka	Kl. 6.1; Annex A 5.1, 5.2, 5.3, 8.2	Polityka BI, metodyka, rejestr ryzyk
2. Nabywanie, rozwój i utrzymanie systemów	Annex A 8.25 – 8.32	Procedura SDLC, raporty z testów
3. Bezpieczeństwo fizyczne i środowiskowe	Annex A 7.1 – 7.14	Polityka ochrony infrastruktury, rejestr wejść
4. Bezpieczeństwo zasobów ludzkich	Annex A 6.1 – 6.8	Rejestr szkoleń, procedura on/offboardingu
5. Łańcuch dostaw ICT	Annex A 5.19 – 5.22	Rejestr dostawców, klauzule umowne, ankiety
6. Zarządzanie tożsamością i dostępem	Annex A 5.15 – 5.18, 8.2 – 8.5	Rejestr uprawnień, dowody przeglądów, konfiguracja MFA
7. Kryptografia i szyfrowanie	Annex A 8.24	Polityka kryptograficzna, rejestr certyfikatów
8. Monitorowanie i reagowanie	Annex A 8.15 – 8.17	Konfiguracja SIEM, rejestr alertów, SLA reakcji
9. Ciągłość działania i odtwarzanie	Annex A 5.29 – 5.30; ISO 22301	BCP/DRP, raporty z testów odtworzeniowych
10. Zarządzanie incydentami	Annex A 5.24 – 5.28	Procedura incydentowa, rejestr incydentów, lessons learned

Gdzie UoKSC wykracza poza ISO 27001

MODUŁ 3

Certyfikat ISO 27001 nie oznacza automatycznie zgodności z ustawą.

Obszar	ISO/IEC 27001:2022	UoKSC / NIS2
Charakter wymagania	Dobrowolna certyfikacja, zakres definiuje organizacja	Obowiązek ustawowy o zakresie wyznaczonym przez usługę kluczową
Zgłaszanie incydentów	Wymaga procesu obsługi incydentów, nie narzuca adresata ani terminu	Zgłoszenie do właściwego CSIRT w terminach 24 h / 72 h / 1 miesiąc
Odpowiedzialność kierownictwa	Wymaga zaangażowania kierownictwa (kl. 5)	Osobista odpowiedzialność finansowa kierownika (art. 73a)
Szkolenia kierownictwa	Wymaga kompetencji i świadomości (kl. 7)	Obowiązek udziału kierownika w szkoleniu min. raz w roku (art. 8e)
Weryfikacja personelu	Kontrola A 6.1 – weryfikacja przed zatrudnieniem	Wymóg niekaralności osób realizujących zadania z art. 8 i 11 (art. 8f)
Audyt	Audyt wewnętrzny i certyfikacyjny wg cyklu jednostki	Audyt bezpieczeństwa z art. 15 – dla PK co najmniej co 3 lata
Rejestracja	Brak	Wpis do wykazu PK/PW w systemie S46 i utrzymanie aktualności danych

Wniosek praktyczny: organizacja z certyfikatem ISO 27001 ma pokryte znaczną część wymagań i powinna wykorzystać istniejący SZBI jako bazę – ale musi osobno zaadresować rejestrację, terminy zgłoszeń, obowiązki kierownictwa oraz audyt ustawowy.

Dokumentacja SZBI – trzy poziomy

MODUŁ 3

Art. 10 ust. 1 UoKSC: podmiot opracowuje, stosuje i aktualizuje dokumentację dotyczącą bezpieczeństwa systemu informacyjnego.

Poziom 1 – strategiczny

- Polityka Bezpieczeństwa Informacji – zatwierdzona przez zarząd
- Kontekst organizacji i strony zainteresowane
- Zakres SZBI
- Cele bezpieczeństwa informacji
- Deklaracja Stosowania (SoA)
- Polityka podziału ról i odpowiedzialności

Poziom 2 – procedury

- Procedura zarządzania ryzykiem + rejestr ryzyk
- Procedura zarządzania incydentami
- Procedura zarządzania użytkownikami i dostępem
- Procedura zarządzania zmianą i podatnościami
- Procedura kopii zapasowych i odtwarzania
- Procedura bezpieczeństwa u dostawców
- Procedura audytu wewnętrznego i przeglądu zarządzania
- Procedura nadzoru nad dokumentacją

Poziom 3 – instrukcje i zapisy

- Instrukcje konfiguracji systemów i harmonogramy przeglądów
- Inwentaryzacja aktywów i dokumentacja systemu informacyjnego
- Rejestry: incydentów, uprawnień, szkoleń, dostawców
- Raporty z audytów i działania korygujące
- Protokoły przeglądu zarządzania
- Raporty z testów odtworzeniowych i testów BCP

Zasady nadzoru nad dokumentacją: dokumentacja musi być identyfikowalna, aktualna i dostępna dla organu nadzoru (art. 10 ust. 1 UoKSC). Każdy dokument ma właściciela, wersję, datę zatwierdzenia, zdefiniowaną częstotliwość przeglądu i zasadę retencji. Dokument bez daty przeglądu i bez śladu dystrybucji jest dla audytora dokumentem nieistniejącym – niezależnie od jakości jego treści.

Analiza ryzyka – twardy obowiązek prawny

MODUŁ 3

Ustawa wskazuje kolejność: najpierw ryzyko, potem zabezpieczenia (spis aktywów)

Systematyczne szacowanie ryzyka jest obowiązkiem z art. 8 ust. 1 pkt 1 UoKSC. To wyniki analizy ryzyka mają determinować dobór środków, a nie odwrotnie.

Analiza musi być udokumentowana, metodyczna i aktualizowana

Minimum raz w roku, a ponadto po istotnych zmianach organizacyjnych lub technologicznych oraz po każdym poważnym incydencie.

Zarządzanie ryzykiem i wdrażanie zabezpieczeń to dwa osobne procesy

Najpierw identyfikujesz i oceniasz ryzyko, dopiero potem dobierasz środki. Zakup narzędzia nie jest postępowaniem z ryzykiem.

Wynik musi być powtarzalny i możliwy do uzasadnienia

Inny analityk stosujący tę samą metodę powinien uzyskać porównywalny wynik. Ryzyko, którego nie potrafisz odtworzyć i uzasadnić, nie ma wartości ani zarządczej, ani zgodnościowej.

Uznane metodyki

- ISO/IEC 27005 – zarządzanie ryzykiem w bezpieczeństwie informacji
- ISO 31000 – rama ogólna zarządzania ryzykiem
- NIST SP 800-30 – metodyka operacyjna
- ENISA Risk Management Framework

Najczęstszy błąd rynkowy

- Analizy generowane automatycznie przez narzędzie, które nie pokazuje metody oceny
- Skutek: jeżeli nie da się uzasadnić wyniku ani go odtworzyć – to jest ustalenie audytowe

Co sprawdza organ: czy rejestr ryzyk istnieje, jaką metodą powstał, kiedy był ostatnio aktualizowany i czy ryzyka akceptowane zostały zatwierdzone przez zarząd.

Analiza ryzyka w 6 krokach – co powstaje na każdym etapie

MODUŁ 3

Metodyka zgodna z ISO/IEC 27005 i NIST SP 800-30. Wzór podstawowy: $R = P \times S$.

1

Kontekst i zakres

Określ systemy, procesy i usługi objęte analizą; zdefiniuj kontekst regulacyjny i sektorowy; ustal kryteria akceptacji ryzyka.

Artefakt: dokument zakresu SZBI z kryteriami ryzyka zatwierdzonymi przez zarząd

2

Inwentaryzacja aktywów

Zidentyfikuj i wyceń aktywa: systemy, dane, procesy, ludzi, dostawców. Określ wartość poufności, integralności i dostępności.

Artefakt: rejestr aktywów z wycenionymi atrybutami CIA

3

Identyfikacja zagrożeń i podatności

Dla każdego aktywa: co może się stać i skąd. Wykorzystaj katalog zagrożeń ENISA, bazę CVE i dane z monitoringu.

Artefakt: tabela aktywa $\times$ zagrożenia oraz lista podatności z przyczyną źródłową

4

Ocena ryzyka wg metodyki

Oceń prawdopodobieństwo i skutek dla każdej pary aktywo–zagrożenie, oblicz poziom ryzyka i porównaj z progami z kroku 1.

Artefakt: rejestr ryzyk z poziomami akceptowalne / nieakceptowalne

5

Postępowanie z ryzykiem

Cztery opcje: modyfikacja (redukcja), akceptacja, unikanie, dzielenie lub transfer. Każde ryzyko dostaje właściciela i termin.

Artefakt: plan postępowania z ryzykiem (RTP) + Deklaracja Stosowania

6

Zatwierdzenie i monitorowanie

Zarząd zatwierdza ryzyka akceptowane. Ustal wskaźniki ryzyka (KRI) i zaplanuj termin kolejnego przeglądu.

Artefakt: protokół zarządu, zestaw KRI, data kolejnego przeglądu

Ćwiczenie 3 – rejestr ryzyk dla NOVENERGII

MODUŁ 3

15 minut pracy + 5 minut omówienia. Szablon: arkusz analizy ryzyka cybernetycznego. Dane wejściowe: karta scenariusza.

Aktywo	Zagrożenie	Podatność	P	S	R	Postępowanie	Właściciel / termin
Urządzenie brzegowe dostępu serwisowego	Wykorzystanie publicznie znanej podatności	Firmware z 2023 r., brak procesu aktualizacji	5	5	25	Modyfikacja: SLA patchowania, skanowanie co miesiąc	IT / 14 dni
Sieć sterowania OT (SCADA, sterowniki GPO)	Ruch poprzeczny z sieci biurowej do OT	Brak zapory segmentacyjnej między IT a OT	4	5	20	Modyfikacja: segmentacja i strefa pośrednia	IT/OT / 60 dni
Konta serwisowe integratora	Przejęcie konta o wysokich uprawnieniach	Hasła fabryczne, konta bezterminowe, brak MFA	4	5	20	Modyfikacja: MFA, dostęp na żądanie, rotacja haseł	IT / 30 dni
Kopie zapasowe na serwerze NAS	Zaszyfrowanie lub usunięcie kopii przez napastnika	Kopia w tej samej domenie, brak kopii offline	4	5	20	Modyfikacja: kopia offline, test odtworzenia co kwartał	IT / 45 dni
Zdolność wykrycia incydentu	Długotrwała obecność napastnika bez wykrycia	Monitoring 8x5, brak obsługi alertów nocą i w weekend	5	4	20	Modyfikacja: monitoring 24/7 własny lub zlecony	Zarząd / 90 dni

Twoje zadanie

- Uzupełnij szósty wiersz o ryzyko, którego w tabeli brakuje, a które wynika z karty scenariusza
- Zweryfikuj oceny P i S – czy zgadzasz się z wartościami wpisanymi przez prowadzącego?
- Wskaż, które ryzyka wymagają decyzji zarządu, a które może zamknąć sam zespół IT
- Przenieś strukturę na własną organizację: pięć aktywów krytycznych dla Twojej usługi

Kryteria akceptacji – przykład do adaptacji

- R = 1–6: ryzyko akceptowalne, monitorowanie
- R = 8–12: plan postępowania w ciągu 6 miesięcy
- R = 15–25: działanie natychmiastowe i decyzja zarządu
- Progi ustala i zatwierdza zarząd – nie kopiuj ich bezrefleksyjnie
- Wszystkie pięć ryzyk z tabeli mieści się w przedziale 20–25: w NOVENERGII żadne z nich nie zostało zaadresowane przed grudniem 2025 r.

Ćwiczenie 3 – rejestr ryzyk dla NOVENERGII

MODUŁ 3

Aktywo	Zagrożenie	Podatność	P	S	R	Postępowanie	Właściciel / termin
Urządzenie brzegowe dostępu serwisowego	Wykorzystanie publicznie znanej podatności	Firmware z 2023 r., brak procesu aktualizacji	5	5	25	Modyfikacja: SLA patchowania, skanowanie co miesiąc	IT / 14 dni
Sieć sterowania OT (SCADA, sterowniki GPO)	Ruch poprzeczny z sieci biurowej do OT	Brak zapory segmentacyjnej między IT a OT	4	5	20	Modyfikacja: segmentacja i strefa pośrednia	IT/OT / 60 dni
Konta serwisowe integratora	Przejęcie konta o wysokich uprawnieniach	Hasła fabryczne, konta bezterminowe, brak MFA	4	5	20	Modyfikacja: MFA, dostęp na żądanie, rotacja haseł	IT / 30 dni
Kopie zapasowe na serwerze NAS	Zaszyfrowanie lub usunięcie kopii przez napastnika	Kopia w tej samej domenie, brak kopii offline	4	5	20	Modyfikacja: kopia offline, test odtworzenia co kwartał	IT / 45 dni
Zdolność wykrycia incydentu	Długotrwała obecność napastnika bez wykrycia	Monitoring 8x5, brak obsługi alertów nocą i w weekend	5	4	20	Modyfikacja: monitoring 24/7 własny lub zlecony	Zarząd / 90 dni
Serwer SCADA i domena AD	Ruch poprzeczny z sieci biurowej do OT	Serwer SCADA w tej samej domenie co sieć biurowa, brak segmentacji	4	5	20	Modyfikacja: Segmentacja IT–OT ze strefą pośrednią, odrębna domena lub odrębne konta dla OT.	IT / 30 dni
Status regulacyjny podmiotu	Kara administracyjna i osobista odpowiedzialność kierownika	Brak wpisu do wykazu, brak analizy ryzyka, brak SZBI	5	4	20	Ustalenie statusu, wpis do wykazu, uruchomienie SZBI. To jest ryzyko, o które pyta pytanie kontrolne (a) — nietechniczne, a mieszczące się w progu nieakceptowalnym.	IT (CISO) / 14 dni

Twoje zadanie

- Ryzyko nietechniczne: Status regulacyjny podmiotu — brak wpisu do wykazu i brak SZBI. To ryzyko prawne i finansowe, nie techniczne. Większość uczestników go nie zapisuje, bo rejestr ryzyk kojarzy się z infrastrukturą. Warto pokazać, że art. 8 wymaga zarządzania ryzykiem, a nie zarządzania ryzykiem technicznym.
- Decyzji zarządu wymagają: monitoring 24/7 (wydatek operacyjny), segmentacja IT–OT (projekt inwestycyjny), aneks do umowy z integratorem (relacja handlowa) oraz akceptacja ryzyk pozostających. Zespół IT może samodzielnie zamknąć: zmianę haseł domyślnych, włączenie weryfikacji podpisu firmware, unikalne hasła na HMI i kopię offline.
- Jako pierwsze zmaterializowało się ryzyko dotyczące kont serwisowych integratora — logowanie 8 grudnia o 21:14. Ryzyko dotyczące zdolności wykrycia zmaterializowało się przez cały czas: od 20 listopada (skanowanie) do 29 grudnia.

Analiza luk (gap analysis) – metodyka krok po kroku

MODUŁ 3

Punkt startowy każdego wdrożenia: nie da się zaplanować drogi bez ustalenia punktu wyjścia.

1

Ustal wymagania źródłowe

Katalog 10 obszarów art. 8 UoKSC, rozbity na pojedyncze, sprawdzalne wymagania. W razie potrzeby uzupełnij o wymagania sektorowe i kontraktowe.

2

Zbuduj listę kontrolną

Każde wymaganie w osobnym wierszu: identyfikator, opis kontrolny, podstawa prawna, wymagany dowód, priorytet.

3

Oceń stan obecny na dowodach, nie na deklaracjach

Trzy statusy: spełnione / częściowo spełnione / niespełnione. Status „spełnione” wymaga wskazania konkretnego dokumentu lub zapisu.

4

Wyceń lukę

Dla każdego braku określ nakład (roboczo), koszt zewnętrzny, zależności od innych działań i czas realizacji.

5

Priorytetyzuj

Kryteria: wpływ na usługę kluczową, ryzyko kary, termin ustawowy, szybkość uzyskania efektu. Wyłóż zestaw działań o wysokim wpływie i krótkim czasie realizacji.

6

Przełóż na plan działań

Każda luka staje się zadaniem z właścicielem, terminem i zdefiniowanym produktem końcowym. To wejście do mapy drogowej z Modułu 5.

Najczęstszy błąd: ocena stanu obecnego na podstawie deklaracji zamiast dowodów. Jeżeli przy wymaganiu nie umiesz wskazać nazwy pliku, numeru rejestru albo daty zapisu, status brzmi „niespełnione” – niezależnie od tego, jak dobrze proces działa nieformalnie.

Ćwiczenie 4 – analiza luk dla stanu NOVENERGII na 1.12.2025

MODUŁ 3

15 minut pracy + 5 minut omówienia. Szablon: checklista audytowa NIS2 / UoKSC dla PK i PW.

ID	Wymaganie kontrolne	Podstawa prawna	Status	Wymagany dowód	Priorytet
A.1	Podmiot ustalił swój status i udokumentował wynik	art. 5, 7 UoKSC	niespełnione	Notatka z akceptacją zarządu	KRYTYCZNY
A.2	Złożono wniosek o wpis do wykazu w systemie S46	art. 7 ust. 2 UoKSC	niespełnione	Potwierdzenie PDF, numer sprawy	KRYTYCZNY
B.1	Wyznaczono osobę odpowiedzialną za cyberbezpieczeństwo	art. 14 UoKSC	częściowo	Zarządzenie, zakres obowiązków	KRYTYCZNY
C.1	Wdrożono udokumentowany proces szacowania ryzyka	art. 8 ust. 1 pkt 1	niespełnione	Metodyka i rejestr ryzyk z datą	KRYTYCZNY
C.2	Polityka bezpieczeństwa informacji jest aktualna	art. 8, art. 10 ust. 1	niespełnione	Polityka z datą przeglądu i zatwierdzenia	WYSOKI
D.1	MFA dla dostępu zdalnego i kont uprzywilejowanych	art. 8 – obszar 6	niespełnione	Konfiguracja, lista wyjątków	KRYTYCZNY
D.2	Konta dostawców mają ograniczony czas i zakres dostępu	art. 8 – obszary 5 i 6	niespełnione	Rejestr kont serwisowych, dowody przeglądu	KRYTYCZNY
E.1	System objęty monitorowaniem w trybie ciągłym	art. 8 – obszar 8	niespełnione	Umowa SOC lub konfiguracja SIEM, SLA reakcji	KRYTYCZNY
F.1	Przeprowadzono test odtworzenia z kopii zapasowej	art. 8 – obszar 9	niespełnione	Raport z testu z datą i wynikiem	WYSOKI
G.1	Sieć OT oddzielona od sieci biurowej	art. 8 – obszary 2 i 8	niespełnione	Schemat sieci, reguły zapory, raport z testu	KRYTYCZNY

Zadanie: wybierz z tej listy 5 luk, które zamknąłbyś w pierwszej kolejności, i uzasadnij wybór jednym zdaniem na każdą. Następnie oszacuj dla nich nakład w roboczodniach. Te pięć pozycji przeniesiesz do planu na 90 dni w Ćwiczeniu 6 – a potem powtórzysz całą checklistę dla własnej organizacji.

Moduł 3 — podsumowanie

MODUŁ 3

SZBI, ISO 27001, ryzyko i analiza luk

SZBI to system procesowy, a nie zestaw dokumentów – wymagane są jednocześnie dokumentacja i operacyjność

Realny czas wdrożenia od zera: około 7–8 miesięcy. Termin ustawowy pełnego wdrożenia to 3 kwietnia 2027 r.

ISO/IEC 27001:2022 jest najlepszą dostępną ramą wdrożeniową, ale nie zastępuje ustawy

Mapowanie 10 obszarów art. 8 na kontrole Załącznika A daje gotową listę zadań; rejestracja, terminy zgłoszeń, obowiązki kierownictwa i audyt z art. 15 wymagają osobnego zaadresowania.

Analiza ryzyka jest obowiązkiem prawnym i musi być powtarzalna, uzasadnialna i aktualizowana

Sześć kroków, sześć artefaktów. Rejestr ryzyk starszy niż 12 miesięcy to gotowe ustalenie audytowe.

Dokumentacja SZBI ma trzy poziomy i każdy dokument musi mieć właściciela, wersję i datę przeglądu

Dokument bez śladu przeglądu i dystrybucji jest dla audytora dokumentem nieistniejącym.

Analiza luk jest punktem wyjścia całego wdrożenia i musi opierać się na dowodach, nie na deklaracjach

Twoje pięć luk krytycznych z Ćwiczenia 4 wraca w planie na 90 dni na końcu dnia.

Przechodzimy dalej: w module 4 schodzimy na poziom techniczny i operacyjny: konkretne zabezpieczenia oraz obsługa i zgłaszanie incydentów.

Środki techniczne, incydenty i CSIRT

14:15 – 15:30 · 1,5 godz. dyd.

- ✓ Konkretnie środki techniczne wymagane przez art. 8: MFA, szyfrowanie, IAM i PAM, logowanie
- ✓ Segmentacja sieci, model Purdue i specyfika środowisk OT / ICS
- ✓ Obowiązek monitorowania w trybie ciągłym oraz modele wdrożenia SOC dla PK i PW
- ✓ Zarządzanie podatnościami, SLA patchowania i przyjmowanie zgłoszeń podatności (CVD)
- ✓ Klasyfikacja incydentu poważnego według rozporządzenia wykonawczego KE 2024/2690
- ✓ Terminy zgłoszeń 24 h / 72 h / 1 miesiąc, właściwość CSIRT i symulacja (Ćwiczenie 5)

Środki techniczne wymagane przez art. 8 – minimalny standard

MODUŁ 4

MFA – uwierzytelnianie wieloskładnikowe

- Obowiązkowe dla dostępu zdalnego, systemów krytycznych i kont administracyjnych
- MFA jest minimalnym standardem – pytanie nie brzmi „czy”, lecz „kiedy i dla których systemów”
- Preferuj FIDO2 lub TOTP zamiast kodów SMS

Szyfrowanie

- Dane w spoczynku: szyfrowanie dysków i baz z danymi wrażliwymi
- Dane w transmisji: TLS 1.2 lub wyższy dla wszystkich połączeń, VPN dla dostępu zdalnego
- Polityka kryptograficzna i zarządzanie kluczami oraz certyfikatami

Zarządzanie dostępem (IAM / PAM)

- Zasada minimalnych uprawnień
- Przeglądy uprawnień co kwartał i po każdej zmianie kadrowej
- Dostęp uprzywilejowany przez PAM: nagrywanie sesji, dostęp na żądanie, rotacja haseł

Logowanie i retencja

- Centralne zbieranie zdarzeń bezpieczeństwa ze wszystkich systemów krytycznych
- Rekomendowana retencja logów: 12 miesięcy, w formie uniemożliwiającej modyfikację
- Synchronizacja czasu we wszystkich systemach – bez niej korelacja zdarzeń jest bezwartościowa

Filozofia Zero Trust

- Nigdy nie ufaj, zawsze weryfikuj – lokalizacja w sieci nie jest podstawą zaufania
- Weryfikuj tożsamość, stan urządzenia i kontekst przy każdym dostępie
- Mikrosegmentacja zamiast płaskiej sieci wewnętrznej
- Zakładaj naruszenie i ograniczaj promień rażenia

Kolejność wdrażania: MFA i przeglądy uprawnień dają największy efekt przy najmniejszym nakładzie. Zacznij od nich, zanim zainwestujesz w zaawansowane narzędzia detekcji.

Segmentacja sieci i specyfika środowisk OT / ICS

MODUŁ 4

Brak segmentacji był głównym mechanizmem rozprzestrzenienia się ataku z grudnia 2025.

Obszar	IT (systemy biurowe)	OT / ICS (sterowanie)
Priorytet triady	Poufność → Integralność → Dostępność	Dostępność → Integralność → Poufność
Cykl życia urządzeń	3–5 lat	15–25 lat, często bez wsparcia producenta
Okno aktualizacji	Praktycznie w każdej chwili	Wyłącznie w zaplanowanym postoju, po akceptacji producenta
Skutek awarii	Utrata danych, przestój usługi	Ryzyko fizyczne: uszkodzenie urządzeń, zagrożenie życia
Protokoły	TCP/IP, HTTPS – z natury zabezpieczone	Modbus, Profinet, DNP3 – bez wbudowanego uwierzytelniania
Dokumentacja	Zwykle aktualizowana	Często historyczna, rozproszona u integratorów

Model Purdue (ISA-95) – warstwy IT / OT

- L4/L5 – systemy biznesowe i ERP (sieć IT)
- L3.5 – strefa zdemilitaryzowana OT: serwer historii, reverse proxy, jump host
- L3 – systemy nadzoru produkcji (MES, historian)
- L2 – SCADA i stacje operatorskie (HMI)
- L1 – sterowniki PLC / RTU
- L0 – urządzenia obiektowe: czujniki, siłowniki

Zasada praktyczna

- Żadne połączenie z sieci IT nie sięga bezpośrednio poniżej warstwy L3.5 – ruch przechodzi przez strefę pośrednią z kontrolą i rejestracją sesji

Norma referencyjna dla OT: ISA/IEC 62443 – definiuje strefy i kanały, poziomy zabezpieczeń (SL) oraz wymagania wobec dostawców systemów przemysłowych. Uzupełnia ISO 27001 tam, gdzie norma ogólna nie sięga.

Obowiązek monitorowania w trybie ciągłym

MODUŁ 4

Co wynika z ustawy

- Art. 8 wymaga objęcia systemu informacyjnego wspierającego świadczenie usługi systemem monitorowania w trybie ciągłym
- Tryb ciągły oznacza 24 godziny na dobę, 7 dni w tygodniu – nie 8 godzin w dni robocze
- Wczesne ostrzeżenie należy przekazać w ciągu 24 godzin od uzyskania wiedzy o incydencie – bez monitorowania ciągłego ten termin jest niewykonalny
- Alerty muszą być obsługiwane, a nie tylko generowane

Minimalny zestaw i realne kryteria

- Minimum narzędziowe: korelacja logów (SIEM) plus detekcja na stacjach i serwerach (EDR)
- Rozwiązania otwarte nie wykluczają zgodności – liczy się skuteczne działanie i obsługa alertów
- Zdefiniuj SLA reakcji: kto i w jakim czasie reaguje na alert krytyczny (np. maksymalnie 15 minut dla P1)
- Outsourcing monitoringu nie przenosi odpowiedzialności – ta pozostaje przy podmiocie

SIEM Korelacja zdarzeń

Centralne zbieranie i korelacja logów z całej infrastruktury; wykrywanie wzorców ataków. Podstawa monitorowania.

EDR Stacje i serwery

Wykrywanie i reagowanie na poziomie punktu końcowego: złośliwe oprogramowanie, anomalie zachowania procesów.

NDR Ruch sieciowy

Analiza ruchu w poszukiwaniu anomalii; wykrywanie ruchu poprzecznego wewnątrz sieci.

XDR Integracja warstw

Połączenie SIEM, EDR i NDR w jednym ekosystemie; korelacja z wielu źródeł i redukcja fałszywych alarmów.

Nawiązanie do przypadku: w incydencie z grudnia 2025 napastnicy działali w systemach wiele dni. Logi w większości powstawały – nikt ich nie analizował. To jest różnica między posiadaniem narzędzia a posiadaniem monitoringu.

SOC – trzy modele wdrożenia dla podmiotów kluczowych i ważnych

MODUŁ 4

MODEL 1

SOC własny (in-house)

Dla dużych podmiotów kluczowych z własnymi zasobami

Zalety: pełna kontrola i znajomość specyfiki organizacji

Wyzwania: koszt, rotacja kadr, trudność z realnym pokryciem 24/7
(min. 10–15 analityków)

MODEL 2

SOC zlecony (MSSP / MDR)

Optimalny kosztowo dla większości podmiotów kluczowych i ważnych

Zalety: pokrycie 24/7 od pierwszego dnia, ekspertyza, skalowalność

Wyzwania: zależność od dostawcy, transfer danych i wymogi RODO

MODEL 3

Model hybrydowy

Własny CISO i zespół bezpieczeństwa plus zlecony monitoring 24/7

Najczęstszy w praktyce dla podmiotów średniej wielkości

Kontrola nad decyzjami pozostaje wewnątrz, ciągłość zapewnia dostawca

Sześć pytań, które zadajesz dostawcy SOC – zanim podpiszesz umowę

- Jak posiada certyfikaty (ISO 27001, SOC 2) i czy udostępni raport z audytu? · Jaki jest gwarantowany czas reakcji na alert krytyczny (P1)? · Gdzie fizycznie przechowywane są logi – czy dane opuszczają Polskę lub UE?
- Czy mamy prawo wglądu we wszystkie logi i alerty oraz prawo do ich eksportu? · Czy SLA dostawcy umożliwia dotrzymanie naszego terminu zgłoszenia 24 h? · Jak wygląda plan wyjścia i przekazania danych po zakończeniu umowy?

Zasada nieprzenoszalna: zlecenie monitoringu na zewnątrz nie zwalnia podmiotu z odpowiedzialności za incydent ani z obowiązku jego zgłoszenia. Odpowiedzialność zostaje po Twojej stronie.

Zarządzanie podatnościami i SLA patchowania

MODUŁ 4

Obowiązek obsługi podatności oraz zbierania informacji o podatnościach i cyberzagrożeniach wynika wprost z art. 8.

1

Identyfikacja

Regularne, automatyczne skanowanie infrastruktury oraz śledzenie CVE dla używanych systemów i komponentów.

2

Ocena

Klasyfikacja według CVSS: krytyczna 9,0–10; wysoka 7,0–8,9; średnia 4,0–6,9; niska 0,1–3,9. Uwzględnij kontekst – czy system jest wystawiony na zewnątrz.

3

Usunięcie lub mitygacja

Aktualizacja, obejście techniczne albo świadoma akceptacja ryzyka – zawsze z uzasadnieniem i zapisem w rejestrze ryzyk.

4

Weryfikacja

Ponowne skanowanie po wdrożeniu poprawki i zamknięcie pozycji w rejestrze podatności.

SLA patchowania – wzorzec do adaptacji

- Krytyczne: 48–72 godziny
- Wysokie: 7–14 dni
- Średnie: 30 dni
- W OT: najbliższe okno serwisowe, po akceptacji producenta

Częstotliwość skanowania

- Infrastruktura krytyczna i systemy wystawione na zewnątrz: co tydzień lub maksymalnie co miesiąc
- Systemy wewnętrzne: minimum kwartalnie
- Każdorazowo po istotnej zmianie w środowisku / incydencie

Obowiązek często pomijany: podmiot musi zapewnić użytkownikom swojej usługi możliwość zgłaszania cyberzagrożeń i podatności. Oznacza to publicznie dostępny kanał kontaktu (adres e-mail lub formularz), procedurę potwierdzania zgłoszeń i zasady współpracy ze zgłaszającym.

TOP 10 podatności wykrywanych w audytach i testach

MODUŁ 4

Te same pozycje wracają w ustaleniach audytowych – dlatego warto zamknąć je zawczasu.

#	Podatność / ryzyko	Jak wykryć	Rekomendowane działanie
1	Słabe zarządzanie tożsamością i dostępem	Przegląd uprawnień, raport kont bez MFA	MFA wszędzie, PAM, minimalne uprawnienia, przeglądy kwartalne
2	Niezałatane podatności krytyczne (powyżej 30 dni)	Skaner podatności, porównanie z bazą CVE	SLA: krytyczne 48 h, wysokie 14 dni, średnie 30 dni
3	Brak segmentacji sieci / płaska sieć	Mapa sieci, analiza reguł zapory, test ruchu poprzecznego	Mikrosegmentacja, zaporę wewnętrzną, dostęp sieciowy Zero Trust
4	MFA wdrożone tylko częściowo	Lista systemów krytycznych bez MFA	FIDO2 lub TOTP dla wszystkich systemów krytycznych i VPN
5	Niepełne logi i brak analizy zdarzeń	Inwentaryzacja źródeł logów, sprawdzenie retencji, test alertu	SIEM ze wszystkich źródeł krytycznych, retencja 12 miesięcy
6	Podatności w łańcuchu dostaw	Rejestr dostawców, weryfikacja certyfikatów, ankiety	Ocena dostawców, klauzule umowne, monitorowanie
7	Błędna konfiguracja usług chmurowych	Audyt konfiguracji, testy zgodności z CIS Benchmarks	Ciągły nadzór konfiguracji, eliminacja zasobów publicznie dostępnych
8	Brak zarządzania dostępem uprzywilejowanym	Lista kont administracyjnych, sprawdzenie nagrywania sesji	PAM, dostęp na żądanie (JIT), rotacja haseł
9	Brak testów kopii zapasowych i niespójne BCP/DR	Data ostatniego testu, wynik odtworzenia, aktualność planu	Test odtworzenia co kwartał, kopia offline, ćwiczenie tabletop raz w roku
10	Brak aktualnej analizy ryzyka i Deklaracji Stosowania	Data ostatniej analizy, porównanie SoA ze stanem wdrożenia	Analiza ryzyka min. raz w roku, aktualizacja SoA po każdej zmianie

Incydent i incydent poważny – definicja i klasyfikacja

MODUŁ 4

Incydent w rozumieniu UoKSC

- Zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo sieci i systemów informacyjnych, wpływa na „CIA” – Poufność/Integralność/Dostępność /
- Nie każde zdarzenie jest incydem – proces zarządzania incydentami musi określać, jak odróżnić awarię techniczną od incydentu bezpieczeństwa

Incydent poważny / na dużą skalę – Definicje

Incydent poważny – incydem, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny, straty finansowe dla tego podmiotu lub wpływa na inne osoby fizyczne, osoby prawne, jednostki organizacyjne nieposiadające osobowości prawnej przez wywołanie poważnej szkody materialnej lub niematerialnej

Incydent w cyberbezpieczeństwie na dużą skalę – incydem, którego skutki przekraczają możliwości reagowania państwa lub który ma poważny wpływ na inne państwo członkowskie Unii Europejskiej

Kryteria z rozporządzenia wykonawczego KE (UE) 2024/2690

- Rozporządzenie określa progi ilościowe – zastępuje ocenę intuicyjną konkretnymi kryteriami
- Kryteria horyzontalne (art. 3): m.in. strata finansowa przekraczająca 500 000 EUR albo 5 % rocznego obrotu
- Wyciek tajemnicy przedsiębiorstwa
- Skutek śmiertelny lub znaczny uszczerbek na zdrowiu
- Złośliwy, nieuprawniony dostęp powodujący zakłócenia operacyjne
- Artykuły 4–14 zawierają kryteria szczegółowe dla poszczególnych rodzajów podmiotów: dostawców DNS, rejestrów TLD, usług chmurowych, centrów danych i CDN, platform handlowych, wyszukiwarek, usług zaufania oraz dostawców usług zarządzanych

Incydent poważny – wymaga zgłoszenia do CSIRT kiedy:

- Spowodował lub może spowodować poważne zakłócenie świadczenia usługi
- Dotknął lub może dotknąć innych podmiotów lub sektorów
- Naruszył lub może naruszyć poufność danych wrażliwych
- Spowodował śmierć lub znaczny uszczerbek na zdrowiu osoby fizycznej
- Spowodował straty finansowe przekraczające próg z rozporządzenia

W pakiecie materiałów: matryca kryteriów incydentu poważnego wg 2024/2690 z progami sektorowymi oraz gotowy rejestr incydentów. Uzupełnij ją o próg finansowy właściwy dla swojej organizacji zanim wystąpi pierwszy incydem.

Terminy: 24 h wczesne ostrzeżenie, 72 h zgłoszenie, 1 miesiąc sprawozdanie

MODUŁ 4

Zegar startuje od momentu uzyskania wiedzy o incydencie, a nie od momentu jego wystąpienia.

24 h

Wczesne ostrzeżenie

Cel: szybkie poinformowanie właściwego CSIRT o wystąpieniu poważnego incydentu

Forma: zgłoszenie przez system S46

Zawiera: czas wykrycia, wstępną klasyfikację, krótki opis zdarzenia, informację o podejrzeniu działania umyślnego

Zgłoszenie można później uzupełnić i skorygować

72 h

Zgłoszenie incydentu

Cel: pełna wstępna ocena incydentu

Zawiera: zakres, wpływ na świadczenie usługi, zasięg, podjęte działania, wstępną ocenę przyczyn

Klasyfikacja: poważny / krytyczny

Informacja o ewentualnych skutkach transgranicznych

1 mies.

Sprawozdanie końcowe

To sprawozdanie, a nie kolejne zgłoszenie incydentu

Cel: pełna analiza poincydentalna

Zawiera: opis incydentu, przyczyny źródłowe, chronologię, skutki, działania podjęte i planowane

Elementy określone w art. 12a UoKSC – sprawozdanie musi być kompletne

Brak wymaganych elementów stanowi podstawę kary

Dwa niezależne zegary, o których trzeba pamiętać jednocześnie

- Jeżeli incydent obejmuje dane osobowe, obok zgłoszenia do CSIRT (24 h) biegnie odrębny obowiązek zgłoszenia naruszenia do Prezesa UODO (72 h). To dwa różne obowiązki, dwa różne organy i dwa różne formularze – zaplanuj obsługę obu w jednej procedurze.

Właściwość CSIRT – gdzie zgłaszasz incydent

MODUŁ 4

Ustal swojego adresata zgłoszenia dziś, a nie w trakcie incydu.

CSIRT NASK

Sektor cywilny

Naukowa i Akademicka Sieć Komputerowa –
Państwowy Instytut Badawczy
Podmioty kluczowe i ważne sektora cywilnego,
przedsiębiorcy, obywatele, sektor akademicki
cert.pl · incydent.cert.pl

CSIRT GOV

Administracja i infrastruktura krytyczna

Agencja Bezpieczeństwa Wewnętrznego
Administracja rządowa, organy władzy
publicznej, infrastruktura krytyczna państwa
gov.pl/csirt-gov

CSIRT MON

Sektor obronny

Ministerstwo Obrony Narodowej
Podmioty systemu obronnego, wojskowa
infrastruktura teleinformatyczna, spółki obronne
mon.gov.pl

CSIRT-y sektorowe

Właściwość branżowa

Ustanawiane przez organy właściwe dla
sektorów, m.in. energetyki, finansów, zdrowia
Jeżeli w Twoim sektorze działa CSIRT sektorowy,
to on jest pierwszym adresatem zgłoszenia

CSIRT-y sektorowe

- CSIRT KNF – sektor finansowy : csirt.knf.gov.pl
- CSIRT PSE – sektor elektroenergetyczny : <https://cert.pse-online.pl/kontakt>
- CSIRT GAZ-SYSTEM – sektor gazowy : <https://www.gaz-system.pl/pl/o-nas/otoczenie-regulacyjne/systemy-zarzadzania/cert.html>
- CSIRT ORLEN / LOTOS – sektor paliwowy : <https://termika.orklen.pl/cyberbezpieczenstwo>
- CSIRT MED – sektor zdrowia : <https://cez.gov.pl/pl>
- CSIRT UZP / e-Zamówienia – zamówienia publiczne : <https://csirt.gov.pl/>
- CSIRT PWPW – dokumenty tożsamości / identyfikacja : <https://csirt.gov.pl/>

Do wpisania w procedurę incydentową jeszcze dziś

- Nazwa właściwego CSIRT i organu sektorowego · adres i kanał zgłoszenia · kto w organizacji jest uprawniony do wysłania zgłoszenia · kto go zastępuje poza godzinami pracy
- Numer telefonu alarmowego, gotowy szablon zgłoszenia 24 h oraz miejsce przechowywania dowodów (logi, zrzuty, chronologia działań)

Pełny proces zarządzania incydem – siedem kroków

MODUŁ 4

1

Wykrycie

Monitoring systemów, analiza logów, alerty bezpieczeństwa, zgłoszenia użytkowników i informacje od CSIRT lub dostawców.

2

Ocena i klasyfikacja

Czy to awaria, czy incydent bezpieczeństwa? Czy spełnia kryteria incydu powaźnego z rozporządzenia 2024/2690? Decyzja o uruchomieniu procedury.

3

Zawiadomienie

Wewnętrzne: kierownictwo, właściciel usługi, dział prawny, IOD. Zewnętrzne: właściwy CSIRT (24 h), organ sektorowy, UODO przy naruszeniu danych osobowych.

4

Reagowanie

Izolacja zaatakowanych systemów bez ich wyłączania, zabezpieczenie dowodów, ograniczenie skutków, przywrócenie świadczenia usługi.

5

Dokumentacja

Wpis do rejestru incydentów, chronologia działań z godzinami, podjęte decyzje i ich uzasadnienie, zabezpieczone dowody.

6

Analiza poincydentalna

Ustalenie przyczyny źródłowej, ocena skuteczności reakcji, wnioski. Podstawa sprawozdania końcowego do CSIRT w terminie miesiąca.

7

Działania doskonalące

Aktualizacja procedur, uzupełnienie zabezpieczeń, aktualizacja rejestru ryzyk, szkolenie zespołu. Zamknięcie pętli PDCA.

Najczęstsze błędy: logi zbierane, ale nieanalizowane · procedura nigdy nieprzećwiczona · brak rejestru incydentów · incydent obsługiwany bez zgłoszenia · brak wniosków.

Ćwiczenie 5 – pierwsze 24 godziny w NOVENERGII, tym razem prawidłowo

MODUŁ 4

Symulacja incydentu poważnego: pierwsze 24 godziny od uzyskania wiedzy o incydencie. 15 minut pracy + 5 minut omówienia.

Przebieg zdarzeń w NOVENERGII

- 08.12 – pulpit zdalny do HMI na koncie lokalnego administratora z hasłem od integratora
- 25.12 – skanowanie sieci i próby logowania na sterownikach GPO; nikt nie analizował logów
- 29.12, 07:40 – wiper na HMI, uszkodzenie firmware RTU, Moxa do ustawień fabrycznych
- 29.12, 08:05 – dyspozytor OSD dzwoni: brak telemetry z czterech farm
- 29.12, 08:20 – brak zdalnego sterowania; Fortigate przywrócony do ustawień fabrycznych
- Element ćwiczeniowy: zgłoszenie do CSIRT poszło dopiero 30.12 o 18:00 – po ok. 34 h

Twoje zadanie

- Odtwórz przebieg pierwszych 24 godzin tak, jak powinien wyglądać
- Wskaż moment, od którego liczy się termin 24 godzin, i uzasadnij wybór
- Rozstrzygnij, czy to incydent poważny – wskaż kryterium z rozporządzenia 2024/2690
- Wypełnij formularz wczesnego ostrzeżenia na podstawie danych z karty scenariusza
- Ustal, czy powstaje równoległy obowiązek zgłoszenia do Prezesa UODO
- Wskaż, które dowody trzeba zabezpieczyć, zanim znikną

A

08:05 – 08:35 Potwierdzenie i eskalacja

Dyżurny potwierdza, że utrata telemetry nie jest awarią łącza. Eskalacja do osoby odpowiedzialnej za cyberbezpieczeństwo i do zarządu. Decyzja o uruchomieniu procedury incydentu poważnego. Od tego momentu biegnie termin 24 godzin.

B

08:35 – 11:00 Izolacja i zabezpieczenie dowodów

Odcięcie zdalnego dostępu serwisowego na wszystkich obiektach, bez wyłączania urządzeń. Zabezpieczenie logów z Fortigate, HMI i sterowników, zanim zostaną nadpisane. Sprawdzenie pozostałych farm.

C

11:00 – 16:00 Wczesne ostrzeżenie i powiadomienia

Formularz wczesnego ostrzeżenia w S46 do CSIRT NASK: czas uzyskania wiedzy, wstępna klasyfikacja, opis, podejrzenie działania umyślnego, podjęte działania. Równoległe powiadomienie Prezesa URE i operatora sieci dystrybucyjnej.

D

16:00 – 08:05 dnia następnego - analiza i odtwarzanie

Analiza śladów i ustalenie zasięgu. Pisemne powiadomienie zarządu. Ocena obowiązku zgłoszenia do Prezesa UODO. Odtwarzanie: czysty firmware od producenta, rekonfiguracja urządzeń, komunikacja z OSD.

Moduł 4 — podsumowanie

MODUŁ 4

Środki techniczne, incydenty i CSIRT

Minimalny standard techniczny: MFA, szyfrowanie, PAM, centralne logowanie i segmentacja

Największy efekt przy najmniejszym nakładzie dają MFA i kwartalne przeglądy uprawnień. Od tego zaczynaj.

Monitorowanie musi być ciągłe – zbieranie logów bez ich analizy nie jest monitoringiem

Bez trybu 24/7 termin 24 godzin na wczesne ostrzeżenie jest niewykonalny. Zlecenie SOC na zewnątrz nie przenosi odpowiedzialności.

Podatnościami zarządzamy procesowo, z ustalonym SLA i publicznym kanałem przyjmowania zgłoszeń

Krytyczne 48–72 h, wysokie 7–14 dni, średnie 30 dni. Obowiązek udostępnienia kanału zgłaszania podatności jest często pomijany.

O tym, czy incydent jest poważny, rozstrzygają kryteria z rozporządzenia 2024/2690, a nie wyczucie

Kryteria horyzontalne z art. 3 oraz kryteria szczegółowe z art. 4–14 dla poszczególnych rodzajów podmiotów.

Terminy: 24 godziny na wczesne ostrzeżenie, 72 godziny na zgłoszenie, miesiąc na sprawozdanie końcowe

Zegar biegnie od uzyskania wiedzy o incydencie. Przy danych osobowych równolegle biegnie termin 72 godzin do UODO.

Przechodźmy dalej: w module 5 zamykamy dzień: dostawcy, ciągłość działania, audyt i Twój indywidualny plan na 90 dni.

Dostawcy, ciągłość, audyt i plan

15:40 – 16:30 · 1 godz. dyd.

- ✓ Bezpieczeństwo łańcucha dostaw ICT – ocena ryzyka dostawców i klauzule umowne
- ✓ Usługi chmurowe: model współdzielonej odpowiedzialności, lokalizacja danych i plan wyjścia
- ✓ Ciągłość działania: BIA, RTO i RPO, kopie zapasowe 3-2-1 oraz testowanie planów
- ✓ Audyt bezpieczeństwa z art. 15 – terminy, zakres i szablon sprawozdania
- ✓ Pięć najczęstszych ustaleń audytowych i komplet dowodów do przygotowania
- ✓ Mapa drogowa wdrożenia i indywidualny plan na 90 dni (Ćwiczenie 6)

Bezpieczeństwo łańcucha dostaw ICT – obowiązek z art. 8

MODUŁ 5

Ataki przez dostawców ICT to czwarte najpoważniejsze zagrożenie 2025 i najszybciej rosnąca kategoria.

Co wymaga ustawa i dyrektywa

- Obowiązek oceny ryzyka związanego z bezpieczeństwem i ciągłością łańcucha dostaw produktów, usług i procesów ICT
- Ocenie podlega jakość i odporność produktów i usług dostawcy oraz stosowane przez niego praktyki cyberbezpieczeństwa, w tym procedury bezpiecznego wytwarzania oprogramowania
- Wymagania bezpieczeństwa muszą trafić do umów z bezpośrednimi dostawcami
- Obowiązek monitorowania zgodności dostawców – to proces ciągły, a nie jednorazowa ankieta

Dostawcy wymagający szczególnej uwagi

- Dostawcy usług zarządzanych (MSP i MSSP) – mają dostęp do Twojej infrastruktury; ich incydent staje się Twoim incydentem
- Dostawcy usług chmurowych – patrz następny slajd
- Integratorzy i serwisanci z dostępem zdalnym do systemów OT
- Dostawcy oprogramowania, którego aktualizacje instalujesz automatycznie

1

Inwentaryzacja dostawców ICT

Lista wszystkich dostawców produktów, usług i procesów ICT; dla każdego: rodzaj dostępu i krytyczność dla usługi kluczowej.

2

Klasyfikacja ryzyka dostawcy

Krytyczny – jego awaria oznacza niedostępność usługi kluczowej. Wysoki – istotny wpływ, ale istnieje alternatywa. Normalny – ograniczony wpływ.

3

Ocena bezpieczeństwa dostawcy

Ankieta samooceny, weryfikacja certyfikatów (ISO 27001, SOC 2), przegląd klauzul umownych; dla dostawców krytycznych prawo do audytu.

Wymagania umowne wobec dostawców – lista kontrolna

MODUŁ 5

Szablon: ankieta oceny dostawcy ICT wraz z zestawem klauzul umownych w pakiecie materiałów.

Klauzule, które muszą znaleźć się w umowie

- Obowiązek zgłoszenia incydentu u dostawcy w określonym terminie – rekomendowane maksimum 24 godziny
- Prawo do przeprowadzenia audytu bezpieczeństwa lub żądania audytu zewnętrznego
- SLA bezpieczeństwa i dostępności wraz z miernikami
- Wymagania certyfikacyjne (ISO 27001, SOC 2) lub równoważne
- Lokalizacja przetwarzania i przechowywania danych
- Wymagania wobec podwykonawców dostawcy i obowiązek ich zgłaszania
- Plan wyjścia: prawo do eksportu danych, format, termin i koszt
- Kary umowne za naruszenie wymagań bezpieczeństwa

Monitorowanie i przegląd

- Roczny przegląd oceny ryzyka dostawców
- Śledzenie publicznych informacji o incydentach u dostawców
- Aktualizacja oceny po istotnych zmianach po stronie dostawcy

Realia negocjacyjne

- Wobec dużych dostawców globalnych negocjacja klauzul bywa niemożliwa
W takim wypadku udokumentuj ocenę ryzyka rezydualnego i decyzję zarządu o jego akceptacji – to również jest zgodność

Uwaga: ocena ryzyka łańcucha dostaw jest dokumentem żywym, a nie jednorazowym ćwiczeniem. Audytor sprawdzi datę ostatniego przeglądu i to, czy lista dostawców odpowiada rzeczywistości – łącznie z dostawcami dodanymi w ostatnim kwartale.

Usługi chmurowe a wymagania UoKSC

MODUŁ 5

Dostawca chmury jest dostawcą ICT i podlega ocenie ryzyka jak każdy inny dostawca krytyczny.

Model współdzielonej odpowiedzialności

- Dostawca odpowiada za bezpieczeństwo infrastruktury – warstwy fizycznej, sieciowej i platformy
- Ty odpowiadasz za konfigurację, zarządzanie dostępem, dane i ich klasyfikację
- Błąd konfiguracji po stronie klienta to najczęstsza przyczyna incydentów w chmurze – i to Twoja odpowiedzialność, nie dostawcy

Wymagania umowne i dokumentacyjne

- Umowa powierzenia przetwarzania danych i klauzule bezpieczeństwa
- Standardowe klauzule umowne przy transferze poza EOG
- Certyfikaty: ISO 27001, SOC 2, CSA STAR
- Uprawnienie do eksportu danych i logów

Trzy pytania przed wyborem usługi

- Gdzie fizycznie przechowywane są dane? Lokalizacja w UE lub w Polsce bywa wymogiem sektorowym
- W jakim terminie dostawca powiadomi Cię o incydencie po swojej stronie?
- Jak wygląda plan wyjścia – w jakim formacie, w jakim czasie i za jaką cenę odzyskasz swoje dane?

Policz, co naprawdę oznacza SLA

- Dostępność 99,99 % to około 52 minuty niedostępności w skali roku
- Dostępność 99,9 % to już około 8,8 godziny rocznie
- Sprawdź, czy Twoje RTO dla usługi kluczowej mieści się w tym budżecie – i czy plan ciągłości to uwzględnia

Ciągłość działania i odtwarzanie po awarii – obowiązek z art. 8

MODUŁ 5

Plan ciągłości działania (BCP) – co musi zawierać

- Identyfikację kluczowych procesów biznesowych i ich zależności od systemów
- Analizę wpływu na działalność (BIA) – skutek przerwania procesu w czasie
- Scenariusze zakłóceń: ransomware, niedostępność dostawcy chmury, awaria centrum danych, utrata kluczowego personelu
- Procedury alternatywne na czas niedostępności systemów
- Cele RTO i RPO dla każdego systemu krytycznego
- Plan komunikacji kryzysowej: kto, kogo i w jakiej kolejności informuje

Plan odtwarzania (DR) – co musi zawierać

- Plan odtworzenia systemów po awarii lub ataku
- Priorytetyzację: kolejność przywracania systemów
- Procedury przywracania z kopii zapasowych
- Środowisko testowe – testy odtworzeniowe nie mogą odbywać się na produkcji
- Dane kontaktowe: dostawcy, integratorzy, wsparcie producenta

RTO

Recovery Time Objective

Maksymalny akceptowalny czas niedostępności systemu – ile czasu mamy na przywrócenie usługi

RPO

Recovery Point Objective

Maksymalna akceptowalna utrata danych mierzona w czasie – do jakiego momentu wstecz możemy odtworzyć dane

3 – 2 – 1

Zasada kopii zapasowych

3 kopie danych, na 2 różnych nośnikach, 1 kopia poza lokalizacją – rozszerzenie: 1 kopia offline lub niemodyfikowalna, 0 błędów w teście odtworzenia

12 mies.

Maksymalny odstęp testu

Testy planów ciągłości i odtwarzania: minimum raz w roku oraz po każdej istotnej zmianie w środowisku

Testowanie planów ciągłości – metodyka i roczny harmonogram

MODUŁ 5

Procedura nieprzetestowana jest procedurą nieistniejącą – to standardowe ustalenie audytowe.

I Ćwiczenie sztabowe (tabletop)

Omówienie scenariusza przy stole, bez ingerencji w systemy. Weryfikuje decyzje, role i komunikację.

II Test odtworzenia z kopii

Faktyczne przywrócenie wybranych systemów w środowisku testowym z pomiarem czasu i weryfikacją kompletności danych.

III Test przełączenia (failover)

Przełączenie usługi do lokalizacji zapasowej i praca na niej przez ustalony czas.

IV Pełna symulacja awarii

Scenariusz obejmujący biznes, IT i komunikację zewnętrzną – najbliższy warunkom rzeczywistym.

Przykładowy harmonogram roczny

- I kwartał: ćwiczenie sztabowe – scenariusz ataku ransomware
- II kwartał: test przywrócenia kopii wybranych systemów krytycznych
- III kwartał: test przełączenia sieci lub przejścia do lokalizacji zapasowej
- IV kwartał: pełny test odtworzenia oraz audyt wewnętrzny planu ciągłości
- Dodatkowo: symulacja braku dostępu do usługi chmurowej

Co powstaje po każdym teście

- Raport z wynikiem: czy osiągnięto zakładane RTO i RPO
- Lista niezgodności i rzeczy, które nie zadziałały
- Plan działań korygujących z właścicielem i terminem
- Zaktualizowany plan, jeśli test wykazał jego nieadekwatność
- Angażuj biznes – IT nie może testować planów w oderwaniu od procesów, które te plany chronią

Co sprawdza audytor: czy testy są udokumentowane, jak stary jest ostatni raport i czy stwierdzone problemy zostały faktycznie naprawione. Raport bez działań korygujących pogarsza sytuację, zamiast ją poprawiać.

Audyt bezpieczeństwa z art. 15 UoKSC

MODUŁ 5

Terminy

- Podmiot kluczowy: pierwszy audyt w ciągu 24 miesięcy od wpisu do wykazu, kolejne co najmniej co 3 lata
- Dla podmiotów kluczowych istniejących w dniu wejścia w życie nowelizacji termin biegnie od 3.04.2026, czyli do 3.04.2028
- Dla podmiotów uznanych decyzją – od dnia doręczenia decyzji
- Podmiot ważny: audyt po incydencie, zgłoszeniu lub skardze, nie prewencyjnie

Zakres audytu – sześć obszarów szablonu

- Obszar 1 – Organizacja zarządzania bezpieczeństwem informacji: role, odpowiedzialności, zaangażowanie kierownictwa
- Obszar 2 – Procesy zarządzania bezpieczeństwem: SZBI, punkt kontaktowy, współpraca z CSIRT
- Obszar 3 – Zarządzanie ryzykiem: metodyka, rejestr ryzyk, plan postępowania, akceptacja zarządu
- Obszar 4 – Monitorowanie i reagowanie na incydenty: detekcja, klasyfikacja, zgłoszenia, rejestr
- Obszar 5 – Zarządzanie zmianą: kontrola zmian w systemach, testowanie, autoryzacja
- Obszar 6 – Zarządzanie ciągłością działania: BCP, DR, kopie zapasowe, testy

Kto może przeprowadzić audyt

- Wyłącznie audytor spełniający wymagania kwalifikacyjne określone w ustawie
- Audyt przeprowadzany jest na koszt podmiotu
- Ministerstwo udostępnia szablon sprawozdania z audytu – korzystaj z niego, także przy audycie wewnętrznym

Wykorzystaj to wcześniej: te same sześć obszarów potraktuj jako strukturę audytu wewnętrznego przeprowadzonego rok przed audytem ustawowym. Znalezienie niezgodności u siebie kosztuje nieporównanie mniej niż znalezienie jej przez audytora.

Pięć najczęstszych ustaleń audytowych

MODUŁ 5

Audytor KSC i audytor ISO 27001 pytają o te same obszary. Znajomość tych błędów pozwala usunąć je przed kontrolą.

1. Dokumentacja bez operacyjności

Polityka istnieje, jest zatwierdzona i ładnie sformatowana – ale nikt jej nie stosuje, a pracownicy nie znają jej treści. Brak właścicieli procesów.

2. Nieaktualny rejestr ryzyk

Brak przeglądu od ponad 12 miesięcy albo brak formalnej akceptacji ryzyk akceptowanych przez zarząd.

3. Brak dowodów szkoleń kierownictwa

Szkolenie się odbyło, ale nie ma listy obecności, zaświadczenia ani protokołu. Z perspektywy audytu obowiązek z art. 8e nie został wykonany.

4. Logi zbierane, ale nieanalizowane

System monitorowania działa, alerty są generowane, ale nikt ich nie przegląda i nie ma zdefiniowanego SLA reakcji.

5. Plany ciągłości nigdy nietestowane

Dokument istnieje, ale brakuje raportu z testu odtworzeniowego. Nie wiadomo, czy plan zadziała.

Wspólny mianownik

- Każde z tych ustaleń to brak dowodu, a nie brak intencji
- Żadne z nich nie wymaga incydentu, aby zostało stwierdzone
- Każde jest możliwe do usunięcia bez inwestycji – wystarczy dyscyplina zapisu

Pakiet dowodów – przygotuj zawczasu

- Polityki z datą zatwierdzenia i wersją
- Rejestr ryzyk z datą ostatniego przeglądu
- Protokoły przeglądu zarządzania
- Listy obecności i zaświadczenia ze szkoleń
- Rejestr incydentów i zgłoszenia do CSIRT
- Raporty z testów odtworzeniowych
- Rejestr dostawców i podpisane klauzule

Mapa drogowa wdrożenia – pięć faz

MODUŁ 5

Punktem wyjścia jest wynik Twojej analizy luk z Ćwiczenia 4.



Tydzień 1–2 • Działania natychmiastowe

Ustal status PK/PW i udokumentuj go z akceptacją zarządu • wyznacz właściciela procesu KSC • sprawdź, czy nie otrzymałeś decyzji organu • przygotuj dostęp do wykaz-ksc.gov.pl i podpis kwalifikowany.



Miesiąc 1–2 • Rejestracja i analiza luk

Złóż wniosek o wpis w S46 • przeprowadź pełną analizę luk wobec 10 obszarów art. 8 • uruchom analizę ryzyka wg ISO 27005 • zidentyfikuj dziesięciu najbardziej krytycznych dostawców ICT.



Miesiąc 3–5 • Wdrożenie podstawowe

Polityka bezpieczeństwa informacji i dokumentacja SZBI • MFA dla systemów krytycznych i dostępu zdalnego • wdrożenie lub weryfikacja monitorowania 24/7 • procedura zarządzania incydentami wraz z szablonem zgłoszenia.



Miesiąc 6–8 • Dojrzałość operacyjna

Pełne wdrożenie wszystkich dziesięciu obszarów • BCP i DR wraz z pierwszym ćwiczeniem sztabowym • zarządzanie podatnościami i SLA patchowania • klauzule bezpieczeństwa w umowach z dostawcami.



Rok 2 i dalej • Cykl ciągły

Roczny przegląd analizy ryzyka • audyt wewnętrzny przed audytem ustawowym • szkolenia kierownictwa i pracowników w cyklu rocznym • aktualizacja dokumentacji po każdej istotnej zmianie.

Sekwencja ma znaczenie: rejestracja i analiza luk poprzedzają wydatki. Kupowanie narzędzi przed analizą ryzyka to najdroższy sposób na osiągnięcie niezgodności.

Ćwiczenie 6 – plan naprawczy NOVENERGII na 90 dni

MODUŁ 5

15 minut pracy + omówienie. Szablon: arkusz planu wdrożenia na 90 dni. Wejście: pięć luk krytycznych z Ćwiczenia 4.

Termin	Działanie (luka z Ćwiczenia 4)	Produkt / dowód	Właściciel	Dlaczego właśnie to
Dni 1–14	Ustalenie i udokumentowanie statusu podmiotu kluczowego (A.1)	Notatka z akceptacją zarządu	Zarząd / CISO	Warunek wszystkich dalszych działań i najtańsza pozycja na liście
Dni 1–14	Wyznaczenie osoby odpowiedzialnej i dwóch osób kontaktowych (B.1)	Zarządzenie, zakres obowiązków	Zarząd	Bez właściciela procesu żadne z pozostałych zadań nie ruszy
Dni 15–30	Złożenie wniosku o wpis do wykazu w systemie S46 (A.2)	Potwierdzenie PDF, numer sprawy	CISO	Termin ustawowy; brak wpisu to naruszenie i podstawa kary dla kierownika
Dni 15–45	Aktualizacja firmware urządzeń brzegowych i uruchomienie procesu podatności	Rejestr podatności, SLA patchowania	IT	To był wektor wejścia napastnika – luka o najwyższym poziomie ryzyka
Dni 15–45	Wdrożenie MFA na dostępie zdalnym i kontach uprzywilejowanych (D.1)	Konfiguracja, lista wyjątków	IT	Największy efekt przy najmniejszym nakładzie
Dni 30–60	Przegląd i ograniczenie kont serwisowych integratorów (D.2)	Rejestr kont, dowody przeglądu	IT / zakupy	Konta bezterminowe z hasłami fabrycznymi umożliwiły ruch poprzeczny
Dni 30–75	Segmentacja sieci IT / OT i strefa pośrednia (G.1)	Schemat sieci, reguły zapory, raport z testu	IT / OT	Bez segmentacji każdy incydent w IT staje się incydem w OT
Dni 45–90	Przeprowadzenie i zatwierdzenie analizy ryzyka (C.1)	Rejestr ryzyk, protokół zarządu	CISO / zarząd	Fundament doboru wszystkich pozostałych środków
Dni 60–90	Uruchomienie monitorowania w trybie ciągłym (E.1)	Umowa SOC lub konfiguracja SIEM, SLA reakcji	Zarząd / IT	Najdłuższa i najdroższa pozycja – dlatego startuje równolegle, nie na końcu
Dni 60–90	Test odtworzenia z kopii zapasowej i kopia offline (F.1)	Raport z testu z wynikiem RTO/RPO	IT	Kopie w tej samej domenie zostały zniszczone razem z systemami

Twoje zadanie: zbuduj taki sam arkusz dla własnej organizacji, wychodząc od pięciu luk krytycznych, które wybrałeś w Ćwiczeniu 4. Każdy wiersz musi mieć produkt końcowy, który da się położyć na stole przed audytorem, oraz jedną osobę z imienia i nazwiska. Działanie bez dowodu i bez właściciela nie jest planem, tylko intencją.

Moduł 5 — podsumowanie

MODUŁ 5

Dostawcy, ciągłość, audyt i plan

Ryzyko dostawców ICT jest obowiązkiem ustawowym i procesem ciągłym, nie jednorazową ankietą

Inwentaryzacja, klasyfikacja krytyczności, ocena bezpieczeństwa, klauzule umowne, roczny przegląd. Szczególna uwaga: MSP, MSSP i dostawcy z dostępem zdalnym.

W chmurze odpowiadasz za konfigurację, dostęp i dane – dostawca tylko za infrastrukturę

Sprawdź lokalizację danych, termin powiadomienia o incydencie po stronie dostawcy i plan wyjścia. Przelicz SLA na realne godziny niedostępności.

BCP i DR wymagają parametrów RTO i RPO zaakceptowanych przez biznes oraz corocznych testów

Kopie zapasowe wg zasady 3-2-1 z kopią offline. Raport z testu bez działań korygujących pogarsza sytuację zamiast ją poprawiać.

Audyt z art. 15 obejmuje sześć obszarów – wykorzystaj je jako strukturę audytu wewnętrznego

Podmiot kluczowy: pierwszy audyt w ciągu 24 miesięcy od wpisu, kolejne co najmniej co 3 lata.

Pięć najczęstszych ustaleń audytowych to braki dowodu, a nie braki bezpieczeństwa

Dokumentacja bez stosowania, nieaktualny rejestr ryzyk, brak dowodów szkoleń, logi bez analizy, nieprzetestowany plan ciągłości.

Przechodźmy dalej: na zakończenie: sesja pytań i odpowiedzi, słowniczek, post-test i podsumowanie kluczowych wniosków.

Najczęstsze pytania uczestników (1/2)

Pytania zadane na szkoleniach realizowanych w 2026 r. – wraz z odpowiedziami.

Gdzie znajdę pełną, oficjalną listę kodów PKD przypisanych do sektorów z załączników?

Ustawa nie posługuje się kodami PKD, lecz opisem rodzajów działalności w Załącznikach nr 1 i 2. Kody PKD są narzędziem pomocniczym: przeglądasz wszystkie kody wpisane w KRS, a następnie weryfikujesz, czy faktycznie prowadzona pod nimi działalność mieści się w opisie z załącznika. Rozstrzyga stan faktyczny, nie sam wpis rejestrowy – dlatego wynik samoidentyfikacji zawsze wymaga uzasadnienia w notatce.

Co dokładnie wypełniamy w systemie S46?

Formularz wniosku o wpis do wykazu obejmuje sekcje: informacje podstawowe (nazwa, NIP, REGON), rejestry działalności regulowanej, klasyfikację (sektor, podsektor, rodzaj działalności wg załączników), dane adresowe i kontaktowe wraz z adresem do doręczeń elektronicznych, osoby kontaktowe i administratora konta oraz specyfikację sieci – zakresy publicznych adresów IP i domen. Łącznie 18 kategorii danych z art. 7 ust. 2.

Czy mamy obowiązek sprawdzania karalności pracowników?

Tak, w zakresie wynikającym z art. 8f: weryfikacji podlegają osoby realizujące zadania z art. 8 i art. 11, czyli personel bezpieczeństwa i obsługi incydentów – zarówno własny, jak i po stronie dostawców realizujących te zadania. Wymaga to zmiany procesu rekrutacji i onboardingu po stronie HR oraz uzgodnienia z inspektorem ochrony danych podstawy i okresu przechowywania zaświadczeń.

Najczęstsze pytania uczestników (2/2)

Na jaki dzień oceniamy wielkość podmiotu w regule size-cap?

Na podstawie danych za ostatni zatwierdzony rok obrotowy, liczonych łącznie z podmiotami powiązanymi i partnerskimi wg rozporządzenia 651/2014. Zmiana statusu następuje dopiero wtedy, gdy przekroczenie lub spadek poniżej progu utrzymuje się przez dwa kolejne okresy obrachunkowe – pojedynczy rok odbiegający od trendu nie zmienia kwalifikacji.

Mamy certyfikat ISO 27001. Czy to wystarczy?

Nie wystarczy, ale bardzo pomaga. Wdrożony SZBI pokrywa większość wymagań z 10 obszarów art. 8. Osobno musisz zaadresować: wpis do wykazu w S46, terminy zgłoszeń do CSIRT, obowiązki kierownictwa z art. 73a i 8e, weryfikację niekaralności z art. 8f oraz audyt ustawowy z art. 15.

Jesteśmy podmiotem ważnym – czy mamy mniej obowiązków niż podmiot kluczowy?

Katalog obowiązków merytorycznych jest ten sam. Różnice dotyczą trybu nadzoru (ex-post zamiast ex-ante), braku obowiązku cyklicznego audytu oraz niższych progów kar. Zakres wdrożenia pozostaje tożsamy.

Czy możemy zlecić całość wdrożenia i monitoring na zewnątrz?

Możesz zlecić wykonanie, ale nie odpowiedzialność. Ustawa dopuszcza zawarcie umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa zamiast budowania własnych struktur, jednak odpowiedzialność za wykonanie obowiązków – w tym osobista odpowiedzialność kierownika – pozostaje po stronie podmiotu.

Słowniczek pojęć i skrótów (1/2)

Pojęcie	Znaczenie
NIS2	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii
UoKSC	Ustawa o krajowym systemie cyberbezpieczeństwa – polska implementacja NIS2; nowelizacja opublikowana jako Dz.U. 2026 poz. 252
PK / PW	Podmiot kluczowy (art. 5 ust. 1) i podmiot ważny (art. 5 ust. 2) – dwie kategorie podmiotów objętych ustawą
S46	System teleinformatyczny Ministerstwa Cyfryzacji do wymiany informacji z organami KSC; portal wykaz-ksc.gov.pl
CSIRT	Zespół reagowania na incydenty bezpieczeństwa komputerowego – w Polsce CSIRT NASK, CSIRT GOV, CSIRT MON oraz CSIRT-y sektorowe
SZBI	System Zarządzania Bezpieczeństwem Informacji – wymagany przez art. 8 ust. 1 UoKSC
SoA	Deklaracja Stosowania (Statement of Applicability) – wykaz kontroli z uzasadnieniem ich stosowania lub niestosowania
RTP	Plan postępowania z ryzykiem (Risk Treatment Plan) – ryzyko, działanie, właściciel, termin
PDCA	Cykl Deminga: Plan – Do – Check – Act; mechanizm zapewniający systematyczność SZBI
Size-cap	Reguła kwalifikacji wielkościowej przedsiębiorstwa wg rozporządzenia Komisji (UE) nr 651/2014
BIA	Analiza wpływu na działalność (Business Impact Analysis) – podstawa ustalenia RTO i RPO
RTO / RPO	Maksymalny akceptowalny czas przywrócenia usługi / maksymalna akceptowalna utrata danych mierzona w czasie

Słowniczek pojęć i skrótów (2/2)

Pojęcie	Znaczenie
MFA	Uwierzytelnianie wieloskładnikowe – wymagane dla dostępu zdalnego i kont uprzywilejowanych
IAM / PAM	Zarządzanie tożsamością i dostępem / zarządzanie dostępem uprzywilejowanym
SIEM	System zbierania i korelacji zdarzeń bezpieczeństwa z całej infrastruktury
EDR / NDR / XDR	Detekcja i reagowanie na poziomie punktu końcowego / sieci / zintegrowana w wielu warstwach
SOC	Centrum operacji bezpieczeństwa – własne, zlecone (MSSP/MDR) albo hybrydowe
MSP / MSSP	Dostawca usług zarządzanych / dostawca zarządzanych usług bezpieczeństwa
CVSS	Standard oceny krytyczności podatności w skali 0–10
CVE	Publiczny katalog ujawnionych podatności w oprogramowaniu i sprzęcie
CVD	Skoordynowane ujawnianie podatności – proces przyjmowania i obsługi zgłoszeń od badaczy i użytkowników
OT / ICS / SCADA	Technologie operacyjne / przemysłowe systemy sterowania / systemy nadzoru i akwizycji danych
Model Purdue	Warstwowy model architektury OT (ISA-95), od urządzeń obiektowych L0 do systemów biznesowych L5
ISA/IEC 62443	Norma bezpieczeństwa przemysłowych systemów automatyki i sterowania
2024/2690	Rozporządzenie wykonawcze Komisji (UE) określające kryteria i progi incydentu poważnego

Gdzie szukać źródeł i pomocy

Akty prawne i dokumenty źródłowe

- Dz.U. 2026 poz. 252 – ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa
- Dyrektywa (UE) 2022/2555 (NIS2) – EUR-Lex
- Rozporządzenie wykonawcze Komisji (UE) 2024/2690 – kryteria incydentu poważnego
- Rozporządzenie Komisji (UE) nr 651/2014 – reguła size-cap (kryterium wielkości przedsiębiorstwa)
- Komunikaty Ministra Cyfryzacji dotyczące harmonogramu i systemu S46

Wytyczne i narzędzia

- ENISA Technical Implementation Guidance – praktyczne wytyczne wdrożeniowe do art. 21 NIS2
- ENISA Threat Landscape – coroczny przegląd krajobrazu zagrożeń
- Szablon sprawozdania z audytu KSC udostępniony przez Ministerstwo
- Normy: ISO/IEC 27001:2022, ISO/IEC 27005, ISO 31000, ISO 22301, ISA/IEC 62443

Portale i systemy

- wykaz-ksc.gov.pl – system S46: rejestracja i zgłoszenia
- gov.pl/cyber – informacje Ministerstwa Cyfryzacji
- cert.pl – CERT Polska: raporty, wytyczne, zgłaszanie incydentów

Wsparcie i literatura

- Bezpłatne szkolenia i materiały informacyjne Ministerstwa Cyfryzacji
- „UoKSC i NIS2 w Praktyce”, P. Szymczyk, ISBN 978-83-981562-0-2
- Konsultacja poszkoleniowa: 30 minut w ciągu 30 dni od szkolenia

Q&A, post-test i podsumowanie

16:30 – 17:00 · 0,5 godz. dyd.

- ✓ Odpowiedzi na pytania zaparkowane w trakcie dnia
- ✓ Post-test walidujący osiem efektów uczenia się (20 pytań, 15 minut)
- ✓ Omówienie odpowiedzi i porównanie wyniku z pre-testem – pomiar przyrostu wiedzy
- ✓ Podsumowanie kluczowych wniosków z pięciu modułów
- ✓ Przegląd pakietu materiałów i zasad konsultacji poszkoleniowej
- ✓ Wydanie certyfikatu i zaświadczenia o ukończeniu usługi rozwojowej

Post-test – walidacja efektów uczenia się

SESJA KOŃCOWA

20 pytań jednokrotnego wyboru · 15 minut · zaliczenie od 60 % poprawnych odpowiedzi.

Struktura testu – zakres tematyczny

- Część I (pyt. 1–5): zakres podmiotowy, size-cap, terminy ustawowe, rejestracja w S46
- Część II (pyt. 6–9): 10 obszarów art. 8, odpowiedzialność kierownictwa, kary, organy nadzoru
- Część III (pyt. 10–13): SZBI, ISO 27001, dokumentacja, analiza ryzyka i analiza luk
- Część IV (pyt. 14–17): środki techniczne, monitorowanie, incydenty, terminy zgłoszeń i właściwość CSIRT
- Część V (pyt. 18–20): dostawcy ICT, ciągłość działania, audyt z art. 15

Powiązanie z efektami uczenia się

- Każde pytanie jest przypisane do jednego z ośmiu efektów uczenia się z początku dnia
- Wynik cząstkowy pokazuje, który efekt wymaga uzupełnienia
- Pytania 1–10 powtarzają zagadnienia z pre-testu – to podstawa pomiaru przyrostu wiedzy

Co dzieje się po teście

- Omówienie wszystkich odpowiedzi wraz z uzasadnieniem
- Porównanie wyniku z pre-testem i wyliczenie przyrostu wiedzy
- Odnotowanie wyniku w dokumentacji usługi zgodnie ze standardem BUR
- Wydanie certyfikatu i zaświadczenia o ukończeniu usługi

Kluczowe wnioski – co zabrać ze szkolenia

SESJA KOŃCOWA

M1

Zakres i rejestracja

Ustawa obowiązuje od 3.04.2026. Wniosek o wpis do wykazu składasz w S46 w oknie 7.05 – 3.10.2026. Sprawdź wszystkie kody PKD i policz size-cap łącznie z podmiotami powiązanymi. Udokumentuj wynik, także negatywny.

M2

Obowiązki i odpowiedzialność

Punktem odniesienia jest katalog 10 obszarów środków bezpieczeństwa z art. 8. Kierownik odpowiada osobiście do 300 % miesięcznego wynagrodzenia. Kary dla podmiotu: 10 mln EUR lub 2 % (PK) i 7 mln EUR lub 1,4 % (PW). Okres ochronny do 3.04.2028 nie odracza obowiązków.

M3

SZBI, ryzyko i luki

SZBI to proces, nie zbiór dokumentów – wymagane są jednocześnie dokumentacja i operacyjność. ISO 27001:2022 daje gotową ramę i mapowanie. Analiza ryzyka minimum raz w roku, powtarzalna i uzasadnialna. Zaczynij od analizy luk.

M4

Technika i incydenty

MFA, szyfrowanie, PAM, centralne logi i segmentacja to minimum. Monitorowanie musi być ciągłe – zbieranie logów bez analizy nim nie jest. Terminy zgłoszeń: 24 h, 72 h, 1 miesiąc, licząc od uzyskania wiedzy o incydencie.

M5

Dostawcy, ciągłość, audyt

Oceniaj dostawców ICT i wpisuj wymagania bezpieczeństwa do umów. Testuj plany ciągłości minimum raz w roku i dokumentuj wyniki. Audyt z art. 15: pierwszy w ciągu 24 miesięcy od wpisu, kolejne co najmniej co 3 lata.

CASE

Czego uczy NOVENERGIA

Żaden z czterech mechanizmów ataku nie był problemem technologicznym: nieaktualne urządzenie brzegowe, brak segmentacji, konta serwisowe bez ograniczeń, brak obsługi alertów nocą. Każdy to obowiązek z art. 8 – i każdy da się zamknąć w 90 dni.

Jedno zdanie na koniec: zgodność to nie stan, który się osiąga, tylko proces, który się utrzymuje – a jego jedynym widocznym śladem jest dowód.

Co otrzymujesz po szkoleniu

SESJA KOŃCOWA

1 Prezentacja i kompendium

Pełna prezentacja szkoleniowa w PDF oraz kompendium wiedzy NIS2 / UoKSC / SZBI / ISO 27001.

2 Checklista audytowa

Lista kontrolna wymagań UoKSC dla podmiotów kluczowych i ważnych, z podstawą prawną, wymaganym dowodem i priorytetem.

3 Roadmapa wdrożenia

Arkusz z fazami wdrożenia, produktami, właścicielami i orientacyjną osią czasu.

4 Spis dokumentów SZBI

Katalog dokumentów wymaganych do wykazania zgodności, z opisem przeznaczenia każdego z nich.

5 Matryca incydentów

Kryteria i progi incydentu poważnego wg rozporządzenia 2024/2690 wraz z procedurą zgłaszania i wzorem rejestru incydentów.

6 Szablony ćwiczeń

Formularz samoidentyfikacji, macierz RACI, arkusz analizy ryzyka, formularz zgłoszenia 24 h / 72 h, ankieta dostawcy, plan na 90 dni.

7 Słowniczek pojęć

Zestawienie pojęć i skrótów z zakresu NIS2, UoKSC, SZBI i bezpieczeństwa operacyjnego.

8 Certyfikat i zaświadczenie

Imienny certyfikat ukończenia szkolenia oraz zaświadczenie o ukończeniu usługi rozwojowej – dokument potwierdzający wykonanie obowiązku z art. 8e.

9 Konsultacja poszkoleniowa

30 minut indywidualnej konsultacji on-line w ciągu 30 dni od zakończenia szkolenia.

ZAKOŃCZENIE

Pytania i odpowiedzi

Wracamy do pytań zaparkowanych w trakcie dnia oraz do tych, które pojawiły się przy ćwiczeniach.

- ✓ Twój pierwszy krok jest już zapisany – w arkuszu planu na 90 dni z Ćwiczenia 6
- ✓ Pięć luk krytycznych z Ćwiczenia 4 to Twoja lista zadań na najbliższy kwartał
- ✓ Zachowaj zaświadczenie ze szkolenia – to dowód wykonania obowiązku z art. 8e UoKSC
- ✓ Konsultacja poszkoleniowa: 30 minut on-line w ciągu 30 dni – umów ją mailowo

Dziękuję za uwagę

Piotr Szymczyk · LT MASTERY Szkolenia dla Biznesu Piotr Szymczyk · marka LegacyTurn

ltmastery.com@gmail.com · Dostawca Usług w Bazie Usług Rozwojowych, ID 204299

Źródła: wykaz-ksc.gov.pl · gov.pl/cyber · cert.pl · enisa.europa.eu

