

KOMPENDIUM WIEDZY: NIS2 / UoKSC / SZBI / ISO 27001

Kompleksowy przewodnik po wymaganiach, wdrożeniu i praktycznych aspektach cyberbezpieczeństwa

Dokument opracowany na podstawie: oficjalnej dokumentacji ustawy i rozporządzenia, wytycznych, stron oraz forów branżowych, transkryptów webinarów i podcastów eksperckich dotyczących NIS2, nowelizacji UoKSC, bezpieczeństwa OT/IT oraz dokumentów systemowych SZBI/ISO 27001.

Przeznaczenie: Materiał szkoleniowy dla organów zarządzających, kadry IT i bezpieczeństwa, działów compliance, audytu oraz menedżerów operacyjnych.

AGENDA

1. Kontekst i geneza – dlaczego NIS2/UoKSC i co to zmienia
 2. Zakres podmiotowy – kogo dotyczy (podmioty kluczowe i ważne, 18 sektorów, progi wielkościowe)
 3. Harmonogram wdrożenia – terminy, etapy, decyzje administracyjne
 4. Wymagania prawne UoKSC – co konkretnie trzeba wdrożyć (3 miesiące, 6 miesięcy, 12 miesięcy)
 5. System Zarządzania Bezpieczeństwem Informacji (SZBI) – definicja, zakres, dokumentacja
 6. ISO 27001 jako rama wdrożeniowa – powiązanie z UoKSC, klauzule normy, kontrole Annex A
 7. Zarządzanie ryzykiem – metodologia, analiza, postępowanie z ryzykiem
 8. Zarządzanie incydentami – definicja, klasyfikacja, terminy zgłoszeń, CSIRT
 9. Bezpieczeństwo OT vs IT – kluczowe różnice, zagrożenia, wymagania NIS2 dla OT
 10. Ciągłość działania (BCP/DRP) – wymagania, plany, testowanie
 11. Łańcuch dostaw – wymagania bezpieczeństwa wobec dostawców
 12. Audyty SZBI – wewnętrzne, zewnętrzne, przegląd zarządu
 13. Sankcje i kary – poziomy kar, odpowiedzialność kierownictwa
 14. Plan działania dla organizacji – priorytety, kroki wdrożeniowe, rekomendacje
-

1. KONTEKST I GENEZA – DLACZEGO NIS2/UoKSC I CO TO ZMIENIA

A. Europejski krajobraz zagrożeń jako motor regulacji

Rosnąca liczba poważnych incydentów cyberbezpieczeństwa wpływających na infrastrukturę krytyczną, łańcuchy dostaw oraz usługi kluczowe dla państw i obywateli

była głównym impulsem do stworzenia Dyrektywy NIS2 (Network and Information Security 2). Europa i cały świat stanęły wobec narastającego zjawiska, które można określić jako **wojnę hybrydową** – skoordynowanych działań cybernetycznych wymierzonych w gospodarkę, bezpieczeństwo i stabilność społeczną państw.

Kluczowe obserwacje, które ukształtowały nowe regulacje:

- **Wzrost aktywności grup przestępczych i sponsorowanych przez obce rządy** – ataki na infrastrukturę krytyczną rosną w tempie logarytmicznym. Grupy hakerskie, działając w interesie obcych rządów lub dla zysku, coraz częściej celują w systemy przemysłowe, energetykę, wodociągi i transport.
- **Upublicznienie informacji o incydentach** – jeszcze kilka lat temu informacje o atakach na infrastrukturę krytyczną nie przedostawały się do opinii publicznej. Dziś cyberbezpieczeństwo trafiło do mainstreamu mediów, co buduje społeczną presję na zapewnienie ochrony usług kluczowych.
- **Skutki dla obywateli** – ataki na infrastrukturę (energetykę, wodociągi, transport, ochronę zdrowia) dotyczą bezpośrednio codziennego życia. Brak dostępu do usług krytycznych podważa zaufanie publiczne i może powodować chaos społeczny.
- **Testowanie odporności** – wiele obserwowanych incydentów ma charakter rozpoznawczy. Przeciwnicy weryfikują poziom przygotowania i identyfikują słabe punkty obrony, by w momencie eskalacji konfliktu móc skutecznie działać.

Historycznym punktem odniesienia jest robak **Stuxnet** sprzed ponad dekady – pierwszy publicznie znany cyberatak wymierzony w fizyczne systemy przemysłowe (irańska elektrownia jądrowa). Pokazał on, że cyberatak może wywołać realne, fizyczne skutki w infrastrukturze krytycznej. Od tamtego czasu metodologia ataków uległa znacznemu rozszerzeniu.

B. Geneza regulacyjna: od NIS1 do NIS2

Dyrektywa NIS1 (2016) była pierwszą europejską regulacją w zakresie cyberbezpieczeństwa sieci i systemów informacyjnych. Ustanowiła podstawowe ramy, lecz praktyka ujawniła jej ograniczenia:

- Zbyt wąski zakres podmiotowy (objęła relatywnie nieliczne sektory)
- Brak harmonizacji między państwami członkowskimi w zakresie wdrożenia
- Niewystarczające mechanizmy egzekwowania
- Brak przepisów o odpowiedzialności kierownictwa

Dyrektywa NIS2 (2022/2555) radykalnie rozszerzyła zakres regulacji:

- **18 sektorów** zamiast pierwotnych kilku
- Podział na **podmioty kluczowe i ważne** (różne wymagania i kary)
- Obowiązkowe **zarządzanie ryzykiem dostawców** (łańcuch dostaw)
- **Kary administracyjne** na poziomie porównywalnym z RODO
- **Odpowiedzialność osobista kierownictwa** – rewolucyjna zmiana w europejskim podejściu

- Obowiązkowe **zgłaszanie incydentów** do organów państwowych w ścisłych terminach
- Wymóg **szkoleń dla kadry zarządzającej** (nie tylko pracowników operacyjnych)

C. Implementacja w Polsce: Ustawa o Krajowym Systemie Cyberbezpieczeństwa (UoKSC)

NIS2 jako dyrektywa wymagała implementacji przez każde z państw członkowskich UE. W Polsce narzędziem implementacji jest **nowelizacja Ustawy o Krajowym Systemie Cyberbezpieczeństwa (UoKSC)**.

Przebieg legislacyjny: - Ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa i niektórych innych ustaw została **podpisana przez Prezydenta 19 lutego** (rok 2026) - Prezydent jednocześnie **skierował ustawę do Trybunału Konstytucyjnego** – specyficzna konstrukcja prawna: podpisuję, ale zgłaszam zastrzeżenia - **2 marca** ustawa ogłoszona w **Dzienniku Ustaw** - Po 30-dniowym **vacatio legis** ustawa wchodzi w życie **3 kwietnia**

Co Prezydent skierował do TK? Zastrzeżenia dotyczyły: - Objęcia ustawą 18 branż gospodarki pogrupowanych w podmioty kluczowe i ważne - Konstruowania **dostawców wysokiego ryzyka** (kontrowersyjny mechanizm eliminacji dostawców z wrażliwych sektorów) - Systemu wydawania **poleceń zabezpieczających** - Systemu podejmowania decyzji przez organy cyberbezpieczeństwa wobec podmiotów - **Systemu kar administracyjnych**

Czy ustawa obowiązuje mimo skierowania do TK? Tak. Skierowanie do Trybunału nie wstrzymuje wejścia w życie ustawy. Jedynie w przypadku stwierdzenia niekonstytucyjności konkretnych przepisów te konkretne przepisy mogłyby stracić moc – nie cała ustawa. Ustawa jest obowiązująca i należy ją stosować.

D. Co zmienia NIS2/UoKSC – kluczowe przesunięcia paradygmatu

Wymiar	Podjęcie poprzednie	Podjęcie NIS2/UoKSC
Odpowiedzialność	Organizacja jako całość	Organizacja + osobista odpowiedzialność kierownictwa
Zakres podmiotowy	Wąski, kilka sektorów	18 sektorów , dziesiątki tysięcy podmiotów
Zabezpieczenia	Dowolność, brak standardów	Obowiązkowe środki z określonymi terminami
Incydenty	Opcjonalne zgłaszanie	Obowiązkowe w rygorystycznych terminach (24h/72h)
Audyt	Nieobowiązkowy	Obowiązkowy co 3 lata (podmioty kluczowe)
Łańcuch dostaw	Poza zakresem	Obowiązkowe zarządzanie ryzykiem dostawców
Kary	Symboliczne lub brak	Do 10 mln EUR lub 2% przychodu

2. ZAKRES PODMIOTOWY – KOGO DOTYCZY

A. Trzy kategorie podmiotów

Ustawa rozróżnia dwie główne kategorie podmiotów objętych wymaganiami:

Podmioty kluczowe

Objęte najwyższymi wymaganiami i najsurowszymi sankcjami. Zgodnie z **art. 5 ust. 1 UoKSC**, podmiotem kluczowym jest podmiot, który: - Działa w **sektorze kluczowym** wymienionym w **Załączniku nr 1** do ustawy - Spełnia kryteria **wielkościowe** (zatrudnienie i/lub obrót) - Lub zostaje **uznany za podmiot kluczowy decyzją administracyjną** organu nadzorczego

Podmioty ważne

Objęte wymaganiami zbliżonymi do podmiotów kluczowych, lecz z nieco łagodniejszymi karami. Zgodnie z **art. 5 ust. 2 UoKSC**, podmiotem ważnym jest podmiot działający w **sektorze ważnym** wymienionym w **Załączniku nr 2** i spełniający kryteria wielkościowe.

Podmioty uznane

Art. 7 UoKSC przewiduje możliwość uznania podmiotu za kluczowy lub ważny **decyzją organu** nawet wówczas, gdy podmiot nie spełnia standardowych kryteriów wielkościowych, jeżeli jego działalność ma istotne znaczenie dla bezpieczeństwa państwa lub generuje wysokie ryzyko.

B. Kryteria wielkościowe – progi

Podstawowe progi klasyfikacji podmiotów:

- **Zatrudnienie:** co najmniej **50 osób** (ekwiwalent pełnych etatów, wliczając osoby na umowach zlecenie)
- **Obrót:** co najmniej **10 milionów euro** rocznie

Ważne: Osiągnięcie choćby jednego z tych progów – przy jednoczesnym działaniu w odpowiednim sektorze – co do zasady kwalifikuje podmiot do kategorii kluczowej lub ważnej. Istnieją wyjątki, w tym dla podmiotów publicznych.

C. 18 sektorów – zakres działalności

Ustawa obejmuje **18 sektorów** podzielonych na:

Sektory kluczowe (Załącznik nr 1): - Energia (elektroenergetyka, ciepłownictwo, ropa naftowa, gaz, wodór) - Transport (lotnictwo, kolej, wodny, drogowy) - Bankowość i infrastruktura rynków finansowych - Ochrona zdrowia - Woda pitna i ścieki - Infrastruktura cyfrowa (węzły wymiany ruchu, dostawcy DNS, rejestry TLD, usługi

chmurowe, sieci CDN, zarządzane usługi bezpieczeństwa) - Administracja publiczna - Przestrzeń kosmiczna

Sektory ważne (Załącznik nr 2): - Usługi pocztowe i kurierskie - Gospodarka odpadami - Produkcja, wytwarzanie i dystrybucja chemikaliów - Produkcja, przetwarzanie i dystrybucja żywności - Produkcja (m.in. urządzenia medyczne, komputery, maszyny, pojazdy) - Dostawcy usług cyfrowych (platformy marketplace, wyszukiwarki, portale społecznościowe) - Badania naukowe

D. Samoidentyfikacja – jak ustalić, czy podmiot podlega UoKSC

Samoidentyfikacja wymaga analizy:

1. **Rodzaju wykonywanej działalności** – co faktycznie robi podmiot (nie tylko co wpisano w rejestrach CEIDG/KRS). Podmioty często mają wiele gałęzi działalności i niektóre mogą kwalifikować do objęcia ustawą.
2. **Poziomu zatrudnienia** (ekwiwalent pełnych etatów, uwzględniający umowy zlecenie)
3. **Wielkości obrotów**
4. **Wpływu działalności** na bezpieczeństwo i ciągłość usług kluczowych

Kluczowa wskazówka: Samo brzmienie wpisu w rejestrze może być niewystarczające. Należy prześledzić faktyczne procesy biznesowe i odpowiedzieć na pytanie, czym podmiot się zajmuje w praktyce.

E. Podmioty w łańcuchu dostaw – rozszerzony krąg oddziaływania

NIS2/UoKSC rozszerza faktyczny krąg podmiotów dotkniętych wymaganiami poza formalną klasyfikację. Jeśli Twój podmiot świadczy usługi dla podmiotu kluczowego lub ważnego:

- Podmiot kluczowy/ważny **może wymagać od swoich dostawców** spełniania wymagań analogicznych do UoKSC
- Podmioty w łańcuchu dostaw będą kontrolowane nie przez organy krajowe, ale przez swoich **klientów/kontrahentów**
- Ryzyko regulacyjne w łańcuchu dostaw wymaga analizy i adresowania jako **ryzyko prawne i biznesowe**

3. HARMONOGRAM WDROŻENIA – TERMINY I ETAPY

A. Kluczowe daty – tabela terminów

Wszystkie terminy liczone są od **daty wejścia w życie ustawy: 3 kwietnia** (rok 2026):

Termin	Data	Obowiązek
Wejście w życie	3 kwietnia 2026	Punkt startowy dla wszystkich terminów

Termin	Data	Obowiązek
+6 miesięcy	3 października 2026	Złożenie wniosku o wpis do wykazu (samoidentyfikacja)
+12 miesięcy	3 kwietnia 2027	Wdrożenie wszystkich obowiązków z rozdziału 3
+24 miesiące	3 kwietnia 2028	Pierwszy obowiązkowy audyt bezpieczeństwa (podmioty kluczowe)
+2 lata od wejścia w życie	3 kwietnia 2028	Możliwość nakładania administracyjnych kar pieniężnych

B. 6 miesięcy: Samoidentyfikacja i rejestracja

Do **3 października 2026** podmiot musi:

1. **Przeprowadzić samoidentyfikację** – czy jest podmiotem kluczowym lub ważnym
2. **Złożyć wniosek o wpis do wykazu** podmiotów kluczowych lub ważnych
 - Wykaz prowadzony przez **Ministra właściwego do spraw cyfryzacji**
 - Na podstawie art. 7 UoKSC
3. W wyniku wpisu podmiot formalnie staje się podmiotem kluczowym lub ważnym

Uwaga: W polskim systemie prawnym przyjęto **system decyzji administracyjnych** (nie samozgłoszeń jak w niektórych innych krajach UE). Organ nadzorczy może wysłać decyzję do podmiotu na podstawie publicznie dostępnych danych (CEIDG, KRS, rejestry publiczne), uznając go za podmiot kluczowy lub ważny. Od momentu otrzymania takiej decyzji bieżą terminy wdrożeniowe.

C. 12 miesięcy: Wdrożenie wszystkich obowiązków

Do **3 kwietnia 2027** podmiot musi mieć wdrożone wszystkie wymagania z **rozdziału 3 UoKSC**, w tym:

- System Zarządzania Bezpieczeństwem Informacji (SZBI)
- Proces systematycznego szacowania ryzyka
- Środki techniczne i organizacyjne w zakresie cyberbezpieczeństwa
- System zarządzania incydentami
- Mechanizmy zgłaszania incydentów, cyberzagrożeń i podatności
- System szkoleń i podnoszenia świadomości
- Dokumentację bezpieczeństwa (opracowaną, stosowaną i aktualizowaną)
- Wyznaczoną osobę odpowiedzialną za SZBI (punkt kontaktowy)

D. Harmonogram szczegółowy po otrzymaniu decyzji

Ustawa określa **wewnętrzny harmonogram obowiązków** liczony od momentu otrzymania decyzji administracyjnej:

Pierwsze 3 miesiące od decyzji:

- Opracowanie i przyjęcie **procesu szacowania ryzyka** (udokumentowany, wdrożony)
- Wdrożenie **procesu zarządzania incydentami** (identyfikacja, klasyfikacja, zgłaszanie)
- **Powołanie osoby odpowiedzialnej** za system cyberbezpieczeństwa

Do 6 miesięcy od decyzji:

- Udokumentowanie całego systemu
- Wdrożenie **zabezpieczeń organizacyjnych** (polityki, procedury, instrukcje)
- Wdrożenie **zabezpieczeń technicznych** (IT/OT)
- Kompletny SZBI operacyjnie wdrożony

Do 12 miesięcy od decyzji:

- **Audyt bezpieczeństwa** oceniający skuteczność wdrożenia
- Wykazanie zgodności z wymaganiami ustawy

E. 24 miesiące: Obowiązkowy audyt (podmioty kluczowe)

Do **3 kwietnia 2028** podmioty kluczowe muszą przeprowadzić **na własny koszt audyt bezpieczeństwa** systemu informacyjnego wykorzystywanego w procesie świadczenia usługi. Następnie audyt taki powtarza się **co najmniej raz na 3 lata**.

F. Grace period – odroczenie kar

Administracyjne kary pieniężne mogą być nakładane dopiero **po upływie 2 lat od wejścia w życie ustawy** (tj. od 3 kwietnia 2028), z wyjątkiem kary za bezpośrednie i poważne cyberzagrożenie dla wartości konstytucyjnych (ta może być nałożona wcześniej).

Ważna interpretacja: Grace period nie oznacza, że można zaniechać wdrożenia. Kara może być nałożona po 2 latach **za cały okres niedostosowania** (włącznie z miesiącami między 12. a 24. miesiącem). Ministerstwo Cyfryzacji komunikowało przychylne podejście do podmiotów faktycznie działających w kierunku wdrożenia, jednak nie można traktować odroczenia jako faktycznego przyzwolenia na beczynność.

4. WYMAGANIA PRAWNE UKSC – CO KONKRETNIE TRZEBA WDROŻYĆ

A. Struktura wymagań z rozdziału 3 UoKSC

Rozdział 3 UoKSC określa **obowiązki podmiotów kluczowych i ważnych**. Wymagania można pogrupować w następujące obszary:

1. System Zarządzania Bezpieczeństwem Informacji (SZBI)

Podmiot musi wdrożyć, stosować i aktualizować **SZBI obejmujący**: - Polityki bezpieczeństwa informacji - Inwentaryzację aktywów i systemów informacyjnych - Procedury operacyjne dla wszystkich kluczowych procesów bezpieczeństwa - System monitorowania i pomiaru skuteczności

2. Systematyczne szacowanie ryzyka

- Opracowanie **metodyki szacowania ryzyka** bezpieczeństwa informacji
- Regularna identyfikacja, analiza i ocena ryzyk
- Ustalenie **progów akceptowalności ryzyka**
- Planowanie i realizacja **postępowania z ryzykami**
- Udokumentowanie całego procesu

3. Środki techniczne i organizacyjne

Ustawa wymaga wdrożenia odpowiednich środków, uwzględniając co najmniej: - Bezpieczeństwo sieci i systemów informacyjnych - Zarządzanie incydentami (wykrywanie, analiza, reagowanie, usuwanie skutków) - Ciągłość działania (backup, przywracanie, zarządzanie kryzysowe) - Bezpieczeństwo łańcucha dostaw - Bezpieczeństwo w zakresie nabywania, rozwoju i utrzymania sieci i systemów - Polityki i procedury w zakresie kryptografii i szyfrowania - Bezpieczeństwo zasobów ludzkich (onboarding, offboarding, dostępy) - Uwierzytelnianie wieloskładnikowe (MFA) i zarządzanie dostępem - Szkolenia i świadomość bezpieczeństwa

4. Zarządzanie incydentami i zgłaszanie

- Wdrożony **proces zarządzania incydentami**
- Obowiązek **zgłaszania incydentów** do właściwych CSIRTów i sektorowych organów nadzorczych
- Rygorystyczne **terminy zgłoszeń** (24h wczesne ostrzeżenie, 72h pełne zgłoszenie)
- **Raport końcowy** po zakończeniu obsługi incydentu

5. Dokumentacja (art. 10 ust. 1 UoKSC)

Podmiot kluczowy lub ważny **opracowuje, stosuje i aktualizuje dokumentację** dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi. To jest jeden z elementów, za którego brak wprost przewidziane są kary.

6. Szkolenia i świadomość

- Szkolenia dla **kadry zarządzającej** (nowość w stosunku do poprzednich regulacji)
- Szkolenia dla pracowników operacyjnych
- Program budowania świadomości bezpieczeństwa

7. Osoba odpowiedzialna / punkt kontaktowy

Art. 14 UoKSC wskazuje, że podmiot powinien: - Powołać **wewnętrzne struktury** odpowiedzialne za cyberbezpieczeństwo, LUB - Zawrzeć umowę z **podmiotem świadczącym usługi** z zakresu cyberbezpieczeństwa

Musi istnieć konkretna **osoba kontaktowa** znająca system, potrafiąca reagować na informacje o incydentach z CSIRTów.

B. Czego NIE wystarczy – typowe błędy (czerwone flagi dla audytora)

Wymagania UoKSC nie sprowadzają się do posiadania dokumentacji. Organ nadzoru ocenia **zdolność organizacji do zarządzania cyberbezpieczeństwem w sposób kompleksowy**:

Czerwone flagi – dokumentacja bez operacyjności: - Polityki i procedury stworzone wyłącznie pod audyt, niezrealizowane w praktyce - Brak **właścicieli procesów** – procedury nieznane pracownikom, brak odpowiedzialności operacyjnej - Zarządzanie incydentami bez **rejestru, logów, lessons learned** - Patch management bez dowodów na łatanie krytycznych podatności w terminie - **Disaster Recovery plan** nigdy nieprzetestowany operacyjnie - Polityka dostępu bez realnych kontroli i przeglądów uprawnień

Czerwone flagi – operacyjność bez dokumentacji: - Faktyczne reagowanie na incydenty, ale brak procedur, rejestru, śladów audytowych - Kupione narzędzia bezpieczeństwa bez opisanych procesów ich używania - Brak **KPI/KRI** (Key Performance/Risk Indicators) dla procesów bezpieczeństwa - Brak raportowania zarządczego – zarząd nie sprawuje nadzoru nad cyberbezpieczeństwem

Zasada kluczowa: Posiadanie polityk NIE oznacza zgodności. Realizacja procesów bez dokumentacji TEŻ nie oznacza zgodności. Wymagane są **oba elementy jednocześnie**.

5. SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI)

A. Definicja i istota SZBI

System Zarządzania Bezpieczeństwem Informacji (SZBI) to systemowe, procesowe podejście do zarządzania bezpieczeństwem informacji w organizacji – nie dokument ani zestaw dokumentów, lecz **żywy system procesów, ról, narzędzi i dokumentacji**, który funkcjonuje w cyklu ciągłego doskonalenia.

SZBI obejmuje: - **Bezpieczeństwo informacji** w szerokim rozumieniu (nie tylko cyberbezpieczeństwo) - **Bezpieczeństwo operacji OT** (Operational Technology) w podmiotach posiadających infrastrukturę przemysłową - **Bezpieczeństwo organizacyjne** – procesy HR, dostępy, onboarding/offboarding - **Bezpieczeństwo techniczne** – sieci,

systemy, aplikacje, urządzenia - **Bezpieczeństwo fizyczne** – serwerownie, miejsca przetwarzania danych - **Ciągłość działania** – plany awaryjne, backup, odtwarzanie

B. SZBI jako system procesowy – cykl Deminga (PDCA)

SZBI funkcjonuje w oparciu o **cykl PDCA** (Plan-Do-Check-Act / Planuj-Wykonaj-Sprawdź-Działaj):

- **Plan (Planuj):** Ustanowienie polityk, celów bezpieczeństwa, metodyki szacowania ryzyka, planów postępowania z ryzykami
- **Do (Wykonaj):** Wdrożenie i realizacja polityk, procedur, środków technicznych i organizacyjnych
- **Check (Sprawdź):** Monitorowanie, pomiar, audyty wewnętrzne, analiza wskaźników, przegląd zarządu
- **Act (Działaj):** Działania korygujące, doskonalenie systemu na podstawie wyników monitorowania i audytów

C. Dokumentacja SZBI – co musi istnieć

Dokumentacja SZBI nie jest celem samym w sobie, lecz **narzędziem zapewnienia powtarzalności, rozliczalności i wykazania zgodności**. Musi być: - **Utrzymywana** – na bieżąco aktualizowana - **Zidentyfikowana** – z numerem wersji, datą, właścicielem - **Aktualna** – odzwierciedlająca obecny stan organizacji i jej procesów - **Dostępna** – tylko dla osób upoważnionych (opisy zabezpieczeń technicznych nie są publiczne)

Kluczowe dokumenty SZBI:

1. **Polityka Bezpieczeństwa Informacji (PBI)** – główny dokument określający cele, zakres, zasady i odpowiedzialności
2. **Metodyka szacowania ryzyka** – opis jak organizacja identyfikuje, analizuje i ocenia ryzyka
3. **Rejestr ryzyk** – wyniki analizy ryzyka, aktualizowany minimum raz w roku
4. **Plan postępowania z ryzykiem** (Risk Treatment Plan)
5. **Deklaracja Stosowania** (Statement of Applicability – SoA) – dla organizacji stosujących ISO 27001: wykaz kontroli z Annex A z uzasadnieniem stosowania/niestosowania
6. **Procedury operacyjne bezpieczeństwa** – zarządzanie incydentami, zarządzanie dostępem, zarządzanie zmianą, zarządzanie podatnościami, backup i odtwarzanie, ciągłość działania
7. **Inwentaryzacja aktywów** – rejestr systemów, aplikacji, urządzeń, danych
8. **Wyniki audytów wewnętrznych** i działania korygujące
9. **Protokoły z przeglądów zarządu**
10. **Rejestry szkoleń** i dowody świadomości pracowników

D. Role i odpowiedzialności w SZBI

SZBI wymaga jasnego podziału ról i odpowiedzialności:

- **Zarząd / Najwyższe Kierownictwo** – odpowiedzialność za cyberbezpieczeństwo (art. 73a UoKSC), zapewnienie zasobów, określenie apetytu na ryzyko, zatwierdzanie polityk
- **Pełnomocnik ds. Bezpieczeństwa Informacji (CISO)** – zarządzanie SZBI, nadzór nad jego funkcjonowaniem, raportowanie do zarządu
- **Pełnomocnik ds. Bezpieczeństwa OT** – dla podmiotów z infrastrukturą przemysłową: ciągłość produkcji, bezpieczeństwo systemów sterowania
- **Dyrektor IT / CIO** – zarządzanie infrastrukturą IT, rola doradcza i wykonawcza
- **Compliance Officer / Dział prawny** – zgodność z wymaganiami prawnymi i regulacyjnymi, komunikacja z organami nadzoru
- **Inspektor Ochrony Danych (IOD/DPO)** – ochrona danych osobowych w kontekście bezpieczeństwa
- **Risk Manager** – zarządzanie ryzykiem korporacyjnym (w tym ryzykiem cyberbezpieczeństwa)
- **Audyt wewnętrzny** – niezależna ocena systemu (musi być organizacyjnie odrębny od CISO)
- **Właściciele aktywów** – odpowiedzialność za bezpieczeństwo konkretnych systemów i danych
- **Właściciele umów** – zarządzanie ryzykiem dostawców w obszarze swoich kontraktów

Ważne: IT i Bezpieczeństwo Informacji to **odrębne role**. IT zajmuje się funkcjonowaniem systemów; bezpieczeństwo zajmuje się ich ochroną. Połączenie tych ról w jedną osobę jest ryzykowne i może prowadzić do konfliktu interesów.

E. Co NIE jest SZBI

Kluczowe nieporozumienie na rynku: SZBI to nie jest: - Zestaw dokumentów kupiony od doradcy zewnętrznego i odłożony na półkę - System IT lub narzędzie technologiczne samo w sobie - Jednorazowy projekt z datą zakończenia - Odpowiedzialność wyłącznie działu IT

SZBI to **ciągły proces** angażujący całą organizację, wymagający zaangażowania zarządu, właścicieli procesów biznesowych, działu prawnego, IT i operacji.

6. ISO 27001 JAKO RAMA WDROŻENIOWA

A. Powiązanie ISO 27001 z UoKSC

Ustawa o Krajowym Systemie Cyberbezpieczeństwa **nie wskazuje wprost ISO 27001** jako obowiązkowego standardu. Niemniej jednak:

- Wymagania rozdziału 3 UoKSC są **w ok. 90% tożsame** z wymaganiami ISO 27001
- **Ministerstwo Cyfryzacji** prowadziło konsultacje dotyczące mapowania wymagań UoKSC na standardy międzynarodowe, w tym ISO 27001/27002 (dostępna tabela mapowania na stronie MC)
- ISO 27001 stanowi **naturalny framework** wdrożeniowy – daje konkretną strukturę, listy kontrolne i metodykę
- Organizacje posiadające **certyfikat ISO 27001** mają znaczącą przewagę w procesie dostosowania do UoKSC

Inne normy i standardy referencyjne wskazywane przez Ministerstwo: - ISO 27001/27002 (główna norma SZBI) - ISO 31000 (zarządzanie ryzykiem) - ISO 27005 (zarządzanie ryzykiem bezpieczeństwa informacji) - NIST Cybersecurity Framework (przetłumaczony na NSC – Narodowe Standardy Cyberbezpieczeństwa) - Wytyczne ENISA dotyczące NIS2 - ISA/IEC 62443 (bezpieczeństwo systemów przemysłowych OT)

B. Struktura normy ISO 27001:2022 – klauzule

ISO 27001 zbudowana jest na **10 klauzulach** (rozdziałach):

Klauzule 1-3 (wprowadzające): - Zakres - Dokumenty powołane - Terminy i definicje

Klauzule 4-10 (wymagania SZBI):

- **Klauzula 4 – Kontekst organizacji:** Analiza otoczenia wewnętrznego i zewnętrznego, zrozumienie potrzeb stron zainteresowanych, zakres SZBI
- **Klauzula 5 – Przywództwo:** Zaangażowanie kierownictwa, polityka bezpieczeństwa, role i odpowiedzialności
- **Klauzula 6 – Planowanie:** Szacowanie ryzyka, postępowanie z ryzykiem, cele bezpieczeństwa
- **Klauzula 7 – Wsparcie:** Zasoby, kompetencje, świadomość, komunikacja, dokumentacja (udokumentowana informacja)
- **Klauzula 8 – Działania operacyjne:** Planowanie i nadzorowanie operacji, ocena i postępowanie z ryzykiem
- **Klauzula 9 – Ocena wyników:** Monitoring i pomiar, audyt wewnętrzny, przegląd zarządu
- **Klauzula 10 – Doskonalenie:** Niezgodności, działania korygujące, ciągłe doskonalenie

C. Załącznik A ISO 27001:2022 – kontrole bezpieczeństwa

Aktualizacja ISO 27001 z 2022 roku przyniósł nową strukturę **Annex A** (dawniej 114 kontroli w 14 domenach, obecnie **93 kontrole w 4 tematach**):

4 tematy Annex A (ISO 27001:2022):

1. **Kontrole organizacyjne (37 kontroli)** – polityki, role, zarządzanie ryzykiem, bezpieczeństwo informacji w relacjach z dostawcami, zarządzanie incydentami, plany ciągłości działania, prawa własności intelektualnej, klasyfikacja informacji
2. **Kontrole dotyczące osób (8 kontroli)** – screening, warunki zatrudnienia, świadomość i szkolenia, dyscyplina, obowiązki po zakończeniu zatrudnienia, praca zdalna, raportowanie zdarzeń
3. **Kontrole fizyczne (14 kontroli)** – bezpieczeństwo fizyczne pomieszczeń, monitoring, zabezpieczenie sprzętu, czyszczenie nośników, polityka czystego biurka/ekranu
4. **Kontrole technologiczne (34 kontrole)** – uwierzytelnianie, prawa dostępu, ochrona przed złośliwym oprogramowaniem, zarządzanie podatnościami, kryptografia, bezpieczna konfiguracja, monitorowanie sieci, filtrowanie treści, maskowanie danych

Nowe kontrole w ISO 27001:2022 (szczególnie istotne dla NIS2): - Analiza wywiadu o zagrożeniach (Threat intelligence) - Bezpieczeństwo informacji dla usług chmurowych - Gotowość ICT na ciągłość działania - Monitorowanie bezpieczeństwa fizycznego - Zarządzanie konfiguracją - Usuwanie informacji - Maskowanie danych - Zapobieganie wyciekom danych (DLP) - Monitorowanie aktywności - Filtrowanie treści webowych

D. Podobieństwa i różnice między ISO 27001 a UoKSC/NIS2

Obszary WSPÓLNE (ISO 27001 pokrywa wymagania NIS2):

Obszar	ISO 27001	UoKSC/NIS2
Zarządzanie ryzykiem	Klauzula 6 + Annex A	Art. 8 rozdz. 3
Inwentaryzacja aktywów	Annex A 5.9	Wymagane
Zarządzanie incydentami	Annex A 5.24-5.28	Art. 20-29 UoKSC
Ciągłość działania	Annex A 5.29-5.30	Art. 8
Zarządzanie dostępem	Annex A 8.2-8.6	Art. 8
Zarządzanie podatnościami	Annex A 8.8	Art. 8
Kryptografia	Annex A 8.24	Art. 8
Świadomość i szkolenia	Klauzula 7.2-7.3	Art. 8 ust. 4
Bezpieczeństwo dostawców	Annex A 5.19-5.22	Art. 8 ust. 2 pkt 11

Kluczowe RÓŻNICE (NIS2/UoKSC wykracza poza ISO 27001):

1. **Obowiązkowe raportowanie incydentów do organów państwowych** – ISO 27001 nie ma takiego wymagania; UoKSC narzuca terminy 24h/72h i raport końcowy
2. **Odpowiedzialność osobista zarządu** – ISO 27001 wymaga “przywództwa i zaangażowania kierownictwa”, ale bez osobistych sankcji finansowych
3. **Rejestracja organizacji** – obowiązek złożenia wniosku o wpis do wykazu; ISO 27001 zna tylko certyfikację

4. **Nadzór regulatora i kontrole państwowe** – ISO 27001 nie podlega kontrolom organów państwowych; UoKSC tak
5. **System sankcji administracyjnych** – ISO 27001 grozi jedynie utratą certyfikatu; UoKSC grozi karą do 10 mln EUR lub 100 mln EUR
6. **Współpraca z CSIRTami** – wymiana informacji o zagrożeniach z organami państwowymi

Wniosek: ISO 27001 jest doskonałym fundamentem wdrożenia UoKSC. Organizacja z certyfikatem ISO 27001 ma znacząco uproszczoną drogę do zgodności. Jednak certyfikat ISO 27001 sam w sobie nie gwarantuje pełnej zgodności z UoKSC – wymagane są działania uzupełniające, szczególnie w zakresie raportowania incydentów i mechanizmów współpracy z organami.

7. ZARZĄDZANIE RYZYKIEM – METODOLOGIA, ANALIZA I POSTĘPOWANIE

A. Znaczenie zarządzania ryzykiem w systemie UoKSC

Zarządzanie ryzykiem jest **fundamentem całego SZBI**. Ustawa jasno wskazuje kolejność: **najpierw szacowanie ryzyka, potem system** – bo to wyniki analizy ryzyka powinny determinować dobór zabezpieczeń organizacyjnych i technicznych.

Brak właściwego zarządzania ryzykiem oznacza: - Brak podstaw do doboru odpowiednich środków bezpieczeństwa - System oparty na “dziurawym fundamencie” - Niespełnienie wymagań UoKSC (kara za brak wdrożenia procesu szacowania ryzyka) - Fałszywe poczucie bezpieczeństwa mimo wdrożonych narzędzi

B. Metodyka szacowania ryzyka – wymagania

Ustawa i normy referencyjne (ISO 31000, ISO 27005) wymagają, aby metodyka szacowania ryzyka:

1. **Określała sposób identyfikacji ryzyk** – co i jak identyfikujemy
2. **Definiowała kryteria oceny** – jak mierzymy prawdopodobieństwo i skutek
3. **Ustalała progi graniczne** – które ryzyka i w jaki sposób adresujemy
4. **Była powtarzalna i odtwarzalna** – inny analityk przeprowadzając ocenę metodą tą samą uzyska porównywalne wyniki
5. **Była uzasadnialna** – każdy wynik analizy ryzyka musi być możliwy do uzasadnienia

Kluczowy błąd na rynku: Wykonywanie analiz ryzyka z użyciem zautomatyzowanych narzędzi, które nie pokazują metody oceny. Ryzyko, którego nie potrafimy odtworzyć i uzasadnić, nie ma wartości zarządczej ani compliance'owej.

C. Etapy procesu zarządzania ryzykiem

Etap 1: Ustalenie kontekstu - Zakres SZBI i analiza ryzyka - Kryteria oceny ryzyka (apetyt na ryzyko, progi akceptowalności) - Metodyka

Etap 2: Identyfikacja ryzyk - Identyfikacja aktywów objętych zakresem - Identyfikacja zagrożeń i podatności - Identyfikacja możliwych skutków

Etap 3: Analiza ryzyka - Ocena prawdopodobieństwa wystąpienia - Ocena potencjalnego skutku - Obliczenie poziomu ryzyka

Etap 4: Ocena ryzyka - Porównanie z kryteriami (progami) - Priorytetyzacja ryzyk do adresowania

Etap 5: Postępowanie z ryzykiem Cztery opcje postępowania z ryzykami: - **Modyfikacja (redukcja)** – wdrożenie zabezpieczeń zmniejszających prawdopodobieństwo lub skutek - **Akceptacja** – świadoma decyzja o zaakceptowaniu ryzyka (musi być udokumentowana i zatwierdzona przez osoby uprawnione) - **Przeniesienie (transfer)** – np. ubezpieczenie, outsourcing, umowy o odpowiedzialności - **Unikanie** – rezygnacja z działania generującego ryzyko

Etap 6: Monitorowanie i przegląd - Regularna aktualizacja rejestru ryzyk (min. raz w roku lub po istotnych zmianach) - Weryfikacja skuteczności wdrożonych środków

D. Rejestr ryzyk – kluczowy dokument

Rejestr ryzyk (Risk Register) to centralny dokument procesu zarządzania ryzykiem. Organ nadzoru sprawdza: - **Czy rejestr ryzyk był aktualizowany** w ciągu ostatnich 12 miesięcy - Czy organizacja **posiada taki rejestr** - **Jaką metodę** przyjęto do analizy ryzyk - Czy **zarząd określił apetyt na ryzyko** (na jakie ryzyka jesteśmy gotowi się zgodzić)

E. Zarządzanie ryzykami prawnymi – dodatkowy wymiar

UoKSC wymaga nie tylko zarządzania ryzykami technicznymi, ale też **ryzykami prawnymi i regulacyjnymi**: - Jakie wymagania regulacyjne odnoszą się do naszej organizacji (UoKSC, RODO, sektorowe)? - Jakie wymagania nakładają kontrahenci w umowach? - Jakie konsekwencje prawne grożą za poszczególne naruszenia? - Które obszary organizacji generują najwyższe ryzyko prawne?

8. ZARZĄDZANIE INCYDENTAMI – DEFINICJA, KLASYFIKACJA, TERMINY

A. Definicja incydentu bezpieczeństwa

Incydent bezpieczeństwa w rozumieniu UoKSC to **jednostkowe lub ciągle zdarzenie**, które wpływa na: - **Integralność** danych lub systemu świadczącego usługę kluczową -

Poufność informacji przetwarzanych w ramach usługi kluczowej - **Dostępność** usługi kluczowej

Przykład: Usługą kluczową jest dostarczanie dostępu do internetu. Jeśli dostęp nagle przestaje działać, mamy zdarzenie. Proces zarządzania incydentami określa, jak ocenić, czy to awaria techniczna, atak cyberprzestępców, problem dostawcy prądu – i jak zakwalifikować to zdarzenie jako incydent lub nie.

B. Znaczenie systemu zgłaszania incydentów

Krajowy System Cyberbezpieczeństwa opiera się w znacznej mierze na **wymianie informacji o incydentach**. Cel: - Jeśli incydent wystąpił w jednym podmiocie, informacja dociera do CSIRTu - CSIRT komunikuje informację do innych podmiotów tego sektora - Inne podmioty mogą ocenić swoją podatność i podjąć działania prewencyjne - Cały system działa jak **wczesne ostrzeżenie** dla sektorów i państwa

Dlatego zgłaszanie incydentów jest **obowiązkiem prawnym** – brak zgłoszenia podlega karze.

C. Terminy zgłaszania incydentów

UoKSC określa **ściśle terminy** zgłaszania incydentów do właściwego CSIRT lub sektorowego organu nadzorczego:

Termin	Działanie	Treść
24 godziny	Wczesne ostrzeżenie	Wstępna informacja o podejrzeniu incydentu
72 godziny	Zgłoszenie incydentu	Pełna informacja, wstępna ocena skutków
30 dni	Raport końcowy	Szczegółowy opis, analiza przyczyn, podjęte działania

D. CSIRTy – struktura krajowa

W Polsce funkcjonuje system CSIRTów (Computer Security Incident Response Teams): - **CSIRT NASK** – dla podmiotów cywilnych spoza administracji publicznej - **CSIRT GOV** – dla administracji publicznej - **CSIRT MON** – dla sektora obronnego

Podmioty kluczowe i ważne zgłaszają incydenty do **właściwego CSIRTu sektorowego** lub do organu nadzorczego właściwego dla swojego sektora.

E. Proces zarządzania incydentami – co musi działać operacyjnie

Pełny proces zarządzania incydentami obejmuje:

1. **Wykrywanie** – monitoring systemów, logi, alerty bezpieczeństwa
2. **Ocena i klasyfikacja** – czy to awaria, czy incydent? Jakie jest jego znaczenie?

3. **Zawiadomienie** – wewnętrzne (osoby odpowiedzialne) i zewnętrzne (CSIRT, organ nadzorczy)
4. **Reagowanie** – izolacja, minimalizacja skutków, przywracanie usługi
5. **Dokumentacja** – rejestr incydentu, chronologia działań, decyzje
6. **Analiza po incydencie (Lessons Learned)** – co poszło nie tak, jak uniknąć w przyszłości
7. **Działania doskonalące** – wdrożenie wniosków z analizy, aktualizacja procedur

F. Cykl Deminga w zarządzaniu incydentami

Do incydentów stosuje się cykl PDCA: - **Plan**: Opracowanie procesu, procedur, planu reagowania - **Do**: Reagowanie na incydent zgodnie z procedurami - **Check**: Analiza po incydencie, ocena skuteczności reakcji - **Act**: Wdrożenie działań korygujących, zapobieganie powtórzeniu

G. Najczęstsze błędy w zarządzaniu incydentami

- **Logi zbierane, ale nikt na nie nie patrzy** – brak analizy zdarzeń bezpieczeństwa
- **Brak korelacji alertów** – narzędzia generują alerty, ale nie ma systemu ich przetwarzania
- **Procedury incydentowe na papierze, nigdy nieprzećwiczone** – procedura nieprzetestowana to procedura nieistniejąca
- **Brak rejestru incydentów** – nie wiemy, ile mieliśmy incydentów, jaki mają charakter, czy się powtarzają
- **Brak zgłoszenia do CSIRT** – poważne incydenty obsługiwane wewnętrznie bez wymaganego raportowania
- **Brak lessons learned** – incydent rozwiązany, ale bez wniosków i działań naprawczych

Scenariusz testowy: Ransomware atakuje Twoją organizację 2 maja o 2:00 w nocy. Czy wiesz, kto po kolei i co ma zrobić? Czy procedury były kiedykolwiek ćwiczzone? Czy jest lista kontaktów alarmowych? Czy wiesz, jakie systemy są najważniejsze i które przywracać w pierwszej kolejności?

9. BEZPIECZEŃSTWO OT vs IT – KLUCZOWE RÓŻNICE, ZAGROŻENIA, WYMAGANIA NIS2

A. Czym jest OT (Operational Technology)?

OT (Operational Technology) to technologie i systemy używane do sterowania procesami przemysłowymi i infrastrukturą krytyczną – w odróżnieniu od IT (Information Technology) obsługującego przetwarzanie danych biznesowych.

Przykłady systemów OT: - **SCADA** (Supervisory Control and Data Acquisition) – systemy nadzoru i akwizycji danych - **DCS** (Distributed Control Systems) – rozproszone systemy sterowania - **HMI** (Human-Machine Interface) – interfejsy operatorskie - **PLC** (Programmable Logic Controllers) – sterowniki programowalne - **Systemy sterowania energetyką, wodociągami, oczyszczalniami ścieków** - **Systemy automatyki przemysłowej w produkcji**

B. Kluczowe różnice między IT a OT

Odwrócona triada CIA

W środowiskach IT priorytet bezpieczeństwa wyrażony triadą **CIA** to: 1. **Confidentiality (Poufność)** – bezpieczeństwo komunikacji i danych 2. **Integrity (Integralność)** – zapewnienie prawdziwości i kompletności danych 3. **Availability (Dostępność)** – dostęp do zasobów

W środowiskach OT **triada CIA jest odwrócona**: 1. **Availability (Dostępność)** – ciągłość procesu jest priorytetem absolutnym; zatrzymanie produkcji jest katastrofalne 2. **Integrity (Integralność)** – poprawność nastaw i parametrów sterowania 3. **Confidentiality (Poufność)** – ważna, ale nie pierwszorzędna

Konsekwencja: W IT można zatrzymać system na czas aktualizacji. W OT **nie ma czegoś takiego jak zatrzymanie procesu na czas patchowania** – istnieją tylko zaplanowane okna serwisowe, często raz na kilka miesięcy lub rok.

Czas życia urządzeń

Wymiar	IT	OT
Typowy czas życia urządzenia	3-5 lat	20-25 lat
Wsparcie producenta	5-10 lat	Niejednoznaczne
Dług technologiczny	Umiarkowany	Bardzo wysoki
Aktualizacje bezpieczeństwa	Regularne	Trudne lub niemożliwe
Redundancja	Standard	Dopiero w nowych instalacjach

Dokumentacja

- **IT:** Dokumentacja bywa niekompletna, ale relatywnie łatwiejsza do odtworzenia
- **OT:** Systemy DCS często dostarczone jako zamknięte środowiska przez jednego producenta; dokumentacja może kończyć się na odbiorze systemu i nie być aktualizowana w trakcie eksploatacji

Specyfika sieci

- Systemy OT historycznie projektowane jako **air-gapped** (odizolowane od internetu)
- **Air-gap jest dziś mitem:** systemy rozrastają się, dostawcy uzyskali zdalne dostępy serwisowe (szczególnie w czasie COVID), integracja z sieciami korporacyjnymi IT postępuje
- Producenci DCS dostarczają **hermetyczne środowiska** – ingerencja zewnętrzna grozi utratą gwarancji, ale stwarza też hermetyczność podatności

C. Zagrożenia dla systemów OT

Motywacje atakujących

W odróżnieniu od IT, gdzie dominuje motyw finansowy (ransomware, kradzież danych), w atakach na OT wyróżnia się:

1. **Sabotaż państwowy / wojna hybrydowa** – sponsorowane przez obce rządy ataki mające na celu destabilizację gospodarki, wzbudzenie paniki, demonstrację siły
2. **Szpiegostwo przemysłowe** – kradzież własności intelektualnej, tajemnic technologicznych
3. **Wymuszenie** – zajęcie kontroli nad infrastrukturą krytyczną dla uzyskania korzyści finansowych
4. **Testowanie odporności** – wiele obserwowanych ataków ma charakter zwiadowczy: sprawdzenie jak głęboko można wejść, jak szybko obrońcy reagują

Typowy scenariusz ataku na OT

1. Uzyskanie dostępu do systemu zewnętrznego (często przez słabo zabezpieczone zdalnych dostępy serwisowe lub sieci IT)
2. Lateral movement – przemieszczanie się po sieci w kierunku systemów SCADA/DCS
3. Próba modyfikacji nastaw sterowania (zmiana parametrów procesu – reaktora biologicznego, turbiny, zaworu ciśnieniowego)
4. Skutki: zatrzymanie produkcji, uszkodzenie urządzeń, zagrożenie bezpieczeństwa ludzi

Realne incydenty (typowe wzorce dla Polski)

- **Oczyszczalnie ścieków:** uzyskanie dostępu do paneli sterowania, próba zmiany parametrów reaktorów biologicznych
- **Elektrownie wodne:** próba zmiany nastaw turbin
- **Systemy energetyczne:** nieuprawnione połączenia z systemami sterowania
- Charakterystyczny wzorzec: **modyfikacja nastaw** a nie wyłączenie systemu – celem jest wzbudzenie niepewności, a nie natychmiastowe unieruchomienie

Wektory ataku specyficzne dla OT

- **Słabe hasła / brak MFA:** systemy OT projektowane bez potrzeby uwierzytelniania wieloskładnikowego (produkcja 24/7, zmianowy operator musi działać szybko)
- **Współdzielone konta operatorskie:** brak rozliczalności – jeśli wszyscy używają jednego konta, po incydencie nie wiadomo kto i kiedy dokonał zmiany
- **Niezabezpieczone zdalne dostępy:** serwisanci pozostawili dostępy VPN/RDP dla wygody serwisowania zdalnego
- **Urządzenia legacy bez aktualizacji:** systemy sprzed 15-20 lat z niezaktualizowanymi podatnościami
- **Brak segmentacji sieci:** bezpośrednie połączenie IT-OT bez firewalla segmentacyjnego

D. Norma ISA/IEC 62443 – standard bezpieczeństwa OT

ISA/IEC 62443 to wiodąca norma bezpieczeństwa dla systemów przemysłowych i SCADA. W odróżnieniu od ISO 27001 **nie jest normą certyfikowaną** (nie można uzyskać formalnego certyfikatu), jednak: - Jest szeroko stosowana przez producentów systemów DCS/SCADA - Definiuje koncepcję **Security Level** (poziomów bezpieczeństwa) dla różnych stref sieci OT - Stanowi podstawę do projektowania bezpiecznych sieci przemysłowych - Jej wymagania są komplementarne do ISO 27001 i NIS2

Kluczowe koncepcje IEC 62443: - **Strefy i kanały (Zones & Conduits):** segmentacja sieci OT na strefy o różnych poziomach bezpieczeństwa - **Security Level (SL):** 4 poziomy bezpieczeństwa przypisywane do stref - **Wymagania dla komponentów:** producenci komponentów OT mogą certyfikować produkty pod kątem IEC 62443

E. Wpływ NIS2/UoKSC na środowiska OT

NIS2 i UoKSC wywołały **konkretne zmiany w podejściu do bezpieczeństwa OT:**

- Działy automatyki i IT, które dotychczas działały w separacji, **muszą teraz współpracować** – biznes wymaga wspólnego zarządzania cyberbezpieczeństwem po obu stronach
- Wymagana jest **rozliczalność** – monitorowanie zasobów i infrastruktury po stronie OT i IT na porównywalnym poziomie
- NIS2 wskazuje **odpowiedzialność osób** za bagatelizację kwestii cyberbezpieczeństwa, w tym w sektorze przemysłowym
- NIS2 rozszerza zakres bezpieczeństwa poza samo cyberbezpieczeństwo – obejmuje też **bezpieczeństwo środowiskowe** i monitoring danych obszarów przetwarzania informacji

F. Rekomendacje dla bezpieczeństwa OT – podejście krok po kroku

Krok 1: Widoczność – inwentaryzacja aktywów OT

Fundamentem jest wiedza o tym, co się chroni. Przed wdrożeniem jakichkolwiek zabezpieczeń konieczne jest: - Przeprowadzenie **audytu inwentaryzacyjnego** (ręcznego lub z narzędziem skanującym) - Zidentyfikowanie wszystkich urządzeń: sterowniki PLC, panele HMI, serwery SCADA, przełączniki sieciowe - Określenie **krytyczności** każdego zasobu (wymagana współpraca z automatykami, szefami utrzymania ruchu) - Zrozumienie **topologii sieci** i punktów połączeń IT-OT

Paradoks OT: Nawet dobry automatyk często nie wie, jakie systemy działają “pod spodem” jego stacji HMI. Producent DCS dostarcza zamknięte środowisko i nie ma dokumentacji wewnętrznych połączeń.

Krok 2: Segmentacja i segregacja sieci

Na podstawie normy IEC 62443: - **Segmentacja logiczna** – VLAN-y, firewalle między strefami - **Segmentacja fizyczna** – oddzielne przełączniki, okablowanie dla stref

krytycznych - **Mikrosegmentacja** – granularne reguły komunikacji między urządzeniami w obrębie strefy - Jasne określenie, co może komunikować się z czym – i blokowanie wszystkiego innego

Krok 3: Systemy monitorowania

Monitoring jest **absolutnym minimum dla OT** – nawet jeśli aktywne blokowanie jest niemożliwe ze względu na ryzyko zakłócenia procesów: - **NDR (Network Detection and Response)** dedykowane do sieci OT - Systemy **IDS** z sygnaturami dla protokołów przemysłowych (Modbus, DNP3, IEC 60870) - Anomaly detection – wykrywanie odchyłeń od normalnych wzorców komunikacji - Monitorowanie połączeń z zewnątrz (zdalny dostęp serwisantów)

Krok 4: PAM (Privileged Access Management)

PAM to systemy zarządzania dostępem uprzywilejowanym – szczególnie istotne w OT: - Pełna wiedza o tym, **kto, kiedy i co zmienił** w systemach sterowania - Nagrywanie sesji zdalnych serwisantów - Możliwość **rollbacku** – jeśli coś przestaje działać, wiemy jaką zmianę cofnąć - Rozwiązanie problemu współdzielonych kont operatorskich

Krok 5: Uwierzytelnianie

- Eliminacja domyślnych haseł lub haseł prostych
- Tam gdzie to możliwe: **MFA** (klucze fizyczne, tokeny, karty zbliżeniowe)
- Alternatywa dla OT: **klucze sprzętowe** (pendrive z certyfikatem) – kompromis między bezpieczeństwem a ergonomią operatora

Krok 6: Świadomość personelu OT

Automatycy muszą być traktowani jak użytkownicy systemów IT w zakresie: - Szkoleń z cyberbezpieczeństwa - Procedur związanych z phishingiem - Zasad używania nośników zewnętrznych (pendrive) - Rozumienia, dlaczego nowe mechanizmy bezpieczeństwa są potrzebne

Krok 7: Plan reagowania na incydenty

Dla OT plan reagowania musi uwzględniać: - Wiedzę o tym, jakie systemy są krytyczne dla usługi kluczowej - Procedury separacji zaatakowanego segmentu bez zatrzymania całości - Role i odpowiedzialności dla IT i automatyków - Priorytety odtwarzania

10. CIĄGŁOŚĆ DZIAŁANIA (BCP/DRP) – WYMAGANIA, PLANY, TESTOWANIE

A. Wymagania UoKSC w zakresie ciągłości działania

Ciągłość działania jest jednym z **kluczowych wymagań** zarówno NIS2/UoKSC, jak i ISO 27001 (Annex A 5.29-5.30). Ustawa wymaga wdrożenia środków zapewniających ciągłość usługi kluczowej, w tym:

- **Planu Ciągłości Działania (BCP – Business Continuity Plan)**
- **Planu Odtwarzania po Awarii (DRP – Disaster Recovery Plan)**
- **Zarządzania kryzysowego** – procedur na wypadek poważnych incydentów
- **Regularnego testowania planów**

B. BCP vs DRP – różnica

BCP (Business Continuity Plan): - Obejmuje cały biznes - Określa jak organizacja funkcjonuje w sytuacji awaryjnej - Dotyczy procesów biznesowych, nie tylko IT - Zawiera procedury alternatywnych sposobów działania

DRP (Disaster Recovery Plan): - Skupia się na odtworzeniu systemów IT/OT - Określa kolejność przywracania systemów - Zawiera konkretne cele: RTO (Recovery Time Objective), RPO (Recovery Point Objective) - Zawiera procedury techniczne odtwarzania

C. Backup – wymagania i najczęstsze błędy

Zasada 3-2-1

Standardem branżowym dla kopii zapasowych jest **reguła 3-2-1**: - 3 kopie danych (oryginał + 2 kopie) - 2 różne nośniki/media (np. dysk + taśma, lub dysk + chmura) - 1 kopia przechowywana **offline** (odizolowana od sieci)

Dlaczego kopia offline jest krytyczna?

Scenariusz ransomware: szyfrowanie ogarnia środowisko produkcyjne. Jeśli backup jest podłączony do tej samej sieci i uwierzytelnia się przez te same systemy (np. Active Directory), zostanie zaszyfrowany razem z resztą. **Backup bez kopii offline może być niedostępny dokładnie wtedy, gdy jest potrzebny.**

Testowanie backupu

Nieprzetestowany backup to backup nieistniejący – to zasada obowiązująca w branży. Organ nadzorczy i audytorzy pytają: - Kiedy ostatnio testowano **odtworzenie danych** z backupu? - Czy istnieje dokumentacja (protokół) z testu odtworzenia? - Czy test obejmował kluczowe systemy wspierające funkcje biznesowe?

Podejście praktyczne: - Zaczynj od **najważniejszych systemów** – nie musisz od razu testować wszystkiego - Dokumentuj każdy test – nawet częściowy test z dokumentacją jest lepszy niż brak testów - Zwiększaj zakres stopniowo

Rejestr w katalogu: większość firm MA backup

W praktyce prawie każda organizacja ma jakieś backupy. Problem nie polega na ich braku, lecz na: - Braku zasady 3-2-1 (szczególnie brak kopii offline) - Braku testów odtworzeniowych - Braku dokumentacji potwierdzającej jakość i funkcjonalność backup - Czasie odtworzenia niezgodnym z celami RTO

D. Plan ciągłości działania – co musi zawierać

Skuteczny plan ciągłości działania (BCP/DRP) powinien zawierać:

1. **Analizę wpływu na biznes (BIA – Business Impact Analysis):** Które procesy są krytyczne? Jaki jest maksymalny dopuszczalny czas przerwy?
2. **Cele RTO i RPO** dla każdego systemu krytycznego
3. **Listę kluczowych systemów** i kolejność odtwarzania (priorytetyzacja)
4. **Procedury przełączenia** do środowiska zapasowego
5. **Role i odpowiedzialności** (kto co robi w sytuacji kryzysowej)
6. **Listę kontaktów awaryjnych** (wewnętrzne, dostawcy, organy)
7. **Procedury komunikacyjne** (jak informować pracowników, klientów, media)
8. **Harmonogram testowania** i wyniki testów

E. Katastrofa w OT – szczególny wymiar

W środowiskach przemysłowych ciągłość działania ma **dodatkowy wymiar finansowy i fizyczny**: - Zatrzymanie produkcji przemysłowej ma bezpośredni, mierzalny koszt (koszt przestoju x godzina) - W IT ten koszt jest trudniej policzalny i często bagatelizowany - W OT koszty przestoju są łatwiej kalkulowane, ale rzadko uwzględniane w planach bezpieczeństwa - Uszkodzenie fizycznych urządzeń (turbina, reaktor) może mieć skutki nieodwracalne

11. ŁAŃCUCH DOSTAW – WYMAGANIA BEZPIECZEŃSTWA WOBEC DOSTAWCÓW

A. Dlaczego bezpieczeństwo łańcucha dostaw jest kluczowe

Kluczowe obserwacje: - Środowisko IT współczesnej organizacji składa się z setek, czasem tysięcy wzajemnie powiązanych usług i produktów - **Wzrost incydentów, których źródłem były strony trzecie (vendorzy, dostawcy)** – jest wyraźnie zauważalny w ostatnich latach - Organizacja jest tak bezpieczna, jak jej **najsłabszy dostawca** - Atak na

SolarWinds (oprogramowanie do zarządzania siecią) dotknął tysiące organizacji klientów – złośliwy kod był dystrybuowany jako legalna aktualizacja

B. Wymagania UoKSC w zakresie łańcucha dostaw

Ustawa nakłada obowiązek **zarządzania bezpieczeństwem łańcucha dostaw**, w tym: - Ocenę ryzyka związanego z dostawcami i podwykonawcami - Weryfikację poziomu bezpieczeństwa dostawców (szczególnie tych z dostępem do sieci lub danych) - Wprowadzenie **wymagań bezpieczeństwa** w umowach z dostawcami - Monitorowanie zgodności dostawców z wymaganiami

C. Praktyczne podejście do zarządzania ryzykiem dostawców (TPRM)

TPRM (Third Party Risk Management) – zarządzanie ryzykiem stron trzecich:

Kategoryzacja dostawców

Nie każdy dostawca wymaga takiej samej głębokości weryfikacji. Kategoryzacja według: - Dostęp do sieci korporacyjnej (tak/nie) - Ilość przetwarzanych danych (i ich wrażliwość) - Reputacja rynkowa i historia bezpieczeństwa - Wielkość firmy i zasoby przeznaczone na bezpieczeństwo

Dostawcy z certyfikatem ISO 27001 lub SOC 2 mogą być traktowani z niższym poziomem weryfikacji (certyfikat nadaje wiarygodność).

Minimalne wymagania bezpieczeństwa dla dostawców

Przed wysyłaniem ankiet z setkami pytań (co jest standardem rynkowym, ale mało efektywnym), warto sprawdzić minimum: - Czy dostawca stosuje **MFA**? - Czy ma **procesy patchowania** i zarządzania podatnościami? - Czy **szyfruje dane** (w transit i at rest)? - Czy ma politykę i procedury bezpieczeństwa? - Czy miał incydenty bezpieczeństwa (i jak reagował)?

Środki umowne

W umowach z dostawcami powinny znaleźć się: - Wymagania dotyczące poziomu bezpieczeństwa - Obowiązek powiadamiania o incydentach bezpieczeństwa w określonym terminie - Prawo do przeprowadzenia audytu u dostawcy - Klauzule o ciągłości działania - Wymagania wobec podwykonawców dostawcy (sub-processory)

D. Pozycja rynkowa a łańcuch dostaw

Jeśli Twoja organizacja świadczy usługi dla podmiotów kluczowych lub ważnych: - Możesz **nie podlegać bezpośrednio** pod UoKSC (nie spełniasz progów lub działasz w innym sektorze) - Ale Twoi klienci będą **wymagać od Ciebie** spełnienia standardów analogicznych do UoKSC - Presja łańcucha dostaw może być **silniejsza i szybsza** niż kontrole organów państwowych - Warto traktować to jako **ryzyko regulacyjne i biznesowe** i wdrożyć SZBI proaktywnie

12. AUDYTY SZBI – WEWNĘTRZNE, ZEWNĘTRZNE, PRZEGLĄD ZARZĄDU

A. Audyt wewnętrzny SZBI

Audyt wewnętrzny jest obowiązkowym elementem każdego poprawnie funkcjonującego SZBI. Cel audytu wewnętrznego:

1. **Ocena funkcjonowania systemu** – czy SZBI działa zgodnie z założeniami?
2. **Identyfikacja niezgodności** – co nie działa tak jak powinno?
3. **Ocena skuteczności zabezpieczeń** – czy wdrożone środki faktycznie ograniczają ryzyko?
4. **Identyfikacja luk** – niedociągnięcia w realizacji planów postępowania z ryzykiem
5. **Weryfikacja**, czy to co jest na papierze, istnieje w praktyce

Audytor wewnętrzny – wymagania

- Musi być **niezależny** od obszaru, który audytuje (nie może audytować własnej pracy)
- Powinien posiadać **kompetencje** w zakresie SZBI i standardów
- Może być pracownikiem organizacji (z innego działu) lub zewnętrznym audytorem

Co audyt wewnętrzny bada?

- Zgodność z **wymaganiami prawnymi** (UoKSC, RODO)
- Zgodność z **normą ISO 27001** (jeśli organizacja stosuje tę normę)
- Zgodność z **własnymi politykami i procedurami** organizacji
- Efektywność **kontroli bezpieczeństwa**

Kluczowa zasada: Audyt wewnętrzny bada, czy to co organizacja opisała w swoich dokumentach jako to jak ma działać, faktycznie tak działa. Kryterium audytu to własne procedury organizacji.

B. Obowiązkowy audyt zewnętrzny (podmioty kluczowe)

Art. 15 UoKSC: Podmioty kluczowe przeprowadzają **na własny koszt** audyt bezpieczeństwa systemu informacyjnego: - **Pierwszy audyt:** do 3 kwietnia 2028 (24 miesiące od wejścia w życie ustawy) - **Kolejne audyty:** co najmniej raz na **3 lata** - Audyt dotyczy systemu informacyjnego **wykorzystywanego w procesie świadczenia usługi**

Audyt zewnętrzny przeprowadza **niezależny podmiot zewnętrzny** (certyfikowany audytor, firma audytorska).

C. Przegląd zarządu

Przegląd zarządu to wymagany przez ISO 27001 (klauzula 9.3) i pośrednio przez UoKSC mechanizm zapewnienia nadzoru najwyższego kierownictwa nad SZBI.

Co obejmuje przegląd zarządu? - Wyniki audytów wewnętrznych - Wyniki monitorowania i pomiarów (KPI/KRI) - Zmiany w kontekście organizacji i wymaganiach stron zainteresowanych - Postęp w realizacji celów bezpieczeństwa - Informacja o incydentach i podatnościach - Informacje zwrotne od stron zainteresowanych - Możliwości doskonalenia

Typowy błąd: Zarząd nie jest angażowany w cyberbezpieczeństwo. Raporty nie trafiają do zarządu lub trafiają w formie niezrozumiałej. Zarząd nie określił apetytu na ryzyko.

Sygnal dla organu nadzorczego: Brak protokołów z przeglądów zarządu lub brak raportowania do zarządu to bezpośrednia podstawa do stwierdzenia niezgodności.

D. Najczęstsze ustalenia audytowe – TOP 5 obszarów niezgodności

1. Zarządzanie podatnościami i patch management

- Brak centralnej inwentaryzacji aktywów
- Brak priorytetyzacji podatności według krytyczności
- Krytyczne podatności łatanie z tygodniowym, miesięcznym lub wieloletnim opóźnieniem
- Brak SLA dla procesu wdrażania poprawek
- Systemy End-of-Life (EoL) bez planu migracji lub kompensacyjnych środków

2. Zarządzanie dostępem i tożsamością

- **Konta współdzielone** – wielu użytkowników, jedno konto; brak rozliczalności
- **Konta sieroty (orphan accounts)** – konta byłych pracowników nieusunięte miesiącami, latami; rekord: 8000 kont nieusuwanym przez 3 lata
- Brak **MFA** dla systemów krytycznych i zdalnego dostępu
- **Zbyt szerokie uprawnienia** – pracownicy mają dostęp do systemów, których nie potrzebują
- Brak **przeglądów uprawnień** (recertyfikacja dostępów)
- Konta administracyjne używane do codziennej pracy

3. Monitoring i wykrywanie incydentów

- Logi zbierane, ale **nieanalizowane** – nikt na nie nie patrzy
- Brak **korelacji zdarzeń** bezpieczeństwa
- Brak procedur: co robić gdy alert zostanie wygenerowany?
- Incydenty wykrywane po tygodniach lub miesiącach
- O incydentach dowiadujemy się od klientów lub z mediów

4. Backup i Disaster Recovery

- Backup nie spełniający zasady **3-2-1** (brak kopii offline)
- **Nieprzetestowany backup** – żaden test odtworzeniowy nigdy nie był przeprowadzony
- Plan DR napisany, ale **nigdy nieweryfikowany operacyjnie**
- Brak protokołów z testów odtworzeniowych
- Backup dostępny przez ten sam system uwierzytelniania co produkcja (ryzyko zaszyfrowania razem z produkcją)

5. Bezpieczeństwo łańcucha dostaw

- Brak **rejestru dostawców** z dostępem do systemów/danych
- Brak **oceny bezpieczeństwa** dostawców przed nawiązaniem współpracy
- Brak **wymagań bezpieczeństwa** w umowach z dostawcami
- Brak monitorowania dostawców po zawarciu umowy
- Nieweryfikowane podwykonawstwo (dostawca korzysta z podwykonawców nieznanych organizacji)

13. SANKCJE I KARY – POZIOMY KAR I ODPOWIEDZIALNOŚĆ KIEROWNICTWA

A. Katalog kar pieniężnych (art. 73 UoKSC)

Kary pieniężne nakładane są za: - Brak uzupełnienia/korekty danych w wykazie pomimo wezwania - **Brak systematycznego szacowania ryzyka** lub zarządzania ryzykiem - **Brak wdrożonego SZBI** - Brak realizacji obowiązku opracowania, stosowania i aktualizowania dokumentacji bezpieczeństwa (art. 10 ust. 1) - Brak zgłoszenia incydentu do właściwego CSIRT - Brak postępowania z incydentem zgodnie z procedurami - Wiele innych naruszeń z katalogu ustawy

B. Wysokość kar – tabela

Podmiot	Maksymalna kara
Podmiot kluczowy	10 milionów EUR lub 2% łącznego rocznego przychodu (wyższa z kwot)
Podmiot ważny	7 milionów EUR lub 1,4% łącznego rocznego przychodu (wyższa z kwot)
Szczególny przypadek (poważne zagrożenie dla bezpieczeństwa państwa, życia i zdrowia ludzi)	100 milionów EUR (art. 73 ust. 5)

C. Odpowiedzialność osobista kierownictwa (art. 73a UoKSC)

To **rewolucyjna zmiana** w polskim ustawodawstwie z zakresu cyberbezpieczeństwa. Kara pieniężna może być nałożona na **kierownika podmiotu kluczowego lub ważnego** (prezesa zarządu, dyrektora, członka organu zarządzającego) gdy:

- Podmiot naruszył przepisy ustawy
- Naruszenie wynikało z **zaniechania obowiązków kierowniczych**

Wysokość kary dla kierownika: - Do **300% wynagrodzenia** – sektor prywatny - Do **100% wynagrodzenia** – sektor publiczny

Kluczowy przekaz: Kara nie ogranicza się do spółki. Prezes, dyrektor, właściciel – jeśli zaniedbali swoje obowiązki w zakresie cyberbezpieczeństwa, odpowiadają osobiście finansowo. To sprawia, że cyberbezpieczeństwo staje się zagadnieniem zarządczym najwyższego szczebla.

D. Odroczenie kar – grace period

Kary administracyjne mogą być nakładane dopiero po 2 latach od wejścia w życie ustawy (od 3 kwietnia 2028), z wyjątkiem kary za bezpośrednie i poważne cyberzagrożenie dla wartości konstytucyjnych (ta może być nałożona wcześniej, bez odroczenia).

Interpretacja grace period: - Odroczenie NIE zwalnia z obowiązku wdrożenia w ciągu 12 miesięcy - Kara po 2 latach może obejmować **cały okres niedostosowania** (między 12. a 24. miesiącem) - Ministerstwo Cyfryzacji deklaruje przychylne podejście do podmiotów **faktycznie działających** w kierunku wdrożenia - Grace period to szansa na korektę, nie na bezczynność

E. Kontrole i nadzór

Organy nadzorcze (właściwe sektorowo, np. UKE dla sektora telekomunikacyjnego, URE dla energetyki) będą przeprowadzać **kontrole podmiotów kluczowych i ważnych**.

Co sprawdza organ nadzoru podczas kontroli? Na podstawie doświadczeń z analogicznych regulacji (np. DORA – Digital Operational Resilience Act dla sektora finansowego), kontrolerzy pytają m.in.:

- Kiedy ostatnio testowano **odtworzenie danych** z backupu? Czy jest dokumentacja?
 - Czy rejestr ryzyk był **aktualizowany** w ciągu ostatnich 12 miesięcy?
 - Czy zarząd **otrzymuje regularne raporty** z zakresu cyberbezpieczeństwa?
 - Jak długo trwa łatanie **krytycznych podatności**? Gdzie opisano procesy?
 - Czy przeprowadzono **szkolenia** i czy pracownicy mogą wykazać posiadanie kompetencji?
 - Jak weryfikowano **bezpieczeństwo dostawców**? Czy przeprowadzono audyty u dostawców?
-

14. PLAN DZIAŁANIA DLA ORGANIZACJI – PRIORYTETY, KROKI WDROŻENIOWE, REKOMENDACJE

A. Model skutecznego wdrożenia – 9 kroków

Krok 1: Identyfikacja obowiązków

- Ustalenie, czy podmiot podlega pod UoKSC (samoidentyfikacja)
- Zrozumienie pełnego zakresu wymagań prawnych, umownych, regulacyjnych
- Określenie wszystkich obowiązujących aktów prawnych i norm

Krok 2: Analiza luki (Gap Analysis)

- Ocena aktualnego stanu bezpieczeństwa vs. wymagania UoKSC
- Identyfikacja, co już mamy (każda organizacja ma coś w obszarze bezpieczeństwa)
- Zidentyfikowanie, co wymaga poprawy, uzupełnienia lub stworzenia od nowa
- **Punkt startowy każdego projektu wdrożeniowego** – bez niego planowanie jest niemożliwe

Krok 3: Governance i role (ład organizacyjny)

- Wyznaczenie właścicieli procesów bezpieczeństwa
- Struktura odpowiedzialności (CISO lub odpowiednik, role w SZBI)
- Zaangażowanie zarządu – definicja apetytu na ryzyko, struktura raportowania
- Powołanie osoby kontaktowej ds. cyberbezpieczeństwa (wymagane przez UoKSC)

Krok 4: Procesy operacyjne

- Opracowanie i wdrożenie polityk, procedur i instrukcji bezpieczeństwa
- Dostosowanie dokumentacji do faktycznych procesów organizacji
- Zapewnienie, że procedury są znane pracownikom (właściciele procesów)

Krok 5: Środki techniczne

- Wdrożenie zabezpieczeń technicznych wynikających z analizy ryzyka
- Inwentaryzacja aktywów (CMDB, asset management)
- MFA dla krytycznych systemów i dostępu zdalnego
- Segmentacja sieci
- Zarządzanie podatnościami (scanner + procesy łatania)
- Backup z kopią offline, zasada 3-2-1
- Monitoring i wykrywanie incydentów

Krok 6: Monitoring i KPI

- Wdrożenie mierników skuteczności procesów bezpieczeństwa (KPI/KRI)
- Dashboard bezpieczeństwa dla zarządu
- Monitorowanie wskaźników incydentów, podatności, dostępów

Krok 7: Testowanie i audyty

- Regularne testy odtworzeniowe systemów backup/DR
- Testy penetracyjne infrastruktury krytycznej
- Ćwiczenia z procedur reagowania na incydenty (tabletop exercises)
- Audyty wewnętrzne SZBI

Krok 8: Zarządzanie dowodami

- Zbieranie i archiwizacja śladów audytowych
- Dokumentowanie wyników procesów bezpieczeństwa (lessons learned, analizy)
- Prowadzenie rejestrów (incydentów, ryzyk, dostępów, szkoleń)

Krok 9: Ciągłe doskonalenie

- Doskonalenie systemu na podstawie wyników audytów i zmian ryzyka
- Aktualizacja metodyki szacowania ryzyka
- Reagowanie na nowe zagrożenia i zmiany w otoczeniu
- Regularne przeglądy zarządu

B. Priorytety – TOP 5 działań wysokiego priorytetu (quick wins)

Na podstawie analizy najczęstszych niezgodności i doświadczeń wdrożeniowych:

1. Inwentaryzacja aktywów – absolutny fundament

Jeśli nie wiesz co posiadasz, nie możesz tego chronić. Centralna inwentaryzacja aktywów (CMDB lub nawet dobrze prowadzony arkusz Excel na początek): - Lista wszystkich systemów, aplikacji, urządzeń - Klasyfikacja według krytyczności dla usług kluczowych - Identyfikacja systemów End-of-Life i planów migracji

Analogia: Inwentaryzacja aktywów to jak tabliczka mnożenia w matematyce. Bez niej nie ma szans na dobre wyniki na maturze. Jeśli nie wiemy co mamy, nie wiemy gdzie jesteśmy podatni, gdzie może nastąpić incydent i jak priorytetyzować działania.

2. MFA i kontrola dostępu – quick win wysokiego wpływu

MFA (Multi-Factor Authentication) wdrożone dla kluczowych systemów i zdalnego dostępu: - Stosunkowo niski koszt i czas wdrożenia - **Znaczące zamknięcie ryzyk** związanych z przejęciem kont i nieautoryzowanym dostępem - Zaczynij od systemów najkrytyczniejszych: VPN, aplikacje biznesowe kluczowe, AD, systemy administracyjne - Równolegle: przegląd i usunięcie kont sierocych, eliminacja kont współdzielonych

3. Vulnerability Management – zarządzanie podatnościami

- Jeśli masz skaner – używaj go (wiele organizacji ma narzędzie i go nie używa)
- Ustanów **proces priorytetyzacji** – skupi się na podatnościach krytycznych wystawionych na internet

- Zdefiniuj **SLA dla łatania** – ile czasu masz na zamknięcie podatności danego poziomu (np. krytyczne: 7 dni, wysokie: 30 dni)
- Systemy Legacy i EoL: zaplanuj co z nimi robić, nie zostawiaj “na zawsze zapomniane”

4. Monitoring sieci i środowisk

- Zaczynij nie od pełnoprawnego SOC 24/7, lecz od podstaw: **centralizacja logów**
- Zrozumienie co się dzieje w logach (korelacja zdarzeń)
- Procedury co robić gdy log wskazuje na zagrożenie
- Monitorowanie End-pointów i sieci

5. Backup i testy odtworzeniowe – zasada 3-2-1

- Weryfikacja, czy backup spełnia zasadę 3-2-1 (szczególnie kopię offline)
- Zaplanowanie pierwszego testu odtworzeniowego od kluczowych systemów
- Dokumentowanie wyników testów
- Zapewnienie, że backup nie uwierzytelnia się przez te same systemy co produkcja

C. Plan czasowy 90 dni – pierwsze kroki

Dni 1-30: Rozpoznanie i planowanie - Przeprowadzenie analizy luki (gap analysis) - Identyfikacja obowiązków prawnych - Wyznaczenie ról i odpowiedzialności - Zinwentaryzowanie istniejących polityk i procedur

Dni 31-60: Fundamenty - Uruchomienie inwentaryzacji aktywów - Wdrożenie MFA dla krytycznych systemów - Pierwsza analiza podatności kluczowych systemów - Opracowanie lub aktualizacja polityki bezpieczeństwa informacji

Dni 61-90: Procesy operacyjne - Wdrożenie / aktualizacja procesu zarządzania incydentami - Pierwsze testy odtworzeniowe backupu - Szkolenie kluczowych pracowników - Opracowanie planu dalszego wdrożenia (roadmap 12 miesięcy)

D. Modele organizacyjne wdrożenia

Zasoby wewnętrzne vs. zewnętrzne

Nie ma jednej odpowiedzi. Modelem który najczęściej się sprawdza jest **model hybrydowy**: - **Wewnętrznie**: osoba nadzorująca SZBI, właściciele procesów biznesowych, znajomość organizacji - **Zewnętrznie**: eksperci dziedzinowi (prawni, techniczni, audytorzy) uzupełniający luki kompetencyjne

Kiedy zasoby wewnętrzne wystarczają: Duże organizacje z rozbudowanymi działami IT, bezpieczeństwa i compliance – mogą poradzić sobie samodzielnie, ewentualnie korzystając z zewnętrznego spojrzenia na audyt.

Kiedy niezbędna pomoc zewnętrzna: Mała organizacja z jednym człowiekiem do obsługi IT, brak doświadczeń z SZBI, krótkie terminy.

Czego szukać w partnerze wdrożeniowym

- Interdyscyplinarne kompetencje (prawo + technologia)
- Doświadczenie z realnym wdrożeniem (nie tylko sprzedaż dokumentów)
- Podejście “razem robimy” a nie “my robimy za was”
- **Red flag:** Partner, który mówi, że wdroży NIS2 w miesiąc lub że klient nic nie musi robić

Co NIE istnieje

- Magiczna dokumentacja za 500 zł do pobrania i odłożenia na półkę
- Magiczny system z pieczętką “zgodny z NIS2” który załatwi wszystko
- Firma zewnętrzna, która wykona całe wdrożenie bez zaangażowania klienta
- Certyfikat ISO 27001 = automatyczna zgodność z UoKSC (ułatwia, ale nie zastępuje)

PODSUMOWANIE – KLUCZOWE WNIOSKI

1. NIS2/UoKSC to nie projekt, to proces

Wdrożenie SZBI nie jest projektem z datą zakończenia. To **trwała zmiana sposobu zarządzania bezpieczeństwem** organizacji. System musi żyć, być aktualizowany, auditowany i doskonalony.

2. Dokumentacja i operacyjność – oba elementy są niezbędne

Dokumentacja bez operacyjności = iluzja zgodności. Operacyjność bez dokumentacji = brak wykazywalności zgodności. Organ nadzoru ocenia zdolność organizacji do zarządzania cyberbezpieczeństwem – nie samą jakość dokumentów.

3. Odpowiedzialność zarządu jest realna i osobista

UoKSC wprowadza kary nie tylko dla organizacji jako całości, ale też **osobistą odpowiedzialność finansową** dla kierownictwa. Cyberbezpieczeństwo musi być agendą zarządu, nie tylko działu IT.

4. Czas jest krótki, ale wymagania są realne

12 miesięcy na pełne wdrożenie to krótki czas dla organizacji większych lub z dużym długiem technologicznym. Jednak same wymagania są osiągalne – przy odpowiednim planowaniu, priorytetyzacji i zaangażowaniu.

5. ISO 27001 to najlepszy framework dla UoKSC

Nie jest obowiązkowy, ale stanowi naturalną ramę wdrożeniową pokrywającą ~90% wymagań UoKSC. Organizacje certyfikowane mają znaczącą przewagę.

6. OT jest dziś równoważne IT w zakresie wymagań NIS2

Środowiska przemysłowe (OT) przez lata były poza zakresem wymagań cyberbezpieczeństwa. NIS2 zmienia to fundamentalnie – i stanowi największe wyzwanie dla sektorów energetyki, produkcji, wodociągów i transportu.

7. Bezpieczeństwo łańcucha dostaw dotyczy wszystkich

Nawet jeśli Twoja organizacja nie jest bezpośrednio objęta UoKSC, Twoi klienci będą wymagać zgodności. “Twoja organizacja jest tak bezpieczna, jak jej najsłabszy dostawca” – to zasada, która w erze NIS2 stała się wymaganiem prawnym.

8. Zaczynij od analizy luki – to fundament wszystkiego

Przed jakimikolwiek działaniami wdrożeniowymi konieczna jest analiza luki (gap analysis). Bez niej nie da się zaplanować realistycznego programu wdrożeniowego ani efektywnie alokować zasobów.

Niniejszy dokument stanowi opracowanie informacyjne na podstawie dostępnych materiałów szkoleniowych i webinarów eksperckich. Nie stanowi porady prawnej. W kwestiach interpretacji przepisów należy konsultować się z prawnikiem specjalizującym się w prawie cyberbezpieczeństwa.