DLB.ONE

MATERIAŁY DLA INŻYNIERÓW IT / OT / EMBEDDED

Źródło: www.dlb.one

CYBERBEZPIECZEŃSTWO 2026 / 2027

NIS2, Cyber Resilience Act
i bezpieczeństwo systemów testowych

5 modułów • 6 godzin • praktyka inżynierska

Wersja: 20 listopada 2026 | opracowanie szkoleniowe

PRZEWODNIK UCZESTNIKA

Jak korzystać z tego szkolenia

To kompletny materiał do przeprowadzenia jednodniowych warsztatów. Łączy wymagania prawne z decyzjami projektowymi dotyczącymi elektroniki, firmware, infrastruktury sieciowej i systemów testowych. W każdym module rozdzielamy **wymóg prawny** od **przykładowej metody technicznej**.

Zakres i ograniczenia
Stan prawny przyjęto na **20 listopada 2026 r.** Dokument jest materiałem edukacyjnym, nie indywidualną opinią prawną ani certyfikatem zgodności. Przed wdrożeniem należy ustalić status podmiotu, klasyfikację produktu i sprawdzić aktualne przepisy oraz normy zharmonizowane.

Cele szkolenia

- Rozpoznać, kiedy zastosowanie ma NIS2/KSC (organizacja), a kiedy CRA (produkt z elementami cyfrowymi).
- Przeprowadzić analizę ryzyka dla urządzenia testowego, sieci OT i procesu aktualizacji firmware.
- Zbudować ślad dowodowy: architektura, wymagania, testy, wersje, SBOM, decyzje o ryzyku.
- Zaprojektować monitoring, klasyfikację zdarzeń, reakcję na incydenty i odzyskiwanie pracy.
- Zorganizować przygotowanie do oceny zgodności CRA i weryfikacji klienta bez mylenia jej z audytem SZBI.

Agenda dnia

Moduł	Zakres	Czas
I	Ramy prawne, zakres, role, Technical File	75 min
II	Security by Design w hardware/software	85 min
III	Łańcuch dostaw, SBOM/HBOM, OSS	70 min
IV	Detekcja, incydenty i ciągłość	70 min
V	CE, weryfikacja techniczna i audyt	60 min

Łącznie: 360 minut aktywnej pracy, bez przerw. Sugerowane przerwy: 2 × 15 minut oraz 30 minut obiadowej.

Case study przewijający się przez całe szkolenie

ST-24 – stanowisko testowe (przykład fikcyjny). Sterownik ATmega4809 zbiera sygnały z czujników, ESP32-C6 komunikuje się z komputerem stacji i serwerem, a komputer Linux/Windows prezentuje wyniki. Wysyłane są rekordy pomiarowe i identyfikator detalu. Serwis aktualizuje firmware, podłącza USB/UPDI, czasem korzysta ze zdalnego dostępu.

Scenariusz ataku
Napastnik uzyskuje dostęp do konta serwisowego, instaluje zmodyfikowany firmware albo modyfikuje raportowane wyniki. Maszyna fizycznie pracuje, ale historia testów przestaje być wiarygodna. Potencjalne skutki: brak identyfikowalności, wadliwe decyzje jakościowe, przestój i spór z klientem.

Schemat architektury ST-24

Strefa	Elementy	Krytyczny punkt kontroli
OT / urządzenie	Czujniki → ATmega4809 → ESP32-C6	Integralność programu, interfejs serwisowy
Stanowisko	PC produkcyjny, aplikacja testowa	Uprawnienia, aktualizacje, identyfikacja operatora
Sieć / DMZ	VLAN OT, brama/API	Reguły ruchu, uwierzytelnienie i TLS
IT / serwer	API, MariaDB, logi, backup	Integralność wyniku, retencja, odzyskiwanie

Przykład dydaktyczny: rzeczywista konfiguracja wymaga inwentaryzacji oraz testów bezpieczeństwa i funkcjonalności.

MODUŁ I / 75 MIN

Nowe ramy prawne dla inżyniera

NIS2 / KSC, CRA, role, zakres produktu, zarządzanie ryzykiem i dowody zgodności.

Po tym module uczestnik potrafi:
Odróżnić obowiązek na poziomie organizacji od obowiązku na poziomie produktu oraz przygotować decyzję o zakresie regulacji.

1. NIS2 i CRA: różne przedmioty regulacji

NIS2 to dyrektywa (UE) 2022/2555, wdrożona w Polsce przede wszystkim przez ustawę o krajowym systemie cyberbezpieczeństwa (KSC). Ustala model zarządzania cyberbezpieczeństwem określonych podmiotów, odpowiedzialność kierownictwa, zarządzanie incydentami, łańcuchem dostaw i ciągłością działania. **CRA** to rozporządzenie (UE) 2024/2847 dotyczące produktów z elementami cyfrowymi wprowadzanych lub udostępnianych na unijnym rynku w toku działalności handlowej. CRA wiąże bezpieczeństwo z cyklem życia produktu, procesem zarządzania podatnościami i oceną zgodności. [R1–R3]

Pytanie	NIS2 / polski KSC	CRA
Co jest objęte?	Podmiot kluczowy / ważny i jego systemy	Produkt z elementami cyfrowymi i producent
Główne wymaganie	SZBI, środki organizacyjne/techniczne, incydenty	Security by design, obsługa podatności, dokumentacja i zgodność
Przykładowy dowód	Polityka, analiza ryzyka, szkolenia, zapis incydentu	Technical File, SBOM, wyniki testów, wersje FW
Typowy błąd	„Każda firma musi wdrożyć NIS2”	„Każde urządzenie z MCU wymaga audytu jednostki notyfikowanej”

Wniosek
Firma może podlegać KSC i jednocześnie produkować urządzenia objęte CRA, ale to nie są te same obowiązki. Przeciwnie, organizacja poza zakresem KSC może być producentem produktu podlegającego CRA.

2. Kalendarium 2026/2027

Termin	Wydarzenie i jego znaczenie
03.04.2026	Wejście w życie polskiej nowelizacji KSC wdrażającej NIS2.
03.10.2026	Termin samorejestracji w Wykazie KSC dla podmiotów objętych takim obowiązkiem.
11.09.2026	Początek obowiązywania zgłoszeń określonych podatności i poważnych incydentów produktu na gruncie CRA.
03.04.2027	Główny termin dostosowania obowiązków przez podmioty objęte KSC, które spełniały kryteria 03.04.2026.
11.12.2027	Początek stosowania zasadniczej części wymagań produktowych CRA.
03.04.2028	Termin pierwszego audytu dla odpowiednich podmiotów kluczowych na warunkach wskazanych w KSC.

Źródła: [R1], [R2], [R4], [R5]. Nie każdy podmiot ma identyczny harmonogram. Ustalenie zakresu i szczegółów terminów wymaga analizy konkretnej sytuacji.

3. Kiedy firma podlega polskiemu KSC?

Przeprowadź **samoidentyfikację** według rodzaju działalności, sektora/podsektora, kryteriów wielkości, wyjątków i przepisów szczególnych. Podmioty kluczowe i ważne mogą zostać objęte ustawą odmiennymi drogami, w tym wpisem z urzędu. Nie wystarczy sprawdzić wyłącznie kodu PKD ani wielkości zatrudnienia. [R2, R4]

- Ustal faktycznie świadczoną usługę i jednostkę odpowiedzialną za jej świadczenie.
- Sprawdź załączniki 1 i 2 oraz art. 5 KSC, w tym progi i wyjątki.
- Udokumentuj decyzję: „objęty / nieobjęty / konieczne potwierdzenie prawne”.
- Dla podmiotu objętego: wpis do wykazu, SZBI, proces incydentowy, odpowiedzialności, audyty i wymagane raportowanie.

4. Czy nasze stanowisko testowe jest „produktem z elementami cyfrowymi”?

Najpierw ustal, **co jest produktem**: sam sterownik, moduł gateway, cała stacja, czy oprogramowanie udostępniane klientowi. Następnie sprawdź, czy następuje udostępnienie na rynku UE w działalności handlowej, jakie jest przewidywane użycie, czy istnieją wyłączenia albo regulacje szczególne, a także kto występuje jako producent. Ocena musi dotyczyć konkretnej konfiguracji i modelu dystrybucji. [R3]

Przykład	Ocena wstępna (nie zastępuje analizy prawnej)
Stacja wyłącznie do wewnętrznych prób, bez udostępnienia na rynku	Brak typowego zdarzenia „udostępnienia na rynku”; przeanalizuj inne przepisy, wymagania klienta i ryzyka.
Sterownik z firmware dostarczany kontrahentowi pod własną marką	Potencjalnie zakres CRA; zweryfikuj charakter produktu, zastosowania i wyłączenia.
Oprogramowanie sterujące sprzedawane lub dostarczane jako część produktu	Może być objęte jako część produktu albo sam produkt; opisz zależności i odpowiedzialności.

Przykład	Ocena wstępna (nie zastępuje analizy prawnej)
Komponent kupiony od dostawcy i wbudowany do stacji sprzedawanej pod własną marką	Odpowiedzialność za wyrób końcowy nie znika; potrzebna weryfikacja komponentów i konfiguracji.

Uwaga na CE
CRA uzupełnia wymagania dotyczące zgodności produktów. Nie oznacza, że każdy produkt wymaga obowiązkowej certyfikacji przez jednostkę zewnętrzną. Ścieżka oceny zależy m.in. od klasyfikacji wyrobu, zastosowanych norm i określonych w CRA warunków. Oznakowanie CE nie zastępuje dokumentacji technicznej.

5. Producent, integrator, dostawca - odpowiedzialność

Przypisz role **dla każdego wyrobu i interfejsu**. Producent odpowiada m.in. za określenie ryzyka produktu, zgodność projektu, informacje dla użytkownika, właściwy okres wsparcia, zarządzanie podatnościami i dokumentację. Integrator powinien zebrać dowody ze źródeł komponentów i przeprowadzić testy integracyjne; „certyfikat komponentu" nie zwalnia automatycznie z odpowiedzialności za całość. [R3]

- W umowie zakupowej wpisz wymagania aktualizacji, termin powiadamiania o podatnościach i format SBOM.
- Określ właściciela kluczy do podpisu firmware, procesu publikacji oraz akceptacji ryzyka.
- Zapisz wersje HW, bootloadera, firmware, biblioteki, testera i oprogramowania PC jako jeden baseline wydania.

6. Ryzyko jako decyzja inżynierska

Analiza ryzyka nie jest listą samych CVE. Powinna uwzględniać cechy produktu, przewidziane zastosowanie, dostęp fizyczny, łatwość ataku, skutki dla poufności, integralności, dostępności, bezpieczeństwa funkcjonalnego i procesu przemysłowego. Zależnie od zastosowania ryzyko błędnego wyniku testu może być groźniejsze niż chwilowa niedostępność serwera.

Przykładowy model warsztatowy (nie jest wzorem ustawowym): prawdopodobieństwo P = 1..5, wpływ I = 1..5, wynik R = P × I. Priorytety: 1–5 niski, 6–12 średni, 15–25 wysoki. Po wdrożeniu środków oszacuj ryzyko rezydualne, określ właściciela decyzji oraz dowód skuteczności.

ID	Zagrożenie	P × I	Środek	Dowód
R-01	Podmiana firmware ATmega4809	4×5=20	Kontrola pochodzenia pakietu i procesu programowania	Manifest wydania, protokół serwisowy
R-02	Sfałszowany wynik testu z PC	3×5=15	Autoryzowany API, identyfikator i integralność rekordu	Test negatywny, log korelacyjny
R-03	Przestój API pomiarowego	4×3=12	Kolejka lokalna + retransmisja z deduplikacją	Test odłączenia sieci i odtworzenia

Warsztat I-1. Kwalifikacja ST-24

Zadanie
W trzech wariantach: A – stanowisko tylko wewnętrzne, B – stacja sprzedawana klientowi pod marką producenta, C – usługa zdalnego utrzymania infrastruktury krytycznej. Zapisz możliwe zastosowanie KSC i CRA, brakujące informacje i odpowiedzialnego za decyzję.

Rezultat do zapisania: Macierz 3 warianty × [KSC / CRA / CE / właściciel / źródła].

Wskazówki dla prowadzącego / odpowiedź: Nie oznaczaj automatycznie „TAK” tylko na podstawie obecności ESP32 lub samej umowy serwisowej. Rozdziel status przedsiębiorstwa i produkt; uwzględnij zasady udostępniania na rynku UE, rolę wykonawcy i typ usługi.

MODUŁ II / 85 MIN

Security by Design w hardware i software

Od modelu zagrożeń do kontroli dostępu, bezpiecznego firmware, segmentacji i testów.

Po tym module uczestnik potrafi:
Zidentyfikować powierzchnię ataku ST-24 i dobrać zestaw proporcjonalnych zabezpieczeń wraz z dowodami ich działania.

1. Security by Design nie jest ostatnim testem przed wydaniem

Bezpieczeństwo zaczyna się od wymagań, jeszcze przed PCB i kodem. W fazie koncepcji opisujemy granice zaufania, dane krytyczne, interfejsy, role, aktualizacje, okres wsparcia, dostawców i zasady wycofania urządzenia. W fazie projektu wybieramy architekturę ograniczającą dostęp, a przy odbiorze testujemy rzeczywiste środki ochrony. Ważne: zabezpieczenie musi być **adekwatne do ryzyka**; sama długa checklista nie daje zgodności. [R3]

Etap	Decyzja i rezultat	Przykład ST-24
Wymagania	Cel bezpieczeństwa, kryterium akceptacji	Wynik testu musi mieć wiarygodne źródło i ID
Projekt	Model zagrożeń i granice zaufania	VLAN OT, rozdział portów admin i API
Implementacja	Kontrole w HW/FW/serwerze	Podpisywanie wydań, autoryzacja żądań
Weryfikacja	Testy pozytywne i negatywne	Odrzuć błędny podpis i błędny token
Eksploatacja	Logowanie, poprawki, odpowiedzialność	Rejestr zgłoszeń, plan wsparcia

2. Inwentaryzacja punktów wejścia i granic zaufania

Na diagramie architektury oznacz: komunikację ESP32-C6 z serwerem, UART/RS485, port serwisowy UPDI, komputer stacyjny, USB, Wi-Fi, połączenia VPN i dostęp fizyczny. Następnie przypisz do każdej granicy tożsamość, sposób uwierzytelniania, protokół, kierunek ruchu i scenariusz awarii.

Interfejs	Przykładowy atak	Kontrola minimalna
UPDI / port serwisowy	Podmiana firmware w czasie obsługi	Dostęp fizyczny, nadzorowany proces, potwierdzenie obrazu i log programowania
ESP32-C6 → API	Podszywanie się pod urządzenie	TLS z weryfikacją certyfikatu, tożsamość urządzenia i autoryzacja
PC → baza / API	Zmiana testu, danych lub parametrów	Role i zatwierdzanie zmian, dostęp tylko przez API
Panel www / zdalny serwis	Przejęcie konta technika	MFA, konta indywidualne, VPN, nadawanie i cofanie uprawnień

Interfejs	Przykładowy atak	Kontrola minimalna
Sieć OT	Ruch boczny z sieci biurowej	Firewall między strefami, reguły allow-list, przegląd wyjątków

3. Secure firmware: MCU z różnymi możliwościami

ESP32-C6: zweryfikuj dostępność i konfigurację mechanizmów platformy, m.in. Secure Boot, szyfrowania flash, ochrony interfejsów debugowania i zapobiegania downgrade. Te funkcje wymagają świadomego provisioningu kluczy, polityki serwisu i bezpiecznej ścieżki ratunkowej. Włączenie pojedynczej opcji w projekcie nie stanowi dowodu, że cały proces aktualizacji jest bezpieczny.

ATmega4809: standardowy proces programowania przez UPDI nie jest równoznaczny z uwierzytelnioną aktualizacją. Jeżeli sprzęt nie oferuje natywnej weryfikacji podpisu przy uruchomieniu, zabezpiecz proces zewnętrznie: kontrolowane narzędzie serwisowe, podpisany manifest paczki, identyfikacja operatora, porównanie wersji/hash po zaprogramowaniu, blokada nieautoryzowanego dostępu fizycznego. Krytyczne zastosowania mogą wymagać zmiany architektury lub dodatkowego układu bezpieczeństwa.

> **CRC ≠ dowód autentyczności**
> CRC wykrywa losowe uszkodzenia danych, ale nie chroni przed intencjonalną podmianą firmware. Do weryfikacji pochodzenia potrzebne są mechanizmy kryptograficzne oraz ochrona kluczy.

Przykładowa polityka wydania firmware

- Kod i konfiguracja kompilacji mają przypisany commit/tag oraz niezależny numer wersji.
- Pipeline generuje manifest: model urządzenia, HW revision, build ID, hash SHA-256, podpis wydania, lista zależności i wynik testów.
- Pracownik serwisu pobiera wyłącznie zatwierdzone pakiety; odebrane artefakty są weryfikowane przed użyciem.
- Każde programowanie zapisuje identyfikator urządzenia, operatora, czas, wersję przed/po i rezultat weryfikacji.
- Rollback jest kontrolowany: tylko zgodne, nadal wspierane wersje; procedura odzyskiwania nie omija polityki integralności.

4. Sieć testowa: segmentacja i zarządzanie dostępem

W modelu ST-24 wyodrębnij strefę urządzeń/sterowników, strefę PC produkcyjnych, DMZ usług pośredniczących oraz IT/administrację. Ruch OT powinien być wąsko zdefiniowany. VLAN jest przydatny organizacyjnie, ale **sam VLAN bez właściwych reguł routingu/firewalla nie stanowi pełnej bariery**.

Relacja	Przykładowa polityka	Uzasadnienie
ESP32-C6 → API	Tylko HTTPS/TCP 443 do jednego hosta	Ogranicza zbędny ruch przychodzący/wychodzący
PC OT → repozytorium aktualizacji	Wyłącznie przez kontrolowaną bramę / proxy	Pozwala weryfikować pakiety i prowadzić log
IT → OT	Domyślnie deny; sesja serwisowa przez bastion z MFA	Audytowalny dostęp tymczasowy

Relacja	Przykładowa polityka	Uzasadnienie
OT → serwer logów	Dedykowany kanał z kontrolą integralności / uwierzytelnieniem	Dane do analizy incydentu
OT ↔ Internet	Blokuj poza wymaganymi adresami i usługami	Zmniejsza powierzchnię ataku

5. Zarządzanie kontami i dostępem do serwisu

Każde konto technika jest indywidualne i ma minimalne uprawnienia. Dostęp uprzywilejowany zatwierdza właściciel stanowiska, ma określony zakres i termin wygaśnięcia. MFA stosuj tam, gdzie jest technicznie możliwe, szczególnie przy VPN, bastionach, panelach administracyjnych i repozytoriach. Jeżeli urządzenie nie ma interaktywnego MFA, wymuszaj silne uwierzytelnienie na bramie dostępowej i kontrolę sesji.

- Bez kont domyślnych i wspólnych loginów serwisowych bez kontroli; unikatowe dane dostępu i ich rotacja.
- Rozdział uprawnień: operator / diagnostyka / konfiguracja / aktualizacja / administrator.
- Rejestr zdalnych sesji oraz zmian parametrów testu, kalibracji i dopuszczalnych progów.
- Awaryjny dostęp „break glass” z udokumentowaną aktywacją i przeglądem po zdarzeniu.

6. Dobór testów negatywnych do wymagań

Test bezpieczeństwa ma mieć warunki początkowe, kroki, oczekiwany wynik, rzeczywisty wynik, log i zatwierdzającego. Przykłady: zły certyfikat HTTPS; nieprawidłowy podpis pakietu; ponownie wysłany rekord pomiarowy; utrata sieci w trakcie zapisu; brak uprawnień do zmiany receptury; próba wgrania starszej nieobsługiwanej wersji.

ID testu	Próba	Oczekiwana reakcja
SEC-01	Podstawienie nieznanego certyfikatu API	Połączenie odrzucone, brak wysłania danych
SEC-02	Zmiana jednego bajtu w podpisanym obrazie	Wydanie/aktualizacja odrzucona
SEC-03	Ręczna zmiana progu testu przez operatora	Odmowa, log próby, brak zmiany parametrów
SEC-04	Wysłanie tego samego ID pomiaru dwa razy	Jeden zapis + ślad deduplikacji

Warsztat II-1. Model zagrożeń ST-24

> **Zadanie**
> Narysuj granice IT–OT i zaznacz 8 punktów wejścia; dla trzech najważniejszych zagrożeń wybierz zabezpieczenie, test oraz właściciela.

Rezultat do zapisania: Diagram architektury, tabela [punkt wejścia / atak / skutek / kontrola / test / właściciel].

Wskazówki dla prowadzącego / odpowiedź: Najwyższym ryzykiem może być cicha manipulacja danymi jakościowymi. Nie akceptuj samego „antywirusa na PC” jako kontroli integralności firmware lub wyniku. Zwróć uwagę na uprawnienia do zmiany receptury i wersji programu.

Warsztat II-2. Próba serwisowa i niepodpisany firmware

Zadanie
W scenariuszu serwisant podłącza UPDI do ATmega4809. Zaprojektuj proces, który rozróżnia poprawne wgranie znanego obrazu od dopuszczenia dowolnego HEX.

Rezultat do zapisania: 5-krokowa instrukcja serwisowa i zapis audytowy.

Wskazówki dla prowadzącego / odpowiedź: Ustal źródło zaufania dla pakietu, niezależną weryfikację podpisanego manifestu, potwierdzenie zgodności modelu/revision, odczyt i hash/wersję po flash oraz archiwizację protokołu. Uwzględnij ograniczenia sprzętowe.

MODUŁ III / 70 MIN

Łańcuch dostaw i integracja komponentów

SCRM, weryfikacja dostawcy, SBOM/HBOM, open source i automatyzacja zarządzania podatnościami.

Po tym module uczestnik potrafi:
Zbudować aktualną listę elementów produktu, wykryć problem w zależności oraz przeprowadzić decyzję o aktualizacji lub środku zastępczym.

1. Ryzyko dostawcy jest ryzykiem produktu

Ocenie podlegają nie tylko zakupiony sterownik i moduł radiowy, ale także SDK, biblioteki, gotowe firmware, narzędzia budowania, usługi aktualizacji i podwykonawcy serwisu. Główne pytania: kto naprawia podatności, jak szybko informuje, jakie wersje są wspierane i czy mamy możliwość przetestowania aktualizacji?

Aspekt	Pytanie do dostawcy	Wymagany dowód
Wsparcie	Do kiedy wydawane są poprawki?	Polityka wsparcia, data końca wsparcia
Podatności	Jak dostawca publikuje advisory?	Kontakt PSIRT / portal / SLA
Aktualizacja	Czy pakiety są podpisywane?	Specyfikacja weryfikacji, demonstracja
Komponenty	Czy dostępny jest SBOM dla wersji?	CycloneDX lub SPDX, wersja i data
Dostęp	Czy są domyślne hasła/debug?	Lista interfejsów i ustawień fabrycznych
Zmiany	Czy zmieniają BOM/SDK bez informacji?	PCN, changelog, procedura zatwierdzania

2. SBOM a HBOM - różnica, która ma znaczenie

SBOM (Software Bill of Materials) identyfikuje komponenty programowe i relacje zależności, np. bibliotekę TLS, framework, serwer i wersje firmware. **HBOM (Hardware Bill of Materials)** opisuje fizyczne moduły i podzespoły, np. ESP32-C6, ATmega4809, moduł Wi-Fi, zasilacz oraz rewizje PCB. HBOM to użyteczny artefakt inżynierski; szczegółowe wymagania prawne i zakres SBOM trzeba odczytać z CRA i dokumentacji technicznej, zamiast zakładać obowiązek publikacji pełnej publicznej listy wszystkich części. [R3]

Typ	Przykładowa pozycja	Dlaczego potrzebna
SBOM	ESP-IDF / Arduino core, dokładne wersje	Sprawdzenie advisory, EOL, zależności
SBOM	Biblioteka JSON / HTTP / TLS	Analiza ścieżki podatności i poprawki
SBOM	Pakiety systemu Linux/Windows i aplikacji stacji	Kontrola oprogramowania operacyjnego
HBOM	ESP32-C6 moduł, producent, part number, revision	Podatności SoC/ROM i zamienniki

Typ	Przykładowa pozycja	Dlaczego potrzebna
HBOM	ATmega4809, rewizja PCB i programator	Metoda flash, kompatybilność i serwis
HBOM	Switch, firewall, brama, serwer	Wersja FW/OS i odpowiedzialność

Minimalny rekord SBOM - wzór warsztatowy

Pole	Przykładowa wartość
produkt / release	ST-24 / rel-1.4.2
nazwa komponentu	Biblioteka komunikacyjna
wersja / identyfikator	2.7.1 / purl lub inne stabilne ID
dostawca / źródło	Repozytorium producenta, URL, commit
licencja	Weryfikacja zgodności licencji OSS
status podatności	CVE / brak znanych / oczekuje oceny
osoba i data	Właściciel produktu, data skanowania

3. Automatyzacja DevSecOps przy małym zespole

Bez skomplikowanej infrastruktury można zacząć od pipeline uruchamianego na każdym wydaniu: build od czystego commita, analiza zależności/SBOM, podstawowy skan kodu i sekretów, testy, archiwum wyników oraz podpisany artefakt. Zmiana zależności podlega przeglądowi z oceną licencji i podatności.

- Repozytorium: ochrona gałęzi, przegląd zmian, unikatowe konta, MFA i logi uprawnień.
- CI: zablokuj ujawnianie sekretów, rozdziel uprawnienia build i release, przypnij wersje narzędzi.
- SCA/SBOM: generuj listę zależności dla konkretnego wydania; nie skanuj wyłącznie pliku README.
- SAST i testy: traktuj wyniki jako punkt startowy do triage, nie jako dowód braku podatności.
- Wydanie: zachowaj wynik pipeline, manifest, sumy kontrolne, podpis i identyfikator urządzeń objętych aktualizacją.

4. Po wykryciu CVE: procedura VEX / triage

Wynik skanera „biblioteka ma CVE” nie oznacza jeszcze, że dany produkt jest podatny. Oceń: wersję, obecność i osiągalność funkcji, konfigurację, możliwość ataku, ekspozycję, skutki oraz dostępność poprawki. Decyzję i uzasadnienie zapisuj w rejestrze. Można używać koncepcji VEX do wyrażenia statusu „affected / not affected / under investigation / fixed”, z uzasadnieniem i identyfikacją wydania.

Krok	Działanie	Czas / kryterium
1. Wykrycie	Przypisz CVE do produktu i wydań	Niezwłoczny triage i rejestr
2. Ocena	Potwierdź ścieżkę ataku i ekspozycję	Ryzyko produktu, nie tylko CVSS

Krok	Działanie	Czas / kryterium
3. Decyzja	Patch, mitigacja, brak wpływu lub wyjątek	Akceptacja właściciela ryzyka
4. Test	Regresja funkcjonalna i bezpieczeństwa	Dowody na danej rewizji HW
5. Dystrybucja	Pakiet, komunikat, instrukcja i rollback	Zgodnie z priorytetem i wsparciem
6. Zamknięcie	Zapis produktu/wydania i ponowny skan	Potwierdzony status

Ważne rozróżnienie
Obsługa podatności komponentu i ustawowe zgłoszenie do organu to różne czynności. CRA przewiduje raportowanie **aktywnie wykorzystywanych podatności** i **poważnych incydentów wpływających na bezpieczeństwo produktu**; nie należy zgłaszać każdej informacji o CVE jako automatycznie spełniającej przesłanki. [R5]

5. Zarządzanie częściami i końcem wsparcia

Utrzymuj mapę kompatybilności: rewizja PCB ↔ moduł ↔ wersja bootloadera ↔ firmware ↔ konfiguracja PC. Dla produktów z długim okresem pracy w fabryce uwzględnij plan wymiany niedostępnych komponentów, EOL narzędzia build i dostawcy chmury, możliwe ograniczenia pamięci MCU na aktualizacje oraz odtworzenie stanowiska po awarii.

Warsztat III-1. CVE w bibliotece sieciowej ESP32

Zadanie
Skan zależności sygnalizuje poważną podatność w bibliotece sieciowej używanej przez firmware ST-24. Zespół nie wie, czy wywoływana jest podatna funkcja. Przygotuj plan działania od pierwszego alarmu po zamknięcie.

Rezultat do zapisania: Karta podatności: produkt/release, komponent, warunki wykorzystywania, ryzyko, działania i dowody.

Wskazówki dla prowadzącego / odpowiedź: Nie opieraj decyzji wyłącznie na poziomie CVSS. Sprawdź ścieżkę wykonania i konfigurację; ustal czy urządzenie jest online, czy istnieje środek zastępczy oraz kto odpowiada za informowanie użytkowników.

Warsztat III-2. Utwórz HBOM i SBOM dla stacji

Zadanie
Sporządź po pięć pozycji dla hardware i software, uwzględniając rewizje, wersje, producenta, status wsparcia i opiekuna.

Rezultat do zapisania: Dwa rejestry i jedno powiązanie z wydaniem ST-24.

Wskazówki dla prowadzącego / odpowiedź: Kluczowe jest jednoznaczne powiązanie komponentów z egzemplarzem/wersją produktu; aktualizowanie SBOM wyłącznie raz w roku nie wystarczy, jeżeli wydania zmieniają skład.

MODUŁ IV / 70 MIN

Detekcja, incydenty i ciągłość działania

Telemetria, procedury reagowania, logi techniczne, obowiązki raportowania, BCP i ćwiczenia odtworzeniowe.

Po tym module uczestnik potrafi:
Zaprojektować minimalny monitoring i przećwiczyć obsługę incydentu, ograniczenie skutków oraz bezpieczne przywrócenie produkcji.

1. Zdarzenie, podatność i incydent - trzy różne pojęcia

Zdarzenie to obserwowalna zmiana stanu (np. błędny login). **Podatność** to słabość, która może zostać wykorzystana. **Incydent** oznacza zdarzenie mogące naruszyć bezpieczeństwo lub działanie systemu; jego definicja i kategorie raportowe zależą od przepisów. Użytkownik powinien mieć prostą ścieżkę zgłaszania nietypowych objawów niezależnie od późniejszej kwalifikacji prawnej.

Objaw	Wstępna reakcja	Możliwy skutek
10 nieudanych logowań do serwisu	Alert, weryfikacja źródła, blokada/ratelimit	Próba przejęcia dostępu
Nowa wersja FW bez zatwierdzonego manifestu	Wstrzymaj stację, zabezpiecz dowody	Manipulacja firmware i wynikami
Baza danych nie odpowiada	Buforowanie i kontrola kolejek	Utrata / opóźnienie danych
Niezgodność wyniku PC i rekordów z urządzenia	Zabezpiecz dane, uruchom diagnostykę	Ryzyko jakości i integralności
Nadmierny ruch OT→Internet	Izolacja logiczna po ocenie wpływu na proces	Eksfiltracja / ruch boczny

2. Co powinno się znaleźć w logu?

Każdy ważny rekord powinien zawierać timestamp w UTC lub jednoznacznej strefie, identyfikator urządzenia/stanowiska, identyfikator korelacyjny zdarzenia, wersję oprogramowania, typ operacji, rezultat, źródło i poziom ważności. Dla zdarzeń autoryzacji także konto/rolę i identyfikator sesji. Utrzymuj synchronizację czasu i kontroluj retencję; nie przechowuj sekretów i danych osobowych bez celu i podstawy.

Pole	Przykładowa wartość	Powód
timestamp_utc	2026-11-20T09:41:21Z	Porządek zdarzeń i korelacja
station_id	ST-24-07	Identyfikacja urządzenia
event_id	e7f4...	Deduplikacja i śledzenie
fw_version	esp32-1.4.2 / avr-1.1.8	Ustalenie wariantu produktu

Pole	Przykładowa wartość	Powód
event_type	measurement_upload	Powołanie reguł detekcji
result / status	rejected / invalid_signature	Powód odrzucenia
actor / source	service-operator-02 / vpn	Audyt działań

3. Minimalna architektura monitoringu dla ST-24

Urządzenia generują tylko niezbędną telemetrię. Komputer stacyjny przekazuje logi do centralnego kolektora, a brama zachowuje logi firewall/VPN. Serwer zbiera logi API, błędy autoryzacji, historię wydań i metryki dostępności. Monitoruj objętość ruchu, nieoczekiwane adresy docelowe, restart MCU, błędne aktualizacje oraz przerwy w przesyłaniu wyników. Alert musi trafić do **konkretnej osoby** i mieć procedurę obsługi.

Przykład: wyniki w access.log
Jeżeli dane pomiarowe trafiają przez HTTP GET do access.log, rozważ przejście na uwierzytelniony HTTPS POST z walidacją danych po stronie API, identyfikatorem idempotencji i buforowaniem lokalnym. Log www nie powinien być jedynym źródłem danych produkcyjnych; nie przechowuj tokenów i danych w URL. To rekomendacja projektowa, a nie dosłowny przepis CRA.

Proste reguły alarmowe - przykłady

- Firmware changed: różnica między zatwierdzoną wersją a deklaracją z urządzenia / rekordem programatora.
- Multiple auth failures: wzrost nieudanych logowań z jednego konta lub adresu.
- Missing heartbeat: brak komunikacji z krytycznym stanowiskiem przez ustalony czas.
- Data integrity: pomiar z niemożliwą sekwencją, nieznanym ID, niezgodną kalibracją lub duplikatem.
- Unexpected egress: połączenia ze strefy OT do niezarejestrowanego adresu w Internecie.

4. Procedura reagowania na incydent - model operacyjny

Faza	Czynności	Artefakt
1. Zgłoszenie	Rejestr, czas wykrycia, źródło, wpływ	Karta incydentu
2. Triage	Zakres, krytyczność, możliwy wpływ na bezpieczeństwo i jakość	Klasyfikacja i priorytet
3. Powstrzymanie	Odłączenie sesji, blokada konta / ruchu, wstrzymanie wydania	Decyzja + log działań
4. Analiza	Zabezpieczenie logów/obrazów, wersje, oś czasu	Timeline i hipoteza
5. Naprawa	Zmiana haseł, nowy FW, reguły sieci, poprawka	Zapis zmian i testy
6. Odtworzenie	Powrót po zgodzie właściciela procesu i testach kontrolnych	Protokół przywrócenia
7. Lessons learned	Przyczyna, nowe kontrole, właściciel działań	Raport i termin weryfikacji

5. Role RACI oraz decyzja o zatrzymaniu linii

Działanie	Inż. OT / FW	IT / SOC	Kier. produkcji	Zarząd / compliance
Triage techniczny	R	R	C	I
Izolacja sieci / kont	C	R	A	I
Wstrzymanie i wznowienie testów	R	C	A	I
Kwalifikacja raportu regulacyjnego	C	R	C	A
Kontakt z klientem	C	C	R	A
Przegląd po incydencie	R	R	C	A

Legenda: R - wykonuje, A - odpowiada za zatwierdzenie, C - konsultowany, I - informowany. Podział przykładowy, do dostosowania organizacyjnie.

6. NIS2 i CRA: ramy zgłaszania incydentów

Dla podmiotu objętego KSC obowiązki, adresaci i procedury wynikają z ustawy krajowej oraz jej przepisów wykonawczych. Dyrektywa NIS2 przewiduje m.in. wczesne ostrzeżenie w 24 h, zgłoszenie incydentu w 72 h i raport końcowy co do zasady w ciągu miesiąca, ale decyzję operacyjną w Polsce należy oprzeć na aktualnym KSC i definicji właściwego incydentu. [R1, R2]

W CRA od **11.09.2026** producenci raportują określone aktywnie wykorzystywane podatności i poważne incydenty wpływające na bezpieczeństwo produktu. Wstępne ostrzeżenie: **24 h** od uzyskania wiedzy; zgłoszenie: **72 h**. Raport końcowy: w przypadku aktywnie wykorzystywanej podatności zasadniczo do **14 dni po udostępnieniu środka naprawczego**, a w przypadku poważnego incydentu do **miesiąca od zgłoszenia 72 h**. Właściwe zdarzenie i procedury opisują przepisy oraz platforma zgłoszeniowa. [R3, R5]

> **Raport to nie każdy błąd serwera**
> Przestój bazy nie jest automatycznie raportowalnym incydentem CRA. Z kolei aktywne wykorzystywanie podatności produktu może uruchomić obowiązek zgłoszenia nawet wtedy, gdy produkcja jeszcze działa. Ustal procedurę kwalifikacji i osobę podejmującą decyzję.

7. BCP/DRP i test odtworzenia produkcji

Plan ciągłości (BCP) opisuje, jak utrzymać krytyczną funkcję przy awarii; DRP opisuje odbudowę zasobów. Dla stanowisk testowych rozdziel **bezpieczne zatrzymanie** od **dalszej produkcji**. Nie wolno automatycznie akceptować niezweryfikowanych wyników tylko po to, by osiągnąć KPI wydajności.

Element	Przykład ST-24
RTO - cel przywrócenia	4 godziny dla serwera, zgodnie z analizą wpływu (przykład)
RPO - dopuszczalna utrata danych	0 zatwierdzonych wyników, dzięki buforowaniu i deduplikacji (cel)
Buforowanie lokalne	Kolejka z trwałym zapisem, limitem pojemności i licznikiem zaległości

Element	Przykład ST-24
Przywracanie	Wersjonowany obraz PC, odtworzenie konfiguracji, testy po wdrożeniu
Próba odtworzeniowa	Odłącz API na 30 min, przywróć i porównaj liczbę rekordów
Komunikacja	Kto zatrzymuje testy, kiedy informuje jakość i klientów

Warsztat IV-1. Incydent: nieznana wersja firmware

Zadanie
O 09:15 operator widzi inną wersję firmware na ST-24. Dwa rekordy pomiarowe różnią się od kopii urządzenia. Zespół podejrzewa ingerencję konta serwisowego. Przeprowadź 15-minutową symulację i rozdziel decyzje na techniczne, produkcyjne i regulacyjne.

Rezultat do zapisania: Karta incydentu, oś czasu pierwszej godziny, RACI, lista dowodów, decyzja o wstrzymaniu i powiadomieniu.

Wskazówki dla prowadzącego / odpowiedź: Priorytet: bezpieczeństwo ludzi i wiarygodność produktu. Nie usuwaj logów/nie nadpisuj dysku bez planu zabezpieczenia śladów. Przegląd dostępu VPN i historii flash; porównanie zatwierdzonej wersji oraz niezależnych wyników testu.

Warsztat IV-2. Awaria MariaDB przy działającym stanowisku

Zadanie
Wyłącz dostęp do bazy. Ustal co dzieje się z danymi, jak oznaczyć stan zaległości i jak odzyskać transmisję bez podwójnych pomiarów.

Rezultat do zapisania: Sekwencja testu awaryjnego i mierniki RTO/RPO.

Wskazówki dla prowadzącego / odpowiedź: Trwała kolejka, unikatowe ID pomiarów, potwierdzenie zapisu, retry/backoff, granica pamięci, alarm o zapełnieniu, uzgodnienie warunków wstrzymania produkcji.

MODUŁ V / 60 MIN

CE, weryfikacja techniczna i audyt

Od mapowania wymagań do Technical File, testów odporności, deklaracji zgodności i nadzoru nad produktem.

Po tym module uczestnik potrafi:
Przygotować plan oceny zgodności i zestaw dowodów produktu oraz rozróżnić test penetracyjny od formalnej procedury oceny zgodności.

1. Jak CRA łączy się z oznakowaniem CE?

Dla produktu w zakresie CRA producent określa klasyfikację, identyfikuje mające zastosowanie wymagania zasadnicze, przygotowuje analizę ryzyka, wdraża środki, prowadzi wymaganą ocenę zgodności i dokumentację techniczną, a następnie sporządza właściwą deklarację zgodności UE oraz oznakowanie CE. CRA współistnieje z innymi aktami wymagającymi CE (np. w zależności od wyrobu i jego funkcji), ale ich zakresy i badania nie są identyczne. [R3]

Możliwe ścieżki CRA obejmują m.in. wewnętrzną kontrolę produkcji (moduł A) oraz - w przypadkach przewidzianych prawem - procedury z udziałem jednostki notyfikowanej. Ocena zależy od klasyfikacji i warunków wskazanych w CRA. Sformułowanie „certyfikacja CE" jest często skrótem myślowym: CE to oznakowanie wynikające z oceny zgodności, a nie jeden certyfikat wydawany wszystkim produktom przez zewnętrzny organ.

Krok	Pytanie kontrolne	Dowód
1. Zakres	Czy to produkt w zakresie CRA? Jakie wyjątki?	Uzasadniona decyzja klasyfikacyjna
2. Wymagania	Które wymagania zał. I mają zastosowanie?	Macierz wymagań i odstępstw
3. Ryzyko	Jakie scenariusze zidentyfikowano?	Ocena ryzyka + decyzje
4. Projekt/testy	Czy środki faktycznie działają?	Plan i raport weryfikacji
5. Ścieżka oceny	Czy dopuszczony jest moduł A?	Uzasadnienie i wynik procedury
6. Dokumenty	Czy Technical File i instrukcja są kompletne?	Kontrolowany zestaw plików
7. Wydanie	Czy deklaracja UE i oznakowanie są prawidłowe?	Deklaracja, release i identyfikacja produktu
8. Nadzór	Jak obsługiwane są podatności i aktualizacje?	PSIRT, polityka wsparcia, rejestr zdarzeń

2. Technical File według CRA - praktyczna struktura

Art. 31 i **załącznik VII CRA** określają zawartość dokumentacji technicznej, stosownie do danego produktu. Poniżej struktura warsztatowa ułożona do pracy inżynierskiej; nie stanowi dosłownego przepisania załącznika. [R3]

Sekcja	Minimalna zawartość projektu ST-24
00. Identyfikacja	Model, producent, intended purpose, wersje HW/FW/SW, zdjęcia/rysunki, warianty
01. Architektura	Schemat blokowy, PCB, firmware, połączenia, granice zaufania i interfejsy
02. Wymagania	Mapa załącznika I, wymagania innych regulacji, zastosowanie / wyłączenia
03. Ocena ryzyka	Scenariusze zagrożeń, kryteria, decyzje, ryzyko rezydualne
04. Kontrole	Dostęp, aktualizacje, tożsamość, logi, zabezpieczenie fizyczne, środki zastępcze
05. Komponenty	SBOM, dostawcy, wersje, HBOM, EOL i monitoring podatności
06. Testy	Test plan, wyniki, błędy, regresja, dowody i wersje testowane
07. Proces podatności	Kanał zgłoszeń, triage, publikacja poprawki, polityka wsparcia
08. Instrukcja	Informacje dla użytkownika, konfiguracja bezpieczna, cykl życia
09. Zgodność	Ścieżka oceny, zastosowane normy, deklaracja UE, rejestr zmian

3. Macierz traceability: wymaganie → implementacja → test → dowód

Audytor lub osoba weryfikująca zgodność powinien przejść od wymagania do konkretnej implementacji i dowodu testu. Zamiast opisów „stosujemy dobre praktyki” twórz identyfikatory, datę, wersję, wynik i lokalizację artefaktu.

ID	Wymaganie / cel	Realizacja	Test i dowód
SEC-R01	Tylko zatwierdzone wydania firmware	Podpisany manifest, kontrolowany serwis	SEC-02, raport wydania R-14
SEC-R02	Ochrona danych transmisji	TLS + autoryzacja urządzenia	SEC-01, log połączenia, konfiguracja
SEC-R03	Zmiana progów tylko przez uprawnionych	Role PC, ślad zmiany konfiguracji	SEC-03, raport dostępu
SEC-R04	Bezpieczne odtworzenie danych	Bufor i deduplikacja	SEC-04, raport prób awaryjnych

4. Testy odporności: co realnie badać?

Wybór metod zależy od modelu zagrożeń. Przykłady: analiza kodu (SAST), analiza zależności (SCA), testy protokołu API, testy uwierzytelniania, fuzzing parsera UART/HTTP, próby modyfikacji firmware, testy odporności na awarię łącza, kontrola konfiguracji fabrycznej, przegląd portów sieciowych i kont. W OT testy prowadzi się w kontrolowanym stanowisku, bez narażania bezpieczeństwa fizycznego i ciągłości produkcji.

Pentest kontra Red Team

Pentest sprawdza zdefiniowany zakres systemów i podatności w ustalonym oknie. **Red Team** zwykle bada zdolność organizacji do wykrycia i powstrzymania realistycznego scenariusza ataku, obejmując ludzi/procesy/technikę. Żadna z tych metod sama nie zastępuje formalnej oceny zgodności produktu. Wynik testów należy powiązać z wymaganiami i oceną ryzyka.

5. Raport testu bezpieczeństwa - wzór

Sekcja raportu	Zawartość
Cel i zakres	Co badano; co wyłączono i dlaczego; środowisko/testbed
Identyfikacja	Produkt, HW revision, FW/SW, model, hash build, data
Metoda	Kryterium akceptacji, standard odniesienia, narzędzia
Wyniki	Testy PASS/FAIL, screenshot/log/PCAP, ryzyko i reprodukcja
Działania	Poprawka lub środek zastępczy, właściciel, termin
Retest	Data, konfiguracja, wynik i zatwierdzenie
Ograniczenia	Co pozostaje niezweryfikowane i ryzyko rezydualne

6. Co jest sprawdzane po wprowadzeniu produktu na rynek?

CRA wymaga podejścia cyklu życia: obsługi zgłoszeń bezpieczeństwa, monitorowania znanych podatności, właściwych aktualizacji i udzielania informacji użytkownikom. Okres wsparcia należy określić na podstawie oczekiwanego czasu używania produktu i przepisów CRA; co do zasady nie może być krótszy niż 5 lat, chyba że oczekiwany okres użytkowania jest krótszy. [R3]

- Zdefiniuj i przekaż użytkownikowi okres wsparcia; przypisz osobę monitorującą podatności.
- Utrzymuj listę wersji produktu oraz dystrybucję poprawek do istniejącej bazy urządzeń.
- Weryfikuj wpływ zmian sprzętowych, architektury i zastosowania na dokumentację i zgodność.
- Nie kończ nadzoru po nadaniu CE - dbaj o proces obsługi podatności i zdarzeń aż do końca właściwych obowiązków.

7. Konsekwencje braku zgodności i przygotowanie do kontroli

Regulacje przewidują administracyjne środki nadzoru i sankcje. Szczegółowy poziom i podstawę sankcji trzeba ustalać w odniesieniu do naruszenia oraz organu nadzoru - bez automatycznego przyjmowania maksymalnej kary jako typowego scenariusza. Ryzyka praktyczne to także opóźnienie dostawy, wycofanie produktu, koszt poprawek, utrata kontraktu i roszczenia klienta.

> **Audyt próbuje odtworzyć decyzję**
> Dobrą dokumentację poznaje się po tym, że niezależny inżynier może wskazać: jaki wariant urządzenia testowano, dlaczego dane zabezpieczenie wybrano, jaki test to potwierdza oraz jakie ryzyko pozostało po wydaniu.

Warsztat V-1. Przegląd kompletności Technical File

Zadanie
Grupa otrzymuje ST-24 w wersji 1.4.2, raport pentestu, listę bibliotek bez wersji, schemat elektryczny i brak historii programowania. Wskaż braki, wyznacz priorytety i przygotuj bramkę wydania.

Rezultat do zapisania: Tabela [artefakt / status / ryzyko braku / właściciel / termin / decyzja].

Wskazówki dla prowadzącego / odpowiedź: Najpierw odróżnij brak dokumentacji od braku rzeczywistej kontroli. Uzupełnij wersje SBOM, ocenę ryzyka i testy powiązane z wydaniem. Pentest nie pokrywa automatycznie całego załącznika I.

MODUŁ A / 0 MIN

Załączniki robocze i gotowe checklisty

Wzory do wydrukowania i użycia w zespole projektowym lub podczas szkolenia.

Po tym module uczestnik potrafi:
Przenieść wiedzę do rzeczywistych procedur, rejestrów i artefaktów projektu.

A1. Checklista kwalifikacji KSC / CRA

Pytanie	Odpowiedź / dowód
Czy firma świadczy usługi w sektorze z załączników KSC?	TAK / NIE / DO ANALIZY; zakres działalności
Czy zastosowanie mają progi wielkości i wyjątki KSC?	TAK / NIE / DO ANALIZY; decyzja prawna
Czy wymagany jest wpis do wykazu KSC i korzystanie z S46?	Właściciel, termin i dowód
Czy produkt jest sprzętem/oprogramowaniem z elementami cyfrowymi?	Opis funkcji i granicy produktu
Czy jest udostępniany na rynku UE w działalności handlowej?	Model sprzedaży, oferta/umowa
Czy występują wyłączenia lub szczególne akty produktowe?	Podstawa prawna i uzasadnienie
Kto jest producentem w rozumieniu CRA?	Właściciel marki, integrator, importer
Jaka jest klasyfikacja CRA i ścieżka oceny zgodności?	Decyzja, źródło, osoba zatwierdzająca

Decyzja: zakres ..... / osoba ..... / data ..... / dokument źródłowy .....

A2. Rejestr ryzyka - formularz

ID / zasób	Atak i skutek	P × I	Kontrola / dowód	Ryzyko resztkowe
R-___ / ___	_____	___	_____	___
R-___ / ___	_____	___	_____	___
R-___ / ___	_____	___	_____	___
R-___ / ___	_____	___	_____	___

Do każdego wiersza dopisz: właściciela, datę przeglądu, plan działania, decyzję o akceptacji i powiązany test. Skala P × I to wyłącznie narzędzie warsztatowe.

A3. Checklista produktu i wydania firmware

- □ Produkt ma jednoznaczny identyfikator, wersję i rewizję hardware.
- □ Źródła, zależności i proces build są przypięte do zatwierdzonego wydania.
- □ Istnieje aktualna ocena ryzyka dla funkcji, konfiguracji i środowiska.
- □ Wykonano przegląd interfejsów serwisowych, kont domyślnych i portów sieciowych.
- □ Klucze i poświadczenia nie są przechowywane w repozytorium w kodzie jawnym.
- □ Paczka aktualizacji ma kontrolowane pochodzenie i jest weryfikowana przed użyciem.
- □ Sprawdzono ograniczenia mechanizmów wbudowanych dla danego MCU.
- □ Wykonano testy regresji, uprawnień, awarii sieci i nieprawidłowych danych.
- □ Powiązano logi, raporty testowe i SBOM z konkretną wersją.
- □ Przygotowano bezpieczny proces rollback/odzyskania urządzenia.
- □ Zatwierdzono instrukcję serwisową, zakres wsparcia i kontakt bezpieczeństwa.

A4. Wzór zawiadomienia wewnętrznego o incydencie

Pole	Do uzupełnienia
Identyfikator i zgłaszający	IR-____; konto / numer telefonu
Oś czasu	Wykryto: ____; rozpoczęto reakcję: ____
Wpływ	Systemy / urządzenia / produkcja / bezpieczeństwo ludzi / dane
Objawy i dowody	Adresy, identyfikatory zdarzeń, wersje, logi, PCAP, nazwa hosta
Decyzje natychmiastowe	Odcięcie konta / segmentu, wstrzymanie produkcji, backup dowodów
Właściciel i komunikacja	Techniczny: ____; prawny/compliance: ____; klient: ____
Ocena raportowalności	NIS2/KSC: ____; CRA: ____; inne: ____; uzasadnienie
Zamknięcie	Retest, decyzja o wznowieniu, przyczyna, działania zapobiegawcze

A5. Checklista Technical File - robocza

- □ Opis produktu, intended purpose, producent, modele i identyfikacja wydań.
- □ Rysunki, zdjęcia, schemat systemu i opis interfejsów.
- □ Wersje software mające wpływ na zgodność i lista komponentów.
- □ Ocena ryzyka cyberbezpieczeństwa i uzasadnienia stosowania wymagań.
- □ Mapowanie wymagań zasadniczych CRA (zał. I) do implementacji.
- □ Opis projektowania, produkcji, procesu aktualizacji i zarządzania podatnościami.
- □ Wyniki testów / weryfikacji i zastosowane normy/specyfikacje.
- □ Instrukcja i informacje o bezpiecznej konfiguracji dla użytkownika.
- □ Dokumentacja procedury oceny zgodności i właściwa deklaracja UE.
- □ Historia zmian i odpowiedzialność za utrzymanie dokumentacji.

Lista służy przygotowaniu dokumentacji; rzeczywiste wymagania należy weryfikować z art. 31 i załącznikiem VII CRA. Nie każda pozycja ma tę samą postać dla każdego wyrobu.

A6. Minimalny plan wdrożenia - pierwsze 90 dni

Okres	Zadanie	Właściciel / rezultat
Dni 1–15	Klasyfikacja KSC i CRA; właściciele; inwentaryzacja systemów i produktów	Zarząd + compliance + inżynierowie; decyzje i rejestr
Dni 16–30	Model zagrożeń ST-24, rejestr ryzyka, zakres monitoringu, mapa sieci	Lider OT/IT; ocena ryzyka i diagram
Dni 31–45	Repozytorium wydań, release manifest, SBOM/HBOM i skan zależności	Embedded + DevOps; artefakty w CI
Dni 46–60	Procedura dostępu i aktualizacji, logowanie, alerty, ćwiczenia incydentu	IT/OT + produkcja; raport testów
Dni 61–75	Technical File, traceability, testy negatywne, plan wsparcia	Właściciel produktu; wersjonowana dokumentacja
Dni 76–90	Przegląd braków, plan budżetu, akceptacja ryzyk i audyt próbny	Kierownictwo; plan zamknięcia i odpowiedzialności

A7. Mini test wiedzy - 12 pytań

1. Czy sama obecność mikrokontrolera przesądza o podleganiu CRA?
2. Dlaczego KSC i CRA trzeba oceniać osobno?
3. Jakie trzy dowody wiążą firmware z konkretnym egzemplarzem urządzenia?
4. Dlaczego CRC nie chroni przed celową podmianą pliku HEX?
5. Czy VLAN bez ACL/firewalla wystarczy do separacji krytycznej strefy?
6. Co oprócz CVSS trzeba sprawdzić po wykryciu podatności biblioteki?
7. Do czego służy SBOM, a do czego HBOM?
8. Jaki jest warunek uruchomienia raportowania CRA po 11.09.2026?
9. Ile czasu przewidziano w CRA na wczesne ostrzeżenie po uzyskaniu wiedzy?
10. Czym różni się RTO od RPO?
11. Czy pentest zastępuje Technical File i ocenę zgodności CRA?
12. Jakie powiązanie powinno istnieć między wymaganiem a testem?

A8. Klucz odpowiedzi - skrót dla prowadzącego

1. Nie: liczy się m.in. definicja produktu, udostępnienie na rynku, wyłączenia i odpowiedzialność producenta.
2. KSC obejmuje określone organizacje i usługi, CRA - określone produkty z elementami cyfrowymi.
3. Na przykład manifest wydania, identyfikator urządzenia i protokół programowania/weryfikacji.
4. CRC nie jest kryptograficznym dowodem autentyczności ani integralności wobec aktywnego napastnika.

5. Nie: niezbędne są kontrolowane relacje ruchu, reguły sieci i monitoring.

6. Wersję, ekspozycję, osiągalność funkcji, konfigurację, wpływ na produkt i środki zaradcze.

7. SBOM mapuje komponenty oprogramowania, HBOM komponenty fizyczne i ich warianty.

8. Zdarzenie musi spełniać przesłanki aktywnie wykorzystywanej podatności lub poważnego incydentu wpływającego na bezpieczeństwo produktu.

9. Co do zasady w ciągu 24 godzin od uzyskania wiedzy, bez zbędnej zwłoki.

10. RTO to cel czasu odtworzenia, RPO to dopuszczalny punkt utraty danych.

11. Nie. Pentest jest jednym z możliwych dowodów weryfikacyjnych, nie procesem oceny zgodności.

12. Macierz traceability: ID wymagania, implementacja, metoda i wynik testu, wersja i artefakt.

BIBLIOGRAFIA I PODSTAWY PRAWNE

Źródła i dokumenty odniesienia

Źródła zweryfikowano na 20.11.2026. Przy stosowaniu materiałów na późniejsze szkolenie trzeba ponownie sprawdzić stan prawny, aktualne dokumenty normalizacyjne i interpretacje.

[R1] Dyrektywa (UE) 2022/2555, NIS2

https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

[R2] Ministerstwo Cyfryzacji - nowelizacja KSC: obowiązki i terminy

https://www.gov.pl/web/cyfryzacja/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ksc---obowiazki-podmiotow-kluczowych-i-waznych

[R3] Rozporządzenie (UE) 2024/2847 - CRA: art. 13, 14, 31–32 i załączniki I, II, VII, VIII

https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R2847

[R4] Ministerstwo Cyfryzacji - KSC: najważniejsze terminy

https://www.gov.pl/web/cyfryzacja/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ksc--najwazniejsze-terminy

[R5] Komisja Europejska - CRA: obowiązki raportowania od 11.09.2026

https://digital-strategy.ec.europa.eu/en/policies/cra-reporting

[R6] ENISA - Single Reporting Platform, FAQ i terminy powiadomień

https://www.enisa.europa.eu/topics/product-security/vulnerability-services/eu-incident-response-and-cyber-crisis-management/single-reporting-platform-srp/frequently-asked-questions

[R7] Komisja Europejska - podsumowanie CRA i modułów oceny zgodności

https://digital-strategy.ec.europa.eu/en/policies/cra-summary

[R8] Tekst wejściowy użytkownika: program warsztatów NIS2 / CRA

Materiał przekazany przez użytkownika 20.11.2026; 5 modułów i proponowana agenda.

> **Co jest wymogiem prawa, a co dobrą praktyką?**
> KSC/NIS2 i CRA określają obowiązki oraz wymogi ramowe. Liczby „12 obszarów / 40 wymagań”, skale P × I, RACI, konkretna topologia VLAN, wybrane pola SBOM/HBOM, KPI i okres 90 dni są ujęte w materiałach jako **narzędzia szkoleniowe lub rekomendowane metody**, a nie katalog ustawowych obowiązków.

KONIEC MATERIAŁÓW • WERSJA SZKOLENIOWA 20.11.2026