WHITEPAPER CRA EVIDENCE

Unijny akt o cyberodporności: praktyczny przewodnik zgodności

Whitepaper dla producentów, importerów i dystrybutorów produktów z elementami cyfrowymi.

Przygotowane przez	CRA Evidence
Wersja	1.0
Status	Aktualizowany na bieżąco
Podstawa	Rozporządzenie (UE) 2024/2847

Historia zmian

Aktualizujemy ten dokument w miarę rozwoju wytycznych Komisji, norm zharmonizowanych i praktyki rynkowej w ramach CRA.

Wersja	Data	Opis
1.0	17 maja 2026 r.	Pierwsze wydanie. Obejmuje zakres, klasyfikację, istotną modyfikację, wymagania zasadnicze, postępowanie z podatnościami, dokumentację techniczną, ścieżki oceny zgodności oraz interakcję z AI Act, Data Act, ESPR i odpowiedzialnością za produkt.

Spis treści

Najważniejsze informacje

W 60 SEKUND

Zakres: połączone produkty sprzętowe i programowe udostępniane na rynku UE. Bezpieczeństwo staje się wymaganiem zgodności produktu, nie tylko dobrą praktyką.

Terminy: zgłoszenia z art. 14 od 11 września 2026 r.; pełne obowiązki techniczne, dokumentacyjne i dotyczące oznakowania CE od 11 grudnia 2027 r.

Wymagane wyniki pracy: ocena ryzyka w cyberprzestrzeni, SBOM, dokumentacja techniczna, instrukcje dla użytkownika, deklaracja zgodności UE, oznakowanie CE oraz zgłoszenia incydentów i podatności z art. 14.

Kto musi działać

Główny ciężar spoczywa na producentach. Importerzy i dystrybutorzy mają kontrole należytej staranności przed udostępnieniem produktów.

Co się zmienia

Cyberbezpieczeństwo staje się częścią zgodności produktu: bezpieczny projekt, obsługa podatności, dokumentacja, CE i działania po wprowadzeniu do obrotu.

Pierwszy termin

Zgłoszenia z art. 14 zaczynają się **11 września 2026 r.** dla aktywnie wykorzystywanych podatności i poważnych incydentów.

Pełne stosowanie

Pełna zgodność techniczna obowiązuje od **11 grudnia 2027 r.** Wcześniejsze produkty są objęte po istotnej modyfikacji, ale zgłaszanie nadal ma zastosowanie.

Kręgosłup dowodowy

Dokumentacja techniczna potrzebuje oceny ryzyka, SBOM, uzasadnienia okresu wsparcia, dowodów z testów, instrukcji, deklaracji i dowodów zgodności z zasadniczymi wymaganiami cyberbezpieczeństwa.

Ścieżka zgodności

Większość produktów może zastosować moduł A. Produkty ważne i krytyczne mogą wymagać jednostki notyfikowanej albo europejskiej certyfikacji cyberbezpieczeństwa.

Czym jest akt o cyberodporności?

Akt o cyberodporności, czyli Rozporządzenie (UE) 2024/2847, jest pierwszym ogólnounijnym aktem, który wprowadza wiążące wymagania cyberbezpieczeństwa dla produktów z elementami cyfrowymi udostępnianych na rynku UE. Tekst autorytatywny jest dostępny w EUR-Lex.

CRA dotyczy producentów, importerów i dystrybutorów połączonego sprzętu oraz oprogramowania. Obejmuje produkty od konsumenckich urządzeń IoT po przemysłowe systemy sterowania. Praktyczna zmiana jest prosta: cyberbezpieczeństwo trzeba projektować, dokumentować, utrzymywać i monitorować jako część zgodności produktu.

Naruszenia zasadniczych wymagań cyberbezpieczeństwa albo obowiązków z art. 13 i 14 mogą prowadzić do kar do 15 mln EUR albo 2,5% całkowitego rocznego światowego obrotu, w zależności od tego, która kwota jest wyższa. Stosowane są niższe progi: do 10 mln EUR albo 2% za naruszenie innych wskazanych obowiązków, oraz do 5 mln EUR albo 1% za podanie nieprawidłowych, niekompletnych lub wprowadzających w błąd informacji jednostkom notyfikowanym albo organom nadzoru rynku. Organy nadzoru rynku mogą też żądać działań naprawczych, ograniczać dostępność produktu, wycofywać produkt z obrotu albo nakazywać odzyskanie produktu od użytkowników.

Kluczowe daty planowania zgodności

CRA weszło w życie **10 grudnia 2024 r.** Praktyczne prace nad zgodnością koncentrują się na trzech terminach: jednostki notyfikowane w **czerwcu 2026 r.**, zgłoszenia we **wrześniu 2026 r.** i pełna zgodność techniczna w **grudniu 2027 r.**.

UWAGA

Aktualny status wytycznych Komisji: Komisja Europejska opublikowała 3 marca 2026 r. projekt wytycznych CRA. Konsultacje zakończyły się 13 kwietnia 2026 r. Wytyczne nie są ostateczne, ale stanowią przydatny materiał planistyczny dotyczący wprowadzania produktu do obrotu, wolnego i otwartego oprogramowania, okresów wsparcia, istotnych modyfikacji, klasyfikacji produktów, należytej staranności wobec komponentów, zdalnego przetwarzania danych, obsługi podatności i nakładania się z innymi przepisami UE. Kwestie graniczne dotyczące AI Act i DORA mogą nadal wymagać dodatkowych wytycznych.

10 grudnia 2024 r.

Wejście w życie

Początek okresu przejściowego

11 czerwca 2026 r.

Jednostki notyfikowane

Stosuje się rozdział IV

11 września 2026 r.

Zgłoszenia

Start zgłoszeń z art. 14

11 grudnia 2027 r.

Pełne stosowanie

Wymagania techniczne, oznakowanie CE, dokumentacja i ocena zgodności

ZACZNIJ OD TEGO

Zacznij od gotowości do zgłaszania. Termin z art. 14 przychodzi wcześniej niż pełna zgodność techniczna i obejmuje produkty już obecne na rynku UE.

Ponieważ zgłaszanie zaczyna się **11 września 2026 r.**, gotowość do zgłoszeń powinna być pierwszym strumieniem wdrożeniowym: **wykrywanie, triage, komunikacja z użytkownikami i zgłoszenia do organów** muszą działać przed terminem pełnej zgodności technicznej.

Produkty wprowadzone do obrotu przed **11 grudnia 2027 r.** podlegają wymaganiom technicznym CRA tylko wtedy, gdy od tej daty przechodzą **istotną modyfikację**. Art. 14 działa inaczej. Obowiązek zgłaszania obejmuje **wszystkie produkty w zakresie CRA**, także te wprowadzone do obrotu wcześniej.

CRA w cyklu życia produktu

KROK 01

Ustal zakres produktu

Zakres, klasyfikacja, okres wsparcia i ocena ryzyka

KROK 02

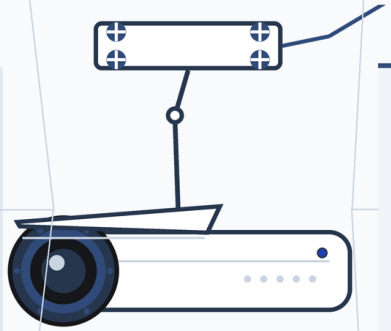
Projektuj bezpiecznie

Bezpieczne ustawienia domyślne, analiza kodu, SBOM i kontrola zależności

KROK 03

Waliduj i dokumentuj

Testy, triage podatności, dokumentacja techniczna i instrukcje



KROK 04

Wprowadź na rynek

Deklaracja zgodności UE, oznakowanie CE i decyzja o wydaniu

KROK 05

Monitoruj i aktualizuj

CVE, komunikaty, exploity, aktualizacje i ujawnienia

KROK 06

Wspieraj i współpracuj

Zgłoszenia z art. 14, powiadomienia użytkowników, żądania organów i koniec wsparcia

Połączona kamera IP od planowania produktu po wsparcie po wprowadzeniu na rynek zgodnie z CRA

Produkty objęte zakresem

Zakres i wyłączenia

CRA dotyczy produktów sprzętowych i programowych, których przeznaczenie albo racjonalnie przewidywalne wykorzystanie obejmuje bezpośrednie lub pośrednie połączenie danych z urządzeniem albo siecią. Obejmuje to komputery, smartfony, sprzęt sieciowy, urządzenia IoT, przemysłowe systemy sterowania i aplikacje do przetwarzania danych.

Wyraźnie wyłączone są następujące kategorie:

- Wyroby medyczne i wyroby medyczne do diagnostyki in vitro objęte rozporządzeniami (UE) 2017/745 i 2017/746
- Systemy pojazdów objęte rozporządzeniem (UE) 2019/2144
- Wyposażenie lotnicze objęte rozporządzeniem (UE) 2018/1139
- Wyposażenie morskie objęte dyrektywą 2014/90/UE
- Produkty opracowane wyłącznie do celów bezpieczeństwa narodowego albo obrony
- Produkty czysto mechaniczne bez elementów cyfrowych albo łączności sieciowej

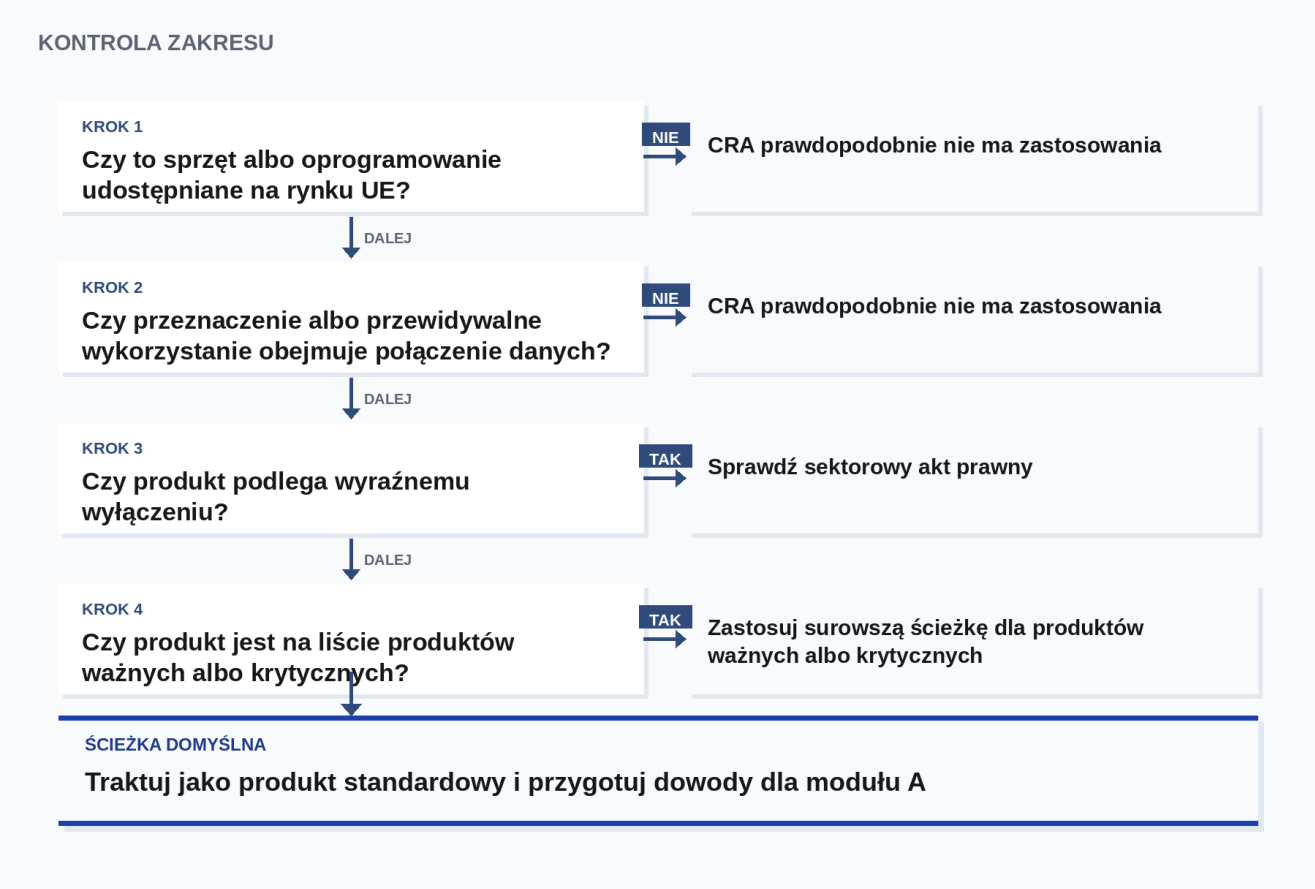
Jeżeli nie ma jasnego wyłączenia, traktuj połączony produkt jako produkt w zakresie CRA.

UWAGA

Produkty dostosowane do indywidualnych potrzeb: wąski wyjątek. Jeżeli producent buduje produkt dopasowany do jednego konkretnego użytkownika biznesowego na podstawie pisemnej umowy między producentem a tym użytkownikiem, można odstąpić tylko od dwóch wymagań: od bezpiecznej konfiguracji domyślnej (musi pozostać ścieżka powrotu do pierwotnego bezpiecznego stanu) oraz od bezpłatnych aktualizacji zabezpieczeń (umowa może ustalić inną podstawę handlową). Wszystko inne obowiązuje w pełni: postępowanie z podatnościami, pozostałe wymagania bezpieczeństwa produktu, zgłaszanie z art. 14, dokumentacja techniczna, oznakowanie CE, ocena zgodności i okres wsparcia. To nie jest ogólne wyłączenie B2B; nie obejmuje gotowych produktów sprzedawanych firmom.

OBOWIĄZKI PODMIOTÓW GOSPODARCZYCH

Producent	Projektuje bezpieczne produkty, ocenia ryzyko, przygotowuje dokumentację techniczną, prowadzi ocenę zgodności, obsługuje podatności i zgłasza zdarzenia z art. 14.
Importer	Sprawdza zgodność po stronie producenta, weryfikuje oznakowanie CE i dokumentację, przechowuje deklarację i reaguje na znane podatności.
Dystrybutor	Sprawdza wskaźniki należytej staranności przed dostawą, weryfikuje wymagane informacje i instrukcje oraz nie udostępnia produktów niezgodnych.



Klasyfikacja produktu wyznacza ścieżkę oceny

Kategoria produktu określa sposób wykazania zgodności.

Kategoria	Przykłady	Ocena zgodności
Standardowy „niesklasyfikowany”	Ogólne oprogramowanie i połączone produkty konsumenckie, które nie należą do kategorii ważnych ani krytycznych	Moduł A: samoocena
Ważny „klasa I”	Zarządzanie tożsamością, przeglądarki, menedżery haseł, antywirusy, VPN, zarządzanie siecią, routery, inteligentne zamki, kamery bezpieczeństwa i produkty podobne	Moduł A tylko wtedy, gdy stosuje się właściwe normy zharmonizowane, wspólne specyfikacje albo systemy certyfikacji; w innym przypadku moduł B+C albo moduł H
Ważny „klasa II”	Hipernadzorcy, środowiska uruchomieniowe kontenerów, zapory sieciowe, IDS/IPS i odporne na manipulacje mikroprocesory	Moduł B+C, moduł H albo właściwy europejski system certyfikacji cyberbezpieczeństwa na co najmniej „istotnym” poziomie uzasadnienia zaufania
Krytyczne	Bezpieczne elementy, karty inteligentne, bramy inteligentnych liczników i sprzętowe moduły bezpieczeństwa	Europejska certyfikacja cyberbezpieczeństwa, gdy jest wymagana i dostępna; w pozostałych przypadkach ścieżki dla klasy II

Cztery kategorie produktów

Tabela powyżej pokazuje przykłady. Pełny wykaz, względem którego porównuje się podstawową funkcjonalność produktu, znajduje się poniżej.

Produkty standardowe

Większość produktów trafia do tej kategorii. Każdy produkt z elementami cyfrowymi, którego podstawowa funkcjonalność nie odpowiada żadnej pozycji z list ważnych ani krytycznych poniżej, traktowany jest jako standardowy. Ścieżka zgodności to samoocena w module A.

Typowe przykłady:

- Telewizory smart i urządzenia streamingowe.
- Drukarki sieciowe i wielofunkcyjne urządzenia biurowe.
- Głośniki Bluetooth i konsumencki sprzęt audio.
- Aplikacje do odtwarzania mediów.
- Konsole do gier, czytniki e-booków i podobna elektronika konsumencka.
- Inteligentny sprzęt AGD: piekarniki, lodówki, zmywarki bez funkcji bezpieczeństwa.
- Inteligentne żarówki i połączone oświetlenie bez funkcji bezpieczeństwa.
- Opaski fitness bez przeznaczenia związanego z monitorowaniem zdrowia.
- Aplikacje mobilne ogólnego przeznaczenia, które nie są przeglądarkami, menedżerami haseł ani aplikacjami VPN.
- Oprogramowanie biurowe, takie jak edytory tekstu i arkusze kalkulacyjne.

Powyższa lista ma charakter ilustracyjny. Listy ważnych i krytycznych są wyczerpujące.

Produkty ważne (klasa I)

Obowiązkowa ocena strony trzeciej, chyba że stosuje się właściwe normy zharmonizowane, wspólne specyfikacje albo systemy certyfikacji.

1. Oprogramowanie i sprzęt do zarządzania tożsamością i uprzywilejowanym dostępem, w tym czytniki uwierzytelniania i kontroli dostępu (także biometryczne).
2. Samodzielne i wbudowane przeglądarki.
3. Menedżery haseł.
4. Oprogramowanie wyszukujące, usuwające albo izolujące złośliwe oprogramowanie.
5. Produkty VPN.
6. Systemy zarządzania siecią.
7. Systemy zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM).
8. Menedżery rozruchu.
9. Oprogramowanie infrastruktury klucza publicznego i wydawania certyfikatów cyfrowych.
10. Fizyczne i wirtualne interfejsy sieciowe.
11. Systemy operacyjne.
12. Routery, modemy przeznaczone do połączenia z internetem i przełączniki.

13. Mikroprocesory z funkcjami związanymi z bezpieczeństwem.
14. Mikrokontrolery z funkcjami związanymi z bezpieczeństwem.
15. ASIC i FPGA z funkcjami związanymi z bezpieczeństwem.
16. Wirtualni asystenci ogólnego przeznaczenia dla inteligentnego domu.
17. Produkty inteligentnego domu z funkcjami bezpieczeństwa (inteligentne zamki, kamery bezpieczeństwa, nianie elektroniczne, systemy alarmowe).
18. Zabawki połączone z internetem z funkcjami interaktywnymi (mówienie, nagrywanie, śledzenie lokalizacji).
19. Osobiste urządzenia ubieralne z funkcjami monitorowania zdrowia (gdy nie stosują się rozporządzenia (UE) 2017/745 albo 2017/746) lub urządzenia ubieralne przeznaczone dla dzieci.

Produkty ważne (klasa II)

Obowiązkowa ocena strony trzeciej, ścieżka surowsza. Samoocena nie jest dostępna, nawet gdy istnieją normy zharmonizowane.

1. Hipernadzorcy i środowiska uruchomieniowe kontenerów wspierające wirtualizowane wykonywanie systemów operacyjnych i podobnych środowisk.
2. Zapory sieciowe, systemy wykrywania i zapobiegania włamaniom.
3. Odporne na manipulacje mikroprocesory.
4. Odporne na manipulacje mikrokontrolery.

Produkty krytyczne

Europejska certyfikacja cyberbezpieczeństwa wymagana, gdy system jest dostępny. W pozostałych przypadkach stosuje się ścieżkę klasy II.

1. Urządzenia sprzętowe z modułami bezpieczeństwa.
2. Bramy inteligentnych liczników w inteligentnych systemach pomiarowych zdefiniowanych w art. 2 pkt 23 dyrektywy (UE) 2019/944 oraz inne urządzenia o zaawansowanych funkcjach bezpieczeństwa, w tym do bezpiecznego przetwarzania kryptograficznego.
3. Karty inteligentne i podobne urządzenia, w tym bezpieczne elementy.

Jeżeli podstawowa funkcjonalność produktu odpowiada pozycji z listy ważnych albo krytycznych, produkt należy do tej klasy. Jeżeli produkt integruje jedną z tych pozycji jako komponent, ale jego własna podstawowa funkcjonalność jest inna, integracja nie zmienia klasy produktu.

Jak klasyfikować: podstawowa funkcjonalność, nie integracja

Powyższe listy mówią, jakie są kategorie. Nie mówią, jak je zastosować do konkretnego produktu. Odpowiedź CRA mieści się w jednym pojęciu: **podstawowa funkcjonalność**.

Klasę wyznacza to, czym jest podstawowa funkcjonalność produktu, a nie to, jakie komponenty produkt integruje. Jeżeli podstawowa funkcjonalność pasuje do listy ważnych, produkt jest ważny (klasa I lub II). Jeżeli pasuje do listy krytycznych, produkt jest krytyczny. Jeżeli do żadnej, produkt jest standardowy. To jest cały test.

Praktyczne zabezpieczenie kryje się w drugim zdaniu art. 7 ust. 1. Zintegrowanie ważnego komponentu nie przesuwa produktu integrującego do klasy ważnych. Wbudowanie biblioteki zapory sieciowej w koncentrator inteligentnego domu nie czyni z koncentratora zapory. Motyw 45 stawia to wprost: zapory i systemy wykrywania włamań są w klasie II ważnych, ale produkty, które je integrują, nie są.

Stosuj tę sekwencję, aby samodzielnie sklasyfikować produkt.

1. **Nazwij podstawową funkcjonalność produktu w jednym zdaniu.** Jeżeli to się nie udaje, reszta analizy się rozsypuje. Skup się na tym, bez czego produkt nie działa.
2. **Sprawdź listy ważnych powyżej.** Trafienie w klasie I lub II oznacza, że produkt jest ważny.
3. **Sprawdź listę krytycznych powyżej.** Trafienie oznacza, że produkt jest krytyczny. Stosuje się europejską certyfikację cyberbezpieczeństwa, gdy system jest dostępny; w pozostałych przypadkach ścieżkę klasy II.
4. **Brak trafienia na żadnej liście.** Produkt jest standardowy. Ścieżka to samoocena w module A.
5. **Udokumentuj rozumowanie.** Jednostronicowa notatka ze zdaniem o podstawowej funkcjonalności, sprawdzeniem list i wybraną ścieżką należy do dokumentacji technicznej.

Dwa praktyczne przykłady.

Koncentrator inteligentnego domu z wbudowanym menedżerem haseł. Podstawowa funkcjonalność: orkiestracja scenariuszy między urządzeniami IoT w domu. Komponent menedżera haseł, sprzedawany osobno przez własnego producenta, jest sam w sobie produktem ważnym klasy I. Podstawowa funkcjonalność koncentratora to automatyka domowa, nie zarządzanie poświadczeniami. Koncentrator pozostaje standardowy.

System operacyjny rozpoznany po zestawie funkcji. Produkt sprzedawany jest jako urządzenie inteligentnego domu, ale jego główne funkcje to inicjalizacja sprzętu i peryferiów, planowanie procesów, zarządzanie pamięcią i interfejs wywołań systemowych. To podstawowa funkcjonalność systemu operacyjnego. Systemy operacyjne są produktem ważnym klasy I. Produkt jest ważny klasy I, niezależnie od marketingu.

Jeżeli klasyfikacja zaskakuje resztę zespołu, zdanie o podstawowej funkcjonalności wymaga jeszcze jednego przejścia, zanim produkt trafi na rynek.

Gdy chmura jest częścią produktu

Większość produktów z elementami cyfrowymi opiera się na czymś poza urządzeniem: backendzie chmurowym, mobilnej aplikacji towarzyszącej, serwerze aktualizacji OTA, portalu uwierzytelniania, systemie zarządzania urządzeniami. CRA nie traktuje wszystkiego tego jak produktu producenta. Traktuje to jako część produktu wyłącznie wtedy, gdy spełnione są **oba** warunki:

- Oprogramowanie zostało **zaprojektowane i opracowane przez zespół producenta albo na jego odpowiedzialność**.
- Bez tego oprogramowania produkt **nie wykonywałby jednej ze swoich funkcji**.

Jeżeli choć jeden warunek nie jest spełniony, usługa zdalna stoi poza granicą produktu w rozumieniu CRA. SaaS strony trzeciej, którego producent nie posiada, nawet jeśli produkt z nim rozmawia, nie jest częścią produktu. Strona internetowa promująca produkt, która nie wspiera jego funkcji, też nie jest częścią produktu.

Gdy komponent zdalny jest w zakresie, jest w zakresie **jako część produktu**. Dokumentacja techniczna, ocena zgodności, deklaracja zgodności, postępowanie z podatnościami i terminy zgłaszania z art. 14 obejmują wtedy komponent chmurowy wraz z urządzeniem.

Stosuj tę macierz, aby szybko rozstrzygnąć przypadek.

Komponent	W zakresie jako część produktu?
Mobilna aplikacja towarzysząca, która paruje się z urządzeniem	**Tak.** Zaprojektowana przez producenta, a urządzenia nie da się skonfigurować ani używać bez niej.
Backend chmurowy, który przechowuje i przetwarza dane urządzenia	**Tak.** Zaprojektowany przez producenta, a panel albo główna funkcja bez niego nie działa.
Serwer aktualizacji OTA	**Tak.** Zaprojektowany przez producenta, a urządzenie bez niego nie odbiera aktualizacji zabezpieczeń.
Portal uwierzytelniania kontrolujący dostęp do urządzenia	**Tak.** Zaprojektowany przez producenta, a użytkownicy bez niego nie mogą się zalogować.
Strona marketingowa produktu	**Nie.** Nie wspiera funkcji produktu.
SaaS strony trzeciej, z którym produkt się integruje (nie należy do producenta)	**Nie.** Nie zaprojektowany przez producenta. Dostawca strony trzeciej ma własne obowiązki na podstawie NIS 2.
Ogólna infrastruktura chmurowa, na której działa usługa (IaaS lub PaaS)	**Nie.** Nie zaprojektowana przez producenta. Dostawca infrastruktury podlega NIS 2.

Częsty wzorzec: urządzenie inteligentnego domu z mobilną aplikacją, serwerem aktualizacji i backendem chmurowym. Wszystkie trzy zaprojektowane przez producenta, a urządzenie bez nich nie wykonuje swoich reklamowanych funkcji. Wszystkie trzy są częścią produktu. Obowiązki CRA dotyczą całego zestawu. Jeżeli backend chmurowy następnie rozmawia z SaaS analitycznym strony trzeciej, ten SaaS nie jest częścią produktu. Dostawca strony trzeciej ma własne obowiązki na podstawie NIS 2.

CRA nie wymaga środków bezpieczeństwa dla całej sieci i systemów informacyjnych producenta. Wymaga bezpieczeństwa dla usług zdalnych, które są częścią produktu. Granica biegnie po produkcie, nie po firmie.

Łańcuch dostaw: kto co robi w ramach CRA

CRA nakłada główne obowiązki na producenta, ale importerzy i dystrybutorzy też mają zadania, które wpływają na to, jak produkt dociera na rynek. Trzy rzeczy są tu istotne dla producenta.

Podmiot	Co weryfikuje przed dostawą	Co robi przy podatności	Kiedy przejmuje obowiązki producenta
Importer	Oznakowanie CE, deklarację zgodności UE, instrukcje w odpowiednim języku, dane kontaktowe producenta na produkcie albo z produktem	Bez zbędnej zwłoki informuje producenta; bezpośrednio informuje organy nadzoru rynku, jeżeli produkt stanowi istotne ryzyko dla cyberbezpieczeństwa	Gdy umieszcza produkt pod własną nazwą albo znakiem towarowym lub istotnie go modyfikuje
Dystrybutor	Oznakowanie CE, to, że producent i importer wykonali swoją część, oraz to, że wymagane dokumenty są dołączone do produktu	Bez zbędnej zwłoki informuje producenta; bezpośrednio informuje organy nadzoru rynku, jeżeli produkt stanowi istotne ryzyko dla cyberbezpieczeństwa; może zaprzestać udostępniania produktu	Ten sam wyzwalacz co dla importerów

Dla producenta oznacza to trzy praktyczne sprawy:

- Oznakowanie CE, deklaracja zgodności UE i instrukcje dla użytkownika muszą być poprawne i w odpowiednim języku w momencie, gdy dystrybutor je sprawdza. Partnerzy kanałowi mają obowiązek je weryfikować i mogą odmówić udostępnienia produktu, jeżeli czegoś brakuje albo coś jest błędne.
- Producent potrzebuje jasnej, niskoprogowej ścieżki kontaktowej, której importerzy i dystrybutorzy mogą użyć do zgłaszania podatności do procesu postępowania z podatnościami. Skorzystają z niej.
- Każdy partner, który zmienia markę, umieszcza produkt pod własną nazwą lub znakiem towarowym albo istotnie modyfikuje produkt, staje się producentem dla tego wariantu. Pełne obowiązki w zakresie dokumentacji technicznej, oceny zgodności, zgłaszania i okresu wsparcia przechodzą na niego dla tej wersji. Zob. *Kiedy producentem staje się ktoś inny* w następnej części, dla reguły istotnej modyfikacji.

Istotna modyfikacja: kiedy zgodność trzeba ocenić ponownie

Gdy produkt jest już na rynku, CRA dzieli późniejsze zmiany na dwa obozy. Większość jest rutynowa i nie wymaga niczego dodatkowo. Część jest istotna. Istotna modyfikacja jest traktowana, do celów CRA, jako wprowadzenie nowego produktu do obrotu. Oznacza to nową ocenę zgodności, odświeżoną dokumentację techniczną, nową deklarację zgodności i oznakowanie CE na nowej wersji.

Test jest krótki i zawarty w definicji istotnej modyfikacji. Zmiana jest istotna, jeżeli prawdziwe jest jedno z dwóch:

- **Wpływa na zgodność** z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa.
- **Zmienia przeznaczenie**, w odniesieniu do którego produkt oceniono.

Jeżeli żaden z tych warunków nie jest spełniony, zmiana nie jest istotna. Mimo to udokumentuj rozumowanie i zachowaj je w aktach. Analiza jest częścią śladu dowodowego.

Co nie liczy się jako istotne

Dwa wyjątki wykonują w praktyce większość pracy.

Aktualizacje zabezpieczeń i poprawki błędów, które zmniejszają ryzyko w zakresie cyberbezpieczeństwa bez zmiany przeznaczenia, nie są istotne. Łatanie znanej podatności, korekta walidacji danych wejściowych w celu zamknięcia luki albo przebudowa komponentu w celu obsłużenia CVE leżą po tej stronie linii.

Odnowienie, konserwacja i naprawy też nie są automatycznie istotne. Stają się istotne dopiero wtedy, gdy zmieniają przeznaczenie albo wpływają na zgodność z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa.

Drobne prace w interfejsie użytkownika również pozostają po bezpiecznej stronie. Dodanie języka, podmiana zestawu ikon czy szlif układu ekranu same w sobie nie są istotną modyfikacją. Dodanie nowego elementu wejściowego, który wymaga odpowiedniej walidacji danych, już może być istotne.

Części zamienne

CRA wyłącza części zamienne w sposób wąski i konkretny. **Identyczne części zamienne**, wykonane według tej samej specyfikacji co komponenty, które zastępują, leżą w całości poza zakresem rozporządzenia. Zamienniki funkcjonalne nie.

Stosuj tę macierz, aby szybko rozstrzygnąć przypadek.

Wymiana	Produkt wprowadzony do obrotu przed 11 grudnia 2027 r.	Produkt wprowadzony do obrotu w dniu 11 grudnia 2027 r. lub po
Identyczna z oryginalnym komponentem, ta sama specyfikacja	Część zamienna poza zakresem CRA. Wymiana nie uruchamia żadnych obowiązków.	Część zamienna poza zakresem CRA. Wymiana nie uruchamia żadnych obowiązków.
Funkcjonalnie równoważna, inny projekt lub specyfikacja	Zamiennik jest sam w sobie produktem objętym CRA. Produkt-gospodarz nie ma obowiązków z CRA, bo poprzedza datę stosowania.	Zamiennik jest produktem objętym CRA. Oceń, czy zamiana w produkcie-gospodarzu jest jego istotną modyfikacją, używając dwuczęściowego testu powyżej.

Dwie praktyczne konsekwencje. Po pierwsze, wyłączenie zależy od identycznej specyfikacji. Moduł bezprzewodowy przebudowany na innym chipsecie nie jest identyczną częścią zamienną, nawet jeżeli klient nie widzi różnicy. Po drugie, producent, który dostarcza zamiennik funkcjonalny, ponosi obowiązki CRA dla tej części, niezależnie od tego, kto wykonał produkt-gospodarz.

Aktualizacje oprogramowania i przełączniki funkcji

Wydania oprogramowania są najczęstszym źródłem pytań o istotną modyfikację. Dwuczęściowy test wciąż je rozstrzyga.

Poprawka, która usuwa podatność, nie jest istotna. Przełącznik funkcji, który włącza zdolność, dla której produkt nigdy nie był oceniany, już tak. Aktualizacja modelu, która pozwala produktowi decydować o nowych kategoriach danych wejściowych, też. Jeżeli wydanie dostarcza zarówno poprawkę, jak i nową funkcję, oceń funkcję.

Pakowanie liczy się mniej niż treść. Czy aktualizacja funkcji przychodzi osobno, czy w tym samym wydaniu co poprawka bezpieczeństwa, nie ma znaczenia dla oceny.

Jeżeli zespół używa przełączników funkcji albo etapowych wdrożeń, momentem liczącym się jest włączenie funkcji dla użytkowników końcowych w produkcji, a nie wysłanie binarki, która zawiera przełącznik.

Decyzja w praktyce

Stosuj tę sekwencję dla każdej zmiany, zanim trafi do produkcji.

1. **Czy zmiana modyfikuje przeznaczenie produktu?** Jeżeli tak: istotna. Powtórz ocenę zgodności dla nowej wersji.
2. **Czy zmiana wpływa na zgodność z zasadniczymi wymaganiami w zakresie cyberbezpieczeństwa?** Jeżeli tak: istotna. Powtórz ocenę zgodności dla nowej wersji.
3. **W pozostałych przypadkach:** nieistotna. Udokumentuj analizę i kontynuuj na podstawie istniejącej dokumentacji technicznej.

Jeżeli produkt jest w klasie ważnej albo krytycznej i ścieżka pierwotna wymagała oceny strony trzeciej, istotna modyfikacja przywraca tę samą ścieżkę. Powiadom stronę trzecią z wyprzedzeniem o każdej zmianie, która prawdopodobnie będzie istotna. Samoocena nie jest tylnymi drzwiami do przeklasyfikowania produktu ważnego po fakcie.

Konsekwencje, gdy modyfikacja jest istotna

Istotna modyfikacja jest traktowana jako wprowadzenie nowego produktu do obrotu. Dla producenta oznacza to:

- Odświeżenie dokumentacji technicznej dla zmienionej wersji.
- Powtórzenie oceny zgodności na ścieżce wymaganej przez klasę produktu.
- Wystawienie nowej deklaracji zgodności UE dla zmodyfikowanej wersji.
- Ponowne naniesienie oznakowania CE z nową deklaracją w aktach.
- Zachowanie dokumentacji poprzedniej wersji przez pełny okres retencji. Nowa wersja jej nie zastępuje.

Dla produktów programowych można w szczególności ograniczyć zakres aktualizacji zabezpieczeń w okresie wsparcia do najnowszej wersji wprowadzonej do obrotu, pod warunkiem że użytkownicy wcześniejszych wersji mogą przejść na najnowszą bezpłatnie i bez nowego sprzętu.

Egzemplarze już sprzedane w ramach poprzedniej zgodności pozostają nienaruszone. Obowiązek wiąże się z udostępnianą zmodyfikowaną wersją, nie z identycznymi egzemplarzami, które ją poprzedzają.

Kiedy producentem staje się ktoś inny

Jeżeli nie jest się pierwotnym producentem, a wykonuje się istotną modyfikację, CRA traktuje wykonawcę modyfikacji jak producenta dla tej wersji. Pełne obowiązki z art. 13 i 14 przechodzą wtedy na ten podmiot. Ta sama reguła obowiązuje, gdy produkt jest wprowadzany do obrotu pod własną nazwą albo znakiem towarowym.

Łapie to więcej sytuacji, niż zespoły zwykle zakładają:

- Integrator systemów, który dostarcza specyficzną dla klienta kompilację firmware'u z nowymi funkcjami.
- Reseller, który robi white-label produktu i zmienia komunikowane przeznaczenie.
- Dostawca usług, który łączy urządzenie strony trzeciej z własnym firmware'em.

W każdym przypadku podmiot, który wprowadził zmianę, dziedziczy obowiązki producenta dla tej wersji: dokumentacja techniczna, ocena zgodności, zgłaszanie, postępowanie z podatnościami i reszta. Etykieta „importer” lub „dystrybutor” przestaje chronić w momencie przekroczenia którejkolwiek z tych linii.

Co należy mieć przygotowane

Ta część działa jak lista robocza. Szczegółowe omówienie wymagań znajduje się dalej.

Ocena ryzyka w cyberprzestrzeni

Przed wprowadzeniem produktu do obrotu producent potrzebuje oceny ryzyka w cyberprzestrzeni w aktach. To dokument, który wyjaśnia, własnymi słowami producenta, dlaczego produkt jest bezpieczny do wysyłki i do utrzymania na rynku.

Ocena powinna obejmować:

- Przeznaczenie produktu i racjonalnie przewidywalne przypadki użycia
- Warunki i środowisko, w których produkt będzie działać
- Dane i funkcje wymagające ochrony
- Zagrożenia mające zastosowanie i kontrole zarządzające nimi
- Czas, przez jaki produkt ma być w użyciu

Jak najczęściej strukturyzują to zespoły. Wiarygodne metodyki schodzą się do tych samych kroków: zidentyfikuj aktywa (dane przetwarzane przez produkt, materiał kryptograficzny, taki jak klucze i poświadczenia, funkcje, których utrata zaszkodziłaby użytkownikom), zmapuj, gdzie każde aktywo żyje i się przemieszcza, zamodeluj zagrożenia per aktywo i środowisko, używając poufności, integralności i dostępności jako wymiarów, oceń wpływ i prawdopodobieństwo, zdecyduj, które ryzyka rezydualne akceptujesz, a które łagodzisz, następnie powtórz ocenę po każdej rundzie kontroli (każdy nowy klucz, certyfikat albo funkcja uwierzytelniania jest sam w sobie nowym aktywem do analizy).

Modelowanie zagrożeń. Krok trzeci powyżej jest najbardziej technicznym ruchem i ma własne ustalone techniki. STRIDE kategoryzuje zagrożenia jako spoofing, tampering, repudiation, information disclosure, denial of service i elevation of privilege; szeroko stosowane, pasuje do większości połączonych produktów. LINDDUN rozszerza obraz dla produktów przetwarzających dane osobowe, dodając linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness i non-compliance; przydatne, gdy reżim ochrony danych nakłada się na obowiązki CRA. PASTA realizuje siedmioetapowy proces od celów biznesowych po akceptację ryzyka rezydualnego; przydatne dla złożonych systemów, w których obraz ataku napędza projekt. Żadna z tych metod nie jest specyficzna dla CRA i CRA nie wymaga żadnej konkretnej. Wybierz tę, która pasuje do profilu ekspozycji produktu.

Gdzie znaleźć wypracowaną metodykę. CRA nie nakazuje metody. Niemiecki Federalny Urząd ds. Bezpieczeństwa Informacji (BSI) publikuje Wytyczną Techniczną TR-03183, najbardziej szczegółową, ugruntowaną metodykę oceny ryzyka zgodną z CRA w obiegu publicznym. ENISA publikuje szersze wskazówki wdrożeniowe dla CRA.

Utrzymuj ocenę aktualną przez cały okres wsparcia. Gdy obraz zagrożeń, komponenty albo przypadek użycia się zmieniają, ocena powinna się zmieniać razem z nimi.

Wyznaczenie okresu wsparcia

Każdy produkt potrzebuje zdefiniowanego okresu wsparcia, a jego datę końcową trzeba opublikować w punkcie zakupu. Okres wsparcia to okno, w którym producent obsługuje podatności, wydaje aktualizacje zabezpieczeń i utrzymuje dokumentację techniczną aktualną.

Jak długi musi być

Co najmniej pięć lat. Jeżeli oczekuje się, że produkt będzie w użyciu krócej niż pięć lat, okres wsparcia musi odpowiadać oczekiwanemu czasowi użytkowania. Jeżeli oczekuje się dłuższego użytkowania, okres wsparcia musi to dłuższe użytkowanie odzwierciedlać; produkty takie jak routery, systemy operacyjne i sterowniki przemysłowe rutynowo wymagają więcej niż pięciu lat.

Czynniki do uwzględnienia

Ustalając okres, uwzględnij w sposób proporcjonalny:

- Rozsądne oczekiwania użytkowników wobec produktu
- Charakter produktu, w tym jego przeznaczenie
- Każdy akt prawa UE, który już ustala czas życia produktu dla tej kategorii
- Okresy wsparcia porównywalnych produktów na rynku
- Dostępność środowiska operacyjnego, od którego produkt zależy
- Okresy wsparcia komponentów zintegrowanych dostarczających podstawowe funkcje
- Każde wytyczne ADCO albo Komisji dla danej kategorii produktów

Uzasadnienie wybranego okresu musi znaleźć się w dokumentacji technicznej. Organy nadzoru rynku mogą o nie poprosić.

Co trzeba opublikować

Podaj koniec okresu wsparcia w punkcie zakupu, z co najmniej miesiącem i rokiem, w łatwo dostępnym miejscu. Gdy produkt ma interfejs użytkownika, wyświetl powiadomienie, gdy okres wsparcia się kończy.

Retencja aktualizacji

Każda aktualizacja zabezpieczeń udostępniona użytkownikom w okresie wsparcia musi pozostać dostępna przez co najmniej 10 lat od jej wydania albo do końca okresu wsparcia, w zależności od tego, co dłuższe.

Należyta staranność wobec komponentów

Produkt składa się z komponentów. Część producent napisał, część kupił, część pobrał z otwartego repozytorium. CRA traktuje produkt jako całość do celów zgodności, więc komponenty też się liczą. Jeżeli podatność tkwi w komponencie, tkwi w produkcie. Jeżeli komponent nie dostaje aktualizacji zabezpieczeń, produkt też ich nie dostaje.

Producent musi dochowywać należytej staranności wobec komponentów stron trzecich, w tym wolnego i otwartego oprogramowania. Komponenty nie mogą zagrażać cyberbezpieczeństwu produktu.

Ile należytej staranności wystarczy, zależy od ryzyka cyberbezpieczeństwa, jakie niesie komponent. Biblioteka obsługująca uwierzytelnianie to nie to samo co biblioteka renderowania czcionek. Stosuj jedną lub więcej z tych kontroli, proporcjonalnie do ryzyka:

1. **Sprawdź oznakowanie CE na komponencie.** Jeżeli komponent jest sam w sobie produktem CRA i dostawca wykazał zgodność, oznakowanie CE jest na komponencie. To pokazuje własną pracę dostawcy w ramach CRA.
2. **Sprawdź historię aktualizacji zabezpieczeń.** Komponent, który wydaje regularne aktualizacje zabezpieczeń, jest lepszym ryzykiem niż taki, który milczał latami. Szukaj rytmu wydań i świeżego rejestru komunikatów bezpieczeństwa.
3. **Sprawdź komponent w bazach podatności.** Europejska baza danych o podatnościach i publiczne bazy CVE mówią, co wiadomo o komponencie. Znane CVE bez łatki to czerwona flaga.
4. **Wykonaj dodatkowe testy bezpieczeństwa.** Gdy powyższe nie wystarcza, przetestuj komponent w kontekście integracji: analiza statyczna, dynamiczna, fuzzing albo ukierunkowany przegląd bezpieczeństwa.

Dla komponentów zintegrowanych, zanim ich własny dostawca jest w pełni objęty CRA (a więc oznakowanie CE nie jest jeszcze dostępne), używaj pozostałych trzech kontroli. Obowiązek należytej staranności nie zatrzymuje się tylko dlatego, że łańcuch dostaw jeszcze nadrabia.

Dowody do trzymania w aktach

Dokumentacja techniczna musi pokazywać należytą staranność, nie tylko ją deklarować. Trzymaj:

- Listę komponentów stron trzecich w produkcie, z możliwością prześledzenia do wersji, w tym wolnych i otwartych. SBOM jest naturalnym miejscem.
- Dokumentację bezpieczeństwa dostawcy, którą przejrzano: polityki bezpieczeństwa, programy ujawniania podatności, zobowiązania dotyczące okresu wsparcia.
- Raporty z testów integracyjnych pokazujące, że komponent zachowuje się bezpiecznie w produkcie.
- Klauzule bezpieczeństwa w umowach lub SLA z dostawcami komercyjnymi: harmonogramy powiadomień o podatnościach, zobowiązania dotyczące okresu wsparcia, reguły eskalacji.
- Zapis działań ograniczających na poziomie produktu, dodanych tam, gdzie należyta staranność wobec komponentu ujawniła ograniczenia: sandboxing, ograniczone uprawnienia, walidacja danych wejściowych, segmentacja sieci.

Gdy znajdziesz podatność w komponencie

Jeżeli należyta staranność albo monitorowanie po wprowadzeniu do obrotu zidentyfikuje podatność w komponencie, trzeba zrobić dwie rzeczy. Po pierwsze, powiadomić osobę albo podmiot utrzymujący komponent. Jeżeli komponent jest otwartoźródłowy, jest to projekt nadrzędny. Po drugie, obsłużyć i usunąć podatność w produkcie w tych samych terminach co każdą inną podatność znalezioną przez producenta. Jeżeli producent opracował poprawkę, dzieli się kodem albo dokumentacją z opiekunem komponentu, w formacie nadającym się do odczytu maszynowego, gdy ma to zastosowanie.

CRA nie pozwala czekać na działanie opiekuna komponentu, zanim producent ochroni własnych użytkowników. Harmonogram postępowania z podatnościami w produkcie biegnie niezależnie od harmonogramu projektu nadrzędnego.

13 wymagań cyberbezpieczeństwa produktu

Każdy produkt z elementami cyfrowymi musi spełniać trzynaście podstawowych wymagań bezpieczeństwa w chwili wprowadzenia do obrotu i utrzymywać je przez cały okres wsparcia. To podłoga dla tego, co cyberbezpieczeństwo oznacza w kategoriach produktowych w ramach CRA.

Trzynaście wymagań to:

- Brak znanych podatności możliwych do wykorzystania w chwili wprowadzenia produktu do obrotu
- Bezpieczna konfiguracja domyślna od razu po uruchomieniu
- Aktualizacje zabezpieczeń, w tym automatyczne aktualizacje z mechanizmem opt-out
- Ochrona przed nieuprawnionym dostępem
- Poufność przechowywanych, przekazywanych i przetwarzanych danych
- Integralność danych, firmware'u i konfiguracji
- Minimalizacja danych
- Dostępność i odporność, także wobec ataków typu „odmowa usługi”
- Brak negatywnego wpływu na inne połączone urządzenia lub sieci
- Ograniczona powierzchnia ataku, w tym interfejsy zewnętrzne
- Ograniczenie wpływu incydentu dzięki łagodzeniu skutków wykorzystania
- Rejestrowanie aktywności związanej z bezpieczeństwem z opcją opt-out dla użytkownika
- Bezpieczne i trwałe usuwanie danych oraz przenoszalność

Każde wymaganie jest rozwinięte dalej w przewodniku, z tym, co oznacza w praktyce i jakie dowody warto trzymać w aktach.

8 wymagań dotyczących postępowania z podatnościami

Producent potrzebuje też procesów postępowania z podatnościami działających przez cały okres wsparcia produktu:

1. Identyfikowanie i dokumentowanie podatności (obejmuje zestawienie SBOM)
2. Zarządzanie ryzykiem i terminowe aktualizacje zabezpieczeń
3. Regularne testy bezpieczeństwa
4. Informacje o aktualizacjach zabezpieczeń i ujawnianiu podatności
5. Polityka skoordynowanego ujawniania podatności (CVD)
6. Kontakt do wymiany informacji i zgłaszania podatności
7. Bezpieczne mechanizmy dystrybucji aktualizacji
8. Bezpłatne aktualizacje zabezpieczeń z komunikatami doradczymi

Terminy zgłoszeń z art. 14

Te obowiązki stosuje się od **11 września 2026 r.** Obejmują producentów produktów z elementami cyfrowymi w zakresie CRA, także produktów wprowadzonych do obrotu przed **11 grudnia 2027 r.** Mikroprzedsiębiorstwa i małe przedsiębiorstwa nie mają ogólnego zwolnienia ze zgłoszeń. Ulga w karach dla małych przedsiębiorstw jest wąska: dotyczy tylko pierwszego **24-godzinnego terminu wstępnego ostrzeżenia**.

CRA rozróżnia trzy poziomy statusu podatności:

- **Podatność:** każda słabość, którą można wykorzystać
- **Podatność możliwa do wykorzystania:** słabość możliwa do użycia w realnych warunkach
- **Aktywnie wykorzystywana podatność:** podatność, której użycie w ataku zostało potwierdzone

Kiedy zaczyna biec zegar

Zegar nie biegnie od momentu, w którym pojawia się sygnał. Zegar zaczyna biec, gdy producent przeprowadzi wstępną ocenę i ma rozsądny stopień pewności, że podatność w produkcie jest aktywnie wykorzystywana albo że poważny incydent naruszył bezpieczeństwo produktu. Nacisk jest na szybkiej wstępnej ocenie, nie na czekaniu, aż pełne dochodzenie się zamknie. Jeżeli klient, badacz, organ albo inna strona trzecia zwraca uwagę na potencjalny problem, oceń go bez zwłoki i uruchom zegar, gdy tylko ocena daje rozsądną pewność.

Po wykryciu **aktywnie wykorzystywanej podatności** obowiązuje ta oś zgłoszeń:

Termin	Co jest wymagane	Gdzie zgłaszać
W ciągu 24 h	Wstępne ostrzeżenie o aktywnym wykorzystaniu	ENISA przez krajowy CSIRT
W ciągu 72 h	Zgłoszenie podatności: dotknięty produkt, ogólny charakter wykorzystania i podatności, środki łagodzące, środki naprawcze dostępne dla użytkowników i oznaczenie wrażliwości, gdy ma zastosowanie	ENISA przez krajowy CSIRT
Najpóźniej 14 dni po udostępnieniu środka naprawczego albo łagodzącego	Raport końcowy: opis podatności, dotkliwość, wpływ, dostępne informacje o złośliwych podmiotach oraz szczegóły aktualizacji zabezpieczeń lub innego środka naprawczego	ENISA przez krajowy CSIRT

Po wykryciu **poważnego incydentu** wpływającego na bezpieczeństwo produktu obowiązuje ta oś zgłoszeń:

Termin	Co jest wymagane	Gdzie zgłaszać
W ciągu 24 h	Wstępne ostrzeżenie, w tym informacja, czy podejrzewa się, że incydent wynika z działań bezprawnych albo złośliwych	ENISA przez krajowy CSIRT
W ciągu 72 h	Zgłoszenie incydentu: charakter incydentu, wstępna ocena, środki łagodzące, środki naprawcze dostępne dla użytkowników i oznaczenie wrażliwości, gdy ma zastosowanie	ENISA przez krajowy CSIRT
W ciągu miesiąca po zgłoszeniu incydentu w terminie 72 h	Raport końcowy: szczegółowy opis incydentu, dotkliwość, wpływ, prawdopodobne zagrożenie lub przyczyna źródłowa oraz zastosowane albo trwające środki łagodzące	ENISA przez krajowy CSIRT

Powiadomienia są aktualizowane w miarę wiedzy

Wpisy 24 h, 72 h i 14-dniowy (albo miesięczny) są etapami tego samego zgłoszenia, nie odrębnymi zgłoszeniami. Każdy etap dokłada informacje, których nie było na poprzednim. Wyznaczony jako koordynator CSIRT może też w dowolnym momencie poprosić o aktualizację pośrednią. Nie ma potrzeby powtarzania informacji już przekazanych.

Zgłoszenia trafiają przez **Jednolitą Platformę Zgłaszania CRA**, kierowane przez krajowy zespół reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) w głównym państwie członkowskim producenta, z jednoczesnym dostępem dla ENISA.

Informowanie użytkowników

Po uzyskaniu wiedzy producent ma poinformować dotkniętych użytkowników o podatności lub incydencie, a gdy to właściwe wszystkich użytkowników, o środkach ograniczających ryzyko i naprawczych, które mogą wdrożyć. To nie jest to samo co publiczne ujawnienie. Obowiązek polega na dostarczeniu informacji użytkownikom, którzy potrzebują jej do ochrony, proporcjonalnie do ryzyka. Dla produktów używanych w środowiskach wrażliwych albo kluczowych ogranicz szczegóły techniczne do zainteresowanych klientów, dopóki podatność jest nieusunięta; przedwczesny szczegół publiczny może ułatwić wykorzystanie.

Po usunięciu lub złagodzeniu podatności szersze ujawnienie może stać się właściwe, aby pomóc użytkownikom zweryfikować, że ich produkty nie są już dotknięte, i podnieść ogólną świadomość. Trzymaj poziom szczegółu i moment proporcjonalne do ryzyka rezydualnego. Jeżeli producent nie informuje użytkowników w odpowiednim czasie, CSIRT może wkroczyć i sam dostarczyć informacje, gdy uzna to za proporcjonalne i konieczne.

Terminy zgłoszeń z art. 14

Aktywnie wykorzystywana podatność

24 godziny	wstępne ostrzeżenie
72 godziny	zgłoszenie podatności
14 dni po środku naprawczym	raport końcowy

Poważny incydent

24 godziny	wstępne ostrzeżenie
72 godziny	zgłoszenie incydentu
miesiąc po zgłoszeniu 72 h	raport końcowy

Działania naprawcze, gdy produkt nie jest zgodny

Jeżeli producent wie albo ma podstawy sądzić, że produkt wprowadzony do obrotu albo jeden z procesów producenta nie jest zgodny z zasadniczymi wymaganiami cyberbezpieczeństwa CRA, musi działać niezwłocznie. Obowiązek biegnie od wprowadzenia do obrotu i przez cały okres wsparcia.

Trzy opcje

1. **Doprowadzenie do zgodności.** Napraw produkt albo proces. Dla produktów programowych jest to zwykle aktualizacja zabezpieczeń albo zmiana procesu. Zastosuj poprawkę do wspieranych wersji.
2. **Wycofanie z obrotu.** Zaprzestań udostępniania produktu na rynku. Wyciągnij go z łańcucha dostaw oraz od integratorów i resellerów, którzy trzymają zapas.
3. **Odzyskanie od użytkowników.** Sprowadź produkt z powrotem od użytkowników, którzy już go mają. Stosuj, gdy ryzyko cyberbezpieczeństwa dla użytkowników jest istotne, a sama poprawka albo wycofanie nie wystarcza.

Wybór jest proporcjonalny do ryzyka, nie stałą sekwencją. Podatność z działającą poprawką zwykle oznacza *doprowadzenie do zgodności*. Produkt, którego nie da się bezpiecznie naprawić w terenie, zwykle oznacza *wycofanie z obrotu* i, gdy jest aktywnie używany z istotnym ryzykiem, *odzyskanie od użytkowników*.

Co trzeba też zrobić

- **Zgłoś łańcuchem z art. 14**, gdy niezgodność jest aktywnie wykorzystywaną podatnością albo poważnym incydentem. Harmonogram zgłaszania jest opisany powyżej.
- **Poinformuj użytkowników** o niezgodności i o środkach naprawczych, które mogą zastosować samodzielnie. Reguły proporcjonalności w sekcji *Informowanie użytkowników* powyżej.
- **Współpracuj** z każdym uzasadnionym żądaniem organu nadzoru rynku, w tym dostarczając dokumentację techniczną w języku, który organ może odczytać.
- **Zachowaj dowody.** Trzymaj zapisy pokazujące, co znaleziono, kiedy, jakie podjęto działania i jak komunikowano się z użytkownikami i organami. Dokumentacja techniczna i deklaracja zgodności UE muszą pozostać dostępne przez co najmniej 10 lat od wprowadzenia do obrotu albo przez pełny okres wsparcia, w zależności od tego, co dłuższe.

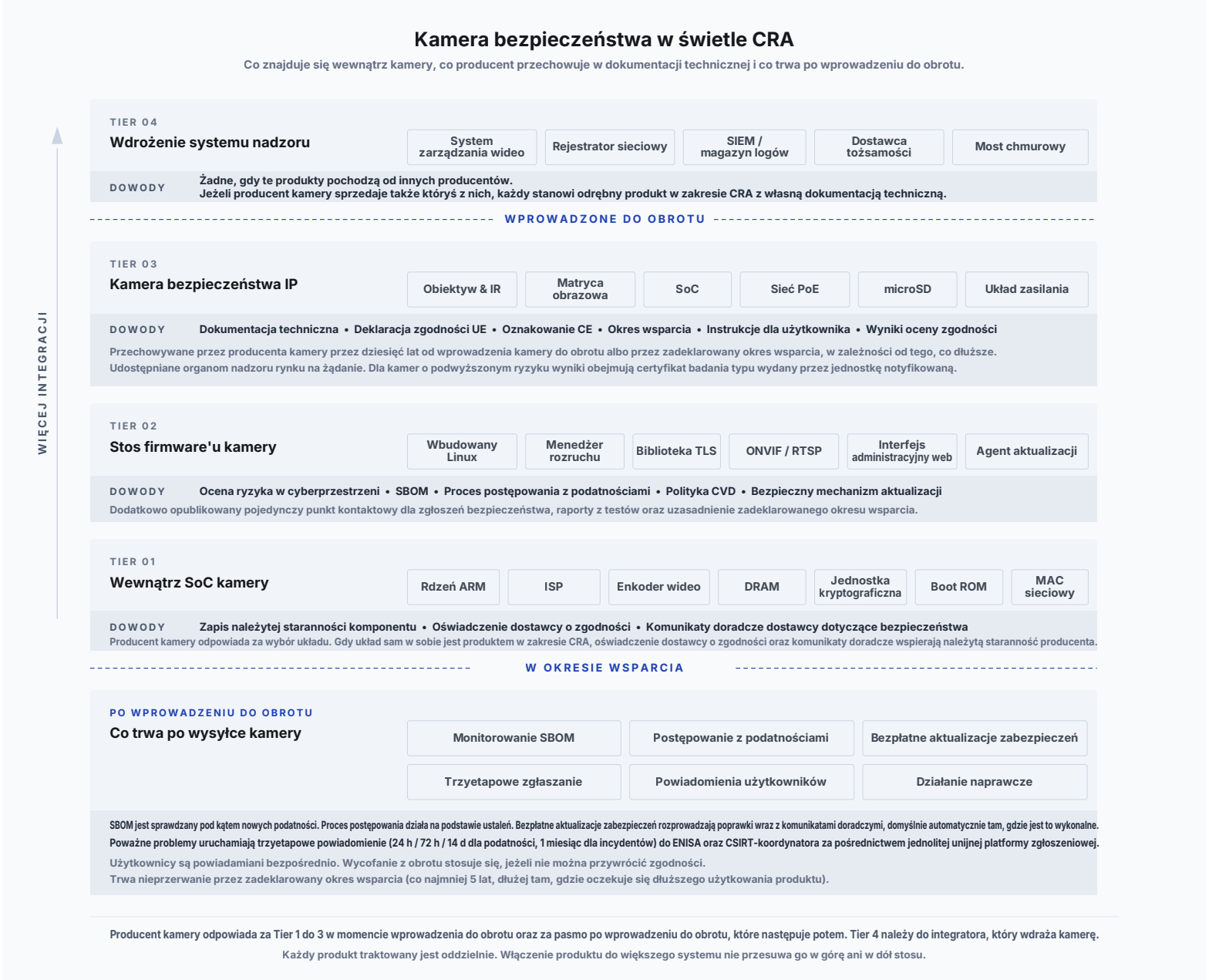
Wymagania dotyczące dokumentacji produktu

Dokumentację trzeba zachować przez **co najmniej 10 lat** od wprowadzenia produktu do obrotu albo przez **pełny okres wsparcia**, w zależności od tego, co dłuższe. W skrócie dokumentacja techniczna potrzebuje ośmiu rodzin dowodowych:

1. Ogólny opis produktu
2. Szczegóły projektu, opracowania i produkcji (w tym SBOM)
3. Ocena ryzyka w cyberprzestrzeni
4. Wyznaczenie okresu wsparcia
5. Zastosowane normy zharmonizowane i specyfikacje
6. Raporty z testów
7. Deklaracja zgodności UE
8. Pełny SBOM (na żądanie organów nadzoru rynku)

Lista kontrolna ścieżki oceny zgodności

Użyj powyższej tabeli klasyfikacji, aby wskazać ścieżkę. Następnie zachowaj decyzję o ścieżce w dokumentacji technicznej wraz z normami, specyfikacjami, schematem certyfikacji albo dowodem jednostki notyfikowanej użytym do jej uzasadnienia.



Przepracowany przykład. Ta sama struktura warstw odnosi się do każdego produktu z elementami cyfrowymi, nie tylko kamer bezpieczeństwa.

Wymagania cyberbezpieczeństwa produktu

a. Brak znanych podatności możliwych do wykorzystania w chwili wprowadzenia do obrotu

Nie wysyłaj produktu z publicznie znanymi podatnościami możliwymi do wykorzystania, które pozostają nieobsłużone. Znana podatność może pochodzić z publicznej bazy danych, powiadomienia dostawcy, zgłoszenia klienta albo wewnętrznego trackera.

Aby spełnić to wymaganie:

- Sprawdzaj bazy podatności (w tym Common Vulnerabilities and Exposures, CVE) przed każdym wydaniem
- Stosuj statyczne i dynamiczne testy bezpieczeństwa aplikacji (SAST/DAST) w pipeline'ie kompilacji
- Wykonuj skanowanie zależności dla wszystkich komponentów stron trzecich i otwartoźródłowych
- Udokumentuj decyzję o akceptacji ryzyka lub działaniu łagodzącym dla każdej zidentyfikowanej kwestii

b. Bezpieczna konfiguracja domyślna

Produkt powinien być bezpieczny do używania w stanie domyślnym. Wyłącz zbędne usługi, unikaj słabych haseł domyślnych i utrzymuj każdy niebezpieczny tryb uruchomieniowy krótki i kontrolowany. Obowiązek konfiguracji domyślnej można zmodyfikować dla produktów dostosowanych do indywidualnych potrzeb dostarczanych użytkownikom biznesowym na podstawie pisemnej umowy, ale musi pozostać ścieżka powrotu do pierwotnego bezpiecznego stanu.

Aby spełnić to wymaganie:

- Wyłącz porty zdalnego dostępu i interfejsy debugowania w domyślnych kompilacjach
- Egzekwuj silne domyślne mechanizmy uwierzytelniania
- Ograniczaj funkcje administracyjne wyłącznie do uprawnionych użytkowników
- Wdrażaj bezpieczny reset fabryczny, który przywraca wszystkie ustawienia i firmware do znanego bezpiecznego stanu, usuwając jednocześnie dane użytkownika

c. Aktualizacje zabezpieczeń, w tym automatyczne aktualizacje z mechanizmem opt-out

Produkt potrzebuje mechanizmu łatania, który radzi sobie z kwestiami bezpieczeństwa po wdrożeniu. Tam, gdzie aktualizacje automatyczne są właściwe, włącz je domyślnie i daj użytkownikom jasny sposób na odroczenie albo opt-out.

Aby spełnić to wymaganie:

- Wdroż kryptograficzne podpisywanie i weryfikację integralności pakietów aktualizacji
- Zapewnij ochronę przed rollbackiem i logowanie zdarzeń aktualizacji
- Zbuduj systemy powiadomień ostrzegające użytkowników o oczekujących aktualizacjach
- Pozwól użytkownikom odroczyć albo wyłączyć aktualizacje automatyczne przez jasny interfejs konfiguracji

d. Ochrona przed nieuprawnionym dostępem

Kontrole dostępu muszą chronić zarówno interfejsy lokalne, jak i zdalne. Celem jest zatrzymanie nieuprawnionych użytkowników przed dotarciem do funkcji, danych, konfiguracji albo powierzchni zarządzania.

Aby spełnić to wymaganie:

- Egzekwuj polityki złożoności haseł i silne poświadczenia domyślne
- Wdrażaj uwierzytelnianie wieloskładnikowe (MFA) tam, gdzie to właściwe
- Stosuj kontrolę dostępu opartą na rolach (RBAC) i obsługę przekroczenia czasu sesji
- Loguj nieudane próby dostępu, używaj wykrywania anomalii do oznaczania nieuprawnionej aktywności i wynoś te zdarzenia do przeglądu i zgłaszania

e. Poufność przechowywanych, przekazywanych i przetwarzanych danych

Dane wrażliwe potrzebują ochrony w spoczynku, w tranzycie i podczas przetwarzania.

Aby spełnić to wymaganie:

- Stosuj standaryzowane algorytmy szyfrowania (na przykład AES-256 dla danych w spoczynku, TLS dla danych w tranzycie)
- Stosuj bezpieczne praktyki zarządzania kluczami
- Oddzielaj dane poufne od niekrytycznych komponentów systemu
- Utrzymuj logi audytowe dla wszystkich zdarzeń dostępu do danych

f. Integralność danych, firmware'u i konfiguracji

To wymaganie obejmuje sam system (firmware, oprogramowanie, pliki konfiguracji) oraz dane, które obsługuje (pomiary, polecenia sterujące, dane wejściowe użytkownika).

Aby spełnić to wymaganie:

- Wdroż bezpieczny rozruch i podpisany firmware, aby tylko zaufany kod był wykonywany
- Stosuj weryfikację w czasie wykonania, aby wykrywać i raportować próby manipulacji
- Stosuj kryptograficzne hashowanie i podpisy cyfrowe do ochrony integralności danych
- Zbuduj infrastrukturę zdolną generować, dystrybuować i weryfikować klucze kryptograficzne przez granice systemowe lub organizacyjne

g. Minimalizacja danych

Zbieraj i przetwarzaj tylko dane potrzebne do przeznaczenia produktu. Dotyczy to danych osobowych i danych technicznych.

Aby spełnić to wymaganie:

- Przeprowadzaj oceny wpływu na prywatność albo ćwiczenia ochrony danych w fazie projektowania, aby zidentyfikować zbędne przepływy danych
- Usuń albo uczyń opcjonalnymi nieużywaną telemetrię, diagnostykę albo zbieranie danych w tle
- Wdroż konfigurowalne ustawienia zbierania danych, aby rozszerzone zbieranie dało się włączyć albo wyłączyć w zależności od kontekstu

h. Dostępność i odporność, także wobec ataków typu „odmowa usługi”

Podczas incydentów albo ataków kluczowe funkcje produktu powinny pozostawać dostępne albo zawodzić w sposób kontrolowany.

Aby spełnić to wymaganie:

- Wdroż wyłączniki, logikę ponowień, mechanizmy awaryjne i liczniki watchdog
- Stosuj limity zasobów, aby zapobiec wyczerpaniu zasobów
- Stosuj ograniczanie tempa żądań i walidację danych wejściowych dla ochrony przed scenariuszami odmowy usługi
- Stosuj filtrowanie na poziomie sieci, aby blokować próby przeciążenia

i. Brak negatywnego wpływu na inne połączone urządzenia lub sieci

Produkt nie powinien zakłócać innych systemów w tym samym środowisku. Powinien zachowywać się przewidywalnie i unikać nadmiernego użycia zasobów wspólnych.

Aby spełnić to wymaganie:

- Wdroż kształtowanie ruchu i ograniczaj użycie broadcast albo multicast
- Zapewnij zgodność ze specyfikacjami protokołów komunikacyjnych
- Stosuj samomonitorowanie, aby wykrywać i zapobiegać zachowaniom zakłócającym, takim jak zalewanie sieci albo wyczerpywanie zasobów

j. Ograniczona powierzchnia ataku, w tym interfejsy zewnętrzne

Zminimalizuj punkty wejścia i odsłoniętą funkcjonalność. Obejmuje to porty fizyczne, interfejsy bezprzewodowe, API, usługi debugowania i zbędne komponenty oprogramowania.

Aby spełnić to wymaganie:

- Wyłącz nieużywane usługi, porty i interfejsy w kompilacjach produkcyjnych
- Utwardzaj ustawienia domyślne systemu i ograniczaj uprawnienia użytkownika
- Modułaryzuj architektury oprogramowania, aby izolować komponenty
- Stosuj bezpieczne zasady projektowania oprogramowania i wykonuj modelowanie zagrożeń, aby identyfikować i usuwać zbędną ekspozycję

k. Ograniczenie wpływu incydentu dzięki łagodzeniu skutków wykorzystania

Zakładaj, że część ataków się powiedzie. Projekt produktu powinien ograniczać, jak daleko może rozprzestrzenić się szkoda.

Aby spełnić to wymaganie:

- Oddzielaj komponenty systemu i uruchamiaj je w izolowanych środowiskach przez sandboxing albo konteneryzację
- Egzekwuj separację uprawnień, aby funkcje krytyczne działały z minimalnymi wymaganymi uprawnieniami
- Projektuj tak, aby kompromitacja jednego komponentu nie dawała atakującemu kontroli nad całym systemem

l. Rejestrowanie aktywności związanej z bezpieczeństwem z opcją opt-out dla użytkownika

Rejestruj aktywność związaną z bezpieczeństwem, taką jak próby dostępu i modyfikacje danych, aby dało się ją monitorować i audytować. Użytkownicy potrzebują mechanizmu opt-out, gdy CRA tego wymaga.

Aby spełnić to wymaganie:

- Wdroż strukturalne logowanie (na przykład logi JSON ze znacznikami czasu)
- Zapewnij lokalne przechowywanie logów z rotacją i opcjami zdalnego strumieniowania logów
- Monitoruj zdarzenia takie jak próby logowania, zmiany konfiguracji i aktualizacje oprogramowania pod kątem anomalii
- Zapewnij jasny mechanizm dla użytkownika, aby wyłączyć logowanie tam, gdzie jest to dozwolone

m. Bezpieczne i trwałe usuwanie danych oraz przenoszalność

Użytkownicy potrzebują praktycznego sposobu, aby trwale usunąć dane i ustawienia. Gdy dane mogą być przenoszone do innego produktu albo systemu, transfer musi być bezpieczny.

Aby spełnić to wymaganie:

- Wdroż funkcję bezpiecznego wymazywania, która nadpisuje regiony pamięci masowej albo kryptograficznie usuwa klucze
- Stosuj uwierzytelnione i szyfrowane kanały dla transferów przenoszalności danych, aby zapobiec ujawnieniu podczas transferu

Wymagania dotyczące postępowania z podatnościami

1. Identyfikowanie i dokumentowanie podatności

Producent musi wiedzieć, jakie komponenty oprogramowania są w produkcie i jakie znane podatności ich dotyczą. SBOM daje ten nadający się do odczytu maszynowego inwentarz.

Aby spełnić to wymaganie:

- Zintegruj generowanie SBOM bezpośrednio w pipeline'ie CI/CD, aby każda kompilacja produkowała aktualny inwentarz komponentów
- Używaj ustalonych formatów, takich jak CycloneDX, SPDX albo SWID, dla interoperacyjności
- Uruchamiaj automatyczne skanowanie podatności względem wykazów CVE i baz takich jak CISA KEV i ENISA EUVD
- Utrzymuj SBOM jako część dokumentacji technicznej przez cały okres wsparcia i udostępniaj go organom nadzoru rynku na żądanie

2. Zarządzanie ryzykiem i terminowe aktualizacje zabezpieczeń

Gdy podatności są znalezione, napraw je szybko i dostarcz aktualizacje zabezpieczeń. Tam, gdzie to możliwe, oddzielaj poprawki bezpieczeństwa od aktualizacji funkcji, aby krytyczne poprawki dało się zainstalować bez zwłoki.

Aby spełnić to wymaganie:

- Projektuj mechanizm aktualizacji tak, aby poprawki bezpieczeństwa dało się wydać bez konieczności pełnej aktualizacji systemu
- Strukturyzuj oprogramowanie i firmware tak, aby krytyczne komponenty dały się łatać niezależnie
- Dostarczaj aktualizacje przez bezpieczne kanały z kontrolą integralności
- Utrzymuj zapisy działań aktualizacyjnych, aby wspierać śledzenie i wykazywać zgodność

3. Regularne testy bezpieczeństwa

Testowanie bezpieczeństwa nie jest jednorazowym ćwiczeniem. Testuj produkty w całym cyklu życia, gdy zagrożenia, zależności i zachowanie produktu się zmieniają. Niech ocena ryzyka napędza typ i częstotliwość testowania.

Aby spełnić to wymaganie:

- Wykonuj testy penetracyjne, aby symulować ataki z realnego świata
- Stosuj statyczną i dynamiczną analizę kodu, aby identyfikować słabości bezpieczeństwa
- Używaj fuzz testingu, aby ujawnić wady obsługi danych wejściowych
- Formalnie planuj i dokumentuj przeglądy kodu bezpieczeństwa oraz przeglądy architektury, szczególnie po istotnych zmianach projektu albo funkcji

4. Przyjmowanie zgłoszeń, polityka CVD i komunikaty doradcze

Obejmuje obowiązki przyjmowania zgłoszeń, skoordynowanego ujawniania i komunikatów doradczych (pozycje 4, 5 i 6 podsumowania powyżej), które w praktyce biegną jako jeden przepływ pracy.

CRA wymienia trzy odrębne wymagania dotyczące tego, jak producent komunikuje się wokół podatności: drogę, którą ludzie mogą zgłaszać problemy, politykę skoordynowanego ujawniania i komunikat doradczy, gdy producent wysyła poprawkę. Oto co każda z tych powinności wymaga.

Przyjmowanie zgłoszeń

Daj zgłaszającym jasną, niskoprogową drogę. Opublikuj widoczną metodę kontaktu do zgłaszania podatności (dedykowany adres e-mail albo formularz internetowy). Wspieraj bezpieczną komunikację, na przykład publikując klucz PGP. Obowiązek obejmuje zgłoszenia dotyczące własnego produktu i komponentów stron trzecich, które produkt zawiera.

Triage

Potwierdź każde zgłoszenie, zaloguj je w systemie śledzenia, przypisz do przeglądu i rozwiąż w zdefiniowanych terminach. Wysyłaj potwierdzenia i aktualizacje statusu z powrotem do zgłaszającego. Gdy kwestia tkwi w komponencie strony trzeciej, kieruj ją do opiekuna nadrzędnego równolegle z własnym usunięciem.

Polityka skoordynowanego ujawniania podatności

Opublikuj politykę CVD, która ustala oczekiwania dla zgłaszających i partnerów: metoda kontaktu, oczekiwane czasy reakcji, do czego producent się zobowiązuje, czego oczekuje od nich. Koordynuj ujawnianie, aby chronić użytkowników, jednocześnie uznając wkład zgłaszającego.

Komunikaty doradcze po poprawce

Gdy poprawka jest dostępna, opublikuj komunikat doradczy dla rozwiązanej kwestii. Załącz identyfikator CVE, dotknięte wersje produktu, standaryzowaną ocenę dotkliwości (na przykład CVSS) i jasne, dostępne informacje o tym, co użytkownicy mają zrobić. Pisz językiem dostępnym zarówno dla administratorów technicznych, jak i użytkowników nietechnicznych.

Opóźnione publiczne ujawnienie

Można opóźnić publiczne ujawnienie tylko wtedy, gdy istnieje należycie uzasadniony powód, że ryzyka cyberbezpieczeństwa natychmiastowego ujawnienia przeważają nad korzyściami, i tylko do czasu, gdy użytkownicy mieli szansę zastosować poprawkę. Udokumentuj rozumowanie.

5. Bezpieczne mechanizmy dystrybucji aktualizacji

Mechanizm aktualizacji musi być niezawodny i odporny na manipulacje. Tam, gdzie automatyczne aktualizacje są technicznie wykonalne, skracają czas, przez który użytkownicy pozostają narażeni.

Aby spełnić to wymaganie:

- Przekazuj aktualizacje bezpiecznymi kanałami i weryfikuj je przez podpisy cyfrowe
- Stosuj aktualizacje w sposób, który zapobiega niepełnym albo uszkodzonym instalacjom
- Używaj aktualizacji różnicowych albo modułowych, aby zmniejszyć zakłócenia i szybciej dostarczać poprawki do systemów
- Utrzymuj logi aktualizacji, aby użytkownicy albo administratorzy mogli weryfikować status aktualizacji

6. Bezpłatne aktualizacje zabezpieczeń z komunikatami doradczymi

Dostarczaj aktualizacje zabezpieczeń bez zwłoki i bez dodatkowych kosztów, z wyjątkiem sytuacji, w której istnieje odrębna umowa dla produktów biznesowych dostosowanych do indywidualnych potrzeb. Każda aktualizacja potrzebuje jasnego komunikatu doradczego, który mówi użytkownikom, co się zmieniło i co zrobić.

Aby spełnić to wymaganie:

- Utrzymuj system dystrybucji, który może powiadamiać użytkowników bezpośrednio albo stosować aktualizacje automatycznie, zależnie od kontekstu produktu
- Pisz komunikaty doradcze językiem zrozumiałym zarówno dla użytkowników technicznych, jak i nietechnicznych
- Załączaj informacje o dotkliwości w komunikatach doradczych, gdy jest to istotne
- Mów użytkownikom, jakie działanie podjąć, takie jak zastosowanie aktualizacji, zmiana konfiguracji albo obserwacja oznak kompromitacji
- Rozpowszechniaj aktualizacje zabezpieczeń bez zwłoki, gdy są dostępne, aby użytkownicy nie zostali narażeni, podczas gdy poprawka już istnieje
- Publikuj komunikaty doradcze przez kanał kontrolowany przez producenta i linkuj do nich ze strony wsparcia produktu

Obowiązki bezpłatności i braku zwłoki biegną przez długość zadeklarowanego okresu wsparcia. Wyjątek dla produktów dostosowanych do indywidualnych potrzeb zmienia tylko podstawę handlową; komunikaty doradcze wciąż obowiązują.

Zawartość dokumentacji technicznej

Dokumentacja techniczna

Dokumentacja techniczna jest centralnym dowodem zgodności z CRA. Musi obejmować środki projektowe, techniczne i proceduralne zastosowane do spełnienia zasadniczych wymagań cyberbezpieczeństwa. Musi istnieć **przed wprowadzeniem do obrotu** i pozostawać aktualna przez cały **okres wsparcia**.

Dowody techniczne w przepływie pracy inżynierskiej

Krok 1	**Określ zakres i klasyfikację**	Cel produktu, zamierzone użycie, decyzja o wprowadzeniu do obrotu, klasa produktu, ścieżka norm.
Krok 2	**Architektura i ryzyko**	Architektura, połączenia danych, warunki użycia, ocena ryzyka, działania ograniczające.
Krok 3	**Komponenty i SBOM**	SBOM w formacie maszynowym, komponenty stron trzecich, dane od dostawców, śledzenie podatności.
Krok 4	**Budowanie, testy, aktualizacje**	Bezpieczne ustawienia domyślne, hardening, raporty z testów, bezpieczny mechanizm aktualizacji, komunikaty doradcze.
Krok 5	**Wydanie i wsparcie**	Instrukcje dla użytkownika, deklaracja UE, dowody CE, uzasadnienie okresu wsparcia, zapisy aktualizacji.

Dokumentacja techniczna ma osiem wymaganych komponentów. Razem wyjaśniają **czym jest produkt**, **jak został zbudowany i przetestowany**, **jakie ryzyka rozważono**, **jakie normy zastosowano** i **jak będzie wspierany**, gdy znajdzie się na rynku. Nie trzeba kopiować nagłówków prawnych, ale każdy temat musi zostać pokryty.

Nr	Komponent	Co musi zawierać
1	Ogólny opis produktu	Przeznaczenie i funkcje, istotne wersje oprogramowania, zdjęcia lub ilustracje (dla sprzętu), informacje i instrukcje dla użytkownika
2	Szczegóły projektu, opracowania i produkcji	Opis architektury (komponenty i interakcje), SBOM, procesy postępowania z podatnościami (polityka CVD, punkt kontaktowy, bezpieczne mechanizmy aktualizacji), procesy produkcji i monitorowania, w tym walidacja
3	Ocena ryzyka w cyberprzestrzeni	Udokumentowana analiza ryzyk produktu, wyjaśnienie, jak każde zasadnicze wymaganie cyberbezpieczeństwa odnosi się do produktu, łagodzenie zidentyfikowanych ryzyk
4	Wyznaczenie okresu wsparcia	Dokumentacja czynników użytych do ustalenia okresu wsparcia, takich jak oczekiwania użytkowników, porównywalne produkty i wytyczne prawne
5	Zastosowane normy zharmonizowane i specyfikacje	Lista zastosowanych norm zharmonizowanych, wspólnych specyfikacji albo systemów certyfikacji UE; wskazanie, czy stosowane w całości czy częściowo; rozwiązania alternatywne tam, gdzie normy nie są stosowane
6	Raporty z testów	Dowody zgodności zarówno produktu, jak i procesów postępowania z podatnościami
7	Deklaracja zgodności UE	Kopia deklaracji łącząca dokumentację techniczną z obowiązkami oznakowania CE
8	Pełny SBOM (na żądanie)	Organy nadzoru rynku mogą wymagać pełnego SBOM do weryfikacji zgodności

Pojedyncza skonsolidowana dokumentacja techniczna może obejmować CRA i inne właściwe akty prawa UE (na przykład dyrektywę o urządzeniach radiowych albo ESPR), pod warunkiem że wszystkie właściwe obowiązki są uwzględnione.

Deklaracja zgodności UE

Deklaracja zgodności UE jest formalnym oświadczeniem producenta, że produkt spełnia właściwe wymagania cyberbezpieczeństwa CRA. Każda deklaracja musi zawierać:

- Nazwę produktu, typ i unikalne identyfikatory
- Nazwę i adres producenta (albo upoważnionego przedstawiciela)
- Oświadczenie o wyłącznej odpowiedzialności dostawcy
- Opis produktu zapewniający identyfikowalność (opcjonalnie ze zdjęciem)
- Wyraźne oświadczenie o zgodności z właściwym prawem Unii
- Odniesienia do zastosowanych norm zharmonizowanych, specyfikacji albo certyfikacji
- Szczegóły dotyczące każdej zaangażowanej jednostki notyfikowanej (nazwa, numer, procedura, numer certyfikatu)
- Blok podpisu: miejsce, data, imię i nazwisko, funkcja oraz podpis sygnatariusza

Po podpisaniu deklaracja jest prawnie wiążąca i potwierdza pełną odpowiedzialność producenta za zgodność w zakresie cyberbezpieczeństwa.

Uproszczona deklaracja jest dopuszczalna do użycia na opakowaniu albo w instrukcjach, w formie: „Niniejszym [producent] oświadcza, że produkt [typ/oznaczenie] jest zgodny z Rozporządzeniem (UE) 2024/2847. Pełny tekst deklaracji zgodności UE jest dostępny pod adresem: [adres strony internetowej].” Ta uproszczona forma utrzymuje przejrzystość, jednocześnie zmniejszając ilość papierowej pracy, i jest szczególnie przydatna dla małych producentów albo portfolio wielu produktów.

Informacje i instrukcje dla użytkownika

Informacje i instrukcje dla użytkownika są warunkiem legalnego wprowadzenia do obrotu. Producenci muszą utrzymywać instrukcje dostępne przez **co najmniej 10 lat** albo przez **pełny okres wsparcia**. Importerzy i dystrybutorzy muszą sprawdzić, czy instrukcje istnieją, są aktualne i dostarczone w odpowiednim języku UE, przed wprowadzeniem albo dostarczeniem produktu.

Instrukcje dla użytkownika muszą zawierać:

- Tożsamość producenta i dane kontaktowe
- Pojedynczy punkt kontaktu do zgłaszania podatności
- Identyfikację produktu, przeznaczenie i bezpieczny kontekst używania
- Znane lub przewidywalne ryzyka cybernetyczne
- Link do deklaracji zgodności UE
- Warunki wsparcia i jasną datę końca wsparcia
- Krok po kroku instrukcje bezpieczeństwa dla konfiguracji, aktualizacji, bezpiecznego używania, wycofania z użycia oraz (jeżeli ma zastosowanie) integracji i dostępu do SBOM

Wybór właściwej ścieżki oceny zgodności

Moduł A: samoocena

Moduł A (kontrola wewnętrzna) pozwala samodzielnie potwierdzić, że produkt jest zgodny z zasadniczymi wymaganiami cyberbezpieczeństwa, biorąc pełną odpowiedzialność zarówno za projekt, jak i produkcję. Ścieżka ta jest dostępna dla producentów produktów standardowych (niesklasyfikowanych). Jest też dostępna dla produktów ważnych klasy I tylko wtedy, gdy właściwe normy zharmonizowane, wspólne specyfikacje albo europejskie systemy certyfikacji cyberbezpieczeństwa są dostępne i stosowane, jak wymagają reguły ścieżek CRA.

W ramach modułu A trzeba:

- Przygotować kompletną dokumentację techniczną
- Wyszczególnić projekt produktu, procesy produkcji, mechanizmy cyberbezpieczeństwa i procedury postępowania z podatnościami
- Utrzymywać ciągłą odpowiedzialność za stałą zgodność przez cały cykl życia produktu
- Wdrożyć plan aktualizacji zabezpieczeń i zarządzania podatnościami przez życie operacyjne produktu
- Przechowywać zapisy dostępne przez co najmniej 10 lat

Moduły B i C: ocena skoncentrowana na produkcie

Moduły B i C stosuje się tam, gdzie wymagana jest weryfikacja strony trzeciej dla konkretnego typu produktu. Stosuje się je do produktów ważnych klasy I, gdy producent nie zastosował, zastosował tylko częściowo albo nie może zastosować właściwych norm zharmonizowanych, wspólnych specyfikacji albo systemów certyfikacji. Dla produktów ważnych klasy II producent musi użyć modułu B+C, modułu H albo właściwego europejskiego systemu certyfikacji cyberbezpieczeństwa na co najmniej „istotnym” poziomie uzasadnienia zaufania.

Moduł B (badanie typu UE): Jednostka notyfikowana bada reprezentatywną próbkę produktu i powiązaną dokumentację techniczną. Weryfikuje zgodność ze wszystkimi zasadniczymi wymaganiami cyberbezpieczeństwa i wydaje certyfikat badania typu UE, gdy projekt produktu spełnia kryteria CRA.

Moduł C (zgodność z typem na podstawie wewnętrznej kontroli produkcji): Producent zapewnia, że wszystkie jednostki produkcyjne są zgodne z zatwierdzonym typem certyfikowanym w module B. Producent nanosi oznakowanie CE, wydaje deklarację zgodności UE i przechowuje zapisy dostępne przez co najmniej 10 lat. Razem moduły B i C zapewniają, że konkretny model produktu jest technicznie zgodny i że każda partia produkcyjna pozostaje spójna z zatwierdzonym projektem.

Moduł H: ocena skoncentrowana na procesie (pełne zapewnienie jakości)

Moduł H (pełne zapewnienie jakości) skupia się na całym wewnętrznym systemie jakości producenta, a nie na testowaniu pojedynczego produktu. Jest dostępny dla produktów ważnych klasy I i klasy II. Produkty krytyczne stosują ścieżkę certyfikacji tam, gdzie spełnione są właściwe warunki; gdy te warunki nie są spełnione, stosują te same ścieżki dostępne dla produktów ważnych klasy II.

W ramach modułu H trzeba:

- Ustanowić i utrzymywać system jakości obejmujący projekt, opracowanie, produkcję, testowanie i postępowanie z podatnościami dla całej kategorii produktu
- Złożyć system jakości jednostce notyfikowanej do oceny i zatwierdzenia
- Akceptować bieżący nadzór (audyty, inspekcje i przeglądy procesów) przez jednostkę notyfikowaną w celu weryfikacji stałej zgodności

Po zatwierdzeniu można wydawać deklaracje zgodności dla wszystkich produktów wyprodukowanych w ramach tego systemu jakości, bez powtarzania badania jednostki notyfikowanej dla każdego pojedynczego typu produktu.

Kluczowe rozróżnienie między ścieżkami:

- Moduły B+C: skupienie na produkcie. Reprezentatywny typ produktu jest testowany i certyfikowany.
- Moduł H: skupienie na procesie. Cały system projektu i produkcji producenta jest certyfikowany i monitorowany.

Przepływ wprowadzenia do obrotu

CRA w szerszym kontekście regulacyjnym UE

CRA nie stoi sam. Praktyczne pytanie producenta brzmi: gdzie praca nad CRA oszczędza wysiłku w innym reżimie UE, a gdzie pozostają odrębne obowiązki do prowadzenia równolegle?

Gdzie pracę nad CRA można ponownie wykorzystać

- **Systemy AI wysokiego ryzyka (AI Act, Rozporządzenie 2024/1689).** Jeżeli produkt jest systemem AI wysokiego ryzyka w zakresie CRA, spełnienie zasadniczych wymagań cyberbezpieczeństwa CRA uznaje się za spełnienie wymagań cyberbezpieczeństwa AI Act w zakresie objętym deklaracją zgodności UE. Procedura oceny zgodności biegnie przez reżim AI Act co do zasady, z wyjątkiem dla produktów ważnych i krytycznych z CRA. Ocena ryzyka cyberbezpieczeństwa w CRA musi uwzględniać ryzyka specyficzne dla AI, takie jak zatruwanie danych i ataki adwersaryjne.
- **Skonsolidowana ocena ryzyka z innym prawem Unii.** CRA wprost dopuszcza, aby ocena ryzyka cyberbezpieczeństwa stanowiła część szerszej oceny ryzyka wymaganej przez inny akt prawa Unii, gdy produkt podlega obu reżimom. Jeden artefakt oceny, dwa zastosowania regulacyjne.
- **Jedna dokumentacja techniczna w różnych reżimach.** Jak już zaznaczono w sekcji o dokumentacji technicznej, pojedyncza skonsolidowana dokumentacja techniczna może obejmować CRA wraz z innymi właściwymi aktami prawa Unii, pod warunkiem że obowiązki każdego reżimu są uwzględnione. Przydatne tam, gdzie ten sam produkt już potrzebuje dokumentacji w ramach dyrektywy o urządzeniach radiowych, Rozporządzenia o ekoprojekcie dla zrównoważonych produktów albo innego prawa produktowego.
- **Wspólne definicje refurbishmentu, konserwacji i napraw.** CRA importuje te definicje z Rozporządzenia o ekoprojekcie dla zrównoważonych produktów. Analizując, czy operacja serwisowa liczy się jako istotna modyfikacja, definicje z ekoprojektu są punktem odniesienia, a nie odrębne pojęcie CRA.

Gdzie pozostają odrębne obowiązki

- **AI Act, cała reszta.** Cyberbezpieczeństwo to tylko jeden wycinek AI Act. Klasyfikacja ryzyka, przejrzystość, zarządzanie zbiorami danych, nadzór ludzki, monitorowanie zachowania AI po wprowadzeniu do obrotu i reszta to powinności z AI Act, których CRA nie obejmuje. Zgodność cyberbezpieczeństwa z CRA nie daje domniemania ogólnej zgodności z AI Act.
- **Ekoprojekt i treść cyfrowego paszportu produktu.** Wymagania ekoprojektu dotyczące efektywności energetycznej, trwałości, oceny naprawialności i treści zrównoważonego rozwoju w cyfrowym paszporcie produktu nie są w zakresie CRA. Ślad dowodowy CRA może stać obok prac nad ekoprojektem, ale ich nie zastępuje.
- **Prawa dostępu do danych IoT z Data Act.** Data Act daje użytkownikom prawa umowne do dostępu, udostępniania i przenoszenia danych, które generują ich połączone produkty. CRA obejmuje bezpieczeństwo tych danych; nie ustanawia reżimu praw dostępu. Inny obowiązek, inne dowody.
- **Odpowiedzialność za produkty wadliwe.** Dyrektywa o odpowiedzialności za produkty wadliwe (2024/2853) utrzymuje na producencie ścisłą odpowiedzialność za szkodę spowodowaną wadliwymi produktami. CRA sygnalizuje, że brak aktualizacji zabezpieczeń po wprowadzeniu do obrotu może być wadą, która wywołuje odpowiedzialność. Umowy, ubezpieczenia i playbooki incydentowe muszą uwzględniać tę ekspozycję niezależnie od zgodności z CRA.

Jak pomaga CRA Evidence

CRA Evidence zamienia obowiązki wynikające z unijnego CRA w weryfikowalne dowody produktowe, łącząc platformę zgodności z doradztwem technicznym.

Platforma

Jedno miejsce do zarządzania dowodami stojącymi za gotowością CRA:

- **SBOM i inwentarz komponentów:** rekordy CycloneDX, SPDX i HBOM dla wersji produktu oraz wydań
- **Automatyzacja dowodów CI/CD:** przepływy CLI i API dla skanów, przesyłania SBOM, bramek wydań i zapisów audytowych
- **Podpisany SBOM i pochodzenie:** wersjonowane dowody, atestacje dostawców i zapisy należytej staranności
- **Operacje podatności:** CISA KEV, EPSS, VEX, monitorowanie, triage i przepływy zgłoszeń
- **Dokumentacja techniczna i dowody CE:** zapisy deklaracji UE, historia retencji i paszporty zgodności produktu powiązane QR

Doradztwo techniczne

Ukierunkowane wsparcie w przekładaniu obowiązków CRA na decyzje inżynieryjne dotyczące produktu, architektury, wydań i dostawców.

- **Sprint gotowości technicznej:** przegląd luk w zasadniczych wymaganiach, rekomendacje architektoniczne i priorytetowy plan działania
- **Lider programu CRA:** model odpowiedzialności, śledzenie obowiązków, kamienie milowe dowodów i utrzymanie dokumentacji technicznej
- **Plan reakcji wobec organów i incydentów:** przepływy zgłoszeń, playbooki zapytań, komunikacja z użytkownikami i gotowość pakietów dowodowych
- **Uzgodnienie regulacyjne:** powiązanie dowodów CRA z Data Act, ESPR, AI Act, RED i wymaganiami sektorowymi
- **Warsztaty techniczne:** sesje zdalne lub na miejscu z zespołami produktu, inżynierii, bezpieczeństwa, zgodności i dostawców

Niezależne od narzędzi: CRA Evidence integruje się z CycloneDX, SPDX, Grype, Trivy, pipeline'ami CI/CD i systemami zgłoszeń.

Praktyczny pierwszy krok

Wybierz jedną rodzinę produktów. Zmapuj właściciela, decyzję zakresu, SBOM, przepływ podatności, luki w dokumentacji technicznej i dowody wydania. To daje zespołowi konkretną bazę CRA bez zamieniania zgodności w osobny projekt.

Zakres CRA Evidence dla produktu jest dostępny na craevidence.com/pl. Ceny i plany są dostępne na craevidence.com/pl/cennik.