SECURE
Cyber Resilience for SMEs

Podstawowe wymagania CRA w zakresie cyberbezpieczeństwa: załącznik I, część I

20/10/2025

Funded by the European Union

Oświadczenie o finansowaniu UE: Projekt finansowany przez Unię Europejską w ramach GA nr 101190325. Wyrażone poglądy i opinie są wyłącznie poglądami autora (autorów) i nie muszą odzwierciedlać poglądów Unii Europejskiej lub Europejskiego Centrum Kompetencji w zakresie Przemysłu, Technologii i Badań nad Cyberbezpieczeństwem. Ani Unia Europejska, ani organ przyznający dotację nie ponoszą za nie odpowiedzialności.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Zastrzeżenie ECCC: Projekt jest wspierany przez Europejskie Centrum Kompetencji w zakresie Cyberbezpieczeństwa i jego członków.

ZASTRZEŻENIE

Niniejszy dokument stanowi część rezultatu D4.1 „Wytyczne i materiały dotyczące zgodności MŚP z CRA" projektu SECURE.

Pierwszy autor: *Centre for Cybersecurity Belgium (CCB)*

Drugi autor: *Autoritatea Pentru Digitalizarea Romaniei-NCC-RO (ADR-NCC-RO)*

Spis treści

Wprowadzenie 9
Podstawowe wymagania CRA w zakresie cyberbezpieczeństwa: załącznik I, część I 10
1. Podejście do cyberbezpieczeństwa oparte na ryzyku 10
Podstawy oceny ryzyka 11
1.1. Ocena ryzyka cyberbezpieczeństwa w cyklu życia 12
1.1.1. Kluczowe etapy oceny ryzyka w cyklu życia 13
1.1.2. Przykłady zastosowań według etapu cyklu życia 14
1.1.3. Narzędzia i struktury wspierające 15
1.2. Indywidualne środki bezpieczeństwa 15
1.2.1. Przeprowadź klasyfikację ryzyka produktu 15
1.2.2. Określ cele bezpieczeństwa dla poszczególnych poziomów ryzyka 16
1.2.3. Przyporządkuj podstawowe wymagania CRA do poziomu ryzyka 17
1.2.4. Wykorzystanie modelowania zagrożeń w celu udoskonalenia środków 18
1.2.5. Wybierz środki kontroli dla poszczególnych poziomów ryzyka 18
1.2.6. Dokumentuj dowody zgodności 19
1.2.7. Przykłady 19
1.3. Rozważenie modeli zagrożeń, powierzchni ataku oraz potencjalnego wpływu na użytkowników i systemy 20
1.3.1. Modele zagrożeń: kto atakuje, dlaczego i w jaki sposób? 20
1.3.2 Powierzchnie ataku: gdzie atakujący może się dostać? 21
1.3.3 Analiza skutków: co się stanie, jeśli coś pójdzie nie tak? 22
1.3.4 Integracja: od analizy do środków zaradczych 22
2. Bezpieczne projektowanie i rozwój 23
2.1. Bezpieczeństwo od samego początku – bezpieczeństwo od momentu powstania projektu 23
2.2. Bezpieczeństwo domyślne – bezpieczeństwo bez konfiguracji przez użytkownika 24
2.3. Bezpieczne praktyki kodowania ..... Error! Bookmark not defined.
2.4. W konkretnym ujęciu dla producentów 25
3. Zarządzanie bezpieczeństwem w cyklu życia 26
3.1. Ciągłe monitorowanie podatności 26
3.2. Terminowe aktualizacje zabezpieczeń i poprawki 27
3.3. Zgłaszanie luk w zabezpieczeniach i przejrzysta polityka komunikacji 28
4. Bezpieczeństwo łańcucha dostaw 29

4.1. Wykaz komponentów oprogramowania (SBOM) 29
4.2. Wymagania bezpieczeństwa dla dostawców 30
4.3. Zarządzanie ryzykiem związanym z bibliotekami open source i zewnętrznymi 31
Wnioski 32

Spis tabel i rysunków

Tabela 1: Przykładowa matryca 11
Rysunek 1: Wizualizacja ryzyka 11
Rysunek 2: Wykres akceptacji ryzyka 12
Tabela 2: Kluczowe etapy oceny ryzyka w cyklu życia 13
Tabela 3: Przykłady zastosowań według etapu cyklu życia 14
Tabela 4: Cele bezpieczeństwa według poziomu ryzyka 16
Tabela 5: Podstawowe wymagania CRA według poziomu ryzyka 17
Tabela 6: Środki kontroli według poziomu ryzyka 18
Tabela 7: Środki wdrożeniowe według poziomu ryzyka 19

Skróty

API – (z ang. Application Programming Interface) interfejs programowania aplikacji

APT – (z ang. Advanced Persistent Threats) zaawansowane trwałe zagrożenia

BSIMM – (z ang. Building Security in Maturity Model) model dojrzałości bezpieczeństwa

CI/CD – (z ang. Continuous Integration and Continuous Delivery/Deployment) ciągła integracja i ciągłe dostarczanie/wdrażanie

CRA – (z ang. Cyber Resilience Act) Rozporządzenie (UE) 2024/2847 (akt o cyberodporności)

CVD – (z ang. Coordinated Vulnerability Disclosure) skoordynowane ujawnianie luk w zabezpieczeniach

CVE – (z ang. Common Vulnerabilities and Exposures) wspólne podatności i zagrożenia

CVSS – (z ang. Common Vulnerability Scoring System) wspólny system oceny podatności

DAST – (z ang. Dynamic Application Security Testing) dynamiczne testowanie bezpieczeństwa aplikacji

DoS – (z ang. Denial of Service) odmowa usługi

DREAD – (z ang. Damage, Reproducibility, Exploitability, Affected Users, and Discoverability) szkody, powtarzalność, możliwość wykorzystania, użytkownicy dotknięci problemem i wykrywalność

ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa

EOL – (z ang. End of Life) koniec cyklu życia

EPSS – (z ang. Exploit Prediction Scoring System) system punktacji prognozowania wykorzystania podatności)

ETSI – (z ang. European Technical Standard Institute) Europejski Instytut Norm Technicznych

FIRST VCMM – (z ang. FIRST Vulnerability Coordination Maturity Model) model dojrzałości koordynacji podatności FIRST

HTTPS/TLS – protokół bezpiecznego przesyłania hipertekstu/bezpieczeństwo warstwy transportowej

ICS – (z ang. Industrial Control System) przemysłowy system kontroli

IEC – (z ang. International Electrotechnical Commission) Międzynarodowa Komisja Elektrotechniczna

IoT – (z ang. Internet of Things) Internet rzeczy

IPSec – (z ang. Internet Protocol Security) protokół bezpieczeństwa internetowego

ISO – (z ang. International Standards Organisation) Międzynarodowa Organizacja Normalizacyjna

JTAG – (z ang. Joint Test Action Group) Wspólna grupa ds. testów

LINDDUN – (z ang. Linking, Identifying, Non-repudiation, Detecting, Data Disclosure, Unawareness and Non-compliance) Łączenie, identyfikacja, niezaprzeczalność, wykrywanie, ujawnianie danych, nieświadomość i niezgodność

MFA – (z ang. Multi-Factor Authentication) uwierzytelnianie wieloskładnikowe

MITRE ATT&CK – taktyki, techniki i powszechna wiedza przeciwników

MŚP – małe i średnie przedsiębiorstwa

MQTT – (z ang. Message Queuing Telemetry Transport) Transport telemetrii z kolejkowaniem wiadomości

NIST – (z ang. National Institute of Standards and Technology) Narodowy Instytut Standardów i Technologii (Stany Zjednoczone)

NIST SSDF – (z ang. NIST Secure Software Development Framework) Ramy bezpiecznego tworzenia oprogramowania NIST

NTIA – (z ang. National Telecommunications and Information Administration) Narodowa Administracja Telekomunikacji i Informacji (Stany Zjednoczone)

OPENSSF VEX – (z ang. Open-Source Security Foundation Vulnerability Exploitability eXchange) Fundacja bezpieczeństwa oprogramowania open source Vulnerability Exploitability eXchange

OS – (z ang. Operating System) system operacyjny

OTA – (z ang. Over The Air) bezprzewodowo

OWASP – (z ang. Open Worldwide Application Security Project) Otwarty światowy projekt bezpieczeństwa aplikacji

OWASP ASVS – (z ang. OWASP Application Security Verification Standard) Standard weryfikacji bezpieczeństwa aplikacji OWASP

OWASP SAMM – (z ang. OWASP Software Assurance Maturity Model) Model dojrzałości zabezpieczeń oprogramowania OWASP

PDE – (z ang. Product with Digital Elements) produkt zawierający elementy cyfrowe

PSIRT – (z ang. Product Security Incident Response Team) Zespół reagowania na incydenty związane z bezpieczeństwem produktów

RODO – ogólne rozporządzenie o ochronie danych

SAST – (z ang. Static Application Security Testing) statyczne testy bezpieczeństwa aplikacji

SBOM – (z ang. Software Bill of Materials) lista komponentów oprogramowania

SCA – (z ang. Software Composition Analysis) Analiza składu oprogramowania

SIEM – (z ang. Security Information and Event Management) zarządzanie informacjami i zdarzeniami bezpieczeństwa

SOC – (z ang. Security Operations Centre) Centrum operacji bezpieczeństwa

SQL – (z ang. Structured Query Language) Strukturalny język zapytań

SSDLC – (z ang. Secure Software Development Lifecycle) Bezpieczny cykl życia oprogramowania

SSL – (z ang. Secure Sockets Layer) protokół SSL

STRIDE – (z ang. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) Fałszowanie, manipulacja, odrzucenie, ujawnienie informacji, odmowa usługi, podwyższenie uprawnień

TPM – (z ang. Trusted Platform Module) zaufany moduł platformy

UART – (z ang. Universal Asynchronous Receiver-Transmitter) uniwersalny asynchroniczny odbiornik-nadajnik

UE – Unia Europejska

USB – (z ang. Universal Serial Bus) uniwersalne złącze USB

VPN – (z ang. Virtual Private Network) wirtualna sieć prywatna

Wprowadzenie

W celu zapewnienia zgodności z **aktem o cyberodporności** (CRA), rozporządzeniem (UE) 2024/2847, każdy producent musi spełnić szereg wymagań i obowiązków nakładanych przez CRA. Najważniejsze z nich to zapewnienie, że produkt zawierający elementy cyfrowe (PDE), który wprowadzasz do obrotu, „został zaprojektowany, opracowany i wyprodukowany zgodnie z zasadniczymi wymogami w zakresie cyberbezpieczeństwa określonymi w części I załącznika I"[1] . Załącznik I składa się z dwóch części – część I koncentruje się na wymogach dotyczących cyberbezpieczeństwa związanych z właściwościami produktu, a część II dotyczy wymogów dotyczących postępowania w przypadku luk z zagrożeniach. Część I składa się z dwóch punktów, z których pierwszy stanowi, że

> *„Produkty zawierające elementy cyfrowe powinny być zaprojektowane, opracowane i wyprodukowane w taki sposób, aby zapewniały odpowiedni poziom cyberbezpieczeństwa w oparciu o ryzyko"*[2] .

Punkt 2 określa wymagania, które muszą spełniać produkty.

Niniejsze wytyczne, opracowane w ramach **projektu SECURE**[3] w celu **wsparcia małych i średnich przedsiębiorstw (MŚP)**, zgłębiają oba punkty części I załącznika I, przedstawiając **niewyczerpujące praktyczne i techniczne sugestie, przykłady i podejścia mające na celu wsparcie zgodności z każdym z wymagań**. Należy zauważyć, że wszelkie odniesienia do istniejących norm, narzędzi i ram mają **charakter** wyłącznie **sugestywny** i mają na celu jak najlepsze uchwycenie wymagań CRA. Zalecenia opierają się na uznanych najlepszych praktykach i powszechnych podejściach. Zarówno narzędzia, o których mowa w wytycznych, jak i same wytyczne będą aktualizowane w miarę postępów w opracowywaniu szczegółowych norm CRA i środków wykonawczych Komisji Europejskiej w okresie adaptacyjnym od 2024 do 2027 r.

[1] Art. 13 ust. 1 CRA.

[2] Załącznik I, część I ust. 1, CRA.

[3] Projekt „Wzmocnienie cyberodporności MŚP w UE" (SECURE) oferuje wsparcie finansowe i wytyczne dla MŚP w zakresie zgodności z CRA.

Podstawowe wymagania CRA w zakresie cyberbezpieczeństwa: załącznik I, część I

1. Podejście do cyberbezpieczeństwa oparte na ryzyku

Punkt 1 załącznika I, część I stanowi, że

> *„Produkty zawierające elementy cyfrowe powinny być projektowane, opracowywane i wytwarzane w taki sposób, aby zapewniały **odpowiedni poziom cyberbezpieczeństwa w oparciu o ryzyko**"*[4].

Jest to kluczowy punkt w CRA i opiera się na zasadzie „security by design and by default", czyli uwzględnienia bezpieczeństwa już na etapie projektowania i domyślnego stosowania zasad bezpieczeństwa. W praktyce oznacza to, że należy opracować **podejście do cyberbezpieczeństwa oparte na ryzyku** dla swojego produktu. Takie rozwiązanie oparte na ryzyku powinno być uzasadnione, udokumentowane i proporcjonalne. Zgodność z CRA należy traktować jako „ścieżkę, którą można prześledzić":

kontekst produktu → ryzyko → środki kontroli → dowód

Uzasadnienie tej ścieżki powinno być starannie udokumentowane w obowiązkowej dokumentacji technicznej[5] , która ma kluczowe znaczenie dla zgodności i możliwości przeprowadzenia audytu.

W praktyce producenci muszą:

1. Ocenić ryzyko cyberbezpieczeństwa związane z PDE w jego całym cyklu życia ;
2. Dostosować środki bezpieczeństwa do poziomu ryzyka (np. inteligentny termostat vs. przemysłowy system sterowania);
3. Rozważyć modele zagrożeń, obszary ataku oraz potencjalny wpływ na użytkowników i systemy.

Pierwszym kluczowym krokiem w zapewnieniu zgodności z CRA jest zatem przeprowadzenie **oceny ryzyka** dla urządzenia PDE. W niniejszym rozdziale omówiono sposób przeprowadzania takiej oceny, przedstawiając możliwe podejścia i rozwiązania techniczne.

Zanim przejdziemy do szczegółów, poniżej przedstawiono dwustronicowy przegląd **oceny ryzyka 101**, aby odświeżyć pamięć. Elementy te pojawiają się ponownie bardziej szczegółowo w pierwszym rozdziale niniejszych wytycznych, z którym zalecane jest zapoznanie się. Jednak ze względu na dostępność uproszczone podsumowanie przedstawia ogólne podejście do oceny ryzyka[6] .

[4] Załącznik I, część I pkt 1, CRA.
[5] Art. 31, CRA.
[6] Należy pamiętać, że Komisja Europejska nie opracowała jeszcze oficjalnych wytycznych dotyczących sposobu przeprowadzania oceny ryzyka w odniesieniu do CRA. Niniejsze wytyczne zawierają podsumowanie głównych etapów każdego podejścia do oceny ryzyka. Można stosować dowolne inne podejście, normę lub metodologię, o ile jest ono zgodne z opisanym podejściem.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Ocena ryzyka 101

Podczas przeprowadzania oceny ryzyka można rozważyć **sześć kroków**:

1) Identyfikacja **aktywów** i **zagrożeń** = *identyfikacja wszystkich aktywów (co należy chronić) zgodnie z ich narażeniem na zagrożenie (co może pójść nie tak);*
2) Ocena **podatności** = *ewaluacja podatności*;
3) Rozważenie i ocena **skutków** oraz **prawdopodobieństwa** = *sporządzenie wykresu skutków i prawdopodobieństwa wystąpienia podatności → w rezultacie uzyskuje się konkretne „ryzyka"*;
4) **Analiza** ryzyka i **akceptacja** = *sporządzenie wykresu każdego ryzyka i rozważenie poziomu akceptacji, aby ustalić priorytety działań;*

Oprócz tej oceny ryzyka, dwa ostatnie kroki obejmują:

5) Wdrożenie **środków ograniczających ryzyko** = *wybór i zastosowanie środków kontroli bezpieczeństwa dla każdego ryzyka;*
6) Monitorowanie i ponowna ocena = *monitorowanie zagrożeń i ryzyka na każdym etapie cyklu życia PDE oraz aktualizowanie oceny ryzyka.*

W przypadku **kroków od pierwszego do trzeciego** można opracować **matrycę**, która pozwala sklasyfikować każde zagrożenie, podatność i wpływ zgodnie z określonym poziomem ryzyka i punktacją. W tym celu należy najpierw zdefiniować, co oznacza każdy poziom (i punktacja) za pomocą tabel opisowych[7].

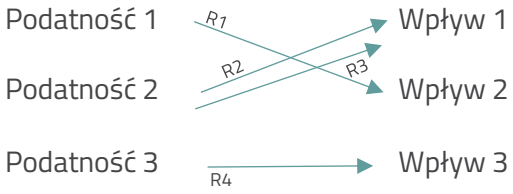
- Niski
- Nisko-średni
- Średni
- Średnio-wysoki
- Wysoki

Tabela 1:
Przykładowa macierz

Ryzyko/zagrożenie	Zagrożenie 1	Zagrożenie 2	Wynik
Wysoki			10
Średnio-wysoki			
Średni			
Nisko-Średni			
Niski			0

Powiązanie podatności z wpływem pozwala następnie na wizualizację różnych rodzajów ryzyka (R):

Rysunek 1:
Wizualizacja ryzyka

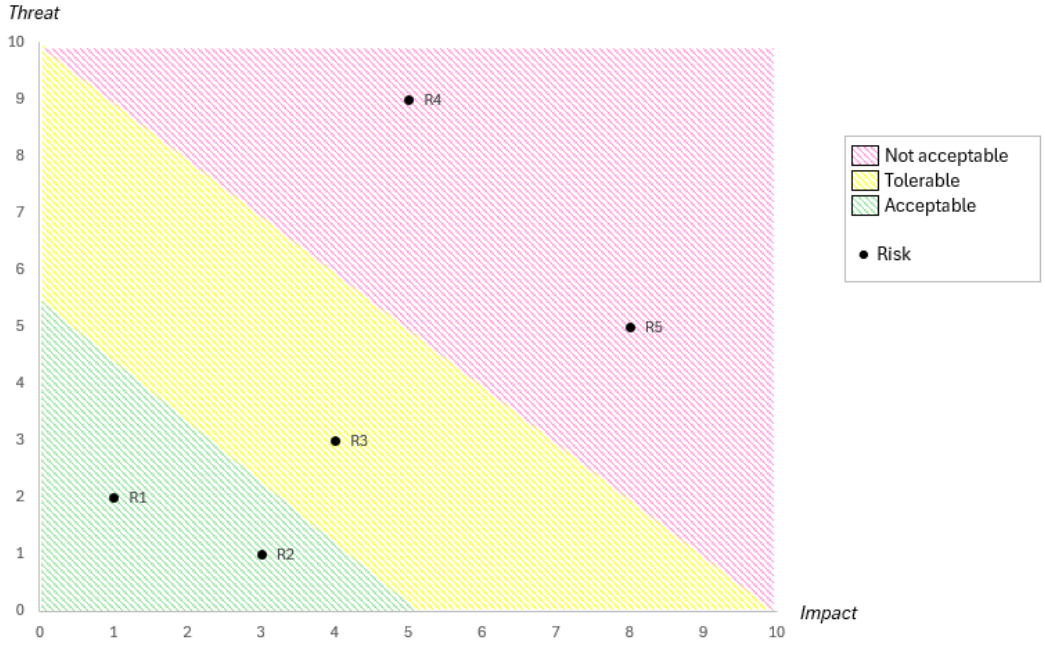


[7] np. w przypadku wystąpienia zagrożenia poziom „niski" może oznaczać zagrożenie, które może wystąpić raz na 10 lat, natomiast poziom „wysoki" może oznaczać zagrożenie, które może wystąpić raz w tygodniu. Potrzebne są oddzielne tabele opisowe dla zagrożeń, podatności i skutków oraz ryzyka – ta ostatnia pomaga w określeniu poziomu akceptowalności.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

W **czwartym kroku** ważne jest, aby sporządzić wykres napotkanych ryzyk i określić poziom akceptacji tych zagrożeń – często odbywa się to za pomocą kodowania kolorami, na przykład:

Rysunek 2:
Wykres akceptacji ryzyka



Pozwala to ustalić priorytety działań oraz opracować środki ograniczające ryzyko i kontrole bezpieczeństwa dla każdego ryzyka, aby zredukować ryzyko resztkowe do akceptowalnego poziomu.

Jak wspomniano wcześniej, te elementy oceny ryzyka zostały omówione bardziej szczegółowo poniżej (rozdział 1 niniejszych wytycznych) wraz z przykładami i zalecanymi narzędziami oraz ramami, które mogą okazać się pomocne.

1.1. Ocena ryzyka cyberbezpieczeństwa w cyklu życia

Ponieważ ryzyko cyberbezpieczeństwa związane z PDE musi być oceniane przez cały cykl życia produktu, przeprowadzenie **oceny ryzyka cyberbezpieczeństwa w cyklu życia produktu** wymaga **identyfikacji, analizy i ograniczania ryzyka cyberbezpieczeństwa** na każdym etapie cyklu życia produktu:

1. Projektowanie
2. Rozwój
3. Produkcja
4. Wdrożenie
5. Eksploatacja i konserwacja
6. Koniec cyklu życia (EOL)

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Ocena ryzyka musi być stale aktualizowana przez cały „okres wsparcia"[8] , czyli okres co najmniej pięciu lat (lub, jeśli okres użytkowania produktu jest krótszy niż pięć lat, co najmniej do końca okresu użytkowania produktu).

1.1.1. Kluczowe etapy oceny ryzyka w cyklu życia produktu

Podczas przeprowadzania oceny ryzyka można rozważyć sześć kroków, z których każdy został wyjaśniony w tabeli 2 poniżej.

Tabela 2:
Kluczowe etapy oceny ryzyka w cyklu życia produktu

Kluczowy etap	Wyjaśnienia i sugestie
1. Identyfikacja aktywów i zagrożeń	Rozróżnienie między: • Aktywa: co wymaga ochrony? np. oprogramowanie sprzętowe, dane użytkowników, kanały komunikacyjne. • Zagrożenia: co może pójść nie tak? np. wprowadzenie złośliwego oprogramowania, nieautoryzowany dostęp.
2. Analiza podatności	Wykorzystanie narzędzi, takich jak: • Statyczna analiza kodu; • Analiza składu oprogramowania (SCA); • Testy penetracyjne; • Modelowanie zagrożeń[9] (np. STRIDE, DREAD). Uwaga: CVSS i STRIDE mogą być stosowane łącznie w procesie modelowania zagrożeń. STRIDE może pomóc w identyfikacji potencjalnych zagrożeń, a CVSS może następnie służyć do oceny stopnia zagrożenia związanego z tymi zagrożeniami, co pozwala na lepsze ustalenie priorytetów działań mających na celu ograniczenie ryzyka[10] .

[8] Art. 13 ust. 8 CRA: Okres wsparcia technicznego określa producent, biorąc pod uwagę przewidywany czas użytkowania produktu, oczekiwania użytkowników, charakter produktu (przeznaczenie) oraz prawo Unii.
[9] Modelowanie zagrożeń omówiono bardziej szczegółowo w pkt 1.3.1.
[10] CVSS ocenia stopień zagrożenia, podczas gdy ryzyko uwzględnia również wpływ na działalność i prawdopodobieństwo wystąpienia.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

3. Ocena wpływu ryzyka i prawdopodobieństwo jego wystąpienia	Wykorzystanie matrycy ryzyka, aby ustalić priorytety w oparciu o: • Wpływ (np. naruszenie bezpieczeństwa danych, awaria systemu); • Prawdopodobieństwo (np. znane luki w zabezpieczeniach, obszar ataku).
4. Analiza ryzyka i jego akceptowalności	Określenie poziomu akceptowalności i narysowanie wykresu ryzyka zgodnie z zagrożeniem i wpływem, aby sklasyfikować i ustalić priorytety działań.
5. Wdrożenie środków ograniczających ryzyko	Zastosowanie środków kontroli bezpieczeństwa: np. szyfrowanie, uwierzytelnianie, bezpieczny rozruch.
6. Monitorowanie i ponowna ocena	Stałe monitorowanie nowych zagrożeń i odpowiednie aktualizowanie oceny ryzyka.

1.1.2. Przykłady zastosowań według etapu cyklu życia

W celu zrozumienia oceny ryzyka w cyklu życia, w tabeli 3 poniżej przedstawiono przegląd przypadków użycia, w tym przykładowe ryzyko i strategie jego ograniczania dla każdego etapu cyklu życia.

Tabela 3:
Przykłady zastosowań według etapu cyklu życia

Etap cyklu życia	Przykład	Ryzyko	Ograniczanie ryzyka
Projektowanie	Kamera inteligentnego domu	Nieautoryzowany dostęp do obrazu wideo	Wdrożenie kompleksowego szyfrowania i bezpiecznych ustawień domyślnych
Rozwój	Oprogramowanie sprzętowe urządzenia	Luka w zabezpieczeniach związana z przepełnieniem bufora	Stosowanie bezpiecznych praktyk kodowania i automatycznego skanowania podatności
Produkcja	Przemysłowa brama IoT	Narażenie podczas produkcji	Zabezpieczenie łańcucha dostaw i sprzętowego źródła zaufania, plomby zabezpieczające przed manipulacją oraz bezpieczne zaopatrzenie

Wdrożenie	Router domowy	Domyślne dane uwierzytelniające pozostają niezmienione	Wymuszanie zmiany hasła przy pierwszym użyciu
Eksploatacja i konserwacja	Podłączony pojazd	Niezałatane luki w zabezpieczeniach oprogramowania	Aktualizacje OTA (Over-The-Air) z kontrolą integralności
Koniec cyklu życia	Inteligentny termostat	Porzucone urządzenie z podatnym na ataki oprogramowaniem sprzętowym	Zapewnienie bezpiecznych instrukcji dotyczących wycofania z eksploatacji i usuwania danych, polityki aktualizacji zabezpieczeń po zakończeniu cyklu życia oraz eksportu danych dla użytkowników

1.1.3. Narzędzia i struktury zapewniające wsparcie

Poniższa lista zawiera kilka narzędzi i ram, które mogą zapewnić wsparcie, jednak bardziej wyczerpująca lista i zharmonizowane normy są nadal w trakcie opracowywania.

- ISO/IEC 27005 – Zarządzanie ryzykiem
- NIST SP 800-30 – Metodologia oceny ryzyka
- ENISA Threat Landscape – zaktualizowane informacje o zagrożeniach
- OWASP ASVS – weryfikacja bezpieczeństwa aplikacji
- Model STRIDE
- Model oceny ryzyka DREAD
- LINDDUN
- CVSS

1.2. Dostosowane środki bezpieczeństwa

Drugim wymiarem podejścia do cyberbezpieczeństwa opartego na ryzyku jest dostosowanie środków bezpieczeństwa do poziomu ryzyka. Dostosowanie musi być proporcjonalne do ryzyka zdefiniowanego w załączniku I część I pkt 1. Wyjaśnimy, co to oznacza, przedstawiając sześć jasnych kroków, zasady i dwa przykładowe produkty: inteligentny termostat (ryzyko od niskiego do umiarkowanego) oraz przemysłowy system sterowania (ICS) (ryzyko wysokie).

1.2.1. Przeprowadzenie klasyfikacji ryzyka produktu

Podczas przeprowadzania oceny ryzyka dla konkretnego produktu należy wziąć pod uwagę następujące wymiary.

- **Narażenie na zagrożenia**:
  - Czy produkt jest podłączony do Internetu?
  - Czy produkt jest szeroko stosowany?
  - Czy produkt jest dostępny publicznie?
  - Przeznaczenie produktu a racjonalnie przewidywalne niewłaściwe użycie?
- **Skutki naruszenia bezpieczeństwa**: Jaki byłby wpływ na bezpieczeństwo, straty finansowe, prywatność, infrastrukturę krytyczną?
- **Atrakcyjność ataku:** Czy byłby to punkt wyjścia do ruchu lateralnego w sieci?
- **Profil użytkownika:** konsument, MŚP, operator infrastruktury krytycznej?

Na podstawie powyższych rozważań produkt można sklasyfikować jako: niskie ryzyko – dopuszczalne, umiarkowane ryzyko – tolerowane lub wysokie ryzyko – niedopuszczalne[11] .

1.2.2. Określenie celów bezpieczeństwa dla poszczególnych poziomów ryzyka

Tabela 4 ilustruje, w jaki sposób cele bezpieczeństwa można dostosować do wcześniej ustalonego poziomu ryzyka produktu.

Tabela 4:
Cele bezpieczeństwa według poziomu ryzyka

Poziom ryzyka	Cele bezpieczeństwa
Niski (np. inteligentny termostat)	• Zapobieganie trywialnym nadużyciom; • Zapewnienie prywatności; • Utrzymanie możliwości aktualizacji.
Średni	• Wykrywanie i ograniczanie znanych wektorów ataków; • Wymuszanie uwierzytelniania; • Zabezpieczanie komunikacji.
Wysoki (np. ICS)	• Wzmocniona ochrona bezpieczeństwa;

[11] Wymaga to wcześniejszego zdefiniowania sposobu oceny tych elementów za pomocą macierzy oraz sposobu, w jaki oceny te odpowiadają poziomom ryzyka. W celu uzyskania bardziej precyzyjnej klasyfikacji można rozważyć pięć, zamiast trzech, poziomów ryzyka: niskie, średnio-niskie, średnie, średnio-wysokie l wysokie ryzyko.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

	• Głęboka ochrona; • Zaufanie łańcucha dostaw; • Bezpieczny start; • Monitorowanie incydentów.

1.2.3. Przyporządkowanie podstawowych wymagań CRA do poziomu ryzyka

W zależności od poziomu ryzyka podstawowe wymagania CRA mogą mieć różne zastosowania praktyczne. Tabela 5 ilustruje to dla niskiego i wysokiego poziomu ryzyka oraz odpowiednich przykładowych przypadków produktów, inteligentnego termostatu i ICS.

Tabela 5:
Podstawowe wymagania CRA według poziomu ryzyka

Wymóg CRA	Niskie ryzyko	Wysokie ryzyko
Bezpieczeństwo w projektowaniu i bezpieczne ustawienia domyślne	Wyłączenie portów debugowania; silne ustawienia domyślne	Pełna lista komponentów oprogramowania (SBOM[12]); bezpieczny start; wzmocniony system operacyjny
Postępowanie w przypadku luk w zabezpieczeniach	Publiczna polityka CVD; plik security.txt; monitorowanie skrzynki odbiorczej; mechanizm poprawek	Skoordynowane ujawnianie; PSIRT; szybka reakcja
Rejestrowanie i monitorowanie	Lokalne dzienniki zdarzeń	Zdalne rejestrowanie; integracja SIEM
Kontrola dostępu	Uwierzytelnianie za pomocą kodu PIN lub aplikacji	Dostęp oparty na rolach; MFA; minimalne uprawnienia
Mechanizm aktualizacji	Aktualizacje OTA za zgodą użytkownika	Podpisane aktualizacje; bezpieczne przywracanie poprzedniej wersji
Ochrona przed nieautoryzowanym dostępem	Podstawowe reguły zapory sieciowej	Systemy wykrywania włamań do hosta; kontrole integralności oprogramowania sprzętowego

[12] SBOM wyjaśniono bardziej szczegółowo w sekcji 4.1.

1.2.4. Wykorzystanie modelowania zagrożeń do udoskonalenia środków

W przypadku modelowania zagrożeń można zastosować metody STRIDE, LINDDUN lub drzewa ataków, aby zweryfikować adekwatność środków kontroli.

W przypadku przykładowych produktów oznacza to:

- **Inteligentny termostat**: skupienie się na spoofingu, manipulacji i odmowie usługi;
- **ICS**: uwzględnienie wszystkich zagrożeń STRIDE oraz zaawansowanych, trwałych zagrożeń (APT).

1.2.5. Wybieranie środków kontroli według poziomu ryzyka

W tabeli 6 przedstawiono różne środki kontroli według dziedziny bezpieczeństwa dla praktycznych przykładów: inteligentnego termostatu (niskie ryzyko) i ICS (wysokie ryzyko).

Tabela 6:
Środki kontroli według poziomu ryzyka

Dziedzina bezpieczeństwa	Niskie ryzyko	Wysokie ryzyko
Uwierzytelnianie	Uwierzytelnianie oparte na aplikacji; zmiana domyślnego hasła	MFA; kontrola dostępu oparta na certyfikatach
Bezpieczeństwo oprogramowania sprzętowego	Podpisane oprogramowanie układowe; aktualizacje OTA; bezpieczne przywracanie poprzedniej wersji	Bezpieczny start; integracja TPM; zapewnienie bezpieczeństwa łańcucha dostaw
Komunikacja	HTTPS/TLS	VPN; IPSec; segmentacja sieci; zero trust
Monitorowanie	Podstawowa rotacja logów	Rejestrowanie w czasie rzeczywistym; wykrywanie anomalii; integracja SOC; logi zsynchronizowane czasowo
Interfejs użytkownika	Prosty panel ustawień	Szczegółowa konsola administracyjna; funkcje ścieżki audytu

1.2.6. Dowody zgodności z przepisami

Jak wspomniano wcześniej, kluczowym elementem zgodności z CRA jest dokumentowanie co najmniej następujących dowodów:

- Uzasadnienie klasyfikacji ryzyka;
- Decyzje kontrolne związane z ryzykiem;
- Wyniki testów i walidacji;
- Polityki aktualizacji i postępowania w przypadku wykrycia luk w zabezpieczeniach;
- Dostosowanie cyklu życia bezpiecznego rozwoju (np. ISO/IEC 27034, IEC 62443-4-1);
- Macierz identyfikowalności przyporządkowująca ryzyko → środki kontroli → testy weryfikacyjne → dowody (do przechowywania w dokumentacji technicznej)

1.2.7. Przykłady

W tabeli 7 przedstawiono dodatkowe przykłady środków wdrożeniowych dla praktycznych przypadków niskiego i wysokiego ryzyka.

Tabela 7:
Środki wdrożeniowe według poziomu ryzyka

Produkt	Inteligentny termostat	ICS
Czynniki ryzyka	• Podłączony do Internetu, steruje ogrzewaniem w prywatnym domu; • Wrażliwy na kwestie prywatności, ale o niewielkim wpływie na bezpieczeństwo lub gospodarkę.	• Wykorzystywany w infrastrukturze krytycznej (np. uzdatnianie wody); • Wysoki wpływ na bezpieczeństwo i funkcjonowanie.
Klasyfikacja ryzyka	Niskie ryzyko	Wysokie ryzyko

Środki wdrożeniowe	• Zmiana domyślnego hasła przy pierwszym użyciu; • Komunikacja HTTPS z zapleczem; • Podpisane aktualizacje oprogramowania sprzętowego; • Tylko lokalne logowanie[13] ; • Podstawowy formularz kontaktowy dotyczący luk w zabezpieczeniach.	• Bezpieczny sprzęt z modułem TPM; • Bezpieczny start i podpisane aktualizacje z możliwością przywrócenia poprzedniej wersji; • Dostęp oparty na rolach i uwierzytelnianie wieloskładnikowe (MFA); • Segmentacja sieci i reguły zapory sieciowej; • Rejestrowanie w centralnym systemie SIEM; • Pełna lista komponentów (SBOM) przy każdej aktualizacji; • Skoordynowany proces ujawniania luk w zabezpieczeniach (CVD);

1.3. Uwzględnienie modeli zagrożeń, obszaru ataku oraz potencjalnego wpływu na użytkowników i systemy.

CRA kładzie nacisk na podejście do cyberbezpieczeństwa oparte na ryzyku. Jak pokazano powyżej, oznacza to, że producenci powinni dostosować swoje środki bezpieczeństwa do realnych zagrożeń, punktów narażenia i potencjalnych konsekwencji dla użytkowników i systemów. Nie jest to pusta dyrektywa, ale wezwanie do przyjęcia uzasadnionego podejścia uwzględniającego kontekst. Skuteczne wdrożenie tego obowiązku wymaga rozważenia łącznie trzech kluczowych pojęć: modeli zagrożeń, obszaru ataku i analizy wpływu, które stanowią trzeci i ostatni wymiar podejścia do cyberbezpieczeństwa opartego na ryzyku. Przyjrzymy się kolejno tym elementom i zobaczymy, jak się ze sobą łączą.

1.3.1. Modele zagrożeń: kto atakuje, dlaczego i w jaki sposób?

Modelowanie zagrożeń to ustrukturyzowany proces, w ramach którego identyfikuje się, kto może zaatakować dany produkt, w jaki sposób może to zrobić i jakie są jego motywy. Należy wziąć pod uwagę początkujących hakerów, zorganizowane grupy cyberprzestępców, a nawet podmioty

[13] Uwaga: dzienniki dostępne tylko lokalnie zmniejszają wartość kryminalistyczną, zaleca się opcjonalny eksport za zgodą użytkownika.

państwowe. Ich motywy są różne – od korzyści finansowych po sabotaż lub szpiegostwo, a ich umiejętności wahają się od podstawowych do zaawansowanych.

W celu uporządkowania tych informacji, można skorzystać z takich metod jak:

- STRIDE;
- MITRE ATT&CK w przypadku znanych technik ataku;
- LINDDUN w przypadku zagrożeń związanych z prywatnością;
- drzewa ataków lub cyber kill chains do mapowania ścieżek ataku.

Wracając do praktycznych przykładów, oznacza to:

- **Inteligentny termostat**: zagrożenia często ograniczają się do ciekawskich sąsiadów lub przypadkowych ataków, w których ktoś może manipulować ustawieniami temperatury lub zużyciem energii;
- **ICS** (np. w stacji uzdatniania wody): zagrożenia są zasadniczo inne — np. grupy APT lub gangi ransomware próbują sabotować procesy fizyczne lub zamknąć działalność.

Wynikiem modelowania zagrożeń jest jasna lista celów bezpieczeństwa specyficznych dla produktu i jego środowiska.

1.3.2 Obszar ataku: gdzie atakujący może się dostać?

Obszar ataku to ogół wszystkich punktów, w których atakujący może wejść w interakcję z systemem lub wpłynąć na niego. Im więcej interfejsów i punktów dostępu, tym większe ryzyko.

Typowe obszary ataku to:

- Interfejsy sieciowe, takie jak Wi-Fi, Bluetooth, MQTT lub HTTP;
- Interfejsy lokalne, takie jak USB, UART, JTAG (do debugowania);
- Mechanizmy aktualizacji, takie jak aktualizacje OTA lub USB;
- API, aplikacje mobilne, panele zarządzania w chmurze;
- Komponenty zewnętrzne z łańcucha dostaw.

Analiza tych obszarów polega na sprawdzeniu, które komponenty są niepotrzebnie narażone, które usługi są włączone, ale nie są potrzebne, oraz czy dostęp jest odpowiednio chroniony. Najlepiej byłoby ograniczyć powierzchnię ataku poprzez:

- Zasady bezpieczeństwa, takie jak minimalna ekspozycja, bezpieczne ustawienia domyślne i wzmocnienie zabezpieczeń;
- Wyłączenie nieużywanych portów lub usług;
- Uwierzytelnianie i szyfrowanie w każdym interfejsie.

W odniesieniu do przykładów oznacza to:

- **Inteligentny termostat**: zazwyczaj korzysta z Wi-Fi i ewentualnie Bluetooth, z prostym połączeniem z chmurą — interfejsy debugowania mogą być otwarte podczas testowania i muszą być wyłączone w środowisku produkcyjnym;
- **Brama ICS**: będzie fizycznie chroniona, z ekranowanymi aktualizacjami USB, segmentowanymi sieciami i bez interfejsów zewnętrznych.

Dokładne mapowanie obszaru ataku jest zatem niezbędne, aby wiedzieć, gdzie naprawdę potrzebne jest zabezpieczenie.

1.3.3 Analiza wpływu: co się stanie, jeśli coś pójdzie nie tak?

Ostatnim krokiem jest określenie potencjalnego wpływu udanego ataku. CRA wymaga, aby środki bezpieczeństwa były proporcjonalne do tego wpływu. Obejmuje to nie tylko szkody techniczne, ale także:

- Zagrożenia dla użytkownika (np. obrażenia spowodowane regulacją temperatury);
- Naruszenie prywatności (np. wnioskowanie o stylu życia na podstawie danych z termostatu);
- Utratę dostępności lub ciągłości działania (np. zamknięcie fabryki);
- Odpowiedzialność prawną (np. naruszenie CRA lub RODO);
- Szkody wizerunkowe i ryzyko rynkowe.

Należy wziąć pod uwagę wpływ na wielu płaszczyznach:

- Użytkownik: od drobnych niedogodności po sytuacje zagrażające życiu;
- Organizacja: od zwiększonego obciążenia działu pomocy technicznej po przerwę w działalności;
- Społeczeństwo: od niewinnych błędów po zagrożenia dla infrastruktury krytycznej.

W tym przypadku również kluczowa jest proporcjonalność – zabawka-robot nie wymaga takiego samego poziomu bezpieczeństwa jak pompa medyczna.

1.3.4 Integracja: od analizy do środków

Połączenie tych trzech elementów – modelu zagrożeń, obszarów ataku i wpływu – tworzy solidną podstawę do dostosowania środków bezpieczeństwa.

Typowe podejście wygląda następująco:

1. Określenie zastosowania i kontekstu produktu;
2. Przeprowadzenie modelowania zagrożeń w celu zrozumienia podmiotów, motywów i ścieżek ataku;
3. Sporządzenie mapy obszarów ataku i zidentyfikowanie słabych punktów;

4. Przeanalizowanie wpływu na użytkowników, organizacje i społeczeństwo;
5. Wybranie środków w oparciu o ryzyko (ryzyko = prawdopodobieństwo × wpływ);
6. Dokumentowanie wszystkiego zgodnie z wymogami CRA i audytami.

W praktycznych przykładach oznacza to:

- **Inteligentny termostat**: szyfrowanie, polityka silnych haseł, podpisane aktualizacje OTA i prosta polityka prywatności.
- **Brama ICS**: otrzymanie bezpiecznego startu, sprzętowy root of trust, segmentowane sieci, rejestrowanie SIEM, zarządzanie rolami oraz kompletny SBOM z monitorowaniem podatności.

2. Bezpieczne projektowanie i rozwój

Wracając do punktu 1 załącznika I, część I CRA, podejście do cyberbezpieczeństwa oparte na ryzyku i dostosowywanie opierają się na zasadzie „security by design and by default ", tzn. PDE muszą być projektowane i opracowywane tak, aby były bezpieczne od samego początku. Nie jest wystarczające dodawanie zabezpieczenia jako opcjonalnej warstwy po fakcie; musi to być istotna część całego procesu rozwoju produktu.
'Secure by Design', 'Secure by Default' i stosowanie bezpiecznych praktyk programistycznych stanowią podstawę strategii dotyczącej odpornych produktów cyfrowych. Gwarantują one, że bezpieczeństwo nie jest dodatkiem, ale strukturalną i wyraźnie zintegrowaną częścią produktu – dokładnie tak, jak wymaga tego CRA.

Korzystając z międzynarodowych norm, takich jak IEC 62443, ISO 27034, OWASP i wytycznych ENISA, producenci mogą skutecznie stosować te zasady, jednocześnie wypełniając swoje obowiązki w zakresie zgodności.

Produkty muszą być:

1. **Secure by design**: bezpieczeństwo jest zintegrowane od najwcześniejszych etapów rozwoju;
2. **Secure by Default**: ustawienia domyślne muszą priorytetowo traktować bezpieczeństwo (np. silne hasła, minimalna liczba otwartych portów itp.);
3. **Bezpiecznie opracowane**: przy użyciu bezpiecznych praktyk kodowania i modelowania zagrożeń.

2.1. Security by Design – bezpieczeństwo od momentu powstania projektu

„Security by design" oznacza, że cyberbezpieczeństwo jest brane pod uwagę już w fazie koncepcyjnej przy podejmowaniu decyzji dotyczących architektury, wyboru komponentów

i interakcji między podsystemami. Bezpieczeństwo musi być tak samo fundamentalne jak funkcjonalność lub łatwość obsługi.

Praktyczny przykład:

Podczas projektowania modułu inteligentnego zamka do drzwi natychmiast podejmuje się następujące decyzje:

- Zastosowanie szyfrowania typu end-to-end między aplikacją a zamkiem;
- Bezpieczne przechowywanie kluczy w module TPM lub Secure Element;
- Fizyczne wyłączenie portów debugowania po zakończeniu produkcji.

Odpowiednie normy i wytyczne w tym zakresie obejmują:

- IEC 62443-4-1: Wymaga integracji zabezpieczeń w cyklu życia oprogramowania;
- ISO/IEC 27034: Bezpieczeństwo aplikacji w cyklu życia oprogramowania;
- NIST SP 800-218 SSDF;
- ENISA Secure Software Development Good Practices.

2.2. Security by Default – bezpieczeństwo bez konfiguracji przez użytkownika

„Security by default" oznacza, że produkty są dostarczane z najbezpieczniejszą konfiguracją jako standardem. Użytkownik nie powinien musieć zgadywać, czy zabezpieczenia są włączone. Bezpieczeństwo jest podstawą, a nie opcjonalnym „zaawansowanym ustawieniem".

Przykłady bezpiecznych ustawień domyślnych:

- Brak domyślnych ustawień współdzielonych, wymuszanie konfiguracji poświadczeń przy pierwszym uruchomieniu lub parowanie bez hasła z bezpiecznymi czynnikami;
- Otwarte tylko niezbędne porty sieciowe (zasada minimalnej ekspozycji);
- Aktualizacje oprogramowania sprzętowego podpisane i zweryfikowane domyślnie;
- Domyślnie włączone rejestrowanie i ścieżka audytu dla funkcji krytycznych.

Odpowiednie wytyczne w tym zakresie obejmują:

- OWASP Secure Configuration: Najlepsze praktyki dotyczące bezpiecznych ustawień domyślnych;
- NIST SP 800-128: Przewodnik po zarządzaniu konfiguracją zorientowanym na bezpieczeństwo.

2.3. Praktyki bezpiecznego kodowania

CRA wymaga, aby tworzenie oprogramowania odbywało się zgodnie ze sprawdzonymi praktykami bezpiecznego programowania i przy ciągłym zwracaniu uwagi na zagrożenia. Oznacza to między innymi:

Bezpieczne kodowanie:

- Weryfikacja danych wejściowych (pod kątem ataków typu SQL injection, przepełnienia bufora itp.);
- Korzystanie z bezpiecznych bibliotek i szyfrowania;
- Testowanie metodą fuzz i statyczna analiza kodu.

Modelowanie zagrożeń:

W przypadku każdego komponentu oprogramowania należy ocenić:

- Kto mógłby zaatakować ten element?
- W jaki sposób mógłby to zrobić?
- Jakie byłyby tego skutki?

Ramy takie jak STRIDE (Microsoft), OWASP Threat Dragon i MITRE ATT&CK mogą pomóc w systematycznej identyfikacji luk w zabezpieczeniach i ścieżek ataku.

Odpowiednie normy i wytyczne w tym zakresie obejmują:

- Lista kontrolna bezpiecznych praktyk kodowania OWASP;
- ISO/IEC 27001 załącznik A.14: Wymagania bezpieczeństwa w zakresie rozwoju;
- Wytyczne ENISA dotyczące modelowania zagrożeń (2022);
- BSI TR-03161 (Niemcy): Tworzenie bezpiecznego oprogramowania.

2.4. Konkretne informacje dla producentów

Podsumowując, organizacja, która chce opracować PDE zgodne z CRA, powinna:

- Przyjąć bezpieczny cykl życia oprogramowania (SSDLC), zgodnie z opisem w normie IEC 62443-4-1 lub NIST SP 800-218 SSDF;
- Posiadać politykę przeglądu kodu i testowania, która koncentruje się na lukach w zabezpieczeniach (SAST, DAST, fuzzing);
- Systematycznie stosować modelowanie zagrożeń do każdego ważnego komponentu;
- Dostarczać produkty ze standardowymi zamkniętymi portami, włączonym rejestrowaniem i bezpiecznymi portami dostępowymi;

- Wdrożyć funkcję PSIRT z jasno określonymi rolami i procesami dyżurnymi;
- Zdefiniować bramki jakości bezpieczeństwa w CI/CD (SAST, DAST, SCA, skanowanie tajemnic) z polityką odrzucania kompilacji.

3. Zarządzanie bezpieczeństwem w cyklu życia produktu

Oprócz bezpiecznego projektowania, rozwoju i produkcji PDE, produkt musi również pozostawać bezpieczny przez cały cykl życia. Produkty cyfrowe ewoluują — podobnie jak ich bezpieczeństwo. Oznacza to, że bezpieczeństwo musi być stale zarządzane i brane pod uwagę również po wprowadzeniu PDE na rynek.

W praktyce oznacza to, że producenci są zobowiązani do zarządzania cyklem życia produktu w następujący sposób [14]:

1. Ciągłe monitorowanie podatności;
2. Dostarczanie aktualnych aktualizacji zabezpieczeń i poprawek;
3. Utrzymywanie polityki ujawniania luk w zabezpieczeniach oraz informowanie w przejrzysty sposób użytkowników i organów nadzorczych o ryzyku.

3.1. Ciągłe monitorowanie podatności i luk w zabezpieczeniach

Po wprowadzeniu produktu na rynek producenci muszą aktywnie i systematycznie kontynuować wykrywanie luk w zabezpieczeniach. Obejmuje to:

- Monitorowanie baz danych luk w zabezpieczeniach, takich jak europejska baza danych luk w zabezpieczeniach[15] ;
- Śledzenie komunikatów oddostawców;
- Śledzenie typowych luk w zabezpieczeniach i zagrożeń (CVE) związanych z używanymi komponentami lub bibliotekami;
- Wykorzystanie SBOM do identyfikacji i śledzenia zależności;
- Wewnętrzne monitorowanie nowych luk w zabezpieczeniach poprzez programy bug bounty, testy penetracyjne lub audyty bezpieczeństwa.

[14] Chociaż wymagania dotyczące postępowania w przypadku podatności są szczegółowo omówione w załączniku I część II, wynikają one z pkt 1 i 2 załącznika I część I i dlatego zostały już poruszone w niniejszych wytycznych.

[15] Art. 17 ust. 5 CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Przykład:

Producent kamer sieciowych korzysta z modułów oprogramowania sprzętowego typu open source. Baza danych CVE ujawnia, że jeden z tych modułów zawiera krytyczną lukę (np. CVE-2023-XXXXX). Producent ma obowiązek monitorować i oceniać te informacje oraz, w razie potrzeby, podejmować odpowiednie działania.

Istotne źródła w tym zakresie obejmują:

- CVE;
- EPSS (system oceny prawdopodobieństwa wykorzystania luki);
- Wytyczne ENISA dotyczące zarządzania lukami w zabezpieczeniach;
- ISO/IEC 30111: Procesy postępowania z lukami w zabezpieczeniach.

3.2. Aktualizacje zabezpieczeń i poprawki w odpowiednim czasie

CRA wymaga od producentów szybkiego reagowania na znane luki w zabezpieczeniach oraz bezpłatnego i skutecznego dystrybuowania aktualizacji zabezpieczeń przez cały okres wsparcia technicznego.

Aktualizacje te muszą:

- Być podpisane cyfrowo i zweryfikowane;
- Posiadać niezawodny mechanizm przywracania poprzedniej wersji;
- Być instalowane automatycznie z opcją rezygnacji i/lub przy minimalnej interakcji użytkownika;
- Być dostępne przez co najmniej 10 lat od daty wydania lub przez pozostałą część okresu wsparcia (w zależności od tego, który z tych okresów jest dłuższy).

Przykład:

Producent inteligentnych termostatów odkrywa lukę w zabezpieczeniach stosu Wi-Fi. W ciągu dwóch tygodni opracowuje się poprawkę bezpieczeństwa, testuje ją i dystrybuuje za pośrednictwem podpisanej aktualizacji OTA. Użytkownicy otrzymują wyraźne powiadomienie, a aktualizacja jest instalowana automatycznie po ponownym uruchomieniu urządzenia.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Istotne źródła w tym zakresie obejmują:

- ISO/IEC 29147: Skoordynowane ujawnianie luk w zabezpieczeniach;
- NIST SP 800-40: Przewodnik po zarządzaniu poprawkami w przedsiębiorstwie;
- ETSI EN 303 645: Podstawowe wymagania bezpieczeństwa dla konsumenckich urządzeń IoT (w tym mechanizmy aktualizacji oprogramowania).

3.3. Zgłaszanie luk w zabezpieczeniach i polityka przejrzystej komunikacji

Przejrzystość ma zasadnicze znaczenie. CRA wymaga od producentów:

- Opublikowania polityki CVD;
- Zapewnienia punktu kontaktowego (np. security@company.eu) do zgłaszania luk;
- Szybkiego informowania użytkowników i organów takich jak ENISA lub krajowy organ nadzorczy w przypadku poważnych zagrożeń;
- Przejrzystego informowania o dostępnych poprawkach, środkach zaradczych i pozostałych zagrożeniach.

Przykład:

Haker etyczny zgłasza krytyczną lukę w zabezpieczeniach podłączonego systemu alarmowego za pośrednictwem publicznej platformy CVD producenta. W ciągu 72 godzin potwierdzono otrzymanie zgłoszenia, a po przeprowadzeniu wewnętrznej analizy poinformowano ENISA za pośrednictwem jednolitej platformy zgłaszania ENISA (krajowe punkty końcowe). W ciągu trzech tygodni wprowadzono poprawkę, a wszyscy użytkownicy zostali powiadomieni o ryzyku i rozwiązaniu za pośrednictwem wiadomości e-mail i powiadomień w aplikacji.

Istotne źródła w tym zakresie obejmują:

- Model dojrzałości koordynacji luk w zabezpieczeniach (VCMM) FIRST;
- ISO/IEC 29147: Wytyczne dotyczące ujawniania luk w zabezpieczeniach;
- Wytyczne ENISA dotyczące skoordynowanego ujawniania luk w zabezpieczeniach (2022);
- OpenSSF VEX (Vulnerability Exploitability eXchange).

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4. Bezpieczeństwo łańcucha dostaw

CRA uznaje, że produkt nigdy nie jest całkowicie „niezależny": składa się z dziesiątek, a czasem setek komponentów pochodzących od zewnętrznych dostawców, projektów open source i partnerów sprzętowych. Dlatego CRA ustanawia wyraźne wymagania dotyczące zarządzania ryzykiem cyberbezpieczeństwa w łańcuchu dostaw.

W praktyce producenci muszą:

1. Utrzymywać aktualny i przejrzysty przegląd komponentów oprogramowania wykorzystywanych za pośrednictwem SBOM;
2. Wymagać od dostawców zgodności z zabezpieczeniami zgodnymi z CRA;
3. Aktywnie monitorować i zarządzać ryzykiem związanym z oprogramowaniem open source i zależnościami zewnętrznymi.

4.1. Lista komponentów oprogramowania (SBOM)

SBOM jest podobny do listy składników oprogramowania: zawiera przegląd wszystkich komponentów, wersji i źródeł wykorzystanych elementów oprogramowania, w tym bibliotek open source.

CRA wymaga od producentów prowadzenia SBOM i możliwości przedłożenia go organom regulacyjnym i władzom na żądanie. Publikacja SBOM dla użytkowników jest opcjonalna[16] . SBOM stanowi podstawę dla:

- Analizy podatności (np. poprzez śledzenie CVE);
- oceny skutków w przypadku luk typu zero-day;
- audytów łańcucha dostaw.

Przykład:

Producent inteligentnych routerów sporządza wykaz SBOM, w którym wyraźnie stwierdza, że produkt wykorzystuje:

- OpenSSL 1.1.1n;
- BusyBox 1.35.0;
- Zmodyfikowaną wersję modułu zapory sieciowej typu open source.

[16] Jeśli są one udostępniane użytkownikom, należy wyjaśnić, gdzie i w jaki sposób użytkownicy mogą uzyskać do nich dostęp.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

W przypadku ujawnienia luki w zabezpieczeniach OpenSSL (CVE-2022-XXXX) producent może natychmiast sprawdzić, czy ma ona wpływ na produkt, i odpowiednio zareagować.

Istotne źródła w tym zakresie obejmują:

- CycloneDX, SPDX: formaty SBOM (zalecane również przez ENISA i NTIA);
- ISO/IEC 5230 (OpenChain): zgodność oprogramowania w łańcuchu dostaw;
- Narzędzia OpenSSF do generowania SBOM i wykrywania luk w zabezpieczeniach.

4.2. Wymagania bezpieczeństwa dla dostawców

CRA wymaga również od producentów zapewnienia, że ich dostawcy i zewnętrzni programiści przestrzegają wymagań bezpieczeństwa porównywalnych z wymaganiami ich własnego zespołu. Odpowiedzialności nie można przenosić na innych; luki w zabezpieczeniach komponentów stron trzecich mogą również prowadzić do obowiązków związanych z przestrzeganiem CRA.

W praktyce oznacza to:

- Włączenie klauzul dotyczących cyberbezpieczeństwa do umów z dostawcami;
- Przeprowadzanie analizy due diligence w zakresie bezpieczeństwa przy wyborze dostawców oprogramowania;
- Okresowe sprawdzanie, czy partnerzy przestrzegają np.
    - ISO/IEC 27001 (bezpieczeństwo informacji);
    - IEC 62443-4-1 (bezpieczne opracowywanie produktów);
    - modele dojrzałości OWASP SAMM lub BSIMM.
- Umowne prawa do audytu i minimalne poziomy zapewnienia (np. certyfikacja zgodności) dla krytycznych komponentów;
- Powiadomienie w ciągu 24 godzin o wykrytych przez dostawcę krytycznych lukach w zabezpieczeniach mających wpływ na Państwa PDE.

Przykład:

Producent medycznych urządzeń IoT współpracuje z dostawcą oprogramowania w Azji. Umowa stanowi, że dostawca ten:

- Opracowuje oprogramowanie w sposób bezpieczny, zgodnie z normą IEC 62443-4-1;
- Dokumentuje wszystkie wykorzystywane komponenty open source;
- Utrzymuje politykę dotyczącą luk w zabezpieczeniach, obejmującą obowiązkowe zgłaszanie w ciągu 24 godzin.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4.3. Zarządzanie ryzykiem związanym z bibliotekami zewnętrznymi i open source

Oprogramowanie open source ma wiele zalet, ale wiąże się też z pewnymi zagrożeniami: lukami w zabezpieczeniach, brakującymi aktualizacjami, niejasnymi licencjami lub zawodnymi administratorami. CRA wymaga od producentów aktywnego zarządzania tymi zagrożeniami i monitorowania ich.

Najlepsze praktyki obejmują:

- Korzystanie ze skanerów zależności (np. OWASP Dependency-Check, Snyk, Trivy);
- Automatyczne alerty o lukach w zabezpieczeniach (np. za pośrednictwem GitHub Advisories);
- Korzystanie wyłącznie z utrzymywanych i dojrzałych projektów open source;
- Zastosowanie zabezpieczenia w procesach CI/CD (blokując kompilacje ze znanymi lukami CVE);
- Użycie VEX, aby zmniejszyć zakłócenia spowodowane niewykorzystywanymi lukami CVE;
- Wymaganie minimalnej responsywności opiekuna podczas wybierania OSS.

Przykład:

Producent używa popularnej biblioteki JavaScript (np. Log4j) w interfejsie internetowym. Po wykryciu Log4Shell (CVE-2021-44228) producent dokładnie wie, które wersje są zagrożone dzięki analizie SBOM i może podzielić na segmenty i załatać zagrożone produkty.

Istotne źródła w tym zakresie obejmują:

- NIST SSDF (Secure Software Development Framework);
- Wytyczne ENISA dotyczące bezpieczeństwa OSS;
- Karta wyników OpenSSF: obiektywna ocena jakości projektów open source.

Wnioski

Niniejsze wytyczne stanowią pierwsze **techniczne przełożenie wymagań zawartych w załączniku I część I CRA na praktyczne sugestie i zalecenia**. Podkreślają one **cztery elementy**, które mają kluczowe znaczenie dla zapewnienia zgodności z CRA: (1) podejście do cyberbezpieczeństwa oparte na ryzyku, które obejmuje ocenę ryzyka, dostosowane środki bezpieczeństwa oraz uwzględnienie modeli zagrożeń, powierzchni ataku i skutków; (2) zasadę bezpieczeństwa od samego początku i domyślnego stosowania zasad bezpieczeństwa; (3) obowiązki w zakresie zarządzania bezpieczeństwem w całym cyklu życia PDE; (4) kwestie związane z łańcuchem dostaw i kontrole. Dla każdego elementu przedstawiono **praktyczne sugestie** dotyczące sposobu wdrażania i wypełniania tych obowiązków w oparciu o uznane najlepsze praktyki i standardy. Mogą one jednak ulec zmianie w zależności od wyników bieżących dyskusji dotyczących standardów i dalszych zmian regulacyjnych. Jako kolejne kroki dla MŚP zaleca się zapoznanie się z dodatkowymi wytycznymi w **repozytorium** SECURE, takimi jak **CRA Methodological Compliance Assessment Framework** (Metodologiczne ramy oceny zgodności CRA), zawierające szczegółowy zestaw narzędzi i listę kontrolną dotyczącą zgodności z CRA wykraczającą poza załącznik I, a także **CRA 101: Understanding CRA Obligations (CRA 101: Zrozumienie obowiązków CRA**), zawierające przyjazny dla początkujących skrócony przegląd obowiązków prawnych wynikających z CRA.