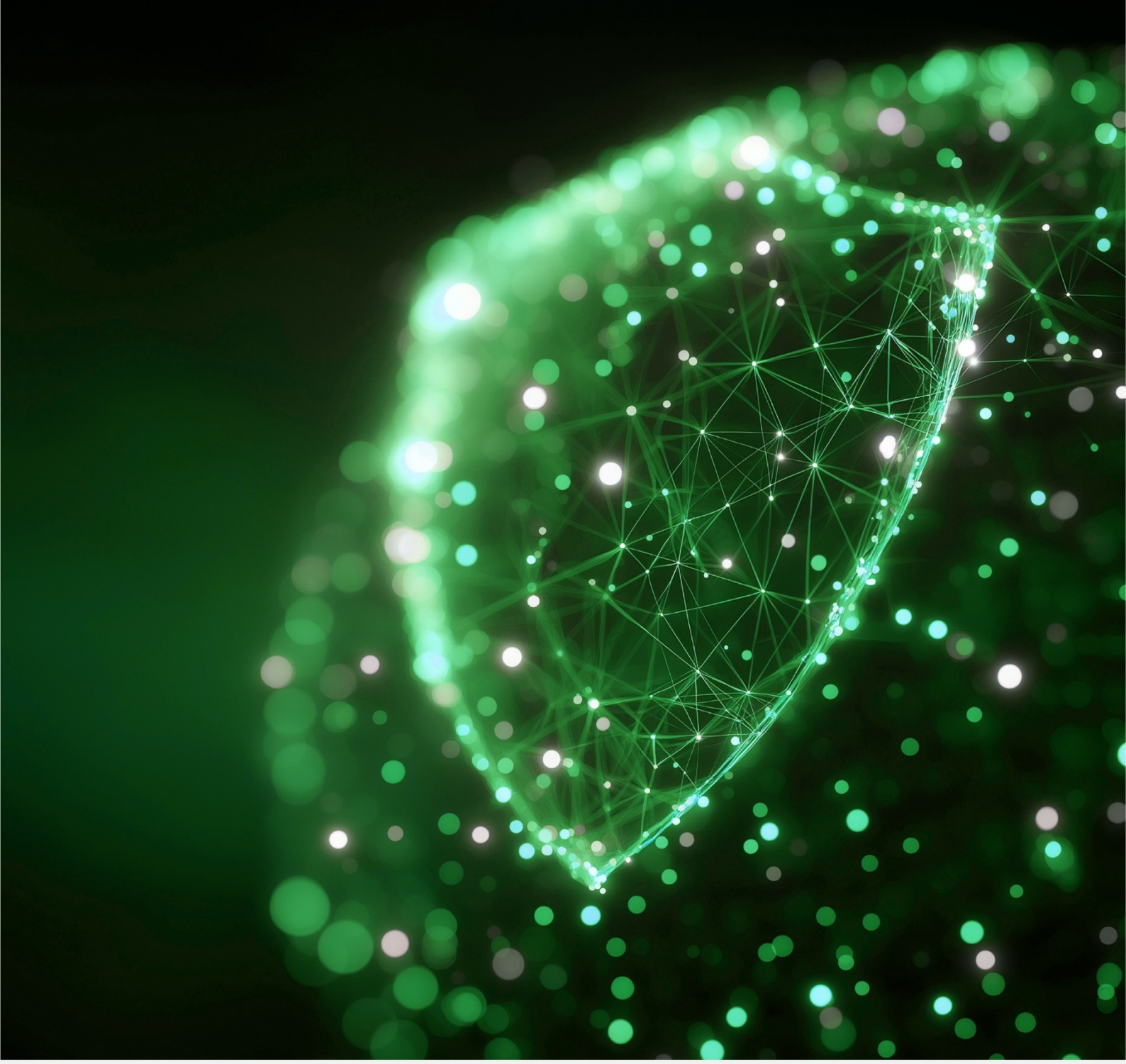

Dobre praktyki zarządzania bezpieczeństwem oprogramowania

Poradnik dla producentów w kontekście Cyber Resilience Act

CERT.PL
NASK

Dobre praktyki zarządzania bezpieczeństwem oprogramowania

Poradnik dla producentów w kontekście Cyber Resilience Act

TLP: CLEAR

NASK-PIB

Wersja 1.0

Warszawa, maj 2026

Wytworzone w CSIRT NASK w ramach dotacji KSC udzielonej przez Ministerstwo Cyfryzacji.

PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

Wprowadzenie

Niniejszy poradnik został przygotowany w celu wsparcia producentów oprogramowania i produktów z elementami cyfrowymi w budowaniu oraz doskonaleniu praktyk zarządzania bezpieczeństwem. Ma on charakter rekomendacyjny i koncentruje się na rozwiązaniach organizacyjnych oraz technicznych, które pomagają w spełnieniu wymagań rozporządzenia CRA oraz w zwiększeniu poziomu ochrony użytkowników.

Poradnik nie stanowi interpretacji prawnej przepisów CRA. Jego celem jest wskazanie dobrych praktyk i wsparcie producentów w ich wdrożeniu.

Zarządzanie bezpieczeństwem oprogramowania w cyklu życia produktu

Skuteczne zarządzanie bezpieczeństwem oprogramowania wymaga podejścia obejmującego cały cykl życia produktu – od projektowania, przez wytwarzanie i utrzymanie, aż po jego wycofanie z rynku. CRA kładzie nacisk na to, aby bezpieczeństwo nie było dodatkiem, lecz integralną częścią procesu tworzenia produktu. Oznacza to, że producent powinien uwzględniać zagrożenia już na etapie projektowania, stosując podejście "security by design": planując mechanizmy uwierzytelniania, szyfrowanie danych, podział uprawnień, ochronę danych wrażliwych, zanim powstanie jeszcze pierwsza linia kodu.

Kluczowym wprowadzanym w CRA obowiązkiem jest przeprowadzanie regularnej oceny ryzyka w kontekście cyberbezpieczeństwa dla produktu oraz aktualizowanie jej przy każdej istotnej zmianie funkcjonalnej, architektonicznej lub środowiskowej. Wyniki oceny ryzyka powinny wpływać bezpośrednio na decyzje projektowe, priorytety rozwojowe oraz sposób reagowania na zgłaszane podatności.

Obowiązkową dobrą praktyką jest również jednoznaczna identyfikacja produktu i jego wersji. Służy to precyzyjnemu określeniu, które wersje produktu są objęte wsparciem oraz identyfikacją komponentów, których dotyczą potencjalne podatności. Nowym wymaganiem CRA wspierającym ten proces jest stosowanie i utrzymywanie aktualnego wykazu komponentów oprogramowania (ang. Software Bill of Materials, SBOM), który umożliwia identyfikację wszystkich bibliotek, zależności oraz innych elementów składowych produktu. Posiadanie aktualnego SBOM pozwala szybko ocenić wpływ nowo ujawnionej podatności na produkt, przyspieszyć analizę ryzyka i skuteczniej planować działania naprawcze.

Po wdrożeniu produktu zarządzanie bezpieczeństwem nie kończy się, a przechodzi w fazę ciągłego utrzymania. Zalecamy systematyczne śledzenie informacji o podatnościach w wykorzystywanych komponentach, zarówno własnych, jak i pochodzących od zewnętrznych dostawców. Powinno to obejmować monitorowanie publicznych baz podatności oraz komunikatów bezpieczeństwa ich producentów. Polecamy subskrypcję publikowanych przez nas komunikatów dla administratorów [1] w usłudze moje.cert.pl. Śledzenie podatności warto uzupełnić o regularne testy bezpieczeństwa, analizę logów orz terminowe instalowanie poprawek - pozwoli to na szybszą reakcję i ograniczenie ryzyka dla użytkowników.

Za zarządzanie bezpieczeństwem produktu powinna odpowiadać jasno określona rola lub zespół. Nawet w niewielkich organizacjach warto formalnie wskazać osobę odpowiedzialną za odbiór zgłoszeń, ocenę ryzyka i koordynację działań naprawczych.

Rekomendowany proces obsługi podatności

CRA wymaga, aby producent reagował na informacje o podatnościach w sposób bezzwłoczny. W praktyce oznacza to konieczność posiadania uporządkowanego procesu obsługi podatności.

Producent powinien jasno komunikować, w jaki sposób przyjmuje zgłoszenia oraz jakie informacje są niezbędne do ich analizy. Dobrą praktyką jest zapewnienie publicznie dostępnego kanału zgłaszania podatności, np. dedykowanego adresu e-mail lub formularza kontaktowego. Rekomendujemy także opublikowanie pliku security.txt (RFC 9116) zgodnie z obowiązującą specyfikacją, który w ustandaryzowany sposób wskazuje, jak i gdzie zgłaszać podatności. Ułatwia to badaczom oraz użytkownikom szybkie i jednoznaczne dotarcie do właściwego kanału kontaktu oraz wspiera sprawną obsługę zgłoszeń.

Po otrzymaniu zgłoszenia podatność powinna zostać zweryfikowana i oceniona pod kątem wpływu na bezpieczeństwo produktu oraz użytkowników. Na tym etapie istotne jest ustalenie, czy podatność jest możliwa do wykorzystania w praktyce oraz czy istnieją przesłanki wskazujące na jej aktywne wykorzystywanie.

W przypadku podatności o istotnym wpływie na bezpieczeństwo produktów zachęcamy do współpracy z zespołem CERT Polska, czyli CSIRT-em wyznaczonym do koordynowania procesu ujawniania podatności. Współpraca ta może obejmować uzgodnienie sposobu dalszego postępowania, harmonogramu działań naprawczych

[1] https://moje.cert.pl/komunikaty/?categories=2

oraz momentu upublicznienia informacji o podatności, co sprzyja ograniczeniu ryzyka dla użytkowników.

Kolejnym krokiem jest opracowanie poprawki lub rozwiązania tymczasowego mitygującego zagrożenie. Poprawki bezpieczeństwa powinny być testowane i udostępniane w możliwie najkrótszym czasie. Producent nie powinien udostępniać wersji produktu z nowymi funkcjami, jeśli posiada wiedzę o istniejącej i nierozwiązanej podatności mającej wpływ na bezpieczeństwo tej wersji.

Rekomendowanym przez nas sposobem komunikowania informacji o podatnościach jest przypisanie identyfikatora i publikacja wpisu CVE. Uzyskanie wpisu CVE jednoznacznie identyfikuje podatność, ułatwia wymianę informacji pomiędzy producentami, użytkownikami i zespołami reagowania na incydenty oraz wspiera automatyzację procesów zarządzania podatnościami. Rezerwować numery CVE mogą organizacje mające status CNA (CVE Numbering Authority) w Programie CVE. Zespół CERT Polska od 2023 r. posiada status CNA i regularnie publikuje zgłaszane podatności na stronie cert.pl/cve/. W celu publikacji wpisu CVE zachęcamy do kontaktu z naszym zespołem. Więcej informacji o tym procesie znajduje się na stronie cert.pl/cvd/.

Producenci, którzy regularnie obsługują podatności w swoich produktach, mogą rozważyć samodzielne uzyskanie statusu CNA w Programie CVE. Pozwala to na samodzielne nadawanie identyfikatorów i publikowanie wpisów CVE dla podatności w swoich produktach oraz usprawnia komunikację ze społecznością etycznych badaczy bezpieczeństwa. Stosowanie identyfikatorów CVE zwiększa przejrzystość i spójność komunikacji o bezpieczeństwie.

Cały proces obsługi podatności, w tym terminy reakcji i podjęte działania, powinien być dokumentowany. Ułatwia to zarówno zarządzanie ryzykiem, jak i wykazanie należytej staranności.

Zgłaszanie incydentów i podatności

CRA nakłada na producentów obowiązek zgłaszania aktywnie wykorzystywanych podatności oraz poważnych incydentów mających wpływ na bezpieczeństwo produktu z elementami cyfrowymi. Zgłoszenia te są składane za pośrednictwem Single Reporting Platform zarządzanej przez ENISA.

Dobrą praktyką jest posiadanie wewnętrznej procedury umożliwiającej szybkie rozpoznanie zdarzeń, które powinny podlegać zgłoszeniu. Źródło informacji

o incydencie nie ma znaczenia – może to być własna obserwacja, zgłoszenie użytkownika lub informacja od niezależnego badacza.

Producent powinien przygotować się do zgłoszenia poprzez zgromadzenie podstawowych informacji, takich jak identyfikacja produktu i wersji, opis wpływu zdarzenia na bezpieczeństwo oraz podjęte lub planowane działania naprawcze. Wczesna i rzetelna komunikacja sprzyja skutecznemu zarządzaniu incydentem.

Aktualizacje zabezpieczeń i komunikacja z użytkownikami

Jednym z kluczowych elementów ochrony użytkowników jest skuteczny mechanizm dostarczania poprawek bezpieczeństwa. Producent powinien zapewnić możliwość eliminowania podatności poprzez aktualizacje, w tym domyślnie poprzez automatyczne instalowanie poprawek.

Użytkownicy powinni być informowani o dostępnych aktualizacjach bezpieczeństwa w jasny sposób oraz mieć możliwość czasowego odroczenia aktualizacji lub rezygnacji z mechanizmu automatycznego. Jeżeli jest to technicznie wykonalne, aktualizacje bezpieczeństwa powinny być dostarczane oddzielnie od zmian funkcjonalnych. Ma to na celu zwiększenie przejrzystości postępowania w przypadku wykrycia podatności oraz niezobowiązywanie użytkowników do instalowania nowych funkcji tylko po to, aby uzyskać najnowsze aktualizacje zabezpieczeń.

CRA wprowadza minimalny okres wsparcia produktu, który co do zasady wynosi co najmniej pięć lat, chyba że przewidywany czas użytkowania produktu jest krótszy.

Dokumentacja i przygotowanie organizacyjne

Producent ma obowiązek prowadzić dokumentację techniczną produktu, obejmującą m.in. opis architektury, mechanizmów bezpieczeństwa, wykaz zastosowanych komponentów oraz rejestr usuwanych podatności i odnotowanych incydentów. Dokumentacja ta nie musi być publikowana przez producenta, ale musi zostać udostępniona na żądanie właściwemu organowi nadzoru rynku.

W praktyce pomocne jest także dokumentowanie decyzji dotyczących akceptacji ryzyka, terminów reakcji i wdrażanych poprawek. Takie podejście porządkuje procesy wewnętrzne i ułatwia reagowanie w sytuacjach kryzysowych.

Dokumentacja powinna powstawać naturalnie, w toku procesu wytwórczego, a nie jako jednorazowy dokument tworzony przed audytem. Narzędzia klasy ALM, takie jak GitLab czy Jira z Confluence, pozwalają połączyć zarządzanie zmianami

i dokumentację w jednym ekosystemie, każda decyzja architektoniczna jest powiązana z konkretnym zadaniem i tworzy audytowalną historię produktu. Wykaz komponentów wymagany przez CRA można generować automatycznie przy każdym buildzie za pomocą narzędzi obsługujących format SBOM, co eliminuje ryzyko nieaktualnej dokumentacji.

Szczegółowe wytyczne dotyczące zawartości i struktury SBOM zawiera przewodnik OWASP CycloneDX: *Authoritative Guide to SBOM*, dostępny pod adresem: https://cyclonedx.org/guides/OWASP_CycloneDX-Authoritative-Guide-to-SBOM-en.pdf

CRA jako element podnoszenia jakości produktów

Cyber Resilience Act wprowadza nowe obowiązki regulacyjne, ale jednocześnie stwarza producentom możliwość uporządkowania i wzmocnienia praktyk zarządzania bezpieczeństwem. Dobrze wdrożone procesy obsługi podatności, aktualizacji i zgłaszania incydentów przyczyniają się do ograniczenia skutków incydentów, zwiększenia zaufania użytkowników oraz podniesienia jakości produktów dostępnych na rynku. Zachęcamy producentów do traktowania wymagań CRA jako elementu długofalowej strategii bezpieczeństwa, a nie wyłącznie obowiązku formalnego.