

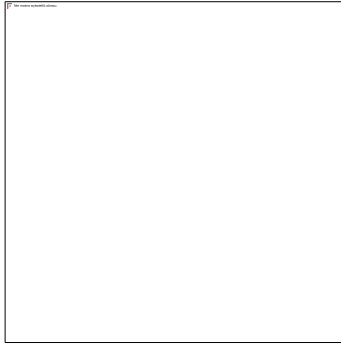


KSC i certyfikacja cyberbezpieczeństwa – od regulacji do zamówień publicznych

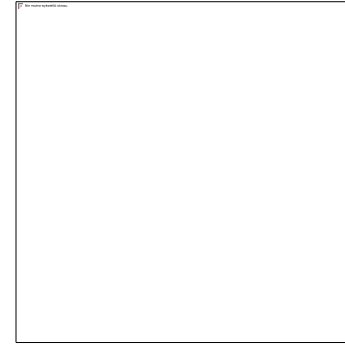
13.10.2026 r.

Łukasz Wojtachnio

KSC a Certyfikacja cyberbezpieczeństwa



KSC dotyczy podmiotów oraz wymogów w
zakresie systemu zarządzania bezpieczeństwem
informacji



Certyfikacja – dostarcza bezpieczne produkty

KSC

Nowelizacja wdrażająca NIS2 weszła w życie 03.04.2026 (Dz. U. poz. 252)

- **Główne zmiany:**

- szerszy zakres podmiotowy: podmioty kluczowe i ważne
- wdrożenie SZBI
- sektorowe zespoły CSIRT
- sprawniejsze zgłaszanie incydentów
- możliwość identyfikacji dostawców wysokiego ryzyka



SZBI

- ❑ **Podmiot ksc wdraża SZBI zapewniający (art. 8):**
- ❑ prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
- ❑ wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, w szczególności:
- ❑ bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego,
- ❑ bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi, z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym,
- ❑ wdrażanie i utrzymywanie planów ciągłości działania umożliwiających ciągle i niezakłócone świadczenie usługi



Bezpieczeństwo łańcucha dostaw

Wdrażając środki w zakresie bezpieczeństwa łańcucha dostaw należy uwzględnić:

podatności związane z dostawcą
sprzętu lub oprogramowania

ogólną jakość produktów ICT
pochodzących od dostawcy

wyniki postępowania ws HRV

Rekomendacje Pełnomocnika ds. Cyberbezpieczeństwa

	Art. 33	Art. 67a
Cel	Ograniczenie zagrożeń związanych z konkretnym sprzętem lub oprogramowaniem	Podniesienie poziomu bezpieczeństwa systemów informacyjnych
Przedmiot	Stosowanie określonych urządzeń lub programów	Środki techniczne i organizacyjne
Przesłanki	Wykrycie podatności mogącej zagrozić bezpieczeństwu; zagrożenie uprawdopodobniające możliwość incydentu krytycznego	Potrzeba zwiększenia poziomu cyberbezpieczeństwa
Procedura	Zasadniczo badanie przez właściwy CSIRT, wniosek i opinia Kolegium; w trybie ust. 4a możliwe działanie z urzędu po konsultacji z CSIRT	Pełnomocnik może zasięgnąć opinii Kolegium, ale nie jest to obowiązkowe
Charakter prawny	ich nieuwzględnienie może zostać zgłoszone organowi nadzorującemu podstawa odrzucenia oferty art. 226 pzp	Ustawa wprost stanowi, że ich stosowanie jest dobrowolne

HRV

- ❑ Dostawca wysokiego ryzyka (HRV) to dostawca, którego określone produkty, usługi lub procesy ICT – po przeprowadzeniu ustawowej procedury – mogą zostać uznane za stwarzające ryzyko dla bezpieczeństwa państwa lub porządku publicznego.
- ❑ Uznanie za dostawcę wysokiego ryzyka następuje wyłącznie w drodze postępowania administracyjnego prowadzonego przez ministra cyfryzacji.
- ❑ Decyzja o uznaniu dostawcy za wysokiego ryzyka nie oznacza wykluczenia firmy z rynku. Obejmuje wyłącznie wskazane w decyzji typy produktów, rodzaje usług ICT lub konkretne procesy ICT. Co do zasady nie dotyczy całej działalności danego dostawcy.
- ❑ Brak listy dostawców wysokiego ryzyka nie zwalnia podmiotów z obowiązku oceny ryzyka przy zakupie produktów, usług i procesów ICT. Warto weryfikować, czy pochodzą one od zaufanych dostawców i spełniają wymagania bezpieczeństwa.

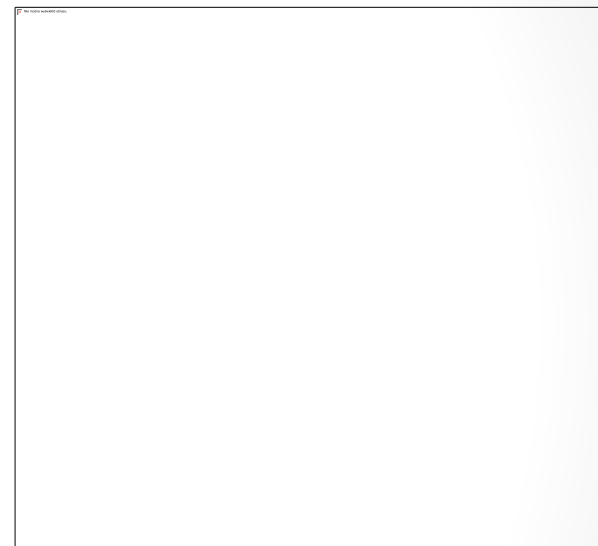


HRV

Procedura HRV ma bezpośrednie znaczenie dla zarządzania ryzykiem dostawców.

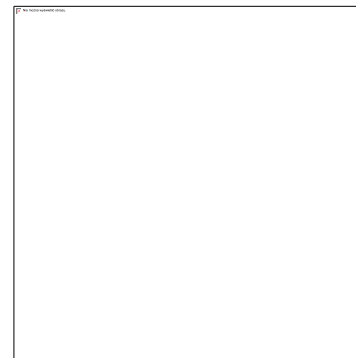
Organizacje powinny w szczególności:

- ☐ prowadzić ewidencję wykorzystywanego sprzętu i oprogramowania ICT;
- ☐ analizować pochodzenie i wiarygodność dostawców;
- ☐ uwzględniać ryzyko dostawcy przy zakupach i zamówieniach publicznych;
- ☐ monitorować decyzje i rekomendacje organów odpowiedzialnych za cyberbezpieczeństwo.



Certyfikacja

© 2010 UZP. Wszelkie prawa zastrzeżone.



procedura formalnego potwierdzenia, że przedmiot certyfikacji
spełnia wymogi przewidziane w odpowiednim programie
lub schemacie certyfikacji cyberbezpieczeństwa.

Pozytywny wynik tej procedury skutkuje wydaniem certyfikatu.

Ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa

Weszła w życie 28 sierpnia 2025 r. – Dz. U. poz. 1017

Służy stosowaniu Aktu o cyberbezpieczeństwie

Podstawowe założenia:

- 10 Certyfikacja cyberbezpieczeństwa jest dobrowolna;
- 10 Obok europejskich programów certyfikacji cyberbezpieczeństwa zostaną wprowadzone krajowe schematy certyfikacji cyberbezpieczeństwa;
- 10 Minister Cyfryzacji jest Krajowym Organem ds. Certyfikacji Cyberbezpieczeństwa
- 10 Certyfikacja będzie prowadzona na podstawie umowy zawieranej z jednostką certyfikującą;

Krajowy system certyfikacji

- ❑ Podmioty krajowego systemu certyfikacji cyberbezpieczeństwa
- ❑ Procedury związane z certyfikacją
- ❑ Wspiera wytwarzanie wysokiej jakości produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa
- ❑ Zapewnia bezpieczeństwo oferowanych produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa



Przedmiot certyfikacji

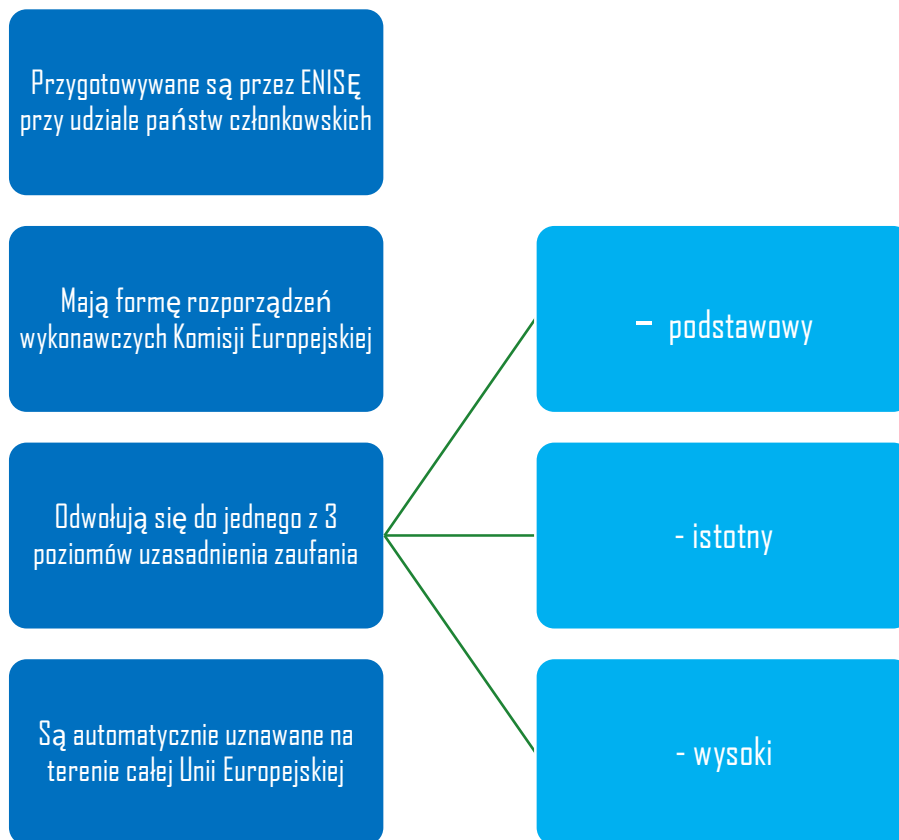
W ramach europejskich programów certyfikacji cyberbezpieczeństwa

- Produkty ICT
- Usługi ICT
- Procesy ICT
- Usługi zarządzane w zakresie bezpieczeństwa

W ramach krajowych schematów certyfikacji cyberbezpieczeństwa

- Produkty ICT
- Usługi ICT
- Procesy ICT
- Usługi zarządzane w zakresie bezpieczeństwa
- Systemy zarządzania cyberbezpieczeństwem
- Osoby

Europejskie programy certyfikacji cyberbezpieczeństwa



Poziomy uzasadnienia zaufania w Europejskich programach certyfikacji cyberbezpieczeństwa

PODSTAWOWY

Podstawowa ochrona przed powszechnie znanymi zagrożeniami

ISTOTNY

Zwiększona odporność na bardziej zaawansowane zagrożenia

WYSOKI

Wysoki poziom bezpieczeństwa przed zaawansowanymi i ukierunkowanymi zagrożeniami

EUCC – pierwszy europejski program certyfikacji cyberbezpieczeństwa

Pierwszy i na razie jedyny obowiązujący europejski program certyfikacji cyberbezpieczeństwa;

Dotyczy produktów ICT, np.: routery, karty inteligentne, chipy kryptograficzne;

Oparty o normę Common Criteria (CC), międzynarodowy standard służący ocenie właściwości bezpieczeństwa produktów i systemów IT;

Certyfikaty CC uznawane są nie tylko w Europie, ale i w szeregu innych państw do których należą USA, Kanada, Japonia czy Malezja

Europejski program certyfikacji usług zarządzanych w zakresie bezpieczeństwa (EUMSS)

Jest w przygotowaniu.
Przewidujemy jego przyjęcie
do końca bieżącego roku

Dotyczy usług takich jak:
zarządzanie incydentami,
audyty cyberbezpieczeństwa
czy testy penetracyjne

Program będzie powiązany z
finansowaniem na poziomie
europejskim

Komisja w lipcu br.
rozpoczęła konsultacje
programu

Krajowe schematy certyfikacji cyberbezpieczeństwa

Przyjmowane na podstawie ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa w drodze rozporządzeń Ministra Cyfryzacji

Certyfikaty krajowe mają promować standardy w obszarach nieobjętych europejskimi programami certyfikacji

Mają wesprzeć konsumentów i administrację przy wyborze rozwiązań zapewniających odpowiedni poziom cyberbezpieczeństwa;

Schematy krajowe

Rozpoczęliśmy prace nad dwoma krajowymi schematami certyfikacji cyberbezpieczeństwa:

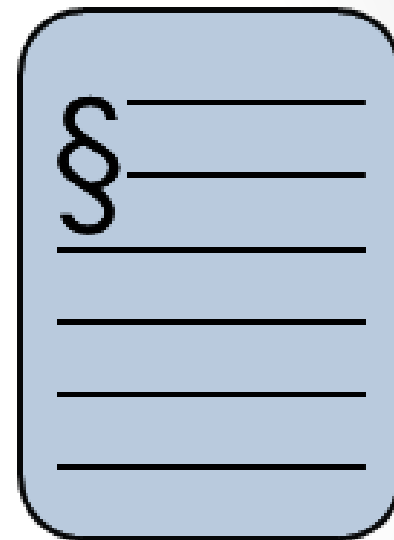
- schematem certyfikacji kompetencji w cyberbezpieczeństwie;
- schematem certyfikacji procesów ICT w zakresie cyberbezpieczeństwa sektora mŚp oraz podmiotów publicznych opartego na dotychczasowym programie „Firma Bezpieczna Cyfrowo” realizowanym przez NASK.



Jesteśmy również otwarci na pomysły w zakresie obszarów gdzie certyfikacja mogłaby przyczynić się do zwiększenia cyberbezpieczeństwa.

CRA

- ❑ CRA to rozporządzenie Unii Europejskiej 2024/2847, ustanawiające wspólne wymagania cyberbezpieczeństwa dla produktów zawierających elementy cyfrowe.
- ❑ Jego głównym celem jest zwiększenie bezpieczeństwa sprzętu i oprogramowania oraz lepsza ochrona użytkowników przed cyberatakami.
- ❑ Obejmuje m.in. urządzenia IoT, inteligentne zegarki, routery, aplikacje i programy komputerowe.
- ❑ Dotyczy przede wszystkim producentów, a także innych podmiotów uczestniczących we wprowadzaniu produktów na rynek UE.



CRA – główne wymagania

Projektowanie i produkcja z uwzględnieniem cyberbezpieczeństwa.

Ograniczanie podatności i zapewnianie aktualizacji bezpieczeństwa.

Reagowanie na wykryte luki oraz informowanie o aktywnie wykorzystywanych podatnościach i poważnych incydentach.

Przeprowadzenie odpowiedniej oceny zgodności i oznakowanie CE, gdy wymagają tego przepisy.

Dziękuję za uwagę



Ministerstwo
Cyfryzacji



NCCA

Krajowy Organ ds. Certyfikacji
Cyberbezpieczeństwa