NASK

Cyber POLICY

Analiza

Akt o cyberbezpieczeństwie – nowy mandat ENISA i certyfikacja cyberbezpieczeństwa

Justyna Balcewicz Rafał Babraj

pod redakcją Magdaleny Wrzosek

Maj 2019

www.cyberpolicy.nask.pl

Wstęp

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie).

Akt o cyberbezpieczeństwie został opublikowany 7 czerwca 2017, ale porozumienie na temat ostatecznego brzmienia regulacji Parlament Europejski i Komisja osiągnęły 10 grudnia 2018. Sam projekt aktu został przedstawiony we wrześniu 2017 roku, jako część tzw. pakietu cyberbezpieczeństwa.

Akt o cyberbezpieczeństwie *(Cybersecurity Act, CA)* to druga po dyrektywie NIS, ogólnoeuropejska regulacja w dziedzinie cyberbezpieczeństwa. CA składa się z dwóch części:

- **nowy permanentny mandat dla ENISA**, której nazwa została zmieniona z Europejskiej Agencji Bezpieczeństwa Sieci i Informacji na Agencja UE ds. Cyberbezpieczeństwa. Rola ENISA została znacznie wzmocniona nie tylko poprzez permanentny mandat, ale także poprzez szereg nowych obowiązków związanych z wejściem w życie Dyrektywy NIS oraz europejskich ram certyfikacji.

- **rozporządzenie tworzące europejskie ramy certyfikacji cyberbezpieczeństwa dla produktów i usług ICT**. Jest to bardzo istotna regulacja, która znacznie zmieni funkcjonujący obecnie model certyfikacji, zdominowany przez SOG-IS *(Senior Official Group Information Security Systems)*.[1]

[1] Porozumienie SOG-IS zostało zawarte w 1997 roku, w odpowiedzi na decyzję Rady UE z marca 1992. Sygnatariusze porozumienia mogą samodzielnie oceniać i certyfikować produkty i usługi sektora IT, zgodnie z międzynarodową normą ISO/IEC 15408, która pozwala zweryfikować bezpieczeństwo systemów teleinformatycznych pod względem formalnym. Polska dołączyła do grupy państw sygnatariuszy porozumienia SOG-IS w 2017 roku.

CZĘŚĆ I:
ENISA (Agencja Unii Europejskiej ds. Cyberbezpieczeństwa

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ang. The European Union Agency for Network and Information Security – ENISA) została założona w 2004 roku. Do jej głównych zadań należy zapewnienie wysokiego poziomu bezpieczeństwa w sieciach i systemach informatycznych w Unii Europejskiej. Główna siedziba ENISA znajduje się w Grecji.
Do tej pory mandat ENISA był czasowy, miał skończyć się w czerwcu 2020 r. Dotychczasowa rola Agencji sprowadzała się głównie do udzielania porad eksperckich i przeprowadzania ćwiczeń. Przepisy, które wprowadza Akt o cyberbezpieczeństwie zapewniają ENISA stały i jasno sprecyzowany mandat, a także większy wpływ na ekosystem cyberbezpieczeństwa UE. Zmieniono także nazwę Agencji, która obecnie brzmi Agencja UE ds. Cyberbezpieczeństwa.

Głównym celem ENISA jest zapewnienie wysokiego poziomu cyberbezpieczeństwa w UE. Agencja wykonuje zadania powierzone jej na mocy przepisów unijnych, działa niezależnie i w taki sposób, aby nie powielać zadań realizowanych przez państwa członkowskie. ENISA utrzymuje własne zasoby, w w tym kompetencje techniczne i kapitał ludzki, niezbędne do wywiązania się z nałożonych na nią obowiązków. Jest organem UE, ma osobowość prawną i w każdym kraju posiada zdolność do czynności prawnych, przyznaną na mocy prawa krajowego, co oznacza, że może nabywać i zbywać mienie ruchome i nieruchome. Może być także stroną w postępowaniu sądowym. Reprezentantem ENISA jest Dyrektor Wykonawczy.

Główne zadania ENISA, to:

- wsparcie dla państw członkowskich, instytucji, organów i jednostek organizacyjnych UE we wdrażaniu europejskiej polityki cyberbezpieczeństwa, a także polityk sektorowych;

- działanie na rzecz budowy zdolności, gotowości i bezpieczeństwa sieci i systemów informacyjnych, rozwijanie potencjału zabezpieczeń przed cyberzagrożeniami i wsparcie kompetencji i umiejętności niezbędnych do zachowania wysokiego poziomu cyberbezpieczeństwa w UE;

- budowa współpracy, a także wymiany informacji na różnych szczeblach: unijnym, pomiędzy państwami członkowskimi, agencjami, odpowiednimi interesariuszami z rynku prywatnego;

- pomoc w budowaniu zdolności państw członkowskich do reagowania na incydenty, zapobieganie przestępstwom w cyberprzestrzeni a w szczególności reagowanie na zdarzenia transgraniczne;

- promowanie certyfikacji w państwach członkowskich, uczestnictwo w ustanawianiu i utrzymaniu ram certyfikacji, koordynacja przejrzystości całego procesu, a także wzmocnienie zaufania do jednolitego rynku cyfrowego i jego konkurencyjności;

- zwiększanie świadomości publicznej i poziomu kompetencji cyfrowych poprzez działania edukacyjne.

Zadania ENISA

Zaangażowanie w rozwój i wdrażanie polityki i prawa UE

ENISA ma realizować to zadanie poprzez udzielanie porad w postaci niezależnych opinii i analiz, opracowywanie wkładu do unijnej polityki i prawa w dziedzinie cyberbezpieczeństwa, polityk sektorowych i projektów prawnych związanych z cyberbezpieczeństwem.

Agencja ma też wspierać państwa członkowskie w tworzeniu narodowych strategii cyberbezpieczeństwa oraz pomagać we wdrożeniu unijnych wytycznych cyberbezpieczeństwa i przepisów prawnych dotyczących ochrony danych i prywatności.

Dodatkowo ENISA uczestniczy w regularnym przeglądzie polityki unijnej i przygotowuje raport, zawierający zgłoszone przez państwa członkowskie incyenty, zidentyfikowane naruszenia bezpieczeństwa, a także powiadomienia o zdarzeniach z Europejskiego Kodeksu Łączności Elektronicznej.

Wspieranie budowy zdolności w zakresie cyberbezpieczeństwa

Nowym zadaniem Agencji jest udzielanie pomocy państwom członkowskim, instytucjom unijnym, agencjom i organizacjom w prewencji, wykrywaniu, analizie i zdolności do odpowiadania na cyberzagrożenia i incydenty. Pomoc ta ma polegać przede wszystkim, na udzieleniu dostępu do niezbędnej wiedzy fachowej. W tym zakresie ENISA w spółpracuje z zespołem CERT-EU[2].

Dodatkowo Agencja może asystować państwom członkowskim (na ich wyraźne życzenie) w tworzeniu narodowych zespołów CSIRT.

ENISA wspiera również CSIRT poziomu krajowego w rozwoju ich kompetencji i wymianie doświadczeń. Przynajmniej raz na dwa lata organizuje także unijne ćwiczenia z cyberbezpieczeństwa (znane powszechnie jako CyberEurope) oraz prowadzi szkolenia dla instytucji publicznych.

Istotne są działania związane z implementacją Dyrektywy NIS, a więc:

- wspieranie grupy współpracy[3] w zakresie identyfikacji operatorów usług kluczowych diałających transgranicznie,
- ułatwianie wymiany informacji pomiędzy sektorami zdefiniowanymi w dyrektywie NIS jako kluczowe,
- opracowywanie dobrych praktyk dla sektorów (wytycznych i wskazówek),
- oferowanie pomocy w rozwiązywaniu problemów regulacyjnych, związanych z dzieleniem się informacjami.

Zaangażowanie ENISA w rozwój i wdrażanie polityki i prawa UE

- Jest zaangażowana w budowanie synergii podmiotów z zespołem CERT-EU, służbami zajmującymi się cyberprzestępczością, organami nadzorującymi ochronę prywatności i danych osobowych;
- Zapewnia sekretariat dla sieci CSIRT,[4] oraz wspiera współpracę między CSIRT krajowymi;
- Oferuje doradztwo w zakresie rozwoju kompetencji CSIRTów;
- Wspiera w ocenie incydentów, analizuje podatności, a także incydenty ex-post;
- Opracowuje, w ścisłej współpracy z państwami członkowskimi, pogłębiony raport techniczny o stanie cyberbezpieczeństwa w UE, z uwzględnieniem zagrożeń i incydentów, które zostały zgłoszone przez państwa członkowskie, sieć CSIRT lub pojedyncze punkty kontaktowe, a także Europejskie Centrum Cyberprzestępczości (EC3) w Europolu;
- Wspiera obsługę incydentów transgranicznych i zagrożeń cyberbezpieczeństwa na dużą skalę: agreguje sprawozdania z państw członkowskich, dba o efektywny przepływ informacji w sieci CSIRT, wspiera komunikację publiczną dotyczącą incydentów, a także testuje procedury reagowania na incydenty transgraniczne na poziomie unijnym.

Działania w obszarze certyfikacji cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT

Nowym zadaniem jest wspieranie i promowanie wdrożenia certyfikacji produktów, usługi procesów ICT poprzez monitorowanie aktualnych standardów i rekomendowanie odpowiednich norm i specyfikacji technicznych zgodnych z europejskimi programami certyfikacji. W procesie europejskiej certyfikacji, to właśnie ENISA przygotuje propozycję programu certyfikacji, który następnie przekazuje do Komisji Europejskiej.

[2] Zespół ds. Reagowania na incydenty komputerowe (CERT-EU) dla instytucji, agencji i organów UE. Zespół składa się z ekspertów ds. Bezpieczeństwa IT z głównych instytucji UE (Komisja Europejska, Sekretariat Generalny Rady, Parlament Europejski, Komitet Regionów, Komitet Ekonomiczno-Społeczny). Ściśle współpracuje z innymi zespołami CERT w państwach członkowskich i poza nimi, a także ze specjalistycznymi firmami zajmującymi się bezpieczeństwem IT.

[3] Grupa współpracy (Cooperation Group) to mechanizm współpracy polityczno-strategicznej, powołany w Dyrektywie NIS. Celem grupy jest wzmacnianie i budowanie współpracy pomiędzy państwami członkowskimi na poziomie strategicznym. W jej skład wchodzą przedstawiciele państw członkowskich, Komisji i ENISA. Jednym z zadań grupy jest wymiana najlepszych praktyk identyfikowania operatorów usług kluczowych (również transgranicznych) przez państwa członkowskie.

[4] W skład sieci CSIRT wchodzą przedstawiciele CSIRT państw członkowskich, CERT-EU i Komisja. Zadaniem sieci jest wzmacnianie współpracy operacyjnej pomiędzy Państwami Członkowskimi. Polskę w sieci CSIRT reprezentuje CERT Polska, znajdujący się w strukturze Państwowego Instytutu Badawczego NASK.

Poza tym ENISA opracowuje i publikuje wytyczne i dobre praktyki w zakresie wymogów cyberbezpieczeństwa produktów, procesów i usług ICT, oraz przyczynia się do budowania zdolności państw członkowskich w zakresie związanym z procesami oceny i certyfikacji, na przykład poprzez wydawanie wytycznych, a także organizację warsztatów czy konferencji.

W ramach działań w obszarze certyfikacji, ENISA, wraz z Komisją, przewodniczy Grupie Interesariuszy Ds. Certyfikacji Cyberbezpieczeństwa, która składa się z uznanych ekspertów reprezentujących wszystkich interesariuszy. Wyboru członków dokonuje KE, na wniosek ENISA, w sposób przejrzysty i transparentny, tak, aby zapewnić równą reprezentację przedstawicieli każdej z grup interesariuszy, także pod względem płci i lokalizacji geograficznej. Główne zadania grupy to:

- Doradzanie KE w kwestiach strategicznych dotyczących europejskich ram certyfikacji cyberbezpieczeństwa;
- Doradzanie ENISA w zakresie zadań dotyczących certyfikacji;
- Wspieranie KE w przygotowaniu i wydawanie opinii dotyczącej unijnego kroczącego programu prac;
- W pilnych przypadkach doradztwo w kwestii potrzeby opracowania dodatkowych programów certyfikacji;

Zarządzanie i udostępnianie informacji z zakresu cyberbezpieczeństwa
Zadaniem ENISA jest także przeprowadzanie analizy rozwoju nowoczesnych technologii i dokonywanie oceny aktualnych trendów pod kątem społecznym, prawnym, ekonomicznym i wpływu innowacji na cyberbezpieczeństwo. Agencja przygotowuje analizy strategiczne incydentów w celu identyfikacji możliwych zagrożeń i zapobiegania im. Zapewnia, we współpracy z ekspertami z państw członkowskich, doradztwo, wytyczne i najlepsze praktyki dla wzrostu poziomu cyberbezpieczeństwa infrastruktury krytycznej, operatorów usług kluczowych i dostawców usług cyfrowych.

Prowadzenie działań z zakresu edukacji i zwiększania świadomości
ENISA działa na rzecz podnoszenia świadomości społeczeństwa na temat zagrożeń związanych z cyberprzestrzenią, dostarcza dobre praktyki i wskazówki obywatelom i organizacjom. We współpracy z państwami członkowskimi, organizuje regularne kampanie informacyjne (m.in. co roku, w październiku, koordynuje Europejski Miesiąc Cyberbezpieczeństwa).[5] Wspiera również lokalne działania edukacyjne państw członkowskich.

Zaangażowanie w badania i innowacje
Kolejnym zdaniem Agencji jest zaangażowanie w budowę programu strategicznych badań i innowacji na poziomie unijnym w dziedzinie cyberbezpieczeństwa. ENISA doradza w identyfikacji potrzeb i priorytetów badawczych, a na życzenie Komisji, uczestniczy we wdrażaniu programów finansowania badań lub bierze w nich udział jako benficjent.

Wspieranie współpracy międzynarodowej
Agencja angażuje się także w działania UE w zakresie współpracy z państwami trzecimi i organizacjami międzynarodowymi w dziedzinie cyberbezpieczeństwa. Jako obserwator, bierze udział w ćwiczeniach międzynarodowych, ułatwia wymianę informacji i dobrych praktyk. Wraz z ECCG (Member States Certification Group – MSCG) przygotowuje ekspertyzy dotyczące umów o wzajemnym uznawaniu certyfikatów bezpieczeństwa z państwami trzecimi.

Organizacja Agencji

W ramach ENISA działa Zarząd, Rada Wykonawcza, Dyrektor Wykonawczy, Grupa Doradcza ENISA (ENISA Advisory Group) i Sieć Krajowych Urzędników Łącznikowych.

Zarząd
W skład Zarządu wchodzi po jednym przedstawicielu z każdego państwa członkowskiego, oraz dwóch przedstawicieli KE. Wszyscy mają prawo głosu, a także wyznaczonego zastępcę w razie nieobecności.

[5] Europejski Miesiąc Cyberbezpieczeństwa to cykliczna, odbywająca się do roku w październiku, inicjatywa Komisji Europejskiej, koordynowana przez ENISA. W tym 2018 roku odbyła się już 6 edycja ECSM. W Polsce kampanię koordynuje Państwowy Instytut Badawczy NASK.

Do Zarządu powoływane są osoby, które posiadają wiedzę z zakresu cyberbezpieczeństwa, kompetencje kierownicze, administracyjne i budżetowe. Zarząd podejmuje decyzje większością głosów. Wyjątkiem są głosowania dotyczące przyjęcia jednolitego dokumentu programowego ENISA (czytaj dalej w: Jednolity dokument programowy), budżetu rocznego, mianowania /przedłużania kadencji / odwołania Dyrektora Wykonawczego, gdzie potrzebna jest większość dwóch trzecich głosów.

Zadania Zarządu:

- Określanie ogólnego kierunku działania Agencji tak, aby był on spójny z działaniami państw członkowskich i innych instytucji unijnych.
- Przygotowanie projektu budżetu i jednolitego dokumentu programowego, który wyznacza cele roczne i wieloletnie.
- Opracowanie rocznego sprawozdania z działalności ENISA i przedłożenie go do Parlamentu Europejskiego, Komisji, Rady i Trybunału Obrachunkowego.
- Uchwalenie regulaminu wewnętrznego, regulaminu pracowniczego i warunków zatrudnienia. Podejmowanie decyzji w sprawie ustanowienia wewnętrznych struktur Agencji.
- Mianowanie Dyrektora Wykonawczego ENISA, a także przedłużenie jego kadencji lub odwołanie ze stanowiska

Przewodniczący Zarządu

Na czele Zarządu stoi przewodniczący, który jest wybierany większością dwóch trzecich głosów, spośród członków Zarządu, na okres czterech lat, z z możliwością jednokrotnego powtórzenia kadencji. Zarząd wybiera także jego zastępcę, (na wypadek gdyby przewodniczący nie mógł wykonywać swoich obowiązków).

Zadania przewodniczącego:

- Prowadzenie posiedzeń Zarządu.
- Obowiązek zwołania posiedzenia Zarządu, co najmniej dwa razy w roku.
- Zwołanie posiedzenia nadzwyczajnego na wniosek własny, KE lub jednej trzeciej członków Zarządu.

Rada Wykonawcza

Organem wspierającym Zarząd jest Rada Wykonawcza. Rada składa się z pięciu członków wybranych z Zarządu i jednego reprezentanta KE, mianowanych na okres czterech lat (z możliwością ponownej kadencji). Posiedzenia Rady odbywają się przynajmniej raz na kwartał. Dyrektor Wykonawczy może brać w nich udział, jednak nie ma prawa głosu.

Zadania Rady Wykonawczej:

- Przygotowanie decyzji do głosowania dla Zarządu.
- Wsparcie Dyrektora Wykonawczego we wdrażaniu decyzji Zarządu.
- Zapewnienie odpowiednich działań naprawczych w przypadku uzyskania przez ENISA zaleceń od audytorów, albo Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych.
- W wyjątkowych sytuacjach, podejmowanie tymczasowych decyzji w imieniu Zarządu[6].

Dyrektor Wykonawczy

Agencją zarządza Dyrektor Wykonawczy, który jest niezależny w wykonywaniu swoich obowiązków i odpowiada przed Zarządem.

Zadania Dyrektora Wykonawczego:

- Bieżące zarządzanie Agencją.
- Wdrażanie decyzji przyjętych przez Zarząd.
- Przygotowanie projektu jednolitego dokumentu programowego i przedłożenie go Zarządowi do zatwierdzenia.
- Wdrożenie jednolitego dokumentu programowego.
- Przygotowanie raportu rocznego.
- Przygotowanie planu działania opartego na wnioskach z ewaluacji działalności Agencji.

[6] **Dotyczy to głównie decyzji administracyjnych i budżetowych i tylko takich, które mogą być podjęte przez Zarząd zwykłą większością głosów. Decyzja tymczasowa jest niezwłocznie przekazywana do Zarządu i musi być przez niego zatwierdzona nie później, niż w ciągu trzech miesięcy od momentu podjęcia decyzji.**

- Przygotowanie planu działania w następstwie wniosków ze sprawozdań z kontroli wewnętrznej, a także sprawozdań Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych, a także składanie do KE, dwa razy w roku, sprawozdania z wdrożenia postępów prac.

- Przygotowanie projektów przepisów finansowych mających zastosowanie dla Agencji.

- Ochrona interesów finansowych UE poprzez wdrożenie środków zapobiegania nadużyciom, korupcji, nielegalnej działalności. Przygotowanie strategii zwalczania nadużyć finansowych.

- Utrzymywanie kontaktów ze środowiskiem biznesowym i podtrzymywanie dialogu ze wszystkimi interesariuszami.

- Regularna wymiana informacji z instytucjami, organami i jednostkami organizacyjnymi UE w celu zapewnienia spójności w opracowywaniu i wdrażaniu unijnej polityki bezpieczeństwa.

Na wniosek Parlamentu Europejskiego lub Rady, Dyrektor przedstawia sprawozdanie z wykonania swoich obowiązków.

Dyrektor Wykonawczy może powoływać **grupy robocze**, składające się z ekspertów z państw członkowskich. Procedura powołania grup jest określona w wewnętrznych zasadach działania ENISA. Jeżeli będzie taka potrzeba, Dyrektor może podjąć decyzję o **utworzeniu biura lokalnego**. Decyzja ta musi być podyktowana koniecznością skutecznego i efektywnego wykonywania zadań ENISA, a także w oparciu o racjonalną analizę kosztów i korzyści. Przed podjęciem decyzji Dyrektor uzyskuje zgodę KE i Zarządu, a także zasięga opinii państwa członkowskiego, w którym ma być ustanowione biuro lokalne. Liczba personelu we wszystkich biurach ENISA powinna być ograniczona do minimum, a zakres działań wyznaczony w taki sposób, aby uniknąć niepotrzebnego powielania funkcji i kompetencji poszczególnych jednostek.

Grupa Doradcza ENISA (ENISA Advisory Group)

W ramach Agencji działa także Grupa Doradcza ENISA. Na wniosek Dyrektora Wykonawczego, Zarząd powołuje grupę ekspertów reprezentujących różnych interesariuszy, takich jak dostawcy sieci, dostawcy usług ICT, MŚP, operatorzy, grupy konsumenckie, przedstawiciele nauki w zakresie cyberbezpieczeństwa, a także przedstawiciele europejskich organizacji odpowiedzialnych za ochronę danych i egzekwowanie prawa. Grupie Doradczej ENISA przewodniczy Dyrektor Wykonawczy lub osoba przez niego powołana. Kadencja członków grupy wynosi dwa i pół roku. Zarząd dąży do zapewnienia równej reprezentacji płci, obszarów geograficznych, a także grup interesariuszy. W skład grupy nie mogą wchodzić członkowie Zarządu. Natomiast eksperci z KE i państw członkowskich mogą być obecni na posiedzeniach grupy. W razie potrzeby, Dyrektor może zaprosić na spotkania przedstawicieli innych organów.

Zadania Grupy Doradczej ENISA:

- Doradztwo Agencji i Dyrektorowi Wykonawczemu w zakresie opracowania programu prac ENISA i zapewnienie odpowiedniej komunikacji z interesariuszami różnych grup.

Sieć Krajowych Urzędników Łącznikowych

W ramach ENISA funkcjonuje również **Sieć Krajowych Urzędników Łącznikowych**, która składa się z przedstawicieli wszystkich państw członkowskich (po jednym przedstawicielu z każdego państwa).

Zadania Sieci Krajowych Urzędników Łącznikowych:

- Umożliwianie sprawnej wymiany informacji pomiędzy ENISA a państwami członkowskimi.

- Wsparcie Agencji w promowaniu jej działalności, wytycznych i zaleceń.

- Zapewnienie komunikacji ENISA z krajowymi ekspertami z dziedziny cyberbezpieczeństwa.

Jednolity dokument programowy

Plan działania ENISA zawarty jest w Jednolitym dokumencie programowym. Dokument zawiera roczny i wieloletni plan prac, w którym opisane są szczegółowe cele i oczekiwane wyniki, wraz ze wskaźnikami wydajności, które pozwolą na ocenę działalności Agencji. W planie zawarty jest również opis działań, a do każdego działania przyporządkowane są odpowiednie zasoby finansowe i ludzkie (przyporządkowanie zasobów powinno być aktualizowane przynajmniej raz w roku). Plan wieloletni określa cele strategiczne i jest spójny z planem rocznym. Projekt planu przygotowuje co roku Dyrektor Wykonawczy. Do 30 listopada Zarząd przyjmuje Jednolity dokument programowy i przesyła go do Parlamentu Europejskiego , Rady i Komisji, nie później niż 31 stycznia następnego roku. Dokument ostatecznie zostaje zaakceptowany wraz z przyjęciem budżetu ogólnego UE. W przypadku nałożenia dodatkowych zadań na Agencję, Zarząd dokonuje zmian w Jednolitym dokumencie programowym. Procedura zmian jest dokładnie taka sama, jak w przypadku złożenia projektu dokumentu.

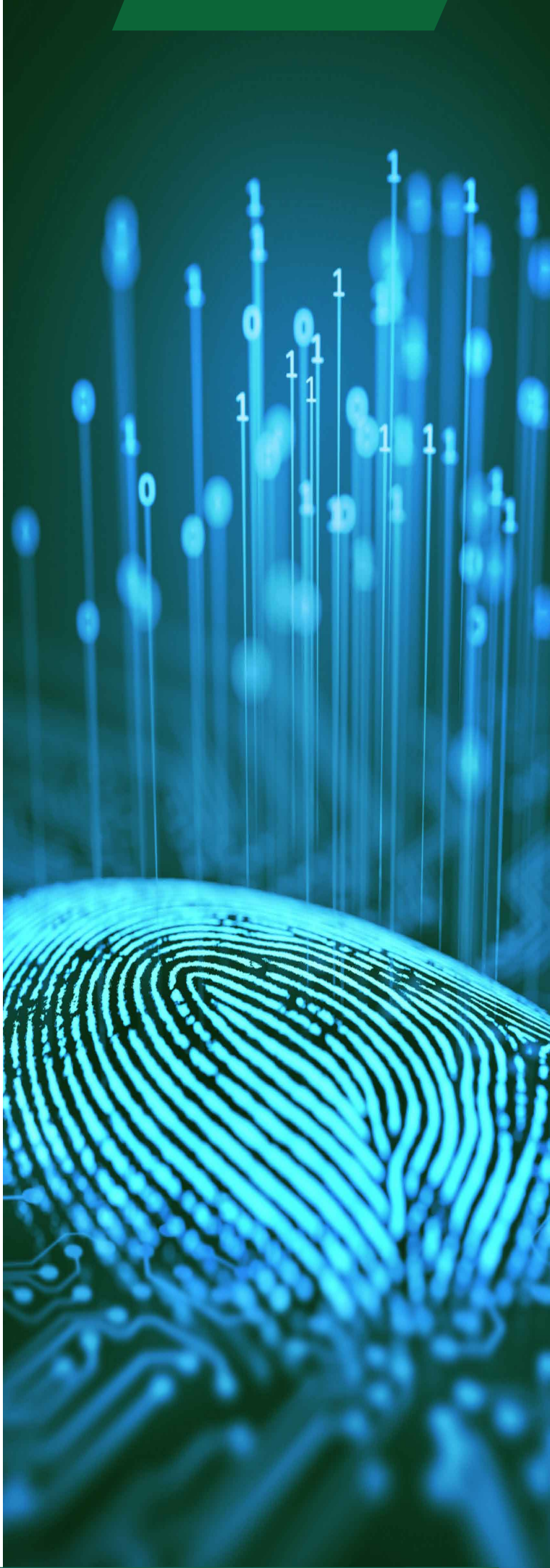
Budżet ENISA

Co roku Dyrektor Wykonawczy przygotowuje projekt preliminarza dochodów na kolejny rok budżetowy i przekazuje go Zarządowi wraz z proponowanym planem zatrudnienia. Projekt zatwierdza Komisja, Parlament i Rada. Budżet ENISA musi zostać dostosowany do budżetu ogólnego UE i zostaje zaakceptowany dopiero po przyjęciu budżetu ogólnego.

Osobą odpowiedzialną za realizację budżetu jest Dyrektor Wykonawczy. ENISA jest zobowiązana do publikowania corocznego sprawozdania finansowego w terminie do 15 listopada następnego roku.

Współpraca z państwami członkowskimi, państwami trzecimi i organizacjami międzynarodowymi

W zakresie niezbędnym do osiągnięcia celów, ENISA może współpracować z państwami trzecimi lub organizacjami międzynarodowymi.



CZĘŚĆ II:
Ramy Europejskiej Certyfikacji Cyberbezpieczeństwa

Rozporządzenie w sprawie certyfikacji cyberbezpieczeństwa to pierwsze prawo dotyczące rynku wewnętrznego, które odpowiada na potrzebę podniesienia poziomu bezpieczeństwa produktów, usług i procesów ICT. Tak więc **stworzenie europejskich ram certyfikacji cyberbezpieczeństwa to przełomowy krok**, który w efekcie umożliwi zniesienie barier, utrzymujących się na rynku cyfrowym. Aby to osiągnąć, konieczne jest wypracowanie harmonijnego podejścia do certyfikacji cyberbezpieczeństwa. Dlatego rozporządzenie określa mechanizm ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa oraz potwierdzania, że dane produkty bądź usługi spełniają określone wymogi bezpieczeństwa (tzw. poziom uzasadnienia zaufania).

Celem tych regulacji jest doprowadzenie do sytuacji, w której konsument będzie mógł wybierać takie urządzenia i rozwiązania, które są przetestowane i spełniają odpowiednie normy bezpieczeństwa. Z kolei firmy będą mogły oszczędzić czas i pieniądze, ponieważ nie będą musiały ubiegać się o certyfikat w każdym kraju, w którym chciałyby oferować swoje usługi bądź produkty. Co więcej, firmy które zainwestują w cyberbezpieczeństwo, będą mogły wykorzystać ten fakt jako swoją przewagę nad konkurencją.

Wejście w życie tych przepisów może jednak oznaczać również pewne wyzwania dla państw, które nie podejmowały dotąd żadnych kroków w kierunku stworzenia krajowych programów certyfikacji cyberbezpieczeństwa. W lepszej sytuacji znajdą się te państwa członkowskie, które nie będą musiały budować od podstaw odpowiednich kompetencji oraz infrastruktury np. do testowania certyfikowanego sprzętu.

Unijny kroczący program prac dotyczący europejskiej certyfikacji cyberbezpieczeństwa

Podstawą europejskiej certyfikacji cyberbezpieczeństwa jest unijny kroczący program prac, który Komisja Europejska musi opublikować w **ciągu dwunastu miesięcy** od wejścia w życie rozporządzenia. Dokument powinien być aktualizowany co najmniej raz na trzy lata.

Po uprzednim zatwierdzeniu przez KE, Agencja może podejmować zobowiązania robocze (nie stanowią one zobowiązań prawnych Unii i państw członkowskich). ENISA jest również otwarta na udział państw trzecich, które mają podpisane w tym celu porozumienia z UE. W porozumieniach określa się charakter, zakres i sposób współpracy wraz z informacją o udziału w inicjatywach, wkładzie finansowym, zaangażowanym personelu itp. Współpraca z państwami trzecimi i organizacjami międzynarodowymi powinna odbywać się w obszarach właściwych dla ENISA i zgodnie ze strategią przyjętą przez Zarząd.

Program zawiera **strategiczne priorytety** dla przyszłych europejskich programów certyfikacji oraz **wykaz produktów, usług i procesów ICT** lub ich kategorii, dla których korzystne będzie objęcie europejskim programem certyfikacji.

Wykaz produktów, usług i procesów ICT

Rozporządzenie podaje kilka przyczyn, które uzasadniają włączenie do wykazu:

1. **Istniejące krajowe programy certyfikacji** – jako że dostępność i rozwój krajowych programów może nieść ze sobą ryzyko fragmentacji kontekście całego rynku UE;
2. odpowiednia unijna czy też krajowa **polityka lub prawodawstwo;**
3. **rosnący popyt** na rynku;
4. **rozwój sytuacji** w zakresie chyberbepieczeństwa
5. **wniosek o przygotowanie propozycji programu** złożony przez Europejską Grupę Certyfikacji Cyberbezpieczeństwa.

Rozpoczęcie procesu certyfikacji

Proces certyfikacji mogą zainicjować zarówno Komisja Europejska, jak i Europejska Grupa Certyfikacji Cyberbezpieczeństwa (ECCG, European Cybersecurity Certification Group). Różnica polega na tym, że ENISA musi przygotować propozycję europejskiego programu certyfikacji na wniosek KE.

Natomiast jeśli o przygotowanie propozycji programu zawnioskuje ECCG, wówczas ENISA może taki wniosek odrzucić. Agencja musi jednak podać uzasadnienie, a każda decyzja odmowna jest podejmowana przez zarząd.

Co do zasady, wniosek powinien dotyczyć programu, który odnosi się do produktów, usług i procesów ICT **ujętych w unijnym kroczącym programie prac.** W uzasadnionych przypadkach możliwe jest jednak wnioskowanie o przygotowanie programu nieuwzględnionego w wykazie. Wówczas unijny kroczący program prac zostanie odpowiednio zaktualizowany.

Europejska Grupa Certyfikacji Cyberbezpieczeństwa

Europejska Grupa Certyfikacji Cyberbezpieczeństwa to jeden z najważniejszych organów, który powołuje do życia Cybersecurity Act. Grupa składa się z przedstawicieli krajowych organów ds. certyfikacji cyberbezpieczeństwa lub innych właściwych organów krajowych. Każdy członek grupy może reprezentować nie więcej niż jedno inne państwo członkowskie.

Grupie przewodniczy Komisja Europejska, która zapewnia jej sekretariat, z pomocą ENISA. W pracach oraz posiedzeniach grupy mogą uczestniczyć również inne zainteresowane strony.

Zadania ECCG:

- doradzanie i pomoc KE, w celu zapewnienia spójnego wdrożenia i stosowania przepisów dotyczących m.in. unijnego kroczącego programu prac, polityki certyfikacji cyberbezpieczeństwa czy europejskich programów certyfikacji cyberbezpieczeństwa;
- doradzanie i współpraca z ENISA przy przygotowaniu propozycji programu certyfikacji, w tym opiniowanie propozycji programu;
- występowanie do ENISA o przygotowanie propozycji europejskiego programu certyfikacji cyberbezpieczeństwa;
- kierowanie do KE opinii dotyczących utrzymania i przeglądu istniejących europejskich programów certyfikacji cyberbezpieczeństwa;
- badanie istotnych zmian w dziedzinie certyfikacji cyberbezpieczeństwa oraz wymiana informacji i dobrych praktyk;
- ułatwianie współpracy między krajowymi organami ds. certyfikacji cyberbezpieczeństwa,
- wsparcie we w drażaniu mechanizmów wzajemnego przeglądu zgodnie z zasadami ustanowionymi w europejskim programie certyfikacji cyberbezpieczeństwa;
- ułatwianie dostosowania europejskich programów certyfikacji cyberbezpieczeństwa do uznanych międzynarodowych standardów. Przedstawianie ENISA zaleceń współpracy z odpowiednimi międzynarodowymi organizacjami standaryzującymi w celu zapełnienia luk w dostępnych standardach.

Ustanowienie programu certyfikacji cyberbezpieczeństwa

1. Przygotowanie propozycji programu

Za przygotowanie propozycji programu certyfikacji odpowiada ENISA. Podczas prac Agencja ma obowiązek konsultacji „programu kandydata" ze wszystkimi zainteresowanymi interesariuszami oraz ustanowienia grupy roboczej, składającej się z ekspertów z państw członkowskich, która opracuje program. Wypracowana propozycja przekazywana jest do KE.

Dodatkowo pomoc i porady ekspertów zapewnia ECCG. Grupa opiniuje również przygotowaną propozycję programu. Opinia ta nie jest wiążąca, a jej brak nie blokuje możliwości przekazania propozycji programu do Komisji Europejskiej. ENISA powinna jednak w jak największym stopniu uwzględnić opinię ECCG. Daje to sektorowi publicznemu możliwość wpływu na przygotowywanie europejskich programów certyfikacji.

2. Przyjęcie propozycji programu

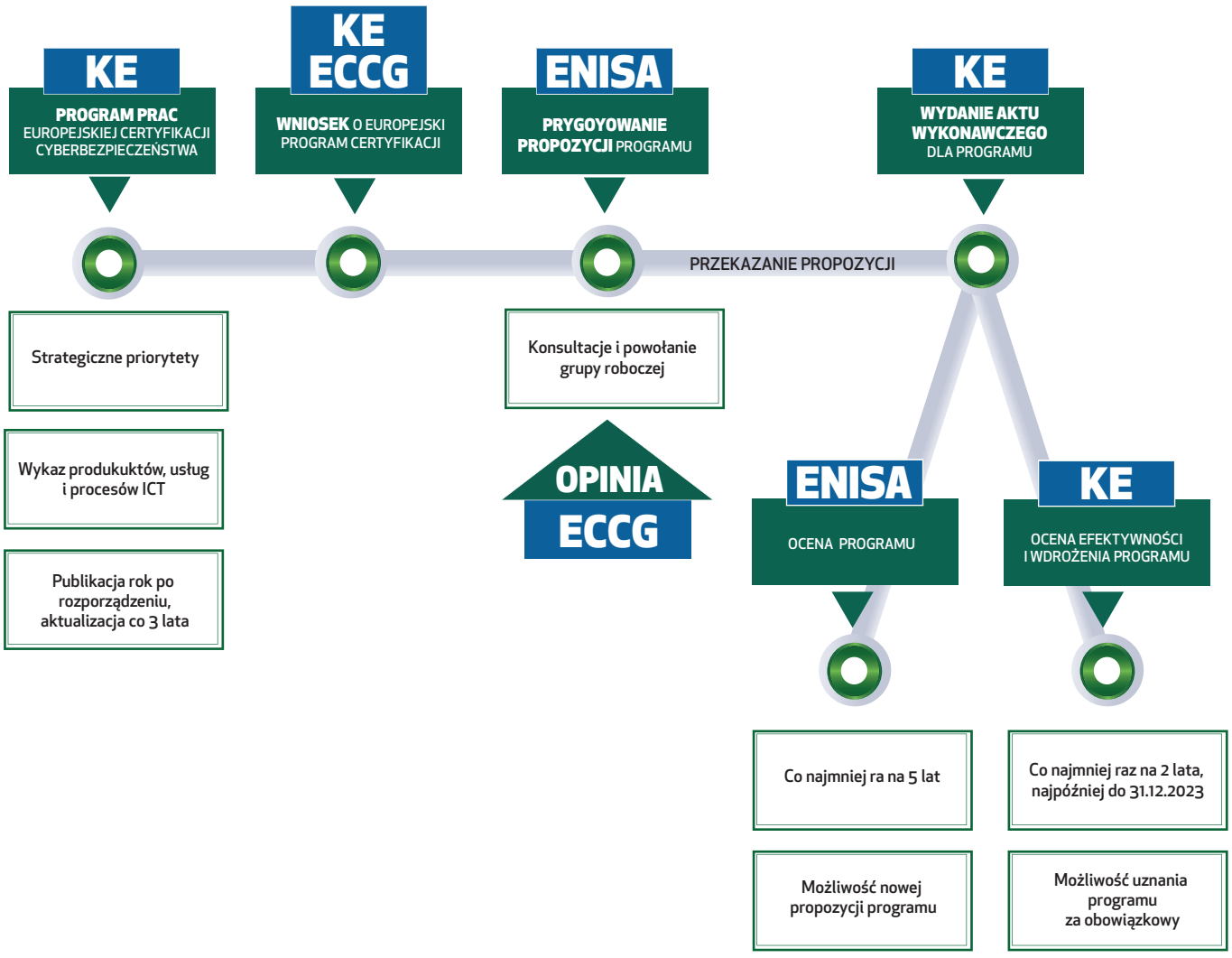
Komisja Europejska, w oparciu o otrzymaną propozycję, może przyjąć akty wykonawcze, które ustanowią europejskie programy certyfikacji cyberbezpieczeństwa dla procesów, produktów i usług ICT.

3. Przegląd programów

Co najmniej raz na 5 lat ENISA ocenia przyjęte europejskie programy certyfikacji cyberbezpieczeństwa pod względem ich użyteczności i aktualności. Komisja Europejska lub ECCG może zwrócić się do Agencji o opracowanie zmienionej propozycji programu.

4. Informacje o europejskich programach certyfikacji cyberbezpieczeństwa

Zadaniem ENISA jest utworzenie specjalnej strony internetowej na temat certyfikacji cyberbezpieczeństwa. Znajdą się tam m.in. informacje o aktualnych, wygasłych lub wycofanych programach, certyfikatach czy unijnych deklaracjach zgodności. Powinno się tam znaleźć również repozytorium linków do informacji dostarczanych przez producentów i dostawców z branży ICT.



Rys. 1. Przygotowanie Europejskiego programu certyfikacji cyberbezpieczeństwa.

Europejski program certyfikacji cyberbezpieczeństwa

Europejski program certyfikacji cyberbezpieczeństwa musi określać co najmniej:

1. **Przedmiot, zakres i cel programu certyfikacji.**

2. Odniesienie do międzynarodowych, europejskich lub krajowych standardów zastosowanych w ocenie (lub przy ich braku do specyfikacji technicznych lub wymogów cyberbezpieczeństwa określonych w programie).

3. **Poziom bezpieczeństwa, czyli poziom uzasadnienia zaufania.**

   a) wskazanie **czy samoocena zgodności (tzw. ocena zgodności przez stronę pierwszą) jest dozwolona** w ramach programu;

   b) szczegółowe lub **dodatkowe wymogi** dla jednostek oceniających zgodność.

4. **Kryteria oraz metody oceny**, które pozwolą wykazać, że osiągnięto wymogi bezpieczeństwa.

5. **Informacje niezbędne dla procesu certyfikacji**, które wnioskodawca musi udostępnić jednostkom oceniającym zgodność.

6. Jeżeli program przewiduje **znaki lub etykiety** należy określić warunki, na jakich mogą być one używane.

7. **Zasady monitorowania zgodności z wymogami** certyfikatu lub unijnej deklaracji zgodności.

8. **Warunki przyznawania, przedłużania i odnawiania ważności certyfikatu**, a także rozszerzania lub zmniejszania zakresu certyfikacji.

9. **Konsekwencje niezgodności** certyfikowanych lub samoocenionych produktów, usług i procesów ICT z wymogami programu.

10. **Sposoby zgłaszania i rozwiązywania wcześniej niewykrytych podatności.**

11. Zasady przechowywania informacji przez jednostki oceniające zgodność.

12. Zidentyfikowane **krajowe lub międzynarodowe programy** certyfikacji cyberbezpieczeństwa, które **obejmują te same** procesy, produkty i usługi ICT.

I. Certyfikat oraz unijna deklaracja zgodności

Niezbędnym elementem każdego programu jest również **określenie treści i formatu wydawanego certyfikatu lub deklaracji zgodności**. Powinny one zawierać:

- Czas przez jaki powinna być udostępniana deklaracja zgodności oraz dokumentacja techniczna.
- Okres ważności certyfikatu.
- Politykę ujawniania informacji o przyznanych, zmienionych i cofniętych certyfikatach.
- Warunki wzajemnego uznawania programu certyfikacji z innymi państwami.
- Zasady wzajemnej oceny dla organów wydających europejskie certyfikaty cyberbezpieczeństwa dla wysokiego poziomu bezpieczeństwa.
- Procedury dostarczania i aktualizacji dodatkowych informacji cyberbezpieczeństwa oraz ich format.

Wymagania programu nie mogą być sprzeczne z obowiązującymi regulacjami prawnymi, zwłaszcza wynikającymi z ujednoliconego prawodawstwa UE.

II. Wymogi bezpieczeństwa

Europejski program certyfikacji cyberbezpieczeństwa powinien być tak zaprojektowany, aby spełniać przynajmniej następujące wymogi bezpieczeństwa:

- **ochrona przetwarzanych danych**, podczas całego cyklu życia produktu lub usługi;
- **dostęp** wyłącznie do tych danych, do których upoważnione osoby, programy lub maszyny mają prawo dostępu;
- identyfikacja i dokumentacja **znanych podatności i słabych punktów;**

- możliwość sprawdzenia, **które dane czy usługi były przetwarzane**, kiedy i przez kogo;

- możliwość sprawdzenia czy produkty, procesy i usługi **nie zawierają znanych podatności;**

- **przywrócenie dostępu** do danych, usług i funkcji w odpowiednim czasie po incydencie;

- produkty, usługi i procesy **są bezpieczne domyślnie i zgodnie z projektem;**

- produkty, usługi i procesy są dostarczane z **aktualnym oprogramowaniem** i przętem pozbawionym znanych luk, oraz z mechanizmami **bezpiecznych aktualizacji.**

III. Poziomy uzasadnienia zaufania europejskich programów certyfikacji cyberbezpieczeństwa

Europejski program certyfikacji cyberbezpieczeństwa może określać trzy poziomy bezpieczeństwa: podstawowy, istotny i wysoki. Poziom uzasadnienia zaufania dla danego urządzenia czy usługi ICT, powinien być proporcjonalny do poziomu ryzyka, na który składa się m.in. prawdopodobieństwo wystąpienia incydentu oraz jego potencjalny wpływ.

Wydany na określonym poziomie certyfikat zapewnia, że produkty, usługi i procesy ICT spełniają odpowiednie wymogi bezpieczeństwa i zostały ocenione zgodnie z obowiązującymi na danym poziomie wytycznymi.

Poziom uzasadnienia zaufania	Ryzyko	Wymagana ocena
Podstawowy	- znane podstawowe cyberzagrożenia	- dokumentacja techniczna
Istotny	- znane cyberzagrożenia - cyberatak prowadzony przez podmioty o **ograniczonych umiejętnościach i zasobach**	- czy nie zastosowano powszechnie znanych podatności - czy produkty bądź usługi prawidłowo wdrażają niezbędne funkcje bezpieczeństwa
Wysoki	- cyberatak prowadzany przez aktorów o **znaczących umiejętnościach i zasobach**	- czy nie zastosowano powszechnie znanych podatności - czy produkty bądź usługi prawidłowo wdrażają niezbędne funkcje bezpieczeństwa - **odporność na ataki za pomocą testów penetracyjnych**

IV. Ocena zgodności przez stronę pierwszą

Europejski program certyfikacji cyberbezpieczeństwa może zezwolić na przeprowadzenie **samooceny zgodności** (tzw. ocena zgodności przez stronę pierwszą).

Przeprowadza ją producent lub dostawca produktów i usług ICT na swoją **wyłączną odpowiedzialność**. Taka ocena może dotyczyć tylko produktów i usług na **podstawowym poziomie bezpieczeństwa**).

Dostawca lub producent stwierdza, że spełnione zostały wymogi określone w europejskim programie certyfikacji i przyjmuje odpowiedzialność za ich zgodność. Unijną deklarację zgodności oraz dokumentację techniczną należy przechowywać przez czas określony w danym europejskim programie certyfikacji. Kopię deklaracji przedkłada się do krajowego organu ds. certyfikacji cyberbezpieczeństwa i ENISA.

Wydawanie deklaracji zgodności jest **dobrowolne**, chyba że inaczej stanowi unijne bądź krajowe prawo. Deklaracja uznawana jest we wszystkich państwach członkowskich.

V. Uzupełniające informacje dotyczące cyberbezpieczeństwa

Producent lub dostawca certyfikowanych lub samoocenionych produktów, usług i procesów ICT musi przekazać następujące informacje uzupełniające:

- wytyczne pomagające użytkownikom w bezpiecznej konfiguracji, instalacji, wdrażaniu, eksploatacji i konserwacji produktów lub usług;
- jak długo użytkownicy będą mieli zapewnione wsparcie bezpieczeństwa, zwłaszcza w kontekście aktualizacji związanych z cyberbezpieczeństwem.
- w jaki sposób użytkownicy lub analitycy cyberbezpieczeństwa mogą zgłaszać informacje o podatnościach;
- wskazanie repozytoriów online, które zawierają ujawnione luki w zabezpieczeniach danego produktu lub usługi, a także odpowiednie porady.

Informacje muszą być dostępne w formie elektronicznej oraz aktualizowane, przynajmniej do wygaśnięcia certyfikatu lub unijnej deklaracji zgodności.

Certyfikacja cyberbezpieczeństwa

Procesy, produkty i usługi ICT, które zostały certyfikowane w ramach europejskiego programu certyfikacji cyberbezpieczeństwa, uznaje się za zgodne z jego wymaganiami. Certyfikaty wydawane są na okres określony w danym programie certyfikacji i mogą być przedłużane, pod warunkiem że odpowiednie wymagania nadal są spełniane.

Europejski certyfikat cyberbezpieczeństwa jest uznawany we wszystkich państwach członkowskich. **Certyfikacja jest dobrowolna**, chyba że prawo unijne lub państwowe stanowi inaczej.

1. Ocena certyfikatów

Komisja Europejska będzie regularnie oceniać efektywność i wdrożenie przyjętych programów certyfikacji. Komisja sprawdza również czy konkretny program powinien zostać uznany jako obowiązkowy, aby zapewnić odpowiedni poziom cyberbezpieczeństwa oraz usprawnić funkcjonowanie rynku wewnętrznego.

2. Obowiązkowa certyfikacja

Przeprowadzając ocenę, KE identyfikuje produkty, procesy i usługi ICT objęte istniejącym programem certyfikacji, które powinny podlegać obowiązkowej certyfikacji. W pierwszej kolejności oceniane pod tym kątem będą sektory szczególnie wrażliwe, wymienione w załączniku II do Dyrektywy NIS: energetyka, transport, bankowość, infrastruktura rynków finansowych, służba zdrowia, zaopatrzenie w wodę pitną oraz infrastruktura cyfrowa. Ocenia się je najpóźniej dwa lata po przyjęciu pierwszego programu.

Oceniając, czy certyfikat powinien być obowiązkowy, Komisja:

- rozważa jaki **wpływ wywrą podjęte środki na producentów lub dostawców, a także samych użytkowników.** Uwzględnia przy tym koszty, ale i przewidywane korzyści wynikające ze zwiększenia poziomu bezpieczeństwa;
- bierze pod uwagę **dostępność oraz wykorzystanie odpowiedniego prawa** – krajowego i międzynarodowego;
- prowadzi **konsultacje** z zainteresowanymi stronami i państwami członkowskimi;

- rozważa terminy wdrożenia, **przejściowe okre-okresy oraz środki**;

- proponuje **najszybszy i najskuteczniejszy sposób przejścia** od dobrowolnych do obowiązkowych programów certyfikacji.

3. Wydawanie certyfikatów cyberbezpieczeństwa

Europejski certyfikat cyberbezpieczeństwa, który odnosi się do **podstawowego** lub **istotnego** poziomu bezpieczeństwa, **wydaje jednostka oceniająca zgodność** na podstawie kryteriów zawartych w europejskim programie certyfikacji cyberbezpieczeństwa. Jednak w uzasadnionych przypadkach określony program może wskazywać, że certyfikat może wydać **wyłącznie organ publiczny**:

- krajowy organ ds. certyfikacji cyberbezpieczeństwa,

- organ publiczny akredytowany jako jednostka oceniająca zgodność.

Gdy europejski program certyfikacji cyberbepieczeństwa wymaga zapewnienia poziomu **wysokiego**, certyfikat może wydać:

- krajowy organ ds. certyfikacji cyberbezpieczeństwa,

- jednostka oceniająca zgodność,tylko jeśli krajowy organ ds.certyfikacji cyberbezpieczeństwa:

  - zatwierdził wcześniej każdy indywidualny certyfikat wydany przez tę jednostkę;
  - lub wcześniej przekazał jej to zadanie.

4. Informowanie jednostek wydających certyfikaty

Osoba fizyczna lub prawna, która ubiega się o certyfikację produktu, procesu lub usługi ICT, udostępnia wszystkie informacje niezbędne do przeprowadzenia procedury.

Po otrzymaniu certyfikatu musi informować jednostkę wydającą certyfikat o wszelkich wykrytych później lukach lub nieprawidłowościach, które mogą mieć wpływ na spełnianie wymogów certyfikacji. Jednostka przekazuje informacje krajowemu organowi ds. certyfikacji cyberbezpieczeństwa.

Certyfikacja na poziomie krajowym – obowiązki państw członkowskich

O ile przygotowanie programów certyfikacji cyberbezpieczeństwa odbywa się na poziomie europejskim, o tyle sam proces certyfikacji **przebiega na poziomie krajowym**. Cybersecurity Act nakłada na państwa członkowskie konkretne obowiązki, które mają pomóc w budowie sprawnego krajowego systemu certyfikacji cyberbezpieczeństwa.

Aby móc przeprowadzić proces certyfikacji, konieczne jest funkcjonowanie:

1. Krajowego organu ds. certyfikacji cyberbezpieczeństwa (KOCC)

2. Krajowej jednostki akredytującej[7]

3. Jednostek oceniających zgodność

Krajowe organy ds. certyfikacji cyberbezpieczeństwa

Najważniejszym obowiązkiem państw członkowskich jest **wyznaczenie co najmniej jednego krajowego organu ds. certyfikacji cyberbezpieczeństwa**. Mają na to 24 miesiące po opublikowaniu rozporządzenia w Dzienniku Urzędowym Unii Europejskiej.

Państwo członkowskie może powołać taki organ na swoim terytorium lub porozumieć się z innym państwem i wyznaczyć organ na jego terenie. Następnie należy poinformować Komisję Europejską o wyznaczonym organie, a jeśli jest więcej niż jeden – o powierzonych im zadaniach. To również na państwach członkowskich spoczywa obowiązek zapewnienia krajowym organom ds certyfikacji cyberbezpieczeństwa zasobów do wykonywania powierzonych zadań.

Krajowe organy certyfikacji pełnią dwoistą rolę:

- wydają certyfikaty,

- prowadzą działania nadzorcze.

[7] Każde państwo członkowskie wyznacza jedną krajową jednostkę akredytującą. W Polsce jest to Polskie Centrum Akredytacji, które akredytuje jednostki oceniające zgodność, gdy spełniają określone wymogi. Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93.

Obie te funkcje muszą być rozdzielone i niezależne od siebie. Krajowe organy muszą być również **niezależne od podmiotów, które nadzorują** – w kwestiach organizacji, decyzji finansowych, struktury prawnej czy przy podejmowaniu decyzji.

Krajowe organy certyfikacji współpracują ze sobą oraz z KE, a w szczególności wymieniają informacje, doświadczenia i dobre praktyki. Żeby skutecznie wprowadzać w życie przepisy rozporządzenia, **powinny również uczestniczyć w pracach Europejskiej Grupy Certyfikacji Cyberbezpieczeństwa.**

Zadania krajowych organów ds. certyfikacji cyberbezpieczeństwa

- **egzekwują zasady zawarte w programach**, aby monitorować zgodność produktów, procesów i usług ICT z wymogami certyfikatów wydanych na ich terytoriach;
- monitorują i **egzekwują zobowiązania producentów lub dostawców**, którzy mają siedzibę na ich terenie, i **którzy wydali deklarację zgodności;**
- **wspierają krajowe jednostki akredytujące** w monitorowaniu i nadzorowaniu działalności jednostek oceniających zgodność;
- monitorują **i nadzorują organy publiczne** wydające certyfikaty;
- **autoryzują jednostki oceniające zgodność** oraz ograniczają, zawieszają lub cofają obowiązujące zezwolenia w przypadkach, gdy jednostki nie spełniają wymogów.
- **rozpatrują skargi** złożone przez osoby fizyczne lub prawne w związku z wydanymi certyfikatami lub unijną deklaracją zgodności;
- przedstawiają roczne zbiorcze sprawozdanie z podjętych działań;
- **współpracują z innymi krajowymi organami ds. certyfikacji cyberbezpieczeństwa** lub organami publicznymi, dzielą się informacjami o niezgodnościach procesów, produktów i usług ICT z wymogami rozporządzenia lub europejskich programów certyfikacji;
- **monitorują istotne zmiany** w dziedzinie certyfikacji cyberbezpieczeństwa.

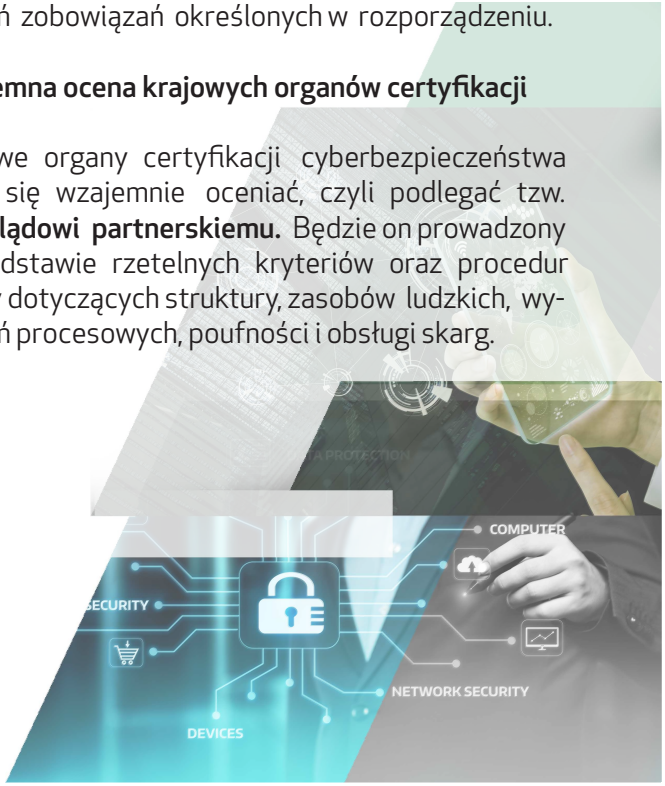
Uprawnienia krajowych organów ds. certyfikacji cyberbezpieczeństwa

Krajowe organy ds. certyfikacj cyberbezpieczeństwa mogą:

- zwracać się do jednostek oceniających zgodność, posiadaczy europejskich certyfikatów cyberbezpieczeństwa oraz podmiotów deklarujących zgodność, o **dostarczenie informacji, których potrzebują do wykonywania swoich zadań;**
- **audytować jednostki oceniające zgodność,** posiadaczy europejskich certyfikatów oraz podmioty deklarujące zgodność;
- podjąć odpowiednie środki, **zgodnie z prawem krajowym, żeby zapewnić przestrzeganie zapisów rozporządzenia lub europejskiego programu certyfikacji** przez jednostki oceniające zgodność, posiadaczy certyfikatów i podmioty deklarujące zgodność;
- **uzyskać dostęp do obiektów** jednostek oceniających zgodność i posiadaczy europejskich certyfikatów cyberbezpieczeństwa, żeby przeprowadzić dochodzenie zgodnie z prawem procesowym UE lub państwa członkowskiego;
- **wycofać certyfikat** wydany przez krajowy organ ds. certyfikacji cyberbezpieczeństwa lub jednostkę oceniającą zgodność, który nie jest zgodny z rozporządzeniem lub europejskim programem certyfikacji cyberbezpieczeństwa;
- **nałożyć sankcje,** zgodnie z prawem krajowym, oraz wymagać natychmiastowego zaprzestania naruszeń zobowiązań określonych w rozporządzeniu.

Wzajemna ocena krajowych organów certyfikacji

Krajowe organy certyfikacji cyberbezpieczeństwa będą się wzajemnie oceniać, czyli podlegać tzw. **przeglądowi partnerskiemu.** Będzie on prowadzony na podstawie rzetelnych kryteriów oraz procedur oceny dotyczących struktury, zasobów ludzkich, wymagań procesowych, poufności i obsługi skarg.



Wzajemny przegląd sprawdzać będzie:

- Czy działania krajowego organu ds. certyfikacji cyberbezpieczeństwa związane z wydawaniem certyfikatów są rozdzielone i niezależne od działań nadzorczych.

- Procedury dotyczące nadzoru i monitorowania:

  - zgodności produktów, usług i procesów ICT z certyfikatami,

  - zobowiązań producentów i dostawców produktów, procesów lub usług ICT,

  - działalności jednostek oceniających zgodność.

- Czy personel organów wydających certyfikaty dla wysokiego poziomu bezpieczeństwa posiada odpowiednią wiedzę specjalistyczną.

Wzajemny przegląd odbywać się będzie **co najmniej raz na pięć lat**. Prowadzą go przynajmniej dwa krajowe organy ds. certyfikacji cyberbezpieczeństwa z innych państw członkowskich oraz Komisja Europejska. W ocenie uczestniczyć może również ENISA.

Komisja może przyjmować akty wykonawcze, ustanawiające **plan wzajemnego przeglądu** na co najmniej pięć lat oraz **określające kryteria** m.in. składu zespołu, metodologii przeglądu partnerskiego, harmonogramu czy cykliczności.

Wyniki wzajemnego przeglądu bada Europejska Grupa Certyfikacji Cyberbezpieczeństwa, po czym przygotowuje streszczenie, które może być udostępnione publicznie. Jeśli zachodzi taka potrzeba, wydaje również wytyczne lub rekomendacje.

Jednostki oceniające zgodność

Jednostki oceniające zgodność to również bardzo istotne ogniwo krajowego systemu certyfikacji cyberbezpieczeństwa. **Mogą one wystawiać certyfikaty dla podstawowego i istotnego poziomu bezpieczeństwa**, a po przekazaniu takiego zadania przez krajowy organ ds. certyfikacji cyberbezpieczeństwa – nawet dla poziomu wysokiego.

Jednostki oceniające zgodność[8] są **akredytowane przez krajową jednostkę akredytującą** tylko wtedy, gdy spełniają określone wymogi.

Akredytacja jest wydawana **maksymalnie na pięć lat** i może być przedłużana na tych samych warunkach, o ile jednostka oceniająca zgodność dalej spełnia wymogi.

Jednostki akredytujące podejmują środki, aby ograniczyć, zawiesić lub odwołać akredytację jednostki oceniającej zgodność, gdy przestała ona spełniać warunki akredytacji lub gdy jej działania naruszają rozporządzenie w sprawie certyfikacji cyberbezpieczeństwa. Jeśli europejski certyfikat cyberbezpieczeństwa zostanie wydany przez krajowy organ ds. certyfikacji cyberbezpieczeństwa, wówczas jako jednostka oceniająca zgodność będzie akredytowana jednostka certyfikująca tego krajowego organu certyfikacji.

Jeśli europejski program certyfikacji określa **specyficzne lub dodatkowe wymogi**, wówczas zadania w ramach tego programu mogą wykonywać jedynie jednostki oceniające zgodność wyznaczone przez krajowy organ ds. certyfikacji cyberbezpieczeństwa, jako spełniające te wymogi.

Krajowe programy certyfikacji i certyfikaty cyberbezpieczeństwa

Cybersecurity Act wpłynie na już funkcjonujące w niektórych państwach programy certyfikacji. Nie należy się jednak obawiać, że wydane wcześniej krajowe certyfikaty nagle stracą ważność. Nawet jeśli zostały objęte nowymi europejskimi programami certyfikacji, **zachowają ważność do daty wygaśnięcia określonej w przyznanym już certyfikacie.**

Jeśli zaś chodzi o krajowe programy certyfikacji cyberbezpieczeństwa, które **zostaną objęte** europejskimi programami certyfikacji, **to przestaną one wywoływać skutki** od daty ustalonej w akcie wykonawczym. Jeśli jednak **nie zostały objęte** europejskim programem certyfikacji, nadal **mogą funkcjonować.**

Państwa członkowskie nie wprowadzają nowych krajowych programów certyfikacji cyberbezpieczeństwa dla produktów, procesów i usług ICT, które zostały już objęte europejskim programem certyfikacji.

Żeby uniknąć rozdrobnienia rynku wewnętrznego, państwa członkowskie informują Komisję i EGCC o planach opracowania nowych krajowych programów certyfikacji.

[8] Wymogi określa załącznik do Rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Tekst mający znaczenie dla EOG)

Powiadamianie, kary, skargi i środki sądowe

Powiadomienie

Po przyjęciu każdego europejskiego programu certyfikacji cyberbezpieczeństwa, krajowe organy ds. certyfikacji **powiadamiają Komisję o akredytowanych jednostkach oceniających zgodność** oraz o wszelkich późniejszych zmianach w tym zakresie.

Rok po wejściu w życie europejskiego programu certyfikacji cyberbezpieczeństwa, **Komisja publikuje wykaz notyfikowanych jednostek oceniających zgodność** w Dzienniku Urzędowym UE. Krajowy organ ds. certyfikacji cyberbezpieczeństwa może wnioskować do KE o usunięcie z wykazu jednostki notyfikowanej przez dane państwo członkowskie. Komisja publikuje odpowiednie zmiany w ciągu miesiąca od otrzymania wniosku.

Komisja Europejska może w aktach wykonawczych określić okoliczności, formaty i procedury przekazywania powiadomień.

Prawo do złożenia skargi

Osoby fizyczne lub prawne mają prawo złożyć skargę do wystawcy certyfikatu lub, jeśli certyfikat wydała jednostka oceniając a zgodność, do odpowiedniego krajowego organu ds. certyfikacji cyberbezpieczeństwa.

Organ, w którym została złożona skarga , informuje skarżącego o przebiegu postępowania i podjętej decyzji, w tym o możliwości sądowego środka odwoławczego.

Prawo do skutecznego środka sądowego

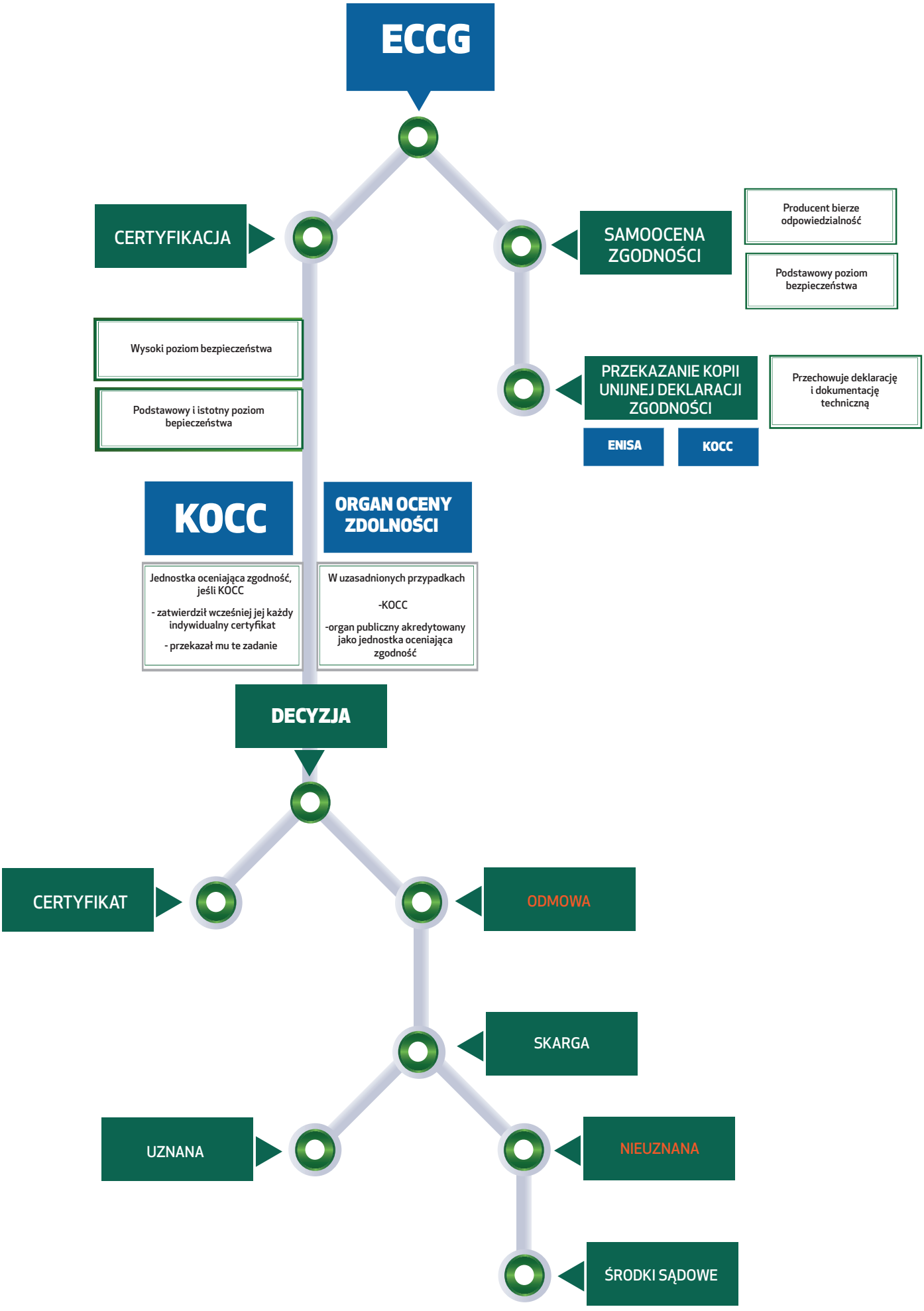
Niezależnie od administracyjnych lub innych pozasądowych środków odwoławczych, osoby fizyczne i prawne mają prawo do skutecznego środka sądowego w odniesieniu do:

- **decyzji organu**, która dotyczy wydania, niewydania bądź uznania europejskiego certyfikatu cyberbezpieczeństwa posiadanego przez te osoby fizyczne i prawne;
- **zaniechania rozpatrzenia skargi** wniesionej do organu.

Postępowania będą prowadzone przez sądy państwa członkowskiego, w którym znajduje się organ będący przedmiotem danego postępowania.

Kary

Państwa członkowskie ustanawiają zasady dotyczące sankcji w przypadku naruszeń przepisów rozporządzenia i europejskich programów certyfikacji cyberbezpieczeństwa. Podejmują też wszelkie niezbędne środki, żeby zapewnić ich wdrożenie. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie powiadamiają Komisję o tych zasadach i środkach oraz o wszelkich późniejszych zmianach



Rys 2. Uzyskanie certyfikatu cyberbezpieczeństwa.

Podsumowanie

Część 1

1. Wraz z Cybersecurity Act ENISA **otrzymała nowy, permanentny mandat** i zmieniła swoją nazwę **na Agencja UE ds. Cyberbezpieczeństwa**.

2. Cybersecurity Act **wzmacnia rolę ENISA** w zakresie współpracy z państwami członkowskimi, zespołami CERT i CERT-EU, służbami i organami nadzorującymi ochronę prywatności. W ramach współpracy ENISA monitoruje stan cyberbezpieczeństwa EU i przygotowuje raport z uwzględnieniem zgłoszeń naruszenia bezpieczeństwa ze wszystkich państw członkowskich.

3. W dokumencie szczegółowo opisano zadania ENISA. Nowym obszarem odpowiedzialności jest **wspieranie i promowanie wdrożenia certyfikacji produktów,** usług i procesów ICT. Do ENISA należy przygotowanie propozycji programu certyfikacji, który następnie przekazuje do KE.

4. ENISA przewodniczy również Grupie Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa. Grupa zajmuje się doradztwem KE w kwestiach strategicznych dot. certyfikacji.

5. Agencją zarządza Dyrektor Wykonawczy, który odpowiada przed Zarządem. W ramach ENISA funkcjonuje także Rada Wykonawcza, Grupa Doradcza ENISA (ENISA Advisory Group) i Sieć Krajowych Urzędników Łącznikowych.

Część 2

6. Wprowadzenie **dobrowolnej certyfikacji** produktów, usług i procesów ICT.

7. Możliwość wprowadzenia **obowiązkowej certyfikacji** dla wybranych produktów, usług i procesów ICT.

8. Określenie **trzech poziomów bezpieczeństwa** dla certyfikowanych usług, produktów i procesów ICT: podstawowy, istotny i wysoki.

9. Obowiązek powołania przez państwa członkowskie **krajowych organów ds. certyfikacji cyberbezpieczeństwa.**

10. Ustanowienie Europejskiej Grupy Certyfikacji Cyberbezpieczeństwa.

11. Rozporządzenie wymaga zmian prawnych w Polsce (np. w Ustawie o krajowym systemie cyberbezpieczeństwa).