



NEWSLETTER

PAŹDZIERNIK/LISTOPAD 2025



NCC-PL
Krajowe Centrum Kompetencji
Cyberbezpieczeństwa



**Ministerstwo
Cyfryzacji**



ECCC 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



**Co-funded by
the European Union**

Szanowni Państwo,

Wdrażanie unijnych regulacji oraz budowanie odporności rynku to tematy przewodnie tego wydania. Relacjonujemy konferencję w Bukareszcie poświęconą CRA oraz szczyt w Kopenhadze, który wyznaczył strategiczne kierunki bezpieczeństwa w ramach duńskiej prezydencji. Wnioski z europejskich spotkań uzupełniamy relacją z Digital Skills Summit w Gdańsku, gdzie analizowaliśmy gotowość MŚP na wyzwania dyrektywy NIS2 i AI Act.

Wracamy również do tematu kondycji rodzimego rynku - nasz raport „Mapa MŚP sektora cyberbezpieczeństwa w Polsce” diagnozuje bariery finansowe i potrzeby polskich firm. Mamy też dobre wiadomości dla innowatorów: informujemy o nowych naborach w ramach Programu Cyfrowa Europa z budżetem 50 mln euro oraz o ustaleniach ze spotkania Rady Zarządzającej ECCC w Hiszpanii.

W dalszej części przybliżamy projekt ASCLEPIUS, wzmacniający cyberbezpieczeństwo w ochronie zdrowia.

Zespół NCC-PL



 <http://www.gov.pl/web/cyber-nccpl>

 ncc@cyfra.gov.pl

Spis treści

Digital Skills Summit: Czy MŚP są gotowe na NIS2 i AI Act?	5
Konferencja Cyberbezpieczeństwa w ramach Duńskiej Prezydencji w Radzie UE	6
Raport: Mapa MŚP sektora cyberbezpieczeństwa w Polsce	7
14. spotkanie Rady Zarządzającej ECCC.....	8
Nabory dla projektów cyberbezpieczeństwa - DEP	9
Projekt ASCLEPIUS: Wzmocnienie cyberbezpieczeństwa w sektorze ochrony zdrowia	10

 <http://www.gov.pl/web/cyber-nccpl>

 ncc@cyfra.gov.pl

Konferencja CRA - Making the EU Market Resilient

8 października 2025 roku w Bukareszcie odbyła się konferencja [*CRA - Making the EU Market Resilient*](#), zorganizowana przez Europejską Agencję ds. Cyberbezpieczeństwa (ENISA) we współpracy z Europejskim Centrum Kompetencji Cyberbezpieczeństwa (ECCC) oraz rumuńskim Dyrektoriatem ds. Cyberbezpieczeństwa (DNSC). W wydarzeniu wzięła udział przedstawicielka NCC-PL, która miała okazję nawiązać cenne kontakty i wymienić się doświadczeniami z ekspertami z różnych krajów europejskich.

Głównym celem spotkania było przygotowanie rynku do wyzwań związanych z Cyber Resilience Act (CRA), budowanie świadomości biznesu (zwłaszcza MŚP) oraz integracja środowiska ekspertów i nadzoru. Przypomniano, że akt ten, który wszedł w życie 10 grudnia 2024 roku, wprowadza obligatoryjne wymagania cyberbezpieczeństwa dla produktów cyfrowych, obowiązujące przez cały cykl ich życia.

Podczas dyskusji omówiono kluczowe aspekty wdrożeniowe, w tym rolę ENISA w tworzeniu [*Single Reporting Platform*](#) (SRP) - narzędzia do zgłaszania podatności przez producentów. Przedstawiono również priorytety Komisji Europejskiej dotyczące standardów przemysłowych, certyfikacji oraz nadchodzących wytycznych dla oprogramowania. Ważnym punktem było zaprezentowanie wsparcia dla MŚP z sektora cyberbezpieczeństwa poprzez projekty z Programu Cyfrowa Europa, takie jak [*CRACY*](#), [*CONFIRMATE*](#), [*OSCRAT*](#), [*SECURE*](#) czy [*CYBERFORT*](#), które mają ułatwić firmom adaptację do nowych wymogów.

Wnioski z konferencji wskazują, że choć CRA formalnie obowiązuje, proces jego operacjonalizacji wciąż trwa. Wiele niezbędnych narzędzi, takich jak platforma SRP czy szczegółowe wytyczne interpretacyjne, znajduje się w fazie konstrukcji. Udział w wydarzeniu pozwolił na zacieśnienie współpracy z europejskimi partnerami i lepsze zrozumienie wyzwań stojących przed rynkiem UE.

 <http://www.gov.pl/web/cyber-nccpl>

 ncc@cyfra.gov.pl

Digital Skills Summit: Czy MŚP są gotowe na NIS2 i AI Act?

Za nami Digital Skills Summit w Gdańsku! Nasza ekspertka, Agata Żydanowicz-Błach, uczestniczyła w panelu „Regulacje prawne jako motor zmiany”. Razem z przedstawicielami wymiaru sprawiedliwości, biznesu i nauki szukaliśmy odpowiedzi na pytania o realny wpływ aktów takich jak NIS2 czy AI Act na polski rynek.

Jakie są kluczowe wnioski z całej dyskusji?

- **Głos MŚP:** Przedstawione przez nas wyniki badań (na grupie ponad 400 firm) pokazują, że polscy przedsiębiorcy są świadomi nadchodzących zmian. Główną obawą pozostają jednak koszty budowania zespołów compliance oraz ryzyko, że skomplikowane procesy certyfikacji będą faworyzować największych graczy rynkowych.
- **Bariery systemowe a AI:** Ważnym wątkiem debaty, poruszonym przez przedstawicieli wymiaru sprawiedliwości i nauki, był stan cyfryzacji danych publicznych. Zgodziliśmy się, że skuteczne wdrażanie sztucznej inteligencji w wymiarze sprawiedliwości jest utrudnione przez brak dostępu do ustrukturyzowanych danych (np. wciąż papierowe akta sądowe). To wyzwanie, które musimy pokonać jako państwo.
- **Nowe zawody:** Regulacje to nie tylko obowiązki, ale też silny impuls rozwojowy. Tak jak RODO stworzyło rynek dla Inspektorów Ochrony Danych, tak nowe przepisy kreują zapotrzebowanie na zupełnie nowe role, w tym "AI Officerów" dbających o etykę i zgodność algorytmów.

Dziękujemy moderatorowi i współpanelistom za merytoryczną wymianę zdań. Jeżeli są Państwo zainteresowani przebiegiem panelu to jego nagranie znajduje się [tutaj](#).

 <http://www.gov.pl/web/cyber-nccpl>

 ncc@cyfra.gov.pl

Konferencja Cyberbezpieczeństwa w ramach Duńskiej Prezydencji w Radzie UE

27 listopada 2025 roku w Kopenhadze odbyła się kluczowa konferencja zorganizowana przez Duńską Agencję ds. Bezpieczeństwa Dostaw i Gotowości. Wydarzenie zgromadziło około 250 wysokich rangą przedstawicieli instytucji unijnych, państw członkowskich oraz sektora prywatnego, stanowiąc platformę do dyskusji na temat strategicznych kierunków cyfrowego bezpieczeństwa Europy.

Konferencję otworzył Torsten Schack Pedersen, duński Minister ds. Bezpieczeństwa Społecznego i Gotowości Kryzysowej, a moderatorem dyskusji był Jakob Ellemann-Jensen, były wicepremier Danii. Wiodącymi tematami spotkania były:

- wzmacnianie odporności na zagrożenia hybrydowe,
- zacieśnianie współpracy publiczno-prywatnej,
- efektywna implementacja unijnych ram prawnych (w tym wspomnianego wcześniej aktu CRA).

Szczególną uwagę poświęcono zagadnieniom suwerenności cyfrowej oraz rozwojowi zaufanych technologii jako fundamentu demokratycznych wartości w przestrzeni cyfrowej.

Wnioski z konferencji w Kopenhadze są spójne z priorytetami ECCC - kluczem do bezpiecznej Europy jest nie tylko legislacja, ale przede wszystkim praktyczna, międzysektorowa współpraca oraz inwestycje w bezpieczną infrastrukturę.

 <http://www.gov.pl/web/cyber-nccpl>

 ncc@cyfra.gov.pl

Raport: Mapa MŚP sektora cyberbezpieczeństwa w Polsce

Pod koniec września 2025 r. opublikowaliśmy raport *Mapa MŚP sektora cyberbezpieczeństwa w Polsce*. Jego fundamentem jest nowatorska metodologia łącząca analizę danych zastanych (desk research na próbie ponad 400 podmiotów) z pogłębionym badaniem rynku. W procesie badawczym wykorzystano 3 różne metody badawcze: badanie ilościowe na grupie 197 firm, 20 wywiadów pogłębionych (IDI) oraz 2 panele eksperckie z liderami branży.

Raport pokazuje, że małe i średnie przedsiębiorstwa w bardzo niewielkim zakresie korzystają z finansowania publicznego krajowego i zagranicznego. Badanie ujawniło istotne bariery rozwoju: niską świadomość rynku, trudności sprzedaży rozwiązań niewidocznych dla użytkownika, brak systemowego wsparcia ekspansji zagranicznej oraz dominację globalnych marek. Dodatkowe wyzwania to braki kadrowe, niedobór kompetencji sprzedażowych, niski poziom współpracy branżowej i nieprzejrzyste otoczenie prawno-podatkowe.

Polski sektor cyberbezpieczeństwa wykazuje silną orientację na rynki zagraniczne. Z danych wynika, że 16% MŚP z sektora cyberbezpieczeństwa prowadzi działalność równolegle w kraju i za granicą, a istotna grupa - 10% małych i aż 35% średnich przedsiębiorstw - operuje wyłącznie poza Polską. W obliczu takiej skali działalności eksportowej, firmy szczególnie mocno akcentują potrzebę wsparcia w zakresie innowacji, wejścia na nowe rynki oraz ułatwień w dostępie do zamówień publicznych.

Zachęcamy do zapoznania się z pełnym raportem (do pobrania [tutaj](#)), który zawiera szczegółowe analizy, rekomendacje oraz praktyczne wskazówki dla przedsiębiorców i instytucji wspierających rozwój sektora cyberbezpieczeństwa w Polsce.

 <http://www.gov.pl/web/cyber-nccpl>

 ncc@cyfra.gov.pl

14. spotkanie Rady Zarządzającej ECCC

W dniach 15-16 października w León w Hiszpanii odbyło się 14. Spotkanie Rady Zarządzającej ECCC, w którym udział wzięła przedstawicielka NCC-PL. W trakcie dwudniowej sesji omówiono strategiczne i operacyjne priorytety ECCC, w tym aktualizacje dotyczące realizacji Programu Cyfrowa Europa oraz Programu Horyzont Europa, rozwój społeczności cyberbezpieczeństwa oraz przygotowania do kolejnej perspektywy finansowej ([MFF 2028-2034](#)). Omówiono także rolę ECCC we wzmocnieniu konkurencyjności europejskiego sektora cyberbezpieczeństwa.

Spotkanie obejmowało również wymianę doświadczeń z dyrektorem Agencji Cyberbezpieczeństwa w Mołdawii, Mihailem Lupascu, dotyczącą najnowszych rozwiązań i wyzwań w obszarze cyberbezpieczeństwa. Kolejne spotkanie odbędzie się w marcu 2026 roku w Bukareszcie.



 <http://www.gov.pl/web/cyber-nccpl>

 ncc@cyfra.gov.pl

Nabory dla projektów cyberbezpieczeństwa - DEP

Europejskie Centrum Kompetencji Cyberbezpieczeństwa ogłosiło cztery nowe nabory projektów w ramach Programu Cyfrowa Europa, skierowane na rozwój i wdrażanie innowacyjnych rozwiązań z zakresu cyberbezpieczeństwa. Łączny budżet dostępnych środków to około 50 mln €, a nabory trwają od 28 października 2025 do 31 marca 2026 roku.

Główne obszary tematyczne naborów

- [Wdrożenie innowacyjnych rozwiązań cyberbezpieczeństwa dla MŚP](#)
Konkurs ma na celu wsparcie MŚP w spełnieniu wymagań regulacyjnych, takich jak CRA czy dyrektywa NIS2, poprzez opracowanie i wdrożenie narzędzi, platform, infolinii czy modułów szkoleniowych. Dofinansowanie do 3 mln euro, przy 75% wsparcia dla MŚP i 50% dla innych podmiotów.
- [Rozwiązania cyberbezpieczeństwa oparte na sztucznej inteligencji](#)
Wykrywanie zagrożeń, reagowanie, analiza i udostępnianie danych. Dofinansowanie od 3 do 5 mln euro, przy 50% wsparcia ze środków UE.
- [Koordynowane testy gotowości i działania przygotowawcze](#)
Wsparcie dla kluczowych sektorów, takich jak zdrowie czy infrastruktura cyfrowa, poprzez testy gotowości, penetracyjne i oceny ryzyka. Dofinansowanie do 1,5 mln euro, przy 50% wsparcia ze środków UE.
- [Regionalne Huby Kabli Podmorskich](#)
Usprawnienie wykrywania zagrożeń i wzmocnienie bezpieczeństwa operacyjnego wokół kabli podmorskich. Dofinansowanie do 3 mln euro, przy 70% wsparcia ze środków UE.

 <http://www.gov.pl/web/cyber-nccpl>

 ncc@cyfra.gov.pl

Projekt ASCLEPIUS: Wzmocnienie cyberbezpieczeństwa w sektorze ochrony zdrowia

Projekt ASCLEPIUS, realizowany przez IS Consulting w ramach Programu Cyfrowa Europa, ma na celu wdrożenie nowoczesnych rozwiązań cyberbezpieczeństwa w sektorze ochrony zdrowia. Projekt, współfinansowany ze środków Programu Cyfrowa Europa, ma na celu zwiększenie odporności instytucji medycznych na cyberzagrożenia oraz wspieranie spełniania wymogów dyrektywy NIS2.

ASCLEPIUS skupia się na budowie kompetencji w dziedzinie cyberbezpieczeństwa wśród pracowników służby zdrowia, organizacji szkoleń i warsztatów oraz wdrażaniu narzędzi wspierających bezpieczeństwo danych pacjentów. W ramach projektu uczestniczą zarówno placówki medyczne, jak i firmy technologiczne, które wspólnie tworzą innowacyjne rozwiązania dostosowane do specyfiki sektora zdrowia.



Projekt ASCLEPIUS to inicjatywa o znaczeniu europejskim - jej efekty będą wykorzystywane przez różne kraje UE, a polskie doświadczenie w tym obszarze może stać się inspiracją dla innych. ASCLEPIUS pokazuje, jak współpraca między administracją, biznesem i instytucjami medycznymi może przyczynić się do zwiększenia bezpieczeństwa cyfrowego w kluczowym sektorze.

Zachęcamy do śledzenia rozwoju projektu. IS Consulting, firma w ramach której realizowany jest ASCLEPIUS, jest członkiem Spółeczności Kompetentnej NCC-PL, zrzeszającej firmy posiadające wiedzę fachową w dziedzinie cyberbezpieczeństwa.

 <http://www.gov.pl/web/cyber-nccpl>

 ncc@cyfra.gov.pl