AGENCJA UNII EUROPEJSKIEJ DS. CYBERBEZPIECZEŃSTWA

EUROPA – ZAUFANIE I CYBERBEZPIECZEŃSTWO

Strategia ENISA

Czerwiec 2020 r.

EUROPA – ZAUFANIE I CYBERBEZPIECZEŃSTWO

AGENCJA UNII EUROPEJSKIEJ DS. CYBERBEZPIECZEŃSTWA

PRZEDMOWA

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) od ponad 15 lat odgrywa kluczową rolę w dążeniu UE do zwiększania wiarygodności i bezpieczeństwa technologii cyfrowych w całej Europie, z uwzględnieniem państw członkowskich oraz instytucji i agencji UE. Przez integrację wspólnot ENISA skutecznie przyczyniła się do wzmocnienia zdolności Europy w zakresie gotowości i reagowania na cyberincydenty.

Jednocześnie bardzo nasiliła się cyfryzacja naszej gospodarki i społeczeństwa, co było widoczne w czasie kryzysu COVID-19, gdy zbiorowe, masowe użycie rozwiązań informatycznych miało zasadnicze znaczenie dla podtrzymania aktywności w wielu obszarach. Kryzys ten uwidocznił, w jakim stopniu sprawcy cyberataków wykorzystują naszą zależność od wspomnianych technologii. Ujawnił też, jak rozszerzyła się przestrzeń zagrożeń dla cyberbezpieczeństwa: obejmuje ona już nie tylko ataki skierowane na konkretne cele, ale także nowe formy masowego zagrożenia dla milionów przedsiębiorstw i użytkowników, w tym rosnącą liczbę wyrafinowanych incydentów z użyciem oprogramowania typu ransomware. Gwałtowny rozwój produktów i usług cyfrowych, od usług w chmurze i wideokonferencji po technologię 5G i sztuczną inteligencję, również doprowadził do nowych wyzwań, które należy zauważać i uwzględniać.

ENISA, mająca stały mandat oraz rozszerzone zadania i zdolności, będzie odgrywać wiodącą rolę – w jeszcze większym stopniu niż dotychczas – we wspieraniu UE i jej państw członkowskich borykających się z pojawiającymi się wyzwaniami, w czasach wchodzenia w nową erę cyberbezpieczeństwa w Europie.

W tym celu ENISA będzie pracować nad przewidywaniem istotnych tendencji oraz pozyskiwać i powszechnie udostępniać najnowszą wiedzę fachową. Będzie wspierać Komisję Europejską i państwa członkowskie w pomaganiu podmiotom publicznym i prywatnym oraz ogółowi społeczeństwa w przeciwdziałaniu zagrożeniom związanym z cyberincydentami i zarządzaniu takimi zagrożeniami. Dzięki wdrożeniu systemu certyfikacji cyberbezpieczeństwa ENISA przyczyni się do zmiany wzorców przez podniesienie poziomu bezpieczeństwa rozwiązań cyfrowych wdrażanych w Europie. Takie działania zwiększą ogólną zdolność wybierania odpowiednich rozwiązań i polegania na nich. Agencja będzie też aktywnie wspierać europejską społeczność zapewniającą cyberbezpieczeństwo przez ścisłą współpracę i przygotowanie się na wspólne reagowanie w momencie, gdy Europa stanie się celem kolejnego cyberincydentu na dużą skalę.

Wraz z podejmowaniem przez ENISA nowej roli otwartość, żywotność i wiarygodność stają się głównymi siłami napędzającymi jej codzienną działalność, a jednocześnie jej bliska współpraca z państwami członkowskimi i Komisją Europejską służy przyjmowaniu zharmonizowanego podejścia. ENISA będzie też dążyć do poprawy wpływu swoich działań na środowisko w kontekście trwającego kryzysu klimatycznego oraz do działania w społecznie odpowiedzialny sposób, oferując inkluzywne środowisko pracy.

Niniejsza strategia, opracowana przy zaangażowaniu wszystkich pracowników ENISA, członków jej zarządu oraz jej grupy doradczej w ramach procesu współpracy i sprzyjając włączeniu społecznemu, określa jasne cele, które będą przyświecać działalności ENISA w nadchodzących latach i pomagać w wielu wyzwaniach w przyszłości.

W imieniu zarządu

Jean-Baptiste Demaison
Przewodniczący zarządu

Krzysztof Silicki
Zastępca przewodniczącego zarządu

WIZJA

Europa
– zaufanie i bezpieczeństwo

MISJA

Misja Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) – osiągnięcie wysokiego poziomu cyberbezpieczeństwa w całej Unii we współpracy z szerokim gronem zainteresowanych stron. ENISA realizuje ten cel przez pełnienie funkcji centrum wiedzy fachowej dotyczącej cyberbezpieczeństwa, gromadząc i przekazując niezależne i jakościowe porady i wsparcie techniczne w zakresie cyberbezpieczeństwa na rzecz państw członkowskich i organów UE. Wnosi wkład w tworzenie i wdrażanie unijnej polityki cyberbezpieczeństwa.

Dążymy do podniesienia zaufania do połączonej gospodarki, zwiększenia odporności i wiarygodności infrastruktury i usług w Unii oraz zapewnienia cyfrowego bezpieczeństwa naszego społeczeństwa i obywateli. Chcemy być energiczną organizacją, która czuje się odpowiedzialna za środowisko i społeczeństwo oraz skupia się na ludziach.

WARTOŚCI

Nastawienie społecznościowe
Aby w jak największym stopniu realizować swoją misję, ENISA pracuje ze społecznościami, respektuje ich kompetencje i wiedzę fachową oraz wspiera efekty synergii i zaufanie.

Doskonałość
W swojej działalności ENISA chce wykorzystywać najnowszą wiedzę fachową, utrzymuje najwyższej jakości standardy działania oraz prowadzi ocenę swojej efektywności w celu dążenia do ciągłej poprawy przez innowacje i dalekosiężną perspektywę.

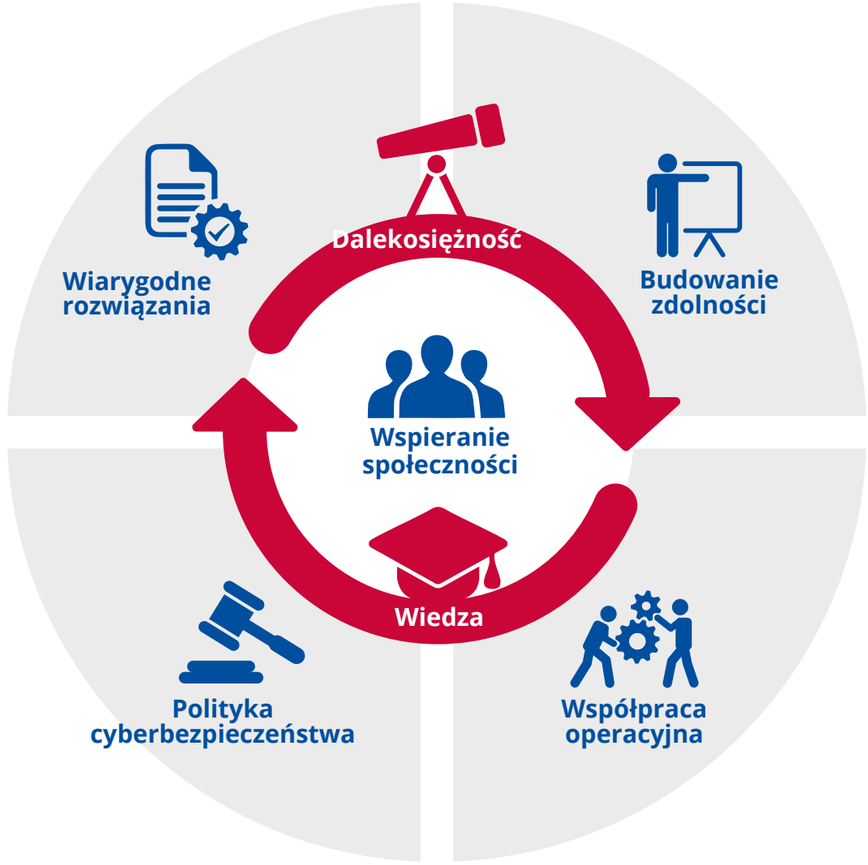
Uczciwość/etyka
ENISA stosuje zasady etyczne oraz odpowiednie unijne przepisy i zobowiązania w ramach swoich usług i w środowisku pracy, zapewniając sprawiedliwość i włączenie społeczne.

Szacunek
ENISA respektuje prawa podstawowe i wartości europejskie w odniesieniu do wszystkich swoich usług i środowiska pracy, a także oczekiwania zainteresowanych stron.

Odpowiedzialność
ENISA podejmuje odpowiedzialność, a tym samym łączy społeczne i środowiskowe wymiary w swoich działaniach i procedurach.

Przejrzystość
ENISA stosuje procedury, struktury i procesy, które są otwarte, rzeczowe i niezależne, a przez to ogranicza stronniczość, dwuznaczność, nadużycia i niezrozumiałość.

CELE STRATEGICZNE



CS1

Cel strategiczny

MOCNA POZYCJA I ZAANGAŻOWANIE SPOŁECZNOŚCI W CAŁYM EKOSYSTEMIE CYBERBEZPIECZEŃSTWA

Kontekst

Cyberbezpieczeństwo jest wspólnym zadaniem. Europa dąży do osiągnięcia przekrojowych i kompleksowych ram współpracy. ENISA odgrywa kluczową rolę z pobudzaniu aktywnej współpracy między podmiotami zapewniającymi cyberbezpieczeństwo w państwach członkowskich oraz instytucjach i agencjach UE. Jej celem jest zapewnienie komplementarności wspólnych działań poprzez podnoszenie wartości dla zainteresowanych podmiotów, szukanie efektów synergii i skuteczne wykorzystywanie ograniczonych informacji i zasobów w zakresie cyberbezpieczeństwa. Społeczności powinny mieć mocniejszą pozycję, aby rozszerzać stosowanie modelu cyberbezpieczeństwa.

Docelowe rezultaty:

- Ogólnounijny, nowoczesny korpus wiedzy na temat koncepcji i praktyk cyberbezpieczeństwa, służący współpracy wśród najważniejszych podmiotów zajmujących się tą dziedziną, zdobywaniu doświadczeń i unijnej wiedzy eksperckiej, a także sprzyjający tworzeniu nowych efektów synergii;
- Mocny ekosystem cyberbezpieczeństwa obejmujący władze państw członkowskich, unijne instytucje, agencje, organy, stowarzyszenia, ośrodki badawcze, a także uczelnie, przemysł, podmioty prywatne i społeczeństwo, przy czym wszystkie te podmioty mają pełnić swoją rolę w zapewnianiu cyberbezpieczeństwa w Europie.

CS2

Cel strategiczny

CYBERBEZPIECZEŃSTWO JAKO INTEGRALNA CZĘŚĆ POLITYKI UE

Kontekst

Cyberbezpieczeństwo jest fundamentem transformacji cyfrowej i jest powszechnie potrzebne we wszystkich sektorach, a zatem należy je uwzględniać w różnorodnych obszarach polityki i inicjatywach. Cyberbezpieczeństwa nie można ograniczać do wyspecjalizowanej społeczności technicznych ekspertów w tym zakresie. Musi ono zatem być nieodłączną częścią wszystkich obszarów polityki UE. Zasadnicze znaczenie ma unikanie rozdrobnienia oraz spójne podejście, przy jednoczesnym uwzględnieniu specyfiki poszczególnych sektorów.

Docelowe rezultaty:

- Aktywne doradztwo i wsparcie dla wszystkich odpowiednich podmiotów na szczeblu UE, przy uwzględnieniu cyberbezpieczeństwa w cyklu tworzenia polityki poprzez solidne i ukierunkowane wytyczne techniczne;
- Ramy zarządzania ryzykiem związanym z cyberbezpieczeństwem wykorzystywane we wszystkich sektorach i w całym cyklu polityki cyberbezpieczeństwa.

CS3

Cel strategiczny

SKUTECZNA WSPÓŁPRACA MIĘDZY PODMIOTAMI OPERACYJNYMI W UNII W PRZYPADKU CYBERINCYDENTÓW NA MASOWĄ SKALĘ

Kontekst

Osiągnięcie pełnych korzyści wynikających z gospodarki cyfrowej i społeczeństwa cyfrowego w Europie jest możliwe jedynie na bazie cyberbezpieczeństwa. Cyberataki nie mają granic. Mogą być wymierzone we wszystkie grupy społeczne, a Unia musi być przygotowana, aby reagować na zmasowane (rozległe i transgraniczne) cyberataki i kryzysy cyberbezpieczeństwa. Transgraniczne współzależności wskazują na konieczność skutecznej współpracy między państwami członkowskimi a instytucjami UE w celu szybszego reagowania i odpowiedniej koordynacji działań na wszystkich poziomach (strategicznym, operacyjnym, technicznym i komunikacyjnym).

Docelowe rezultaty:

- Stałe transgraniczne i przekrojowe wsparcie na rzecz współpracy między państwami członkowskimi oraz instytucjami UE. Szczególnie w odniesieniu do potencjalnych incydentów i kryzysów na dużą skalę należy rozszerzać zakres technicznej, operacyjnej, politycznej i strategicznej współpracy między najważniejszymi podmiotami operacyjnymi w celu terminowego reagowania, wymiany informacji, rozeznania sytuacji i komunikacji w czasie kryzysu w całej Unii;
- Kompleksowe i szybkie techniczne rozwiązania na żądanie państw członkowskich w celu zaspokajania technicznych i operacyjnych potrzeb w zarządzaniu incydentami i kryzysami.

CS4

Cel strategiczny

NOWATORSKIE KOMPETENCJE I ZDOLNOŚCI W ZAKRESIE CYBERBEZPIECZEŃSTWA W CAŁEJ UNII

Kontekst

Cyberataki szybko stają się coraz częstsze i coraz bardziej wyrafinowane, a jednocześnie gwałtownie rozpowszechnia się użycie infrastruktury informacyjno-komunikacyjnej wśród użytkowników indywidualnych, organizacji i w poszczególnych branżach. Zapotrzebowanie na wiedzę i kompetencje związane z cyberbezpieczeństwem jest większe niż ich dostępność. UE musi inwestować w budowanie kompetencji i umiejętności w obszarze cyberbezpieczeństwa na wszystkich poziomach, od laików po wysoko wykwalifikowanych specjalistów. Inwestycje te powinny się skupiać nie tylko na rozszerzaniu zestawu umiejętności związanych z cyberbezpieczeństwem w państwach członkowskich, ale również na dopilnowaniu, aby różne społeczności specjalistów operacyjnych miały odpowiednie zdolności do radzenia sobie w warunkach zagrożenia dla cyberbezpieczeństwa.

Docelowe rezultaty:

- Ujednolicone kompetencje, doświadczenia zawodowe i struktury edukacyjne w obszarze cyberbezpieczeństwa w celu sprostania stale zwiększającemu się zapotrzebowaniu na wiedzę i kompetencje w tym zakresie w UE;
- Wysoki podstawowy poziom wiedzy i kompetencji w zakresie cyberbezpieczeństwa w całej UE przy jednoczesnym wdrażaniu tych aspektów w nowych dziedzinach;
- Solidnie przygotowane i przetestowane zdolności oraz odpowiednie możliwości radzenia sobie z rozszerzającym się otoczeniem zagrożeń w całej UE.

CS5

Cel strategiczny

“

WYSOKI POZIOM ZAUFANIA DO BEZPIECZNYCH ROZWIĄZAŃ CYFROWYCH

Kontekst

Produkty i usługi cyfrowe niosą ze sobą korzyści oraz zagrożenia, a zagrożenia te należy rozpoznawać i łagodzić. W procesie oceny bezpieczeństwa rozwiązań cyfrowych i zapewnienia ich wiarygodności zasadnicze znaczenie ma przyjęcie wspólnego podejścia, a celem jest znalezienie równowagi między potrzebami społeczeństwa, rynków, gospodarki i cyberbezpieczeństwa. Neutralny podmiot działający w przejrzysty sposób przyczyni się do wzrostu zaufania klientów do rozwiązań cyfrowych i szerzej pojętego otoczenia cyfrowego.

Docelowe rezultaty:

- Bezpieczne pod względem cybernetycznym otoczenie cyfrowe w całej UE, w którym można ufać produktom, usługom i procesom informacyjno-komunikacyjnym dzięki zastosowaniu systemów certyfikacji w najważniejszych obszarach technologicznych.

CS6

Cel strategiczny

DALEKOSIĘŻNE PODEJŚCIE DO POJAWIAJĄCYCH SIĘ I PRZYSZŁYCH WYZWAŃ W ZAKRESIE CYBERBEZPIECZEŃSTWA

Kontekst

Przyjęcie perspektywicznych metod jest korzystne dla licznych nowoczesnych technologii, nadal będących w początkowych fazach rozwoju lub na etapie przed wprowadzeniem do powszechnego użytku. Dzięki usystematyzowanemu procesowi pozwalającemu na dialog między zainteresowanymi stronami decydenci mogą formułować strategie wczesnego łagodzenia ryzyka zwiększające odporność UE na zagrożenia w zakresie cyberbezpieczeństwa, a także znajdować rozwiązania w odniesieniu do nowych wyzwań.

Docelowe rezultaty:

- Rozumienie pojawiających się tendencji i wzorców dzięki przyjęciu dalekosiężnej perspektywy i analizowaniu scenariuszy na przyszłość, co przyczynia się do łagodzenia wyzwań cybernetycznych, z jakimi borykają się zainteresowane podmioty;
- Wczesna ocena wyzwań i zagrożeń po przyjęciu i dostosowaniu pojawiających się opcji na przyszłość, przy jednoczesnej współpracy z zainteresowanymi stronami w zakresie odpowiednich strategii łagodzenia ryzyka.

CS7

Cel strategiczny

“

EFEKTYWNE I SKUTECZNE ZARZĄDZANIE INFORMACJAMI I WIEDZĄ W ZAKRESIE CYBERBEZPIECZEŃSTWA W EUROPIE

Kontekst

Fundamentem cyberbezpieczeństwa są informacje i wiedza. Aby specjaliści od cyberbezpieczeństwa mogli efektywnie realizować swoje cele, działać w stale zmieniającym się – pod względem rozwiązań cyfrowych i uczestniczących podmiotów – otoczeniu oraz radzić sobie z wyzwaniami naszych czasów, potrzebny jest ciągły proces gromadzenia, organizowania, kompilowania, analizowania i przekazywania informacji i wiedzy oraz zapewniania ich cyberbezpieczeństwa. Wszystkie te etapy są istotne dla wymiany i poszerzania wiedzy i informacji w unijnym ekosystemie cyberbezpieczeństwa.

Docelowe rezultaty:

- Zarządzanie wymianą informacji i wiedzy w odniesieniu do unijnego ekosystemu cyberbezpieczeństwa w przystępnej, dopasowanej, terminowej i możliwej do stosowania formie, przy wykorzystaniu odpowiednich metod, infrastruktury i narzędzi, w połączeniu z metodami zapewnienia jakości w celu osiągania stałej poprawy usług.

INFORMACJE O ENISA

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) jest unijną agencją działającą na rzecz osiągnięcia wysokiego ogólnego poziomu cyberbezpieczeństwa w całej Europie. ENISA – utworzona w 2004 r. i wzmocniona unijnym aktem o cyberbezpieczeństwie – wnosi wkład w politykę cybernetyczną UE; podnosi wiarygodność produktów, usług i procesów informacyjno-komunikacyjnych dzięki systemom certyfikacji cyberbezpieczeństwa; współpracuje z państwami członkowskimi i organami UE; oraz pomaga przygotować Europę na przyszłe wyzwania cybernetyczne. Przez wymianę informacji, budowanie zdolności i zwiększanie wiedzy Agencja współdziała z kluczowymi zainteresowanymi stronami, aby zwiększać zaufanie do połączonej gospodarki i odporność unijnej infrastruktury oraz, ostatecznie, zapewnić cyfrowe bezpieczeństwo społeczeństwa i mieszkańców Europy. Więcej informacji na temat ENISA i jej działalności można znaleźć na stronie www.enisa.europa.eu.

TP-02-20-759-PL-N

ENISA
Agencja Unii Europejskiej ds. Cyberbezpieczeństwa

Biuro w Atenach
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Biuro w Heraklionie
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Grecja

enisa.europa.eu