Rada
Unii Europejskiej

Bruksela, 14 września 2017 r.
(OR. en)

Międzyinstytucjonalny numer referencyjny:
2017/0225 (COD)

12183/17
ADD 2

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139

PISMO PRZEWODNIE

Od:	Sekretarz Generalny Komisji Europejskiej, podpisał dyrektor Jordi AYET PUIGARNAU
Do:	Jeppe TRANHOLM-MIKKELSEN, Sekretarz Generalny Rady Unii Europejskiej
Nr dok. Kom.:	SWD(2017) 501 final
Dotyczy:	DOKUMENT ROBOCZY SŁUŻB KOMISJI STRESZCZENIE OCENY SKUTKÓW towarzyszący dokumentowi: wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY w sprawie „Agencji UE ds. Bezpieczeństwa Cybernetycznego" ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji bezpieczeństwa cybernetycznego w zakresie technologii informacyjno-komunikacyjnych („akt ws. bezpieczeństwa cybernetycznego")

Delegacje otrzymują w załączeniu dokument SWD(2017) 501 final.

Zał.: SWD(2017) 501 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 13.9.2017 r.
SWD(2017) 501 final

DOKUMENT ROBOCZY SŁUŻB KOMISJI

STRESZCZENIE OCENY SKUTKÓW

Towarzyszący dokumentowi:

wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie „Agencji UE ds. Bezpieczeństwa Cybernetycznego" ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji bezpieczeństwa cybernetycznego w zakresie technologii informacyjno-komunikacyjnych („akt ws. bezpieczeństwa cybernetycznego")

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A. ZASADNOŚĆ DZIAŁAŃ

Na czym polega problem i dlaczego jest to problem?

Technologie cyfrowe i internet stanowią filary unijnej gospodarki i społeczeństwa. Sektory gospodarki o znaczeniu krytycznym, takie jak transport, energetyka, ochrona zdrowia i finanse, stały się coraz bardziej uzależnione w prowadzeniu swojej podstawowej działalności od sieci i systemów informatycznych. Internet rzeczy łączy ludzi i przedmioty za pośrednictwem sieci komunikacyjnych. Ta nowa rzeczywistość otwiera niespotykane dotąd możliwości, ale stwarza też zagrożenia. Nasila się zjawisko incydentów cybernetycznych. Ich złożoność, częstotliwość i zasięg ich oddziaływania – od dostępu do podstawowych usług po procesy demokratyczne – cały czas narastają.

W związku z tym wskazano następujące powiązane ze sobą problemy:

- rozdrobnienie działań politycznych i podejścia do kwestii bezpieczeństwa cybernetycznego w różnych państwach członkowskich;
- rozproszone zasoby i podejścia do bezpieczeństwa cybernetycznego w instytucjach, agencjach i organach UE;
- niewystarczający poziom świadomości i wiedzy na temat zagrożeń cybernetycznych i niewystarczające informacje dotyczące właściwości w zakresie bezpieczeństwa nabywanych produktów i usług ICT u obywateli i przedsiębiorstw, w połączeniu z narastającym pojawianiem się wielu krajowych i sektorowych systemów certyfikacji.

Problemy te wywołują skutki dla ogólnej odporności cybernetycznej UE i skutecznego funkcjonowania rynku wewnętrznego.

Co należy osiągnąć?

Określono następujące szczegółowe cele strategiczne w ramach tej inicjatywy:

1. zwiększenie potencjału i gotowości do reagowania państw członkowskich i przedsiębiorstw, zwłaszcza w zakresie infrastruktury krytycznej;
2. poprawa współpracy i koordynacji między państwami członkowskimi oraz instytucjami, agencjami i organami UE;
3. zwiększenie zdolności do uzupełniania działań państw członkowskich na szczeblu UE, zwłaszcza w przypadku transgranicznych kryzysów cybernetycznych;
4. podniesienie poziomu świadomości obywateli i przedsiębiorstw w kwestiach bezpieczeństwa cybernetycznego;
5. zwiększanie ogólnej przejrzystości zapewniania bezpieczeństwa cybernetycznego produktów i usług ICT w celu wzmocnienia zaufania do jednolitego rynku cyfrowego i innowacji cyfrowych;
6. unikanie rozdrobnienia systemów certyfikacji w UE oraz powiązanych wymogów w zakresie bezpieczeństwa i kryteriów oceny we wszystkich państwach członkowskich i sektorach.

Na czym polega wartość dodana podjęcia działań na poziomie UE?

Ponieważ cyfryzacja i wzajemne powiązanie gospodarki i społeczeństwa mają zasięg ogólnoświatowy, wymiary problemu wykraczają poza terytoria pojedynczych państw członkowskich. Wymaga to zatem interwencji na szczeblu unijnym. W obecnej sytuacji i biorąc pod uwagę przyszłe scenariusze, wydaje się, że indywidualne działania podejmowane przez państwa członkowskie i rozproszone podejście do bezpieczeństwa cybernetycznego, zwłaszcza wobec jego wyraźnego wymiaru transgranicznego, nie poprawią wspólnej odporności Unii na zagrożenia cybernetyczne.

B. ROZWIĄZANIA

Jakie są różne warianty działań służących osiągnięciu celów? Czy wskazano preferowany wariant?

W ocenie skutków analizuje się konkretny zestaw wariantów działań politycznych, obejmujących przegląd Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz certyfikację bezpieczeństwa cybernetycznego.

Przegląd ENISA

Wariant 0 – **Scenariusz odniesienia** – Ten wariant utrzymuje stan obecny. Mandat ENISA zostanie przedłużony, a cele i zadania Agencji pozostają zasadniczo niezmienione, przy jednoczesnym uwzględnianiu zadania powierzonych ENISA w kolejnych unijnych aktach prawnych (np. w dyrektywie w sprawie bezpieczeństwa sieci i informacji).

Wariant 1 – **Wygaśnięcie mandatu ENISA** (zakończenie działalności przez ENISA). Wariant ten doprowadziłby do zakończenia działalności ENISA z końcem jej mandatu (czerwiec 2020 r.) i ewentualnie do redystrybucji kompetencji/działań na szczeblu unijnym lub krajowym.

Wariant 2 - **„Zreformowana ENISA”**. Ten wariant byłby oparty na obecnym mandacie ENISA z zamiarem przyjęcia wybiórczych zmian, uwzględniających zmiany w krajobrazie bezpieczeństwa cybernetycznego. Agencja uzyskałaby stały mandat, oparty na następujących elementach podstawowych: wspieranie procesu opracowywania i wdrażania unijnej polityki; budowanie zdolności; wiedza i informacje; zadania związane z rynkiem; badania i innowacje; oraz współpraca operacyjna i zarządzanie kryzysowe.

Wariant 3 – **Agencja UE ds. Bezpieczeństwa Cybernetycznego z pełnym potencjałem operacyjnym**. Wariant ten zakłada reformę ENISA polegającą na połączeniu trzech głównych funkcji: 1. funkcji politycznej/doradczej; 2. ośrodka informacji i wiedzy fachowej, oraz 3. zespołu reagowania na incydenty komputerowe (CERT). Wariant ten pociąga za sobą w znacznym zakresie taką samą zmianę zakresu mandatu jak w wariancie 2. Zostałyby jednak dodane dodatkowe zadania w zakresie reagowania na incydenty cybernetyczne i zarządzania kryzysowego, tak aby Agencja mogła objąć cały cykl życia bezpieczeństwa cybernetycznego i zajmować się zapobieganiem incydentom cybernetycznym, ich wykrywaniem i reagowaniem na nie.

Certyfikacja

Wariant 0 – Scenariusz odniesienia – Niepodejmowanie działań. W tym wariancie Komisja utrzymałaby stan obecny i nie podejmowała żadnych działań politycznych lub legislacyjnych.

Wariant 1 – Środki nielegislacyjne („prawo miękkie"). W tym wariancie Komisja zastosowałaby miękkie instrumenty polityczne (np. komunikaty interpretacyjne, wsparcie inicjatyw samoregulacyjnych i działań normalizacyjnych o zasięgu ogólnounijnym) w celu poprawy przejrzystości i zmniejszenia fragmentacji.

Wariant 2 – Unijny akt ustawodawczy o rozszerzeniu umowy SOG-IS na wszystkie państwa członkowskie. W tym wariancie Komisja przedłożyłaby wniosek dotyczący aktu ustawodawczego, aby z mocy prawa rozszerzyć członkostwo w SOG-IS na wszystkie państwa członkowskie.

Wariant 3 – unijne ogólne ramy certyfikacji bezpieczeństwa cybernetycznego w odniesieniu do ICT. Ten wariant zakłada ustanowienie europejskich ram certyfikacji bezpieczeństwa cybernetycznego produktów i usług ICT (w tym powołanie grupy ekspertów wywodzących się z organów krajowych) w oparciu w możliwie jak największym wymiarze o istniejące systemy certyfikacji bezpieczeństwa cybernetycznego. Zasadniczo ramy umożliwiłyby utworzenie unijnych systemów certyfikacji, przyjmowanych we wszystkich państwach członkowskich.

Wariantem preferowanym jest połączenie rozwiązań wariantu 2 w odniesieniu do ENISA i wariantu 3 w zakresie certyfikacji.

Kto należy do zainteresowanych stron? Jak kształtuje się poparcie dla poszczególnych wariantów?

Przeważająca większość zainteresowanych stron we wszystkich kategoriach (państwa członkowskie, przemysł, instytucje unijne, społeczność badawcza), które wzięły udział w konsultacjach, z zadowoleniem przyjęła wariant preferowany, gdyż opowiadają się za wzmocnieniem ENISA oraz stworzeniem europejskich ram certyfikacji bezpieczeństwa cybernetycznego.

W szczególności istnieje zgoda co do potrzeby posiadania (jako niezbędnego minimum) dobrze funkcjonującej agencji UE wyposażonej w stały mandat, dysponującej odpowiednimi zasobami i upoważnionej do stawienia czoła obecnym i przyszłym wyzwaniom w zakresie bezpieczeństwa cybernetycznego. Istnieje także szeroki konsensus wśród zainteresowanych stron w sprawie utworzenia dobrowolnych, stopniowo dostosowywanych ram europejskich.

Po stronie przemysłu to rozwiązanie w zakresie certyfikacji uzyskało wsparcie przedsiębiorstw, które już podlegają wymogom certyfikacji i które odniosłyby korzyść z ogólnounijnego mechanizmu opartego wzajemnym uznawaniu certyfikatów. Także MŚP udzieliły temu rozwiązaniu wsparcia, gdyż cierpią najbardziej w sytuacji, gdy muszą obecnie – lub musiałyby w przyszłości – poddawać się różnym procedurom certyfikacyjnych we wszystkich państwach członkowskich. Niektóre państwa członkowskie, w szczególności dysponujące mniejszymi zasobami, i niektórzy przedstawiciele przemysłu oraz instytucji unijnych wyrazili pozytywną opinię również na temat wariantu 3 w odniesieniu do ENISA.

C. SKUTKI WDROŻENIA PREFEROWANEGO WARIANTU

Jakie korzyści przyniesie wdrożenie preferowanego wariantu lub – jeśli go nie wskazano – głównych wariantów?

W ramach preferowanego wariantu UE zyskałaby agencję skoncentrowaną na zapewnianiu państwo członkowskim, instytucjom unijnym i przedsiębiorstwom pomocy w obszarach, w których wartość dodana takiego wsparcia byłaby najwyższa. Obejmują one: wspieranie wdrażania dyrektywy w sprawie bezpieczeństwa sieci i informacji; opracowanie i realizację polityki; informację, wiedzę i świadomość; badania naukowe; współpracę operacyjną i zarządzanie kryzysowe; rynek. W szczególności ENISA będzie wspierać działania UE w obszarze certyfikacji bezpieczeństwa cybernetycznego przez zapewnienie obsługi administracyjnej i zarządzania technicznego dotyczącego europejskich ram certyfikacji bezpieczeństwa cybernetycznego. Takie ramy zapewnią skuteczne wprowadzenie zbioru przepisów regulujących certyfikację bezpieczeństwa cybernetycznego w UE, co będzie sprzyjać systemowi wzajemnego uznawania certyfikatów wydanych w różnych państwach członkowskich. Rozwiązanie łączące te warianty uznano za najskuteczniejszy sposób osiągnięcia założonych przez UE celów, którymi są: zwiększenie zdolności w zakresie bezpieczeństwa cybernetycznego; gotowość; współpraca; świadomość; przejrzystość; oraz unikanie fragmentacji rynku. Wariant ten uznano również za najbardziej spójny z priorytetami politycznymi strategii UE w zakresie bezpieczeństwa cybernetycznego i związanych z nią działań (np. z dyrektywą w sprawie bezpieczeństwa sieci i informacji) oraz ze strategią jednolitego rynku cyfrowego. Ponadto wariant ten pozwoliłby osiągnąć cele poprzez racjonalne wykorzystywanie zasobów.

Jakie są koszty wdrożenia preferowanego wariantu lub – jeśli go nie wskazano – głównych wariantów?

Mimo zyskania nowej roli „zreformowana ENISA” pozostaje sprawną organizacją. Wymagany wkład finansowy z budżetu UE byłby wyższy niż obecnie, ale nadal znacznie niższy niż w przypadku innych agencji, które również działają w najważniejszych obszarach.

Stworzenie europejskich ram certyfikacji bezpieczeństwa cybernetycznego nie pociągnęłoby za sobą dodatkowych kosztów początkowych dla przemysłu (w tym MŚP). Raczej pozwoliłoby na znaczne oszczędności dla tych przedsiębiorstw, które już poddają swoje produkty certyfikacji bezpieczeństwa lub chcą uzyskać odnośne certyfikaty, z korzyścią dla konkurencyjności tych przedsiębiorstw na świecie. Z drugiej strony wiązałoby się to z pewnymi zobowiązaniami budżetowymi w celu zapewnienia utrzymania ram, które byłoby zadaniem „zreformowanej ENISA” w zakresie zadań technicznych i obsługi sekretariatowej.

Czy przewiduje się znaczące skutki dla budżetów i administracji krajowych?

Nie. Koszty związane ze wzmocnieniem ENISA pochodziłyby głównie z budżetu UE, państwa członkowskie natomiast nadal mogłyby wnosić dowolny wkład finansowy na rzecz Agencji. W przypadku certyfikacji główny wpływ na budżety i administracje krajowe wynikałby z utworzenia – w stosownych przypadkach – organu ds. certyfikacji.

Czy wystąpią inne znaczące skutki?

Nie.

Proporcjonalność

Wariant preferowany obejmuje wyważone środki, z których wszystkie uznaje się za konieczne do realizacji wyznaczonych celów, bez nakładania nadmiernego obciążenia na stosowne zainteresowane strony. Z tej perspektywy inicjatywę uważa się za zgodną z zasadą proporcjonalności.

D. DZIAŁANIA NASTĘPCZE

Kiedy nastąpi przegląd przyjętej polityki?

Obecnie proponuje się, aby pierwsza ocena została dokonana po upływie pięciu lat od wejścia w życie instrumentu prawnego. Następnie Komisja będzie przedstawiać Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny, któremu w stosownych przypadkach towarzyszyć będzie wniosek o dokonanie przeglądu. Dalsze oceny będą się odbywać co pięć lat.