Rada
Unii Europejskiej

Bruksela, 22 marca 2022 r.
(OR. en)

Międzyinstytucjonalny numer referencyjny:
2022/0085(COD)

7474/22
ADD 3

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	22 marca 2022 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, sekretarz generalny Rady Unii Europejskiej
Nr dok. Kom.:	SWD(2022) 68 final
Dotyczy:	DOKUMENT ROBOCZY SŁUŻB KOMISJI - SPRAWOZDANIE ZE STRESZCZENIA OCENY SKUTKÓW - towarzyszący dokumentowi: Wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii

Delegacje otrzymują w załączeniu dokument SWD(2022) 68 final.

Zał.: SWD(2022) 68 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 22.3.2022 r.
SWD(2022) 68 final

DOKUMENT ROBOCZY SŁUŻB KOMISJI

STRESZCZENIE OCENY SKUTKÓW

Towarzyszący dokumentowi:

Wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY

ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii

{COM(2022) 122 final} - {SWD(2022) 67 final}

1. Wprowadzenie

W 2020 r. gwałtownie wzrosła liczba znaczących incydentów mających wpływ na instytucje, organy i agencje Unii, za którymi to incydentami stali agresorzy stwarzający zaawansowane, trwałe zagrożenie. Jest to również odzwierciedlone w liczbie kopii danych wykonanych na potrzeby informatyki śledczej, które CERT-UE analizował w 2020 r., trzykrotnie wyższej w stosunku do 2019 r., podczas gdy liczba znaczących incydentów wzrosła od 2018 r. ponad dziesięciokrotnie.

Zdolności w zakresie cyberbezpieczeństwa i wydatki na bezpieczeństwo informatyczne w instytucjach, organach i agencjach Unii są jednak w niektórych przypadkach uderzająco nierówne, czego skutkiem jest szerokie zróżnicowanie poziomów dojrzałości w zakresie cyberbezpieczeństwa między instytucjami, organami i agencjami Unii. Ponadto analiza krajobrazu zagrożeń i statystyki dotyczące incydentów związanych z bezpieczeństwem informatycznym pokazują, że narażenie instytucji, organów i agencji Unii na zagrożenia związane z cyberbezpieczeństwem jedynie się zwiększy.

2. Cele

Zidentyfikowane niedociągnięcia ostatecznie prowadzą do niewystarczającego poziomu cyberodporności we wszystkich instytucjach, organach i agencjach Unii, fragmentarycznego pozyskiwania zasobów na potrzeby bezpieczeństwa informatyczna i niewyważonych stanowisk w zakresie bezpieczeństwa informatycznego.

Celem aktu ustawodawczego byłoby zapewnienie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i agencjach Unii. Przyczyniłoby się to do przyspieszenia procesu cyfryzacji instytucji, organów i agencji Unii i zagwarantowałoby, że dojrzałość w zakresie cyberbezpieczeństwa będzie nadążać za przyspieszającą cyfryzacją.

3. Międzyinstytucjonalna Rada ds. Cyberbezpieczeństwa i ramy cyberbezpieczeństwa

We wniosku dotyczącym Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa i ram cyberbezpieczeństwa zostaną wprowadzone środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i agencjach Unii umożliwiające dostosowanie się do ram, które uwzględniają zagrożenia cyberbezpieczeństwa wszystkich instytucji, organów i agencji Unii, oraz zostaną ustanowione zasady nadzoru przez Międzyinstytucjonalną Radę ds. Cyberbezpieczeństwa i sprawozdawczości wobec tej rady.

We wniosku uaktualniono misję i zadania CERT-UE, uwzględniając zmieniony charakter i wyższy poziom cyfryzacji instytucji, organów i agencji Unii w ostatnich latach, jak również zmieniający się krajobraz zagrożeń cyberbezpieczeństwa.

Nie ma bezpośrednich skutków ani konsekwencji budżetowych dla państw członkowskich ani obywateli UE.

Podstawą prawną rozporządzenia jest art. 298 Traktatu o funkcjonowaniu Unii Europejskiej, który przewiduje, że wykonując swoje zadania, instytucje, organy i jednostki organizacyjne Unii korzystają ze wsparcia otwartej, efektywnej i niezależnej administracji europejskiej.

Niniejszy wniosek opiera się na strategii UE w zakresie unii bezpieczeństwa (COM(2020) 605 final) oraz strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę (JOIN(2020) 18 final).

4. Wniosek

Międzyinstytucjonalna Rada ds. Cyberbezpieczeństwa i ramy cyberbezpieczeństwa osiągają większość zamierzonych celów w stosunkowo skuteczny, wydajny i spójny sposób w połączeniu z innymi politykami Unii, przy wsparciu jak najszerszego grona zainteresowanych stron. To wybrane rozwiązanie jest najbardziej realnym wariantem, biorąc pod uwagę obecne granice prawne, w ramach których działamy; również podejście uniwersalne nie byłoby odpowiednie z uwagi na niejednorodną obecnie dojrzałość instytucji, organów i agencji Unii oraz na różnice w ryzyku technologicznym i złożoność, z którymi się one borykają.