Rada
Unii Europejskiej

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

Międzyinstytucjonalny numer referencyjny:
2022/0085(COD)

7474/22
ADD 1

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

WNIOSEK

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.:	COM(2022) 122 final
Dotyczy:	ZAŁĄCZNIKI do wniosku dotyczącego 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 COM(2022) 122 final.

Zał.: COM(2022) 122 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 22.3.2022 r.
COM(2022) 122 final

ANNEXES 1 to 2

ZAŁĄCZNIKI

do

wniosku dotyczącego ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY

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

{SWD(2022) 67 final} - {SWD(2022) 68 final}

ZAŁĄCZNIK I

W podstawowym poziomie cyberbezpieczeństwa uwzględnia się następujące dziedziny:

1) polityka w zakresie cyberbezpieczeństwa, w tym cele i priorytety w zakresie bezpieczeństwa sieci i systemów informatycznych, w szczególności w odniesieniu do korzystania z usług w chmurze (w rozumieniu art. 4 pkt 19 dyrektywy [wniosek dotyczący dyrektywy NIS 2]) i ustaleń technicznych umożliwiających telepracę;
2) organizacja cyberbezpieczeństwa, w tym określenie ról i obowiązków;
3) zarządzanie aktywami, w tym baza zasobów informatycznych i mapy sieci informatycznych;
4) kontrola dostępu;
5) bezpieczeństwo operacji;
6) bezpieczeństwo łączności;
7) zakup, rozwój i utrzymanie systemów;
8) relacje z dostawcami;
9) zarządzanie incydentami, w tym podejścia mające na celu poprawę gotowości na wypadek incydentów, reagowania na nie i usuwania ich skutków oraz usprawnienie współpracy z CERT-UE, np. prowadzenie monitorowania bezpieczeństwa i rejestrowanie zdarzeń;
10) zarządzanie ciągłością działania i zarządzanie kryzysowe oraz
11) programy edukacji, podnoszenia świadomości i szkoleń w zakresie cyberbezpieczeństwa.

ZAŁĄCZNIK II

Instytucje, organy i agencje Unii uwzględniają co najmniej następujące konkretne środki w zakresie cyberbezpieczeństwa przy wdrażaniu podstawowego poziomu cyberbezpieczeństwa i w swoich planach dotyczących cyberbezpieczeństwa, zgodnie z wytycznymi i zaleceniami IICB:

1) konkretne kroki służące przejściu na architekturę zerowego zaufania (oznaczającą model bezpieczeństwa, zbiór zasad projektowania systemu oraz skoordynowaną strategię cyberbezpieczeństwa i zarządzania systemem oparte na przekonaniu, że zagrożenia istnieją zarówno wewnątrz tradycyjnych granic sieci, jak i poza nimi);

2) przyjęcie uwierzytelniania wieloskładnikowego jako normy we wszystkich sieciach i systemach informatycznych;

3) ustanowienie bezpieczeństwa łańcucha dostaw oprogramowania poprzez kryteria regulujące opracowywanie i ocenę bezpiecznego oprogramowania;

4) wzmocnienie przepisów dotyczących zamówień publicznych w celu ułatwienia wysokiego wspólnego poziomu cyberbezpieczeństwa poprzez:

   a) usunięcie barier umownych, które ograniczają wymianę z CERT-UE informacji pochodzących od dostawców usług informatycznych na temat incydentów, podatności i cyberzagrożeń;

   b) zobowiązanie umowne do zgłaszania incydentów, podatności i cyberzagrożeń, a także do zapewnienia odpowiedniego reagowania na incydenty i ich monitorowania.