Rada
Unii Europejskiej

Bruksela, 10 czerwca 2022 r.
(OR. fr, en)

9716/22

LIMITE

CYBER 198
TELECOM 255
CSC 228
CSCI 74
FIN 590

NOTA DO PUNKTU I/A

Od:	Sekretariat Generalny Rady
Do:	Komitet Stałych Przedstawicieli / Rada
Nr poprz. dok.:	9317/2/22 REV 2
Dotyczy:	Projekt konkluzji Rady w sprawie sprawozdania specjalnego nr 05/2022 Europejskiego Trybunału Obrachunkowego pt. „Cyberbezpieczeństwo instytucji, organów i agencji UE: poziom przygotowania ogólnie nieadekwatny do zagrożeń” – Zatwierdzenie

1. W dniu 30 marca 2022 r. Europejski Trybunał Obrachunkowy opublikował sprawozdanie specjalne nr 05/2022 pt. „Cyberbezpieczeństwo instytucji, organów i agencji UE: poziom przygotowania ogólnie nieadekwatny do zagrożeń”.[1]

2. Podczas posiedzenia w dniu 13 kwietnia 2022 r. Komitet Stałych Przedstawicieli przekazał to sprawozdanie specjalne Horyzontalnej Grupie Roboczej ds. Cyberprzestrzeni.[2]

[1] 8040/22.
[2] 8041/22.

3. W dniu 3 maja 2022 r. przedstawiciele Trybunału Obrachunkowego przedstawili sprawozdanie specjalne Horyzontalnej Grupie Roboczej ds. Cyberprzestrzeni. W następstwie przeprowadzonych podczas tego samego posiedzenia grupy roboczej dyskusji nad sprawozdaniem prezydencja przygotowała projekt konkluzji Rady, który został omówiony przez grupę roboczą na posiedzeniu w dniu 24 maja 2022 r.

4. W dniu 10 czerwca 2022 r. Horyzontalna Grupa Robocza ds. Cyberprzestrzeni osiągnęła porozumienie w sprawie tekstu zamieszczonego w załączniku.

5. Komitet Stałych Przedstawicieli jest proszony o zatwierdzenie niniejszego projektu konkluzji i o zwrócenie się do Rady, by przyjęła je na jednym z kolejnych posiedzeń.

ZAŁĄCZNIK

PROJEKT KONKLUZJI RADY

w sprawie sprawozdania specjalnego nr 05/2022 Europejskiego Trybunału Obrachunkowego pt. „Cyberbezpieczeństwo instytucji, organów i agencji UE: poziom przygotowania ogólnie nieadekwatny do zagrożeń”

RADA UNII EUROPEJSKIEJ,

PRZYWOŁUJĄC swoje konkluzje w sprawie usprawnienia analizy sprawozdań specjalnych sporządzanych przez Trybunał Obrachunkowy w związku z procedurą udzielania absolutorium[3],

1. ODNOTOWUJE sprawozdanie specjalne nr 05/2022 Europejskiego Trybunału Obrachunkowego pt. „Cyberbezpieczeństwo instytucji, organów i agencji UE: poziom przygotowania ogólnie nieadekwatny do zagrożeń”[4].

2. PODKREŚLA znaczenie i pilną potrzebę wzmocnienia poziomu cyberbezpieczeństwa w instytucjach, organach i agencjach UE, biorąc pod uwagę niedawną intensyfikację transformacji cyfrowej w instytucjach, przetwarzane przez nie informacje szczególnie chronione, stale rosnącą liczbę i dotkliwość ataków na instytucje, organy i agencje UE oraz poziom zagrożenia, które ich dotyczy.

[3] 7515/00 + COR 1.
[4] 8040/22.

3. PRZYPOMINA o konkluzjach Rady Europejskiej z dnia 20 czerwca 2019 r.[5], w których Rada Europejska zwróciła się do instytucji UE, aby wraz z państwami członkowskimi pracowały nad środkami na rzecz zwiększenia odporności i poprawy kultury bezpieczeństwa UE w obliczu cyberzagrożeń i zagrożeń hybrydowych spoza UE, a także na rzecz skuteczniejszej ochrony unijnych sieci informacyjnych i komunikacyjnych oraz unijnych procesów decyzyjnych przed wszelkiego rodzaju złośliwymi działaniami.

4. PRZYPOMINA swoje konkluzje z dnia 10 grudnia 2019 r. w sprawie dodatkowych wysiłków na rzecz zwiększenia odporności i zwalczania zagrożeń hybrydowych[6], w których zaapelowała do instytucji, organów i jednostek organizacyjnych UE, by przy wsparciu ze strony państw członkowskich zapewniły zdolność Unii do chronienia jej integralności i do zwiększania ochrony unijnych informacji, sieci komunikacyjnych i procesów decyzyjnych przed szkodliwymi działaniami wszelkiego rodzaju, na podstawie kompleksowej oceny zagrożenia. W tym celu, jak określono w przedmiotowych konkluzjach, instytucje, organy i jednostki organizacyjne UE powinny przy wsparciu ze strony państw członkowskich opracować i wdrożyć kompleksowy zestaw środków w celu zapewnienia sobie bezpieczeństwa, zgodnie z mandatem Rady Europejskiej z czerwca 2019 r.[7]

5. PRZYPOMINA o swoich konkluzjach z dnia 22 marca 2021 r. w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę[8], w których podkreśliła, że cyberbezpieczeństwo odgrywa podstawową rolę w funkcjonowaniu administracji publicznej i instytucji publicznych zarówno na poziomie krajowym, jak i UE oraz, ogólnie, naszego społeczeństwa i naszej gospodarki.

---

5 EUCO 9/19.
6 14972/19.
7 EUCO 9/19.
8 6722/21.

6. PRZYPOMINA o swoich konkluzjach z dnia 23 maja 2022 r. w sprawie rozwijania pozycji Unii Europejskiej w kwestiach cyberprzestrzeni[9], w których zwróciła się do instytucji, organów i jednostek organizacyjnych UE, by sporządziły zestawienie istniejących narzędzi bezpiecznej łączności w cyberprzestrzeni, które powinno zostać omówione przez odpowiednie organy Rady i odpowiednie grupy współpracy, takie jak sieć CSIRT i EU CyCLONe.

7. PODKREŚLA potrzebę zajęcia się ryzykiem systemowym, które istnieje w przypadku wzajemnych powiązań między instytucjami, organami i jednostkami organizacyjnymi UE, a także między nimi oraz instytucjami państw członkowskich, pomimo ich niezależności instytucjonalnej i autonomii administracyjnej.

8. ODNOTOWUJE spostrzeżenia zawarte w sprawozdaniu specjalnym, zgodnie z którymi instytucje, organy i jednostki organizacyjne UE nie osiągnęły poziomu gotowości w zakresie cyberbezpieczeństwa na poziomie współmiernym do zagrożeń i mają różny poziom dojrzałości w zakresie cyberbezpieczeństwa. UZNAJE, że należy poprawić poziom gotowości instytucji, organów i jednostek organizacyjnych UE w zakresie cyberbezpieczeństwa, a także synergie między nimi.

9. Zdecydowanie ZACHĘCA zatem instytucje, organy i jednostki organizacyjne UE do dalszego wdrażania środków zarządzania ryzykiem w cyberprzestrzeni, które zapewniają proporcjonalny poziom cyberbezpieczeństwa, jak przewidziano w proponowanej dyrektywie w sprawie środków na rzecz wspólnego wysokiego poziomu cyberbezpieczeństwa w całej Unii, uchylającej dyrektywę (UE) 2016/1148, w celu poprawy ich poziomu gotowości.

10. ZWRACA SIĘ do instytucji, organów i jednostek organizacyjnych UE o zintensyfikowanie zarówno wysiłków na rzecz ochrony przed cyberzagrożeniami, jak i współpracy w zakresie ustanowienia spójnych norm i specyfikacji, w szczególności w odniesieniu do zamówień publicznych, projektów i usług związanych z cyberbezpieczeństwem, oraz do poprawy interoperacyjności ich systemów informatycznych, w tym z myślą o zapewnieniu bezpiecznego przekazywania treści jawnych.

---

[9] 9364/22.

11. ZWRACA SIĘ do Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) i zespołu reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT-UE), by w ramach swoich kompetencji zintensyfikowały współpracę we wspieraniu instytucji, organów i jednostek organizacyjnych UE w ich wysiłkach na rzecz cyberbezpieczeństwa, w szczególności w odniesieniu do budowania zdolności tych instytucji, organów i jednostek organizacyjnych UE, które mają niższy poziom dojrzałości w zakresie cyberbezpieczeństwa.

12. ODNOTOWUJE wnioski i zalecenia zawarte w sprawozdaniu specjalnym i UZNAJE, że należy znacząco poprawić poziom gotowości instytucji, organów i jednostek organizacyjnych UE w zakresie cyberbezpieczeństwa, a także synergie między nimi. Instytucje, organy i jednostki organizacyjne UE powinny mieć kompleksowe ramy zarządzania ryzykiem w zakresie cyberbezpieczeństwa, przeprowadzać regularne oceny i audyty pod względem ryzyka w oparciu o wspólną lub dobrze znaną metodykę i normy międzynarodowe oraz usystematyzować programy podnoszenia świadomości w zakresie cyberbezpieczeństwa i programy szkoleniowe dla pracowników.

3. PODKREŚLA również, że instytucje, organy i jednostki organizacyjne UE powinny przeznaczyć wystarczający budżet na wdrożenie środków ochrony przed cyberzagrożeniami przy jednoczesnym poszanowaniu wieloletnich ram finansowych, i ODNOTOWUJE zalecenie zawarte w sprawozdaniu specjalnym, zgodnie z którym należy powołać organ reprezentujący wszystkie instytucje, organy i jednostki organizacyjne UE oraz dysponować odpowiednim mandatem i środkami w celu monitorowania zgodności ze wspólnymi przepisami dotyczącymi cyberbezpieczeństwa.

14. UZNAJE, że CERT-UE powinien być niezwłocznie informowany o poważnych cyberincydentach w instytucjach, organach i jednostkach organizacyjnych UE i w tym celu powinien dysponować odpowiednimi zasobami, które będą przewidywalne i dostosowane do aktualnego poziomu zagrożenia oraz do potrzeb instytucji, organów i jednostek organizacyjnych UE, w szczególności w zakresie personelu, wyposażenia technicznego i infrastruktury.

15. ZAUWAŻA, że należy wzmocnić i usystematyzować współpracę i wymianę informacji na temat cyberbezpieczeństwa, a także interoperacyjność bezpiecznych kanałów komunikacji między instytucjami, organami i jednostkami organizacyjnymi UE. APELUJE, aby taka współpraca i wymiana informacji obejmowały również organy publiczne odpowiedzialne za cyberbezpieczeństwo w państwach członkowskich.

16. ODNOTOWUJE odpowiedzi Komisji, CERT-UE i ENISA towarzyszące sprawozdaniu specjalnemu.

17. ZWRACA SIĘ do Komisji, by uwzględniła zalecenia zawarte w sprawozdaniu specjalnym i wykazała się ambicją przy opracowywaniu strategii politycznych w zakresie cyberbezpieczeństwa instytucji, organów i jednostek organizacyjnych UE, a także by opowiadała się za większą synergią między nimi.