ODPOWIEDZI KOMISJI EUROPEJSKIEJ

NA SPRAWOZDANIE SPECJALNE EUROPEJSKIEGO TRYBUNAŁU OBRACHUNKOWEGO

Cyberbezpieczeństwo instytucji, organów i agencji UE – poziom przygotowania nieadekwatny do zagrożeń

PL

PL

Spis treści

Niniejszy dokument zawiera odpowiedzi Komisji Europejskiej na uwagi zawarte w sprawozdaniu specjalnym Europejskiego Trybunału Obrachunkowego, zgodnie z art. 259 rozporządzenia finansowego. Jest on publikowany wraz ze sprawozdaniem specjalnym.

I. ODPOWIEDZI KOMISJI W SKRÓCIE

a) Wstęp

Cyberbezpieczeństwo stało się priorytetem politycznym i operacyjnym Komisji Europejskiej. Kryzys związany z COVID-19 zwiększył naszą zależność od usług cyfrowych (chmury obliczeniowe, urządzenia mobilne, sztuczna inteligencja). W ciągu ostatnich dwóch lat zaobserwowaliśmy masowe przejście na pracę z domu. Oznacza to, że zarówno cyberprzestępczość, jak i cyberszpiegostwo, czyli dwa główne zagrożenia, przed którymi stoją instytucje, organy i agencje Unii Europejskiej (EUIBA), również przybrały na sile. Komisja zauważa tę tendencję i konsekwentne i zdecydowane przoduje w dziedzinie cyberbezpieczeństwa. W 2019 r. wszedł w życie akt o cyberbezpieczeństwie, w którym między innymi rozszerzono mandat ENISA i nadano mu stały charakter. W akcie tym ustanowiono również formalną współpracę między ENISA a CERT-UE (zespołem reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE). W 2020 r. Komisja zaproponowała wzmocnienie dyrektywy w sprawie bezpieczeństwa sieci i informacji, i obecnie wniosek ten jest bliski przyjęcia przez prawodawców.

W strategii w zakresie cyberbezpieczeństwa z 2020 r. również przedstawiono trzy działania mające wpływ na cyberbezpieczeństwo EUIBA. Zapowiedziano w niej przyjęcie rozporządzenia w sprawie bezpieczeństwa informacji w instytucjach, organach i agencjach UE oraz rozporządzenia w sprawie wspólnych zasad cyberbezpieczeństwa dla instytucji, organów i agencji UE a także ogłoszono zamiar ustanowienia nowej podstawy prawnej dla CERT-UE w celu wzmocnienia jego mandatu i finansowania, aby zapewnić mu odpowiednie zasoby w obliczu rosnących zagrożeń i ryzyka oraz coraz większej liczby incydentów.

Prace nad przygotowaniem tych wniosków posuwają się do przodu. Chociaż wnioski nie zostały jeszcze przyjęte przez kolegium, oczekuje się, że zostaną przyjęte w pierwszym kwartale 2022 r. Istotne kwestie omawiane przez instytucje na tym etapie dotyczą podstawy prawnej wniosków, a także zdolności budżetowej wszystkich EUIBA do spełnienia wymogów zarówno w zakresie finansowania własnych potrzeb dotyczących cyberbezpieczeństwa, jak i znalezienia zasobów niezbędnych do wsparcia CERT-UE, zwiększania budżetu, a w szczególności stworzenia nowych stanowisk.

Poziom gotowości instytucji, organów i agencji UE w zakresie cyberbezpieczeństwa jest zróżnicowany. Pewne EUIBA osiągają dobre wyniki pod względem gotowości w zakresie cyberbezpieczeństwa i powinny nadal odgrywać rolę liderów, stymulując i inspirując postępy i dalsze usprawnienia w całym obszarze cyberbezpieczeństwa. Aby osiągnąć wymierne postępy, trzeba dostrzec zróżnicowane poziomy zaawansowania instytucji, organów i agencji UE oraz ustalić priorytety, dzięki czemu działania usprawniające skupią się przede wszystkim na tych instytucjach, organach i agencjach UE, w których stwierdzone luki powodują najwyższe ryzyko.

b) Stanowisko Komisji w sprawie kluczowych uwag i zaleceń ETO

Komisja z zadowoleniem przyjmuje sprawozdanie Europejskiego Trybunału Obrachunkowego w sprawie cyberbezpieczeństwa instytucji, organów i agencji UE. Odnotowuje, że w sprawozdaniu podkreślono znaczenie wspólnych ram prawnych dotyczących bezpieczeństwa informacji

i cyberbezpieczeństwa dla wszystkich EUIBA w celu podniesienia ogólnego poziomu cyberbezpieczeństwa we wszystkich obszarach. Komisja zauważa, że główne uwagi i zalecenia Europejskiego Trybunału Obrachunkowego nie dotyczą cyberbezpieczeństwa operacyjnego samej Komisji, lecz raczej jej strategicznej roli w zakresie proponowania przepisów mających na celu poprawę zaawansowania cyfrowego EUIBA.

Przyszłe rozporządzenia w sprawie „bezpieczeństwa informacji w instytucjach, organach i agencjach UE" oraz „wspólnych zasad cyberbezpieczeństwa dla instytucji, organów i agencji UE" będą określać wspólne zasady mające na celu osiągnięcie wysokiego poziomu bezpieczeństwa informacji i cyberbezpieczeństwa, ale ich wdrożenie, w kontekście organizacyjnym i operacyjnym poszczególnych EUIBA (w szczególności ich profili zagrożenia i ryzyka), pozostaje w zakresie autonomicznej odpowiedzialności EUIBA. Proponowane rozporządzenie w sprawie cyberbezpieczeństwa będzie przewidywało mechanizmy kontroli zgodności, które będą odpowiednie i współmierne do celu i zakresu nowych przepisów, bez uszczerbku dla autonomii instytucji, organów i agencji.

Komisja przewodniczy obecnie podgrupie ds. cyberbezpieczeństwa w Międzyinstytucjonalnym Komitecie ds. Transformacji Cyfrowej (ICDT); przewodnictwo to ma charakter rotacyjny (na okres do 2 lat). Należy zauważyć, że na prace podgrupy nie przeznaczono żadnych ukierunkowanych zasobów: wszystkie działania opierają się na wysiłkach podejmowanych przez uczestników na zasadzie dobrowolności.

Komisja zgadza się z ogólną ideą wzmocnienia zasobów i mandatu CERT-UE.

Zgodnie z powyższym Komisja popiera główne uwagi i zalecenia zawarte w sprawozdaniu. Nasze szczegółowe stanowisko wyjaśniono w dodatkowych uwagach w sekcji III. Jeśli chodzi o zalecenia, Komisja przyjmuje zalecenia 1a, b, c, d, e, f, g oraz 2a, b, c.

c) Najnowszy rozwój wydarzeń i dalsze działania

Zakończono formalne konsultacje na szczeblu dyrektorów generalnych instytucji, organów i agencji UE w sprawie skonsolidowanych projektów obu rozporządzeń (bezpieczeństwo informacji, cyberbezpieczeństwo), a obecnie trwa ocena otrzymanych informacji zwrotnych. Następnym etapem jest finalizacja pakietu i jego przyjęcie przez kolegium w pierwszym kwartale 2022 r.

II. ODPOWIEDZI KOMISJI NA GŁÓWNE UWAGI TRYBUNAŁU OBRACHUNKOWEGO

1. Poziomy zaawansowania EUIBA w zakresie cyberbezpieczeństwa

Komisja zgadza się, że przy analizowaniu poziomu wydatków EUIBA na cyberbezpieczeństwo należy uwzględnić zagrożeń i ryzyka.

Jeśli chodzi o aspekt zasobów ludzkich, na stabilność zatrudnienia w EUIBA również wpływa szereg czynników. Rynek, na którym rekrutuje się specjalistów w dziedzinie cyberbezpieczeństwa, jest coraz

bardziej złożony. W wielu przypadkach przepisy dotyczące zasobów ludzkich nie są dostosowane do specjalistycznych profili (rekrutacja, rozwój kariery, szkolenia). Ponadto ogólna presja władzy budżetowej na poziomy zatrudnienia we wszystkich EUIBA oznacza, że w nowych obszarach o wysokim priorytecie, takich jak cyberbezpieczeństwo, nie ma wystarczającej liczby stanowisk, zwłaszcza w wewnętrznych służbach operacyjnych.

Omawiając postępy w zarządzaniu cyberbezpieczeństwem i zarządzaniu ryzykiem należy uwzględniać fakt, że kontrola zgodności dopiero teraz przechodzi z etapu pilotażowego do pełnego wdrożenia. W związku z tym to normalne, że jej zakres jest jak dotąd dość ograniczony. Wspomniany projekt dotyczący kontroli zgodności to kolejny etap w długoterminowym procesie zwiększania zaawansowania cyfrowego, który rozpoczął się od określenia wspólnej metodyki oceny ryzyka, opracowania wspólnego oprzyrządowania, wprowadzenia zarządzania podatnością na zagrożenia oraz monitorowania wykazu zasobów, testowania i walidacji. W tym długofalowym procesie poczyniono już postępy pomimo złożoności zasobów Komisji – obejmuje ono ponad 1000 systemów informacyjnych obsługiwanych przez ponad 50 dyrekcji generalnych i agencji wykonawczych.

2. Mechanizmy współpracy w ramach EUIBA

CERT-UE ma doskonałe osiągnięcia w promowaniu współpracy nie tylko między EUIBA, ale również na szczeblu europejskim, dzięki swojej roli pełnoprawnego członka sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) utworzonej na mocy dyrektywy w sprawie bezpieczeństwa sieci i informacji. Jest najlepszym przykładem tego, w jaki sposób można wzmocnić współpracę i usługi w zakresie cyberbezpieczeństwa. Uwagi ETO dotyczące CERT-UE bardzo wyraźnie unaoczniają, jak znakomicie CERT-UE wypełnia swoje obowiązki w obliczu coraz większych cyberzagrożeń i utrzymujących się niedoborów zasobów.

Na mocy obecnego porozumienia międzyinstytucjonalnego zdecentralizowane agencje i wspólne przedsięwzięcia UE są oficjalnie reprezentowane w radzie sterującej CERT-UE przez ENISA. Ponadto ich opinie są wyrażane na posiedzeniach rady sterującej przez przedstawiciela Komitetu Doradczego ds. ICT, który może uczestniczyć w posiedzeniach jako wsparcie dla ENISA w jej roli przedstawiciela agencji, ale nie jest formalnie członkiem i nie ma prawa głosu. Kwestia odpowiedniej reprezentacji agencji w radzie sterującej CERT-UE zostanie rozwiązana w proponowanym rozporządzeniu. Skład rady sterującej zostanie uzupełniony maksymalnie trzema przedstawicielami wyznaczonymi przez sieci agencji UE (EUAN), na wniosek jej Komitetu Doradczego ds. ICT.

Uczestnictwo w podgrupie ds. cyberbezpieczeństwa ICDT odbywa się na zasadzie dobrowolnych wysiłków, na poziomie zaangażowania określonym przez każdą EUIBA. Podczas opracowywania nowej umowy ramowej w zakresie cyberbezpieczeństwa uwzględnione zostaną usprawnienia w zakresie wymiany informacji na temat zamówień publicznych, ważnego zagadnienia w ramach grupy zadaniowej 2 podgrupy ds. cyberbezpieczeństwa.

Jeżeli chodzi o wspólne oprzyrządowanie dla usług takich jak poczta elektroniczna i wideokonferencje, istnieje już możliwość korzystania z systemu SECEM-2, wdrożonego przez Komisję w odniesieniu do wszystkich EUIBA w celu szyfrowania poczty elektronicznej w oparciu o skuteczne zarządzanie kluczami szyfrującymi i certyfikatami. Ponadto obecnie trwają prace nad stworzeniem SECABC, narzędzia umożliwiającego szyfrowanie poczty elektronicznej przesyłanej

między instytucjami. W założeniu dostęp do niego zostanie zaoferowany wszystkim zainteresowanym EUIBA od 2022 r. Zapewniono już bezpieczne wideokonferencje dla służb SNC; możliwe jest doraźne rozszerzenie tych usług na inne EUIBA poprzez zarządzanie tożsamością uczestników posiedzenia. We wniosku dotyczącym rozporządzenia w sprawie bezpieczeństwa informacji zostanie również uwzględniona wymiana informacji szczególnie chronionych (np. poprzez wspólne oznakowanie i etykietowanie).

3. Wymiana informacji na temat istotnych incydentów lub słabych punktów

W projekcie rozporządzenia w sprawie cyberbezpieczeństwa uwzględniono fakt, że nie wszystkie EUIBA zgłaszają CERT-UE istotne incydenty lub słabe punkty, zgodnie z wnioskiem Komisji zawartym w dyrektywie NIS-2[1]. Poziom wdrożenia będzie zależał od dodatkowych zasobów przeznaczonych na ten cel przez autonomiczne EUIBA. Możliwości egzekwowania takich powiadomień pozostają ograniczone, również w ramach proponowanego rozporządzenia w obecnym kształcie, ze względu na autonomię instytucjonalną EUIBA. Proponowane rozporządzenie w sprawie cyberbezpieczeństwa będzie przewidywało mechanizmy kontroli zgodności, które będą odpowiednie i współmierne do celu i zakresu nowych przepisów, bez uszczerbku dla autonomii instytucji, organów i agencji.

III. ODPOWIEDZI KOMISJI NA WNIOSKI I ZALECENIA ETO

Zalecenie 1 – Zwiększenie stopnia przygotowania EUIBA w zakresie cyberbezpieczeństwa za pomocą wspólnych wiążących przepisów oraz większych zasobów przeznaczonych dla CERT-UE

Proponowany tekst rozporządzenia będzie obejmował konkretne środki mające na celu dalsze zwiększenie wspólnego poziomu cyberbezpieczeństwa. Wspomniane środki przełożą się na plany w zakresie cyberbezpieczeństwa, określane i wdrażane na szczeblu EUIBA w ramach ich własnych ram zarządzania cyberbezpieczeństwem.

Komisja przyjmuje to zalecenie. W odniesieniu do konkretnych zaleceń szczegółowych Komisja zauważa, co następuje:

a) Komisja przyjmuje zalecenie 1a. Projekt rozporządzenia będzie zawierał przepisy dotyczące ram zarządzania i kontroli ustanowionych na najwyższym szczeblu kierownictwa wykonawczego każdej EUIBA w celu zapewnienia skutecznego i ostrożnego zarządzania wszystkimi zagrożeniami dla cyberbezpieczeństwa.

[1] Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148, COM(2020) 823 final

b) Komisja przyjmuje zalecenie 1b. W projekcie rozporządzenia wyraźniej zapisane zostanie podejście do zarządzania cyberbezpieczeństwem w oparciu o analizę ryzyka, poprzez doprecyzowanie, że działania, plany bezpieczeństwa informatycznego i faktyczne wdrożenie podstawowych kontroli powinny opierać się na wynikach ocen.
c) Komisja przyjmuje zalecenie 1c. Programy kształcenia, podnoszenia świadomości i szkoleń w zakresie cyberbezpieczeństwa zostaną wymienione w projekcie rozporządzenia jako część podstawy cyberbezpieczeństwa.
d) Komisja przyjmuje zalecenie 1d. Z naszego doświadczenia wynika, że chociaż regularne kontrole i testy mają zasadnicze znaczenie, nie są one wystarczające do zapewnienia postępów. W związku z tym konieczne jest ujęcie w ramach zarządzania cyberbezpieczeństwem, o których mowa w lit. a), regularnej sprawozdawczości i przejrzystości.
e) Komisja przyjmuje zalecenie 1e. Projekt rozporządzenia będzie zawierał przepisy dotyczące powiadamiania CERT-UE przez EUIBA o znaczących cyberzagrożeniach, słabych punktach i incydentach.
f) Komisja przyjmuje zalecenie 1f. Komisja popiera potrzebę zwiększenia zasobów CERT-UE. Przepisy dotyczące personelu i wkładów finansowych z EUIBA zostaną włączone do tekstu projektu rozporządzenia.
g) Komisja przyjmuje zalecenie 1g. Proponowane rozporządzenie będzie przewidywało mechanizmy kontroli zgodności, które będą współmierne i proporcjonalne do celu i zakresu przepisów, z poszanowaniem autonomii instytucjonalnej EUIBA. Treść przyszłego rozporządzenia jest uzależniona od przebiegu procedury ustawodawczej i jest rezultatem decyzji podjętych przez prawodawcę UE w odniesieniu do wniosku przedstawionego przez Komisję.

Zalecenie 2 – Wspieranie dalszej synergii między EUIBA w wybranych obszarach

Komisja, która obecnie przewodniczy podgrupie ds. cyberbezpieczeństwa w Międzyinstytucjonalnym Komitecie ds. Transformacji Cyfrowej (ICDT), zgadza się z zaleceniami dotyczącymi promowania rozwiązań w zakresie spójnej i bezpiecznej wymiany informacji szczególnie chronionych, systematycznej wymiany informacji na temat projektów w dziedzinie cyberbezpieczeństwa oraz wspólnych ram zamówień publicznych i umów dotyczących usług w zakresie cyberbezpieczeństwa.

Komisja przyjmuje to zalecenie. W odniesieniu do konkretnych zaleceń szczegółowych Komisja zauważa, co następuje:

a) Komisja przyjmuje zalecenie 2a. Komisja proponuje inicjatywy i usługi techniczne w podgrupie ds. cyberbezpieczeństwa ICDT, aby promować i wspierać wspólne oprzyrządowanie do wymiany informacji szczególnie chronionych, umożliwiające świadczenie takich usług, jak poczta elektroniczna i wideokonferencje. Zwracamy również uwagę, że wspólne oznaczenia i wspólne zasady postępowania w przypadku szczególnie chronionych informacji jawnych zostaną uwzględnione we wniosku dotyczącym rozporządzenia w sprawie bezpieczeństwa informacji.
b) Komisja przyjmuje zalecenie 2b. Istniejąca grupa zadaniowa działająca w ramach podgrupy ds. cyberbezpieczeństwa ICDT zajmują się tą kwestią i będzie ona dalej rozwijana. Podczas opracowywania nowej umowy ramowej w zakresie cyberbezpieczeństwa uwzględnia się usprawnienia w zakresie wymiany informacji na temat zamówień publicznych.

c) Komisja przyjmuje zalecenie 2c. EUIBA mają już dostęp do międzyinstytucjonalnych umów ramowych w dziedzinie ICT zarządzanych przez Komisję. Przygotowanie nowej umowy ramowej w zakresie cyberbezpieczeństwa będzie koordynowane z podgrupą ds. cyberbezpieczeństwa ICDT.

Zalecenie 3 – Zwiększenie nacisku CERT-UE i ENISA na mniej zaawansowane EUIBA

To zalecenie skierowane jest do CERT-UE i ENISA.