



Odpowiedzi przewodniczącego Rady Sterującej CERT-UE, CERT-UE i ENISA na sprawozdanie specjalne Europejskiego Trybunału Obrachunkowego dotyczące cyberbezpieczeństwa instytucji, organów i agencji UE

1. Streszczenie

W świetle stale zmieniającego się krajobrazu cyberzagrożeń cyberbezpieczeństwo stało się niezwykle ważne i niezbędne dla instytucji, organów i jednostek organizacyjnych Unii Europejskiej (EUIBA), które w ostatnich latach coraz częściej stanowiły cel wysoce wyrafinowanych cyberataków. W ramach swoich mandatów zarówno ENISA, jak i CERT-UE mogą zapewnić organom EUIBA cenne wsparcie w zakresie cyberbezpieczeństwa na różnych poziomach. Kluczowym instrumentem w tym kontekście jest wniosek Komisji Europejskiej dotyczący rozporządzenia w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i agencjach UE, który to instrument ENISA, CERT-UE i przewodniczący Rady Sterującej CERT-UE zdecydowanie popierają.

W związku z tym ENISA, CERT-UE i przewodniczący Rady Sterującej CERT-UE z zadowoleniem przyjmują sprawozdanie specjalne Europejskiego Trybunału Obrachunkowego dotyczące cyberbezpieczeństwa instytucji, organów i agencji UE, które pojawia się w bardzo odpowiednim momencie, aby zająć się poziomem gotowości wszystkich organów EUIBA. W sprawozdaniu wyraźnie zaznaczono główną rolę, jaką w tej dziedzinie mogą odegrać ENISA i CERT-UE. Przedstawiono w nim również zapotrzebowanie na dalsze zasoby i konkretne działania ukierunkowane na poprawę sytuacji w zakresie cyberbezpieczeństwa w EUIBA.

Mając to na uwadze, ENISA, CERT-UE i przewodniczący Rady Sterującej CERT-UE popierają kluczowe uwagi i zalecenia zawarte w sprawozdaniu, które są również zgodne z wnioskami ustawodawczymi Komisji Europejskiej w dziedzinie cyberbezpieczeństwa i bezpieczeństwa informacji dla EUIBA.

Uwagi w następnej sekcji mają na celu przedstawienie dalszych wyjaśnień dotyczących niektórych obszarów sprawozdania, w szczególności w odniesieniu do odpowiednich prac już podjętych przez ENISA lub CERT-UE, jak również planowanych działań, które ENISA lub CERT-UE przewidziały, zwłaszcza w obszarach budowania zdolności EUIBA. Jeśli chodzi o zalecenia, ENISA i CERT-UE przyjmują zalecenie 3 (Zwiększenie koncentracji CERT-UE i ENISA na mniej



dojrzałych EUIBA), które skierowano konkretnie do tych dwóch podmiotów.

2. Główne spostrzeżenia

ENISA i CERT-UE popierają kluczowe uwagi sformułowane przez Trybunał Obrachunkowy. W związku z tym poniżej przedstawiono kilka dodatkowych wyjaśnień, w szczególności w odniesieniu do obecnych działań podjętych przez ENISA lub CERT-UE, a także ustalonych już planów dotyczących przyszłych działań.

Ustęp 49

W odniesieniu do formalnego wniosku wysłanego przez ICTAC do przewodniczącego Rady Sterującej CERT-UE o przyznanie prawa głosu w Radzie, chcielibyśmy wyjaśnić następujące kwestie:

ze względu na znaczne koszty ogólne, jakie pociągałyby za sobą przegląd obecnego porozumienia międzyinstytucjonalnego, oraz ze względu na fakt, że trwające prace nad „rozporządzeniem w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i agencjach Unii” dotyczyły już reprezentacji agencji zdecentralizowanych, uzgodniono, że kwestia ta zostanie formalnie uregulowana, w perspektywie długoterminowej, w drodze rozporządzenia. Do tego czasu, jak potwierdził przewodniczący, obecne praktyki będą kontynuowane, a przedstawiciele ICTAC nadal będą mogli wyrażać swoje opinie i będą one brane pod uwagę, w najlepszym możliwym zakresie i z zachowaniem wszelkiej uczciwości.

Ustęp 66

Pod koniec 2021 r. ENISA ustanowiła plan działania dotyczący ćwiczeń w dziedzinie cyberbezpieczeństwa, który obejmuje w szczególności EUIBA. Odpowiedni plan działania w zakresie szkoleń dla EUIBA zostanie przedstawiony w I kwartale 2022 r.

Pole 3

Choć Agencji ENISA nie wymieniono wyraźnie jako produktu operacyjnego, zapewniała ona wsparcie operacyjne różnym organom EUIBA i współpracowała z nimi na podstawie ich wniosków. Na przykład w 2018 r. w ramach celu 2.2. Wspieranie wdrażania polityki Unii



Europejskiej:

- Europejski Bank Centralny zwrócił się z wnioskiem o wsparcie przy opracowywaniu ram testowania Eurosystemu przez zespół czerwony;
- Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego zwróciła się o wsparcie w opracowaniu celów Europejskiego Centrum ds. Cyberbezpieczeństwa w Lotnictwie, w podnoszeniu świadomości w zakresie cyberbezpieczeństwa oraz w sektorowym wdrażaniu dyrektywy w sprawie bezpieczeństwa sieci i informacji;
- Agencja Kolejowa Unii Europejskiej zwróciła się o wsparcie we wdrażaniu dyrektywy dotyczącej cyberbezpieczeństwa w sektorze kolejowym, w szczególności o wsparcie w tworzeniu ośrodka wymiany i analizy informacji dla zarządców infrastruktury i przedsiębiorstw kolejowych, a także w budowaniu zdolności (organizowanie szkoleń i sesji informacyjnych);
- ENISA wspierała Agencję Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA) w ramach działań na rzecz poprawy swoich umiejętności w zakresie cyberbezpieczeństwa i ciągłości działania. W szczególności ENISA służyła swoją wiedzą specjalistyczną w zakresie organizacji ćwiczeń i opracowywania scenariuszy, a także zaoferowała w pełni rozwinięty ENISA CEP Agencji eu-LISA w celu zorganizowania ćwiczenia gotowości dla jednego z kluczowych systemów informatycznych Unii Europejskiej.

Ponadto ENISA od 2019 r. aktywnie współpracuje z EUIBA (np. ERA, EMSA, EASA, ACER), wspierając dyrektywę dotyczącą cyberbezpieczeństwa, w zakresie działań związanych z budowaniem wiedzy na temat poszczególnych sektorów i podnoszeniem świadomości w zakresie cyberbezpieczeństwa, a także powiązanych sektorowych inicjatyw politycznych w zakresie cyberbezpieczeństwa.

Ustęp 71

ENISA opracowała w 2021 r. i wyda w 2022 r. specjalistyczne szkolenie pt. „How to Build an Awareness Program & Using Table Top Exercises” („Jak stworzyć program na rzecz podnoszenia świadomości i korzystanie z ćwiczeń symulacyjnych”) przeznaczone specjalnie



dla EUIBA. W kontekście zorganizowanej współpracy ENISA i CERT-UE przeprowadzą również wspólne szkolenia dla EUIBA w 2022 r.

Ustęp 72

Należy zauważyć, że ćwiczenia ENISA w zakresie cyberbezpieczeństwa mają szeroki zakres i są skierowane do szerokiego grona odbiorców, w tym również do EUIBA. Podejście to odpowiada również potrzebom EUIBA, ponieważ mogą one odnieść znaczne korzyści z takich ćwiczeń z udziałem przedstawicieli państw członkowskich. Warto zauważyć, że ENISA od 2016 r. angażuje personel techniczny EUIBA jako uczestników ćwiczeń Cyber Europe, pod kierunkiem CERT-UE, który jest dedykowanym planistą dla tego okręgu. W ramach kontynuacji tych wysiłków ENISA planuje w swojej strategii ćwiczeń na 2022 r., w ramach działań związanych z budowaniem zdolności, promowanie nowego produktu do ćwiczeń, który zostanie udostępniony przy wsparciu CERT-UE, aby umożliwić organom EUIBA szkolenie w zakresie ćwiczeń samooceny.

3. Wnioski i zalecenia

ENISA i CERT-UE przyjmują zalecenie 3 (Zwiększenie koncentracji CERT-UE i ENISA na mniej dojrzałych EUIBA), które skierowano konkretnie do tych dwóch podmiotów.