PL 2022

05

Sprawozdanie specjalne

Cyberbezpieczeństwo instytucji, organów i agencji UE

Poziom przygotowania ogólnie nieadekwatny do zagrożeń

CURIA RATIONUM

EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY

Spis treści

Załączniki

Streszczenie

I W unijnym akcie o cyberbezpieczeństwie definiuje się cyberbezpieczeństwo jako „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami”. Ze względu na przetwarzanie informacji szczególnie chronionych instytucje, organy i agencje UE (EUIBA) są atrakcyjnym celem potencjalnych ataków, dokonywanych zwłaszcza przez grupy zdolne do przeprowadzania podstępnych ataków nader wyrafinowanymi metodami z zamiarem cyberszpiegostwa i w innych celach. EUIBA to wprawdzie niezależne podmioty, które posiadają autonomię administracyjną, ale są one ze sobą silnie powiązane. Oznacza to, że słabe punkty w jednej z instytucji czy agencji lub w jednym z organów UE mogą narazić pozostałe z nich na zagrożenia bezpieczeństwa.

II Zważywszy, że liczba cyberataków na EUIBA gwałtownie rośnie, celem niniejszej kontroli było ustalenie, czy instytucje, organy i agencje UE postrzegane w ujęciu całościowym ustanowiły odpowiednie rozwiązania zapewniające im ochronę przed zagrożeniami cyberbezpieczeństwa. Z ustaleń Trybunału wynika, że nie osiągnęły one poziomu przygotowania w zakresie cyberbezpieczeństwa, który byłby adekwatny do zagrożeń.

III Trybunał stwierdził, że nie zawsze wdrażane były kluczowe dobre praktyki w zakresie cyberbezpieczeństwa (w tym niektóre niezbędne środki bezpieczeństwa), a szereg EUIBA przeznacza jednoznacznie zbyt mało funduszy na cyberbezpieczeństwo. Co więcej, w niektórych EUIBA nie ustanowiono jeszcze solidnego systemu zarządzania cyberbezpieczeństwem. W wielu przypadkach brakuje strategii w zakresie bezpieczeństwa IT lub strategie takie nie zostały zatwierdzone przez kadrę kierowniczą wyższego szczebla, polityka bezpieczeństwa nie zawsze jest sformalizowana, a oceny ryzyka nie obejmują całego środowiska informatycznego. Nie we wszystkich EUIBA cyberbezpieczeństwo podlega regularnie przeprowadzanej procedurze niezależnego poświadczenia.

IV Szkolenia w zakresie cyberbezpieczeństwa nie zawsze są przeprowadzane systematycznie. Jedynie nieco ponad połowa EUIBA oferuje na bieżąco szkolenia w tym obszarze dla informatyków i specjalistów w dziedzinie bezpieczeństwa informatycznego, a niewielka ich liczba zapewnia obowiązkowe szkolenia w zakresie cyberbezpieczeństwa dla kierowników odpowiedzialnych za systemy informatyczne zawierające informacje szczególnie chronione. Ćwiczenia polegające na symulacji phishingu są ważnym narzędziem szkolenia personelu i podnoszenia poziomu świadomości, ale nie wszystkie EUIBA przeprowadzają je systematycznie.

V Chociaż w EUIBA ustanowiono struktury współpracy i wymiany informacji na temat cyberbezpieczeństwa, Trybunał zauważył, że nie wykorzystuje się w pełni potencjalnej synergii w tym obszarze. EUIBA nie wymieniają się systematycznie między sobą informacjami na temat projektów związanych z cyberbezpieczeństwem ani informacjami na temat ocen bezpieczeństwa i umów o świadczenie usług. Ponadto podstawowe narzędzia komunikacji, takie jak rozwiązania umożliwiające szyfrowanie poczty elektronicznej lub wideokonferencji, nie są w pełni interoperacyjne, co może prowadzić do mniej bezpiecznej wymiany informacji, dublowania wysiłków i wzrostu kosztów.

VI Zespół reagowania na incydenty komputerowe EUIBA (CERT-UE) i Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) to dwa najważniejsze podmioty, których zadaniem jest wspieranie EUIBA w zakresie cyberbezpieczeństwa. Z uwagi na ograniczone zasoby lub priorytetowe traktowanie innych obszarów podmioty te nie były jednak w stanie zapewnić EUIBA potrzebnego wsparcia, w szczególności jeśli chodzi o budowanie zdolności w mniej zaawansowanych EUIBA. Chociaż CERT-UE jest wysoko ceniony przez EUIBA, jego skuteczność jest zagrożona ze względu na rosnące obciążenie pracą, niestabilne finansowanie i niestabilną sytuację kadrową oraz niewystarczającą współpracę ze strony niektórych EUIBA, które nie zawsze przekazują w odpowiednim czasie informacje o słabych punktach w ich systemach oraz o istotnych cyberincydentach, które zakłóciły ich funkcjonowanie lub mogą mieć wpływ na inne EUIBA.

VII Na podstawie tych wniosków Trybunał zaleca, by:

- Komisja zwiększyła stopień przygotowania EUIBA w zakresie cyberbezpieczeństwa, przedstawiając w tym celu wniosek ustawodawczy w sprawie wprowadzenia wspólnych wiążących zasad w tym obszarze obowiązujących wszystkie instytucje, organy i agencje UE oraz zapewniając większe zasoby na rzecz CERT-UE;

- Komisja, w ramach Międzyinstytucjonalnego Komitetu ds. Transformacji Cyfrowej, promowała dalszą synergię między EUIBA w wybranych obszarach;

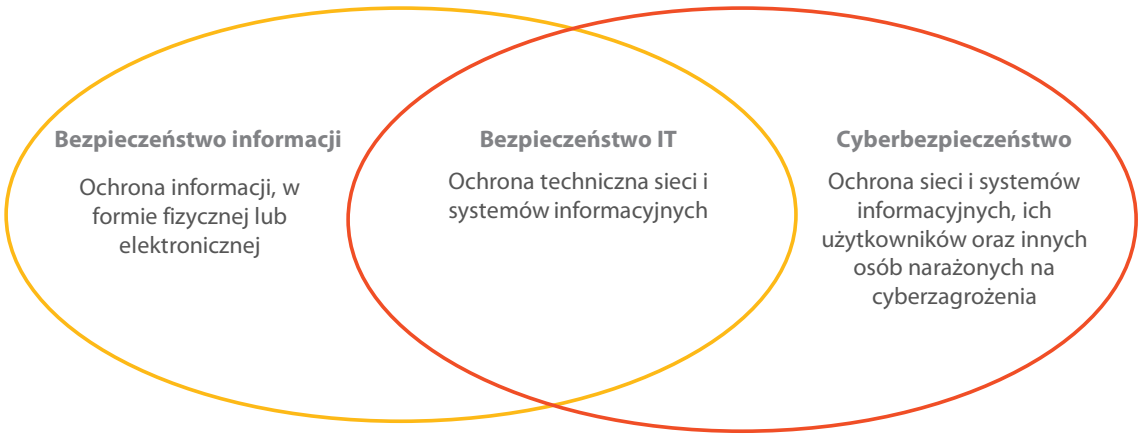
- CERT-UE i ENISA w większym stopniu koncentrowały się na tych EUIBA, które są mniej zaawansowane pod względem cyberbezpieczeństwa.

Wstęp

Czym jest cyberbezpieczeństwo?

01 W unijnym akcie o cyberbezpieczeństwie[1] definiuje się cyberbezpieczeństwo jako „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami”. Cyberbezpieczeństwo opiera się na bezpieczeństwie informacji, które z kolei polega na zachowaniu poufności, integralności i dostępności informacji[2], zarówno w formie fizycznej, jak i elektronicznej. Ochrona sieci i systemów informatycznych, w których przechowywane są takie informacje, określana jest mianem bezpieczeństwa technologii informatycznych (bezpieczeństwa IT) (zob. ***rys. 1***).

Rys. 1 – Cyberbezpieczeństwo jest powiązane z bezpieczeństwem informacji i bezpieczeństwem IT



Źródło: Europejski Trybunał Obrachunkowy.

02 Cyberbezpieczeństwo jako dyscyplina obejmuje identyfikowanie cyberincydentów i zapobieganie im, ich wykrywanie, reagowanie na nie oraz usuwanie ich skutków. Incydenty mogą obejmować na przykład przypadkowe ujawnienie informacji, ataki na infrastrukturę krytyczną oraz kradzież tożsamości i danych osobowych[3].

---

[1] Rozporządzenie (UE) 2019/881.

[2] ISO/IEC 27000:2018.

[3] Przegląd Trybunału nr 2/2019 pt. „Unijna polityka cyberbezpieczeństwa – wyzwania związane ze skuteczną realizacją” (dokument analityczny).

03 Ramy cyberbezpieczeństwa obejmują wiele elementów, w tym wymogi i kontrole techniczne w zakresie bezpieczeństwa sieci i systemów informatycznych, a także odpowiednie rozwiązania w zakresie zarządzania oraz programy podnoszenia świadomości w dziedzinie cyberbezpieczeństwa dla pracowników.

Cyberbezpieczeństwo w instytucjach, organach i agencjach UE

04 Ze względu na przetwarzanie informacji szczególnie chronionych instytucje, organy i agencje UE (EUIBA) są atrakcyjnym celem potencjalnych ataków, dokonywanych zwłaszcza przez grupy zdolne do przeprowadzania podstępnych ataków nader wyrafinowanymi metodami („zaawansowane, trwałe zagrożenia") z zamiarem cyberszpiegostwa i w innych celach[4]. Cyberataki na EUIBA – w razie powodzenia – mogą mieć poważne konsekwencje polityczne, narazić na szkodę ogólną reputację UE i podważyć zaufanie do jej instytucji.

05 Pandemia COVID-19 zmusiła EUIBA, podobnie jak wiele innych organizacji na całym świecie, do nagłego przyspieszenia transformacji cyfrowej i wprowadzenia na dużą skalę pracy zdalnej. Doprowadziło to do znacznego zwiększenia liczby potencjalnych punktów dostępu dla atakujących (większa „powierzchnia ataku") i do tego, że w obręb strefy bezpieczeństwa każdej organizacji weszły podłączone do internetu domy pracowników i urządzenia mobilne, w których można wykorzystać nowe słabe punkty. Usługi zdalnego dostępu są jedną z najczęściej wybieranych dróg, za pomocą których grupy stwarzające dla EUIBA zaawansowane, trwałe zagrożenia zyskują wstępny dostęp do ich sieci[5].

06 Liczba cyberincydentów rośnie, a szczególnie niepokojącą tendencją jest drastyczny wzrost liczby istotnych incydentów mających wpływ na EUIBA[6]. Rok 2021 był pod tym względem rekordowy. Istotne incydenty wyróżniają się tym, że nie są powtarzalne, a ich wpływ jest bardziej poważny. Dochodzi do nich zwykle z wykorzystaniem nowych metod i technologii, a ich zbadanie i wyeliminowanie ich skutków może zająć wiele tygodni, jeśli nie miesięcy. W latach 2018–2021 liczba istotnych incydentów wzrosła ponad dziesięciokrotnie[7]. Zaledwie w ciągu ostatnich

---

[4] CERT-UE, „Threat Landscape Report", czerwiec 2021 r.

[5] Tamże.

[6] Tamże.

[7] Tamże.

dwóch lat istotne incydenty dotknęły co najmniej 22 EUIBA. Jednym z niedawnych przykładów był cyberatak na Europejską Agencję Leków, w następstwie którego doszło do wycieku danych wrażliwych i manipulowania nimi w sposób mający na celu podważenie zaufania do szczepionek[8].

07 EUIBA to bardzo niejednorodna grupa, składająca się z instytucji, agencji i szeregu różnych organów. Wszystkie siedem instytucji UE zostało ustanowionych na mocy Traktatów. Z kolei agencje zdecentralizowane i inne organy UE są ustanawiane na mocy aktów prawa wtórnego i jako takie stanowią odrębne podmioty prawne. Wyróżnia się przy tym dwie formy prawne agencji – istnieje sześć agencji wykonawczych Komisji i 37 agencji zdecentralizowanych UE[9]. W skład EUIBA wchodzą również biura UE, korpus dyplomatyczny (Europejska Służba Działań Zewnętrznych), wspólne przedsięwzięcia i inne organy. Podmioty te są odpowiedzialne za ustanawianie własnych wymogów w zakresie cyberbezpieczeństwa i wdrażanie własnych środków bezpieczeństwa.

08 Aby wzmocnić cyberbezpieczeństwo EUIBA, w 2012 r. Komisja powołała zespół reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT-UE) jako stałą grupę zadaniową. CERT-UE działa w roli centrum wymiany informacji na temat cyberbezpieczeństwa i stanowi dla EUIBA punkt koordynacji działań w odpowiedzi na incydenty. Współpracuje on z innymi zespołami reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) w państwach członkowskich i z wyspecjalizowanymi przedsiębiorstwami zajmującymi się bezpieczeństwem IT. Organizacja i funkcjonowanie CERT-UE są obecnie regulowane porozumieniem międzyinstytucjonalnym z 2018 r.[10] między poszczególnymi EUIBA, które CERT-UE obsługuje, określanymi mianem „podmiotów uczestniczących”. Obecnie CERT-UE liczy 87 podmiotów uczestniczących.

09 Innym kluczowym podmiotem wspierającym EUIBA jest Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), której zadaniem jest osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej UE. Misją ustanowionej w 2004 r. ENISA jest zwiększenie wiarygodności produktów, procesów i usług technologii informacyjno-komunikacyjnych (ICT) w ramach programów certyfikacji

---

[8] „Cyberattack on EMA – update 6”, 25.1.2021.

[9] Sprawozdanie specjalne Europejskiego Trybunału Obrachunkowego nr 22/2020 pt. „Przyszłość agencji UE – istnieją możliwości, by zwiększyć elastyczność i zacieśnić współpracę”, pkt 1.

[10] Dz.U. C 12 z 13.1.2018, s. 1.

cyberbezpieczeństwa, współpraca z EUIBA i państwami członkowskimi oraz pomoc im w przygotowaniu się na zagrożenia cyberbezpieczeństwa. ENISA wspiera EUIBA w budowaniu zdolności i we współpracy operacyjnej.

10 Pomimo niezależności instytucjonalnej EUIBA są ze sobą ściśle powiązane. Codziennie wymieniają się one informacjami oraz korzystają z szeregu wspólnych systemów i sieci. Słabe punkty w jednej instytucji czy agencji lub w jednym z organów UE mogą narazić pozostałe z nich na zagrożenia bezpieczeństwa, ponieważ wiele cyberataków wymaga więcej niż jednego etapu do osiągnięcia ostatecznego celu[11]. Udany atak na słabszą EUIBA może stanowić przyczółek do ataków na inne podmioty. EUIBA są również powiązane z podmiotami publicznymi i prywatnymi w państwach członkowskich, w związku z czym – w przypadku niewystarczającego stopnia przygotowania pod względem cyberbezpieczeństwa – mogą narazić je na cyberzagrożenia.

11 Obecnie nie ma ram prawnych, które dotyczyłyby bezpieczeństwa informacji i cyberbezpieczeństwa w EUIBA. Instytucje, organy i agencje UE nie podlegają najszerszemu prawodawstwu UE w dziedzinie cyberbezpieczeństwa, tj. dyrektywie w sprawie bezpieczeństwa sieci i informacji z 2016 r.[12] ani jej proponowanej zmienionej wersji, tj. dyrektywie NIS 2[13]. Brak jest również kompleksowych informacji na temat kwoty wydatków EUIBA na cyberbezpieczeństwo.

---

[11] ENISA, „Threat Landscape 2020”, sektorowa/tematyczna analiza zagrożeń.

[12] Dyrektywa (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

[13] Wniosek dotyczący dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii.

12 W lipcu 2020 r. Komisja opublikowała komunikat w sprawie strategii UE w zakresie unii bezpieczeństwa[14] na lata 2020–2025. Do kluczowych działań przewidzianych w tym komunikacie należą „wspólne dla wszystkich instytucji, organów i agencji Unii przepisy dotyczące bezpieczeństwa informacji i cyberbezpieczeństwa". Te nowe ramy mają stanowić podstawę silnej i skutecznej współpracy operacyjnej, w której centralną rolę odgrywa CERT-UE. W strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę[15], opublikowanej w grudniu 2020 r., Komisja zobowiązała się do przedstawienia wniosku dotyczącego rozporządzenia w sprawie wspólnych zasad cyberbezpieczeństwa dla wszystkich EUIBA. Zaproponowała w niej również ustanowienie nowej podstawy prawnej dla CERT-UE w celu wzmocnienia jego mandatu i zwiększenia finansowania.

[14] COM(2020) 605 final.

[15] JOIN(2020) 18 final.

Zakres kontroli i podejście kontrolne

13 Zważywszy na to, że liczba cyberataków na EUIBA gwałtownie rośnie, a słabe punkty w jednej instytucji bądź agencji lub w jednym z organów UE mogą narazić pozostałe z nich na zagrożenia bezpieczeństwa, celem niniejszej kontroli było ustalenie, czy EUIBA w ujęciu całościowym ustanowiły odpowiednie rozwiązania zapewniające im ochronę przed zagrożeniami cyberbezpieczeństwa. Aby odpowiedzieć na to główne pytanie kontrolne, Trybunał podzielił je na trzy pytania szczegółowe:

1) Czy wszystkie EUIBA przyjęły kluczowe praktyki w zakresie cyberbezpieczeństwa?

2) Czy istnieje skuteczna współpraca między poszczególnymi EUIBA w zakresie cyberbezpieczeństwa?

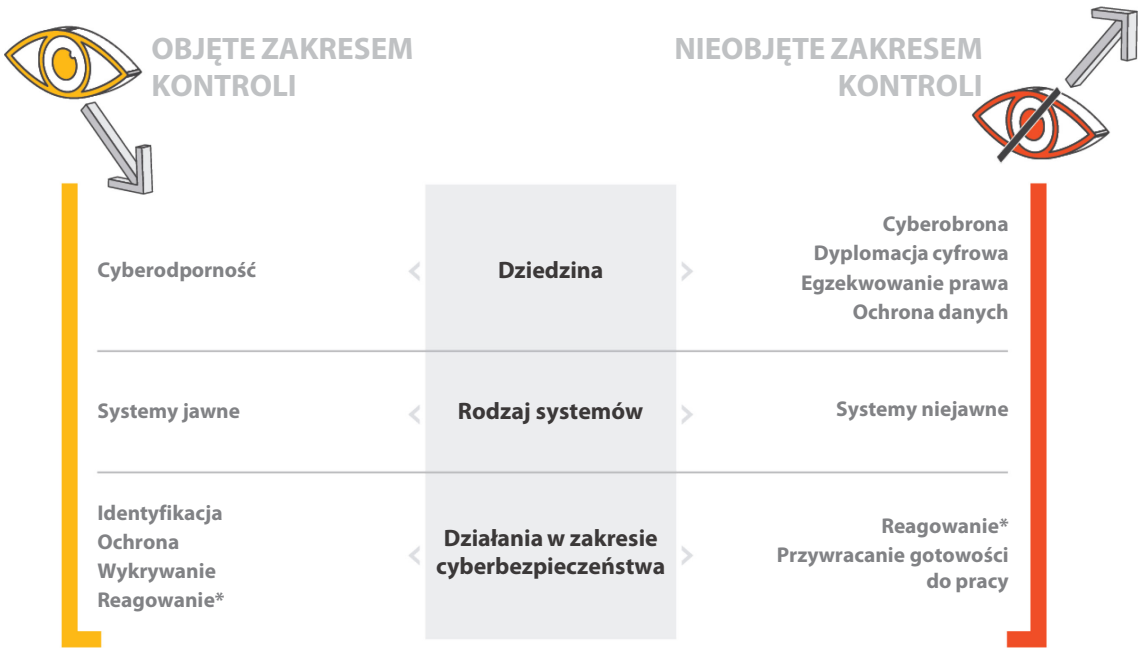
3) Czy ENISA i CERT-UE zapewniają EUIBA odpowiednie wsparcie w dziedzinie cyberbezpieczeństwa?

14 Moment przeprowadzenia kontroli wybrano z uwzględnieniem prac nad strategią UE w zakresie unii bezpieczeństwa. Dokonując oceny obecnych rozwiązań przyjętych przez EUIBA w zakresie cyberbezpieczeństwa, Trybunał pragnie wskazać obszary wymagające poprawy, co Komisja może wziąć pod uwagę przy sporządzaniu wniosku ustawodawczego dotyczącego wspólnych wiążących zasad cyberbezpieczeństwa obowiązujących wszystkie EUIBA.

15 Kontrolą objęto zmiany i inicjatywy w dziedzinie cyberbezpieczeństwa począwszy od stycznia 2018 r. (kiedy przyjęto porozumienie międzyinstytucjonalne dotyczące CERT-UE) do października 2021 r.

16 Trybunał ograniczył się w swojej kontroli do cyberodporności i systemów jawnych. Skoncentrował się na przy tym na aspektach gotowości (działania związane z „identyfikacją, ochroną, wykrywaniem”), natomiast „reagowanie” i „przywracanie gotowości do pracy” wykraczały poza zakres kontroli. Trybunał zbadał jednak pewne elementy organizacyjne reagowania na incydenty. Aspekty ochrony danych, egzekwowania prawa, cyberobrony i dyplomacji cyfrowej nie weszły w zakres kontroli (zob. ***rys. 2***).

Rys. 2 – Zakres kontroli



** Trybunał zbadał tylko niektóre aspekty organizacyjne reagowania na incydenty. Pozostałe aspekty nie wchodziły w zakres kontroli.*

Źródło: Europejski Trybunał Obrachunkowy.

17 Ustalenia z kontroli przeprowadzonej przez Trybunał opierają się na dogłębnej analizie dostępnej dokumentacji oraz na wywiadach. Trybunał przeprowadził także ankietę skierowaną do 65 EUIBA w celu zebrania informacji na temat przyjętych przez nie rozwiązań w zakresie cyberbezpieczeństwa oraz ich opinii na temat współpracy międzyinstytucjonalnej. Ankietę przeprowadzono we wszystkich EUIBA, które wchodzą w zakres uprawnień kontrolnych Trybunału i które zarządzają własną infrastrukturą informatyczną, a także w samym Trybunale. Ankieta objęła zatem instytucje, agencje zdecentralizowane, wspólne przedsięwzięcia i organy. Trybunał skierował również ankietę do misji cywilnych, które są tymczasowymi autonomicznymi podmiotami finansowanymi z budżetu UE, niezależnymi z punktu widzenia IT.
W ***załączniku I*** zamieszczono pełną listę EUIBA objętych ankietą. Europejski Rzecznik Praw Obywatelskich i Europejski Inspektor Ochrony Danych nie weszli w zakres niniejszej kontroli.

18 Odsetek podmiotów, które udzieliły odpowiedzi, wyniósł 100%, a zebrane dane posłużyły za punkt wyjścia do dalszej analizy. Ponadto Trybunał dobrał próbę siedmiu EUIBA, która jest reprezentatywna z punktu widzenia ich różnorodności, i po otrzymaniu ich odpowiedzi przeprowadził wywiady z ich przedstawicielami i zwrócił się o przekazanie odnośnej dokumentacji. Dokonując wyboru EUIBA, Trybunał jako kryteria wziął pod uwagę podstawę prawną, wielkość (pod względem personelu i budżetu) oraz sektor działalności. W skład próby dobranej przez Trybunał weszły

Komisja Europejska, Parlament Europejski, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), Europejski Urząd Nadzoru Bankowego (EUNB), Europejska Agencja Bezpieczeństwa Morskiego (EMSA), misja doradcza UE na Ukrainie (EUAM Ukraine) oraz Wspólne Przedsięwzięcie na rzecz Drugiej Inicjatywy w zakresie Leków Innowacyjnych (Wspólne Przedsięwzięcie IMI).

19 Trybunał przeprowadził również wideokonferencje z CERT-UE, Komitetem Doradczym ds. Technologii Informacyjno-Komunikacyjnych (ICTAC), Międzyinstytucjonalnym Komitetem ds. Transformacji Cyfrowej (ICDT) i innymi zainteresowanymi stronami.

Uwagi

EUIBA wykazują bardzo zróżnicowane poziomy zaawansowania w zakresie cyberbezpieczeństwa i nie zawsze przestrzegają dobrych praktyk

20 W niniejszej sekcji przeanalizowano rozwiązania i ramy cyberbezpieczeństwa przyjęte przez poszczególne EUIBA. Trybunał ocenił, czy ich podejście do cyberbezpieczeństwa jest spójne i odpowiednie, jeśli chodzi o zarządzanie bezpieczeństwem IT, zarządzanie ryzykiem, przydział zasobów, szkolenia, środki bezpieczeństwa i niezależne poświadczenie.

Zarządzanie bezpieczeństwem IT w EUIBA często nie jest dobrze rozwinięte, a oceny ryzyka nie są kompleksowe

W wielu EUIBA występują luki w zarządzaniu bezpieczeństwem IT

21 Dobre zarządzanie odgrywa zasadniczą rolę w skutecznych ramach bezpieczeństwa informacji i systemów informatycznych, ponieważ wytycza cele organizacji i wyznacza kierunek poprzez ustalanie priorytetów i podejmowanie decyzji. Według Stowarzyszenia Audytu i Kontroli Systemów Informacyjnych (ISACA)[16] ramy zarządzania bezpieczeństwem IT powinny zasadniczo obejmować kilka elementów:

- kompleksową strategię bezpieczeństwa nierozerwalnie związaną z celami biznesowymi;
- politykę zarządzania bezpieczeństwem odnoszącą się do wszystkich aspektów strategii, środków bezpieczeństwa i regulacji;
- kompletny zestaw standardów dla każdej polityki opisujący kroki operacyjne niezbędne do zapewnienia zgodności z tą polityką;
- zinstytucjonalizowane procesy monitorowania w celu zapewnienia zgodności i przekazywania informacji zwrotnych na temat skuteczności;
- skuteczną strukturę organizacyjną, w której nie występują konflikty interesów.

[16] ISACA, „Certified Information System Review Manual”, 2019.

22 Trybunał wykrył niedociągnięcia w zarządzaniu bezpieczeństwem IT w wielu EUIBA. Zaledwie 58% z nich (38 z 65) posiada strategię bezpieczeństwa IT lub przynajmniej plan bezpieczeństwa IT zatwierdzony na szczeblu zarządu/kierownictwa wyższego szczebla. Jak wynika z rozbicia EUIBA na poszczególne kategorie, odsetek ten jest najniższy wśród misji cywilnych i agencji zdecentralizowanych (które łącznie stanowią 71% ankietowanych EUIBA) (zob. ***tabela 1***). Brak zatwierdzenia strategii w zakresie bezpieczeństwa IT lub planu bezpieczeństwa IT przez kadrę kierowniczą wyższego szczebla wiąże się z ryzykiem, że kadra ta nie będzie świadoma problemów w zakresie bezpieczeństwa IT lub nie będzie w wystarczającym stopniu nadawać im priorytetu.

Tabela 1 – Odsetek EUIBA posiadających strategię lub plan bezpieczeństwa IT zatwierdzony przez kadrę kierowniczą wyższego szczebla

Podział według liczby pracowników

< 100 pracowników (22 EUIBA)	100 – 249 pracowników (17 EUIBA)	Od 250 do 1 000 pracowników (16 EUIBA)	> 1 000 pracowników (10 EUIBA)
45%	53%	69%	80%

Podział według rodzaju EUIBA

Agencje zdecentralizowane (35 EUIBA)	Misje cywilne (11 EUIBA)	Organy (4 EUIBA)	Instytucje (6 EUIBA)	Wspólne przedsięwzięcia (9 EUIBA)
45%	56%	75%	83%	89%

Źródło: ankieta Europejskiego Trybunału Obrachunkowego.

23 Trybunał przeanalizował strategie/plany bezpieczeństwa IT przedstawione przez siedem EUIBA dobranych do próby kontrolnej (zob. pkt ***18***). Stwierdził on, że strategie te są dość dobrze powiązane z celami biznesowymi. Na przykład strategia Komisji w zakresie bezpieczeństwa IT obejmuje wymiar bezpieczeństwa informatycznego strategii cyfrowej Komisji Europejskiej[17] i została opracowana z myślą o wspieraniu planu działania i celów Komisji. W swoich strategiach/planach bezpieczeństwa IT tylko trzy EUIBA objęte próbą Trybunału uwzględniły jednak konkretne cele i ramy czasowe ich realizacji.

[17] Komunikat do Komisji, Strategia cyfrowa Komisji Europejskiej: Przekształcona pod względem cyfrowym, zorientowana na użytkownika i oparta na danych Komisja, C(2018) 7118 final, 21.11.2018.

24 Polityka bezpieczeństwa określa zasady i procedury, których muszą przestrzegać osoby korzystające z informacji i zasobów informatycznych lub nimi zarządzające. Pomagają one ograniczać zagrożenia dla cyberbezpieczeństwa i wskazują, jak należy postępować w przypadku incydentów. Trybunał ustalił, że 78% EUIBA posiada formalną politykę bezpieczeństwa informacji, a jedynie 60% przyjęło formalną politykę bezpieczeństwa IT (definicje bezpieczeństwa informacji i bezpieczeństwa IT – zob. ***rys. 1***). Trybunał stwierdził również, że cztery z siedmiu EUIBA objętych próbą mają politykę bezpieczeństwa zgodną z ich własnymi strategiami w zakresie bezpieczeństwa IT. Jednak w trzech z tych czterech EUIBA strategiom w zakresie bezpieczeństwa IT jedynie częściowo towarzyszą aktualne szczegółowe standardy bezpieczeństwa zawierające opis działań operacyjnych niezbędnych do wdrożenia tych polityk. Brak formalnych standardów bezpieczeństwa zwiększa ryzyko, że problemy w zakresie bezpieczeństwa IT nie zostaną odpowiednio i spójnie rozwiązane w ramach tej samej EUIBA. Ponadto utrudnia to ocenę przestrzegania przez organizację jej polityki w zakresie bezpieczeństwa IT. Spośród siedmiu EUIBA objętych próbą jedynie Komisja posiada ustrukturyzowane procedury monitorowania zgodności ze swoimi politykami i standardami w zakresie bezpieczeństwa IT, chociaż korzysta z nich jedynie ograniczona liczba dyrekcji generalnych (zob. ***ramka 1***).

Ramka 1

Przestrzeganie przepisów w zakresie bezpieczeństwa IT w Komisji

Zgodnie z modelem zdecentralizowanego zarządzania IT przyjętym w Komisji osoba stojąca na czele każdej dyrekcji generalnej jest właścicielem usługi, rozliczalnym i odpowiedzialnym za to, by systemy spełniały standardy bezpieczeństwa IT. Dyrekcja Generalna ds. Informatyki (DG DIGIT) i Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa (DG HR) monitorują i ułatwiają wdrażanie praktyk w zakresie zarządzania zgodnością z tymi standardami. DG DIGIT stworzyła narzędzie (pod nazwą „GRC"), które umożliwia dyrekcjom generalnym pomiar przestrzegania środków bezpieczeństwa w ramach polityki bezpieczeństwa informatycznego oraz przekazywanie odnośnych sprawozdań.

580 środków bezpieczeństwa dzieli się na trzy grupy: ogólne środki bezpieczeństwa (głównie w zakresie zarządzania), środki bezpieczeństwa dotyczące poszczególnych dyrekcji generalnych oraz środki dotyczące poszczególnych systemów. Narzędzie to jest dostępne, ale jak dotąd korzysta z niego tylko pięć dyrekcji generalnych. DG DIGIT nie ma zatem pełnego obrazu sytuacji, jeśli chodzi o zgodność ze standardami w całej Komisji. Działająca przy Komisji Rada ds. Technologii Informacyjnej i Cyberbezpieczeństwa (ITCB) może jednak zwrócić się do DG DIGIT o zbadanie zgodności z konkretnym standardem (np. uwierzytelnianie wieloskładnikowe w 2021 r.) i może wydawać niewiążące opinie i zalecenia lub – w przypadku krytycznych zagrożeń – również nakładać wymogi formalne.

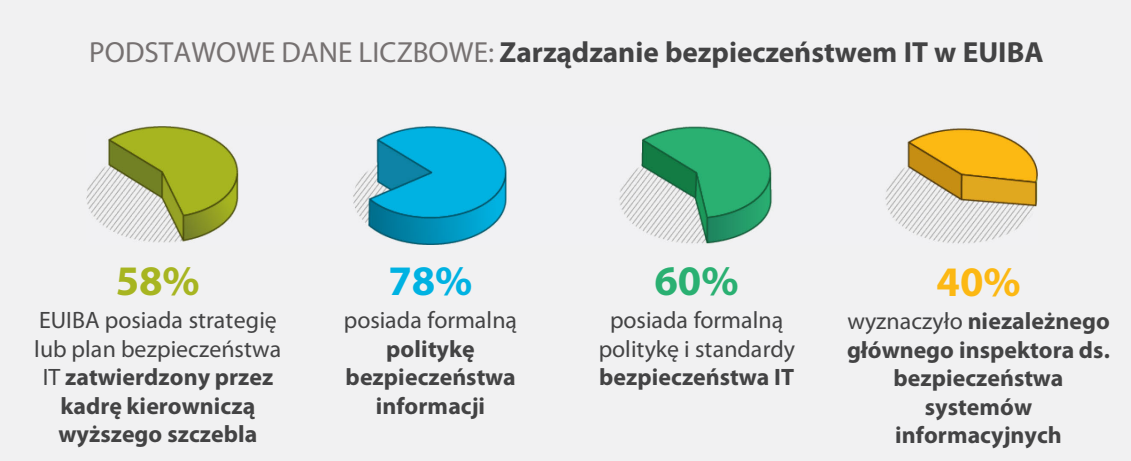
25 Kolejnym elementem istotnym dla dobrego zarządzania cyberbezpieczeństwem jest mianowanie głównego inspektora ds. bezpieczeństwa systemów informacyjnych (CISO). Chociaż nie jest to wyraźnie wymagane na mocy norm ISO 27000[18], funkcja CISO lub równoważna stała się powszechną praktyką w organizacjach i stanowi część wytycznych ISACA. Zazwyczaj CISO ponosi ogólną odpowiedzialność za programy bezpieczeństwa informacji i bezpieczeństwa IT danej organizacji. Aby uniknąć konfliktu interesów, CISO powinien być w pewnym stopniu niezależny od pionu/działu IT[19].

26 Jak wynika z ankiety przeprowadzonej przez Trybunał, 60% EUIBA nie wyznaczyło niezależnego CISO ani nie stworzyło równoważnej funkcji. Nawet w przypadku mianowania CISO (lub stworzenia równoważnej funkcji) jego rola różni się znacznie pod względem charakteru w zależności od EUIBA, a jego zadania są różnie rozumiane. Zwłaszcza w przypadku małych i średnich EUIBA CISO są zazwyczaj powiązani

[18] Norma ISO/IEC 27000:2018, rozdział 5.

[19] COBIT 5 – Bezpieczeństwo informacji, sekcja 4.2.

z funkcjami o charakterze bardziej operacyjnym i nie są funkcjonalnie niezależni od działu IT.
Może to ograniczać autonomię CISO w realizacji priorytetów w zakresie bezpieczeństwa. ENISA pracuje obecnie nad unijnymi ramami umiejętności w zakresie cyberbezpieczeństwa, których celem jest m.in. wypracowanie wspólnego rozumienia ról, kompetencji i umiejętności.



Oceny ryzyka w zakresie bezpieczeństwa IT przeprowadzane przez EUIBA w większości przypadków nie obejmują ich całego środowiska informatycznego

27 We wszystkich międzynarodowych standardach bezpieczeństwa IT podkreśla się znaczenie ustanowienia odpowiedniej metody oceny i procedur postępowania w przypadku wystąpienia zagrożeń dla bezpieczeństwa systemów IT i zawartych w nich danych. Oceny ryzyka powinny być przeprowadzane okresowo, tak aby uwzględnić zmiany w wymogach danej organizacji w zakresie bezpieczeństwa informacji oraz zagrożenia, na jakie jest ona narażona[20]. Po dokonaniu oceny należy sporządzić plan ograniczenia ryzyka (lub plan bezpieczeństwa IT).

28 Większość zbadanych EUIBA (58 z 65) wskazała, że posiada ramy lub metodykę przeprowadzania ocen ryzyka dotyczących ich systemów informatycznych. Brak jest jednak wspólnej metodyki, która byłaby stosowana przez wszystkie EUIBA. Co najmniej 26 EUIBA wykorzystuje częściowo lub w pełni metody opracowane przez Komisję, a 31% EUIBA korzystało w szczególności z metodyki zarządzania ryzykiem w zakresie bezpieczeństwa IT z 2018 r. (ITSRM2). Pozostałe z nich stosują metody oparte na dobrze znanych standardach branżowych (takich jak ISO27001, ISO27005, ramy cyberbezpieczeństwa Krajowego Instytutu Norm i Technologii (NIST-CSF) lub środki

[20] Zob. np. ISO/IEC 27000:2018, sekcja 4.5.

bezpieczeństwa opracowane przez Center for Internet Security) bądź stosują inne metody wewnętrzne.

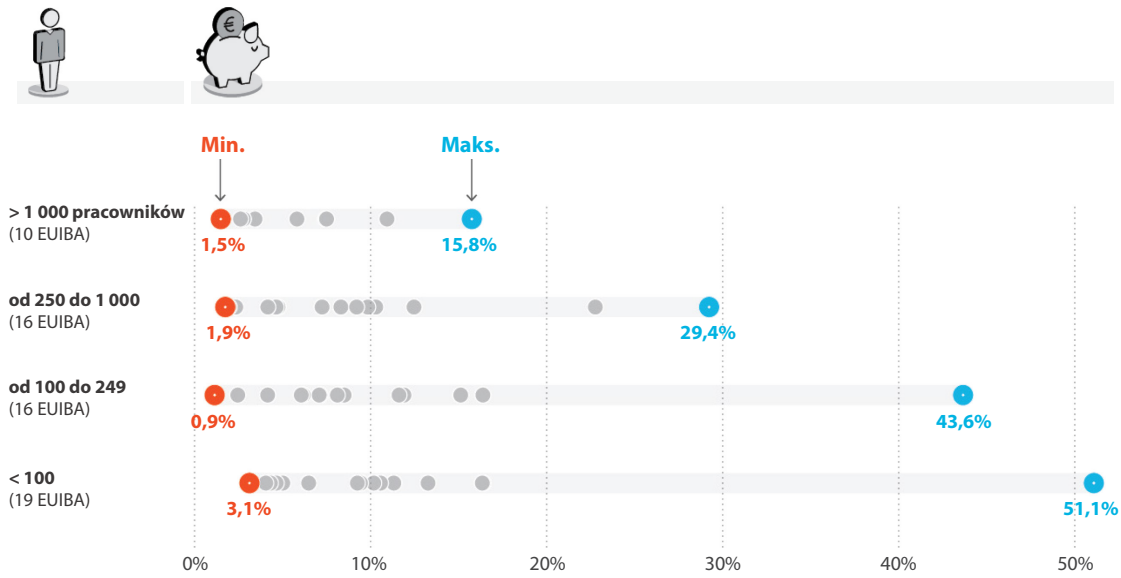
29 Spośród siedmiu EUIBA objętych próbą tylko dwa podmioty przeprowadzają kompleksowe oceny ryzyka obejmujące całe środowisko informatyczne (tj. wszystkie systemy informatyczne). Większość przeprowadza indywidualne oceny ryzyka wyłącznie w odniesieniu do swoich najważniejszych systemów informatycznych. Trybunał zidentyfikował kilka przykładów ocen ryzyka przeprowadzonych przed wdrożeniem nowych systemów. Nie znalazł jednak dowodów, które świadczyłyby o kolejnych ocenach ryzyka, na przykład w następstwie późniejszych zmian w systemach/infrastrukturze.

EUIBA nie mają spójnego podejścia do cyberbezpieczeństwa, a podstawowe środki bezpieczeństwa nie zawsze są stosowane

Przydział zasobów na cyberbezpieczeństwo znacznie się różni w poszczególnych EUIBA

30 W ankiecie Trybunał zwrócił się do EUIBA o podanie łącznej kwoty wydatków na technologie informatyczne w 2020 r. oraz szacunkowej kwoty wydatków na cyberbezpieczeństwo. Uzyskane przez Trybunał dane wskazują na znaczne różnice, jeśli chodzi o odsetek wydatków na IT, jaki poszczególne EUIBA przeznaczyły na cyberbezpieczeństwo. Dotyczy to nawet EUIBA podobnej wielkości pod względem liczby pracowników. Jak pokazano na ***rys. 3***, różnice są szczególnie duże w przypadku EUIBA zatrudniających mniejszą liczbę pracowników.

Rys. 3 – Wydatki na cyberbezpieczeństwo jako odsetek całkowitych wydatków na IT (EUIBA pogrupowane według liczby pracowników)



Uwaga: Cztery EUIBA nie przedstawiły danych na temat wielkości wydatków na cyberbezpieczeństwo.

Źródło: ankieta Europejskiego Trybunału Obrachunkowego.

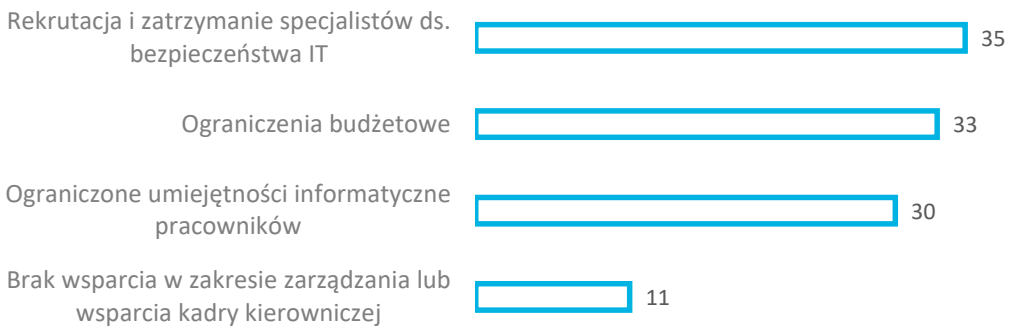
31 Optymalny poziom wydatków na cyberbezpieczeństwo jest trudny do oszacowania w ujęciu bezwzględnym. Zależy on od wielu czynników, takich jak powierzchnia ataku danej organizacji, wrażliwość przetwarzanych przez nią danych, profil ryzyka i apetyt na ryzyko oraz sektorowe wymogi prawne/regulacyjne. Z danych uzyskanych przez Trybunał wynika jednak, że różnice są znaczne, a ich przyczyny nie zawsze są oczywiste. W niektórych EUIBA kwota wydatków na cyberbezpieczeństwo jest znacznie mniejsza niż w innych, mimo iż są one podobnych rozmiarów. Może to wskazywać na niedoinwestowanie, w przypadku gdy są one narażone na podobne zagrożenia i ryzyko.

32 Większość EUIBA to małe i średnie organizacje zarówno pod względem liczby pracowników, jak i wydatków na IT, przy czym dwie trzecie z nich zatrudnia mniej niż 350 pracowników. Najmniejsza EUIBA zatrudnia jedynie 15 pracowników. Zarządzanie cyberbezpieczeństwem jest trudniejsze i wymaga większych zasobów w przypadku mniejszych EUIBA. W większości przypadków takie EUIBA nie mogą korzystać z korzyści skali i nie posiadają wystarczającej wewnętrznej wiedzy specjalistycznej. Jak wynika z ankiety i wywiadów Trybunału, największe instytucje, takie jak Komisja i Parlament Europejski, posiadają zespoły ekspertów, którzy zajmują się cyberbezpieczeństwem w pełnym wymiarze czasu pracy. W najmniejszych EUIBA z kolei, w których personel i zasoby są szczególnie ograniczone, nie ma w ogóle ekspertów, a cyberbezpieczeństwem zarządza – w niepełnym wymiarze czasu pracy – personel

posiadający doświadczenie informatyczne. Ponieważ EUIBA są silnie ze sobą powiązane, przekłada się to na większe ryzyko (zob. również pkt ***10***).

33 W ankiecie Trybunał zapytał EUIBA o najważniejsze wyzwania, jakie stoją przed nimi w związku z wdrażaniem skutecznej polityki w zakresie cyberbezpieczeństwa (zob. ***rys. 4***). Największym wyzwaniem jest brak wystarczającej liczby ekspertów ds. cyberbezpieczeństwa, a wiele EUIBA ma trudności z ich pozyskaniem ze względu na konkurencję zarówno ze strony sektora prywatnego, jak i innych EUIBA. Ponadto często wspominały one o długich procedurach rekrutacyjnych, niekonkurencyjnych warunkach umownych i braku atrakcyjnych perspektyw zawodowych. Niedobór wyspecjalizowanych pracowników stanowi poważne zagrożenie dla prowadzenia skutecznych działań w zakresie cyberbezpieczeństwa.

Rys. 4 – Wyzwania związane z wdrażaniem skutecznej polityki w zakresie cyberbezpieczeństwa w EUIBA (można było wskazać więcej niż jeden czynnik)



Źródło: ankieta Europejskiego Trybunału Obrachunkowego.

Większość EUIBA oferuje szkolenia na temat cyberbezpieczeństwa, ale nie są one systematyczne ani właściwie ukierunkowane

34 Wykorzystanie słabych punktów w systemach i urządzeniach nie jest jedynym sposobem na spowodowanie szkód przez potencjalnych sprawców ataków. Mogą oni również skłonić użytkowników do ujawnienia informacji szczególnie chronionych lub do pobrania złośliwego oprogramowania, na przykład za pomocą phishingu lub ataków socjotechnicznych. Personel to część pierwszej linii obrony w każdej organizacji. W związku z tym kluczowym elementem skutecznych ram cyberbezpieczeństwa są programy mające na celu podniesienie poziomu świadomości oraz szkolenia w tym zakresie.

35 Zdecydowana większość ankietowanych EUIBA (95%) – z wyjątkiem trzech – zapewnia wszystkim pracownikom jakąś formę ogólnych szkoleń podnoszących świadomość w dziedzinie cyberbezpieczeństwa. Jednak tylko 41% EUIBA organizuje specjalne szkolenia lub sesje informacyjne dla kadry kierowniczej, a jedynie 29% zapewnia obowiązkowe szkolenia w zakresie cyberbezpieczeństwa dla kierowników odpowiedzialnych za systemy informatyczne zawierające informacje szczególnie chronione. Tymczasem świadomość i zaangażowanie kadry kierowniczej mają kluczowe znaczenie dla skutecznego zarządzania cyberbezpieczeństwem. Spośród jedenastu EUIBA, w których brak wsparcia ze strony kadry kierowniczej wskazano jako wyzwanie dla skutecznego cyberbezpieczeństwa, tylko trzy zapewniły swojemu kierownictwu szkolenia mające na celu podniesienie świadomości. 58% EUIBA oferuje na bieżąco szkolenia w tym obszarze dla informatyków, a 51% dla specjalistów w dziedzinie bezpieczeństwa informatycznego.

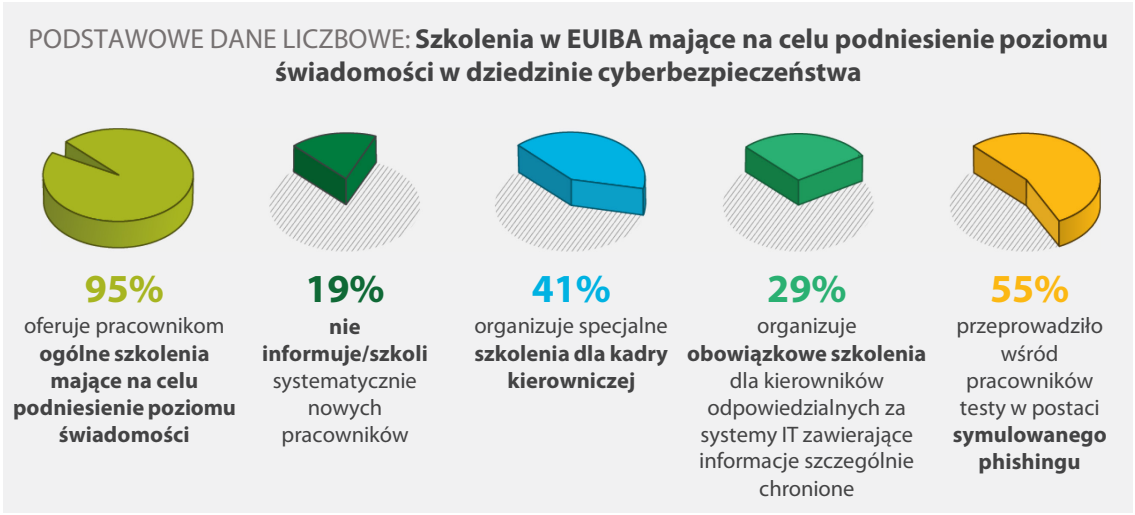
36 Nie wszystkie EUIBA dysponują mechanizmami umożliwiającymi monitorowanie uczestnictwa pracowników w szkoleniach w dziedzinie cyberbezpieczeństwa oraz zachodzących w ich następstwie zmian w poziomie wiedzy i zachowaniu pracowników. Zwłaszcza w mniejszych organizacjach sesje informacyjne na temat cyberbezpieczeństwa można organizować w ramach nieformalnych spotkań pracowników. Głównym sposobem pomiaru przez organizacje poziomu wiedzy pracowników jest okresowe testowanie ich zachowań, w tym poprzez ankiety dotyczące ich umiejętności lub ćwiczenia polegające na symulacji phishingu. W ciągu ostatnich pięciu lat 55% EUIBA zorganizowało co najmniej jedną symulowaną kampanię phishingową (lub podobne ćwiczenia). Jako że phishing jest jednym z głównych zagrożeń dla pracowników administracji publicznej[21], ćwiczenia w tym zakresie są ważnym narzędziem szkolenia personelu i podnoszenia świadomości. Trybunał stwierdził, że działania Komisji na rzecz podnoszenia świadomości w dziedzinie cyberbezpieczeństwa stanowią dobrą praktykę i są dostępne dla innych zainteresowanych EUIBA (zob. ***ramka 2***).

[21] ENISA, Thread Landscape 2020, sektorowa/tematyczna analiza zagrożeń.

Ramka 2

Szkolenia na rzecz podnoszenia świadomości w dziedzinie cyberbezpieczeństwa w Komisji

Komisja posiada specjalny zespół „Cyber Aware” w DG DIGIT, który kieruje korporacyjnym programem na rzecz podnoszenia świadomości w dziedzinie cyberbezpieczeństwa. Program jest zarządzany i prowadzony wspólnie z DG HR, Sekretariatem Generalnym, Dyrekcją Generalną ds. Sieci Komunikacyjnych, Treści i Technologii (DG CNECT) i CERT-UE. Szkolenia są wysokiej jakości i w wielu przypadkach mają zasięg międzyinstytucjonalny. Sesje szkoleniowe są ogłaszane w biuletynie edukacyjnym, który dociera do około 65 000 pracowników UE. Za pośrednictwem platformy „Cyber Aware” w ciągu ostatnich pięciu lat Komisja zorganizowała 15 ćwiczeń phishingowych, a ostatnio przeprowadziła pierwsze ćwiczenie obejmujące całą instytucję.



Podstawowe środki bezpieczeństwa nie zawsze są wdrażane lub nie są sformalizowane w postaci standardów

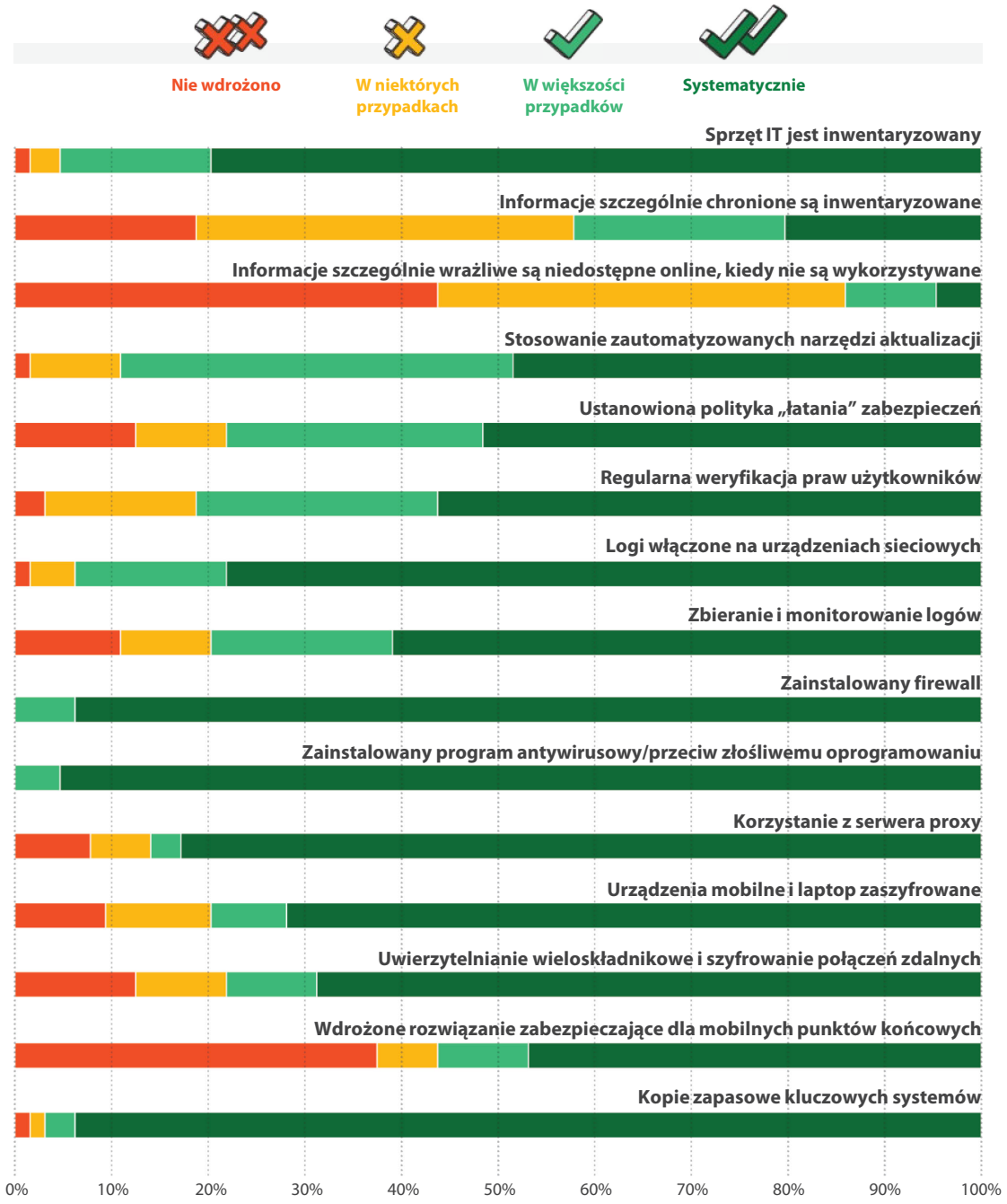
37 Trybunał zwrócił się do EUIBA o samoocenę wdrożenia przez nie wybranych podstawowych środków bezpieczeństwa[22]. Wybrał w tym celu zestaw najlepszych praktyk, które nawet mniejsze organizacje mogłyby w rozsądny sposób wdrożyć[23]. Rezultaty przedstawiono na ***rys. 5***. Większość zbadanych EUIBA przyjęła wybrane

[22] Zestaw środków bezpieczeństwa pochodzący z ramowego dokumentu CIS 7.1, w którym przedstawiono najlepsze praktyki opracowane przez Centre for Internet Security.

[23] Grupa wdrożeniowa 1 (IG1) środków bezpieczeństwa CIS.

podstawowe środki bezpieczeństwa. W co najmniej 20% EUIBA w niektórych obszarach środki bezpieczeństwa wydają się jednak niewystarczające lub ograniczone.

Rys. 5 – Wdrożenie podstawowych środków bezpieczeństwa w EUIBA (wyniki samooceny)



Źródło: ankieta Europejskiego Trybunału Obrachunkowego.

38 W przypadku siedmiu EUIBA objętych próbą Trybunał zwrócił się o dokumentację i odnośne standardy/strategie w odniesieniu do każdego środka bezpieczeństwa, który EUIBA zadeklarowały jako wdrożony. Trybunał uzyskał te dokumenty w odniesieniu do 62% środków bezpieczeństwa. Jak wyjaśniono w trakcie wywiadów, w kilku

przypadkach wprowadzono techniczne środki bezpieczeństwa, ale nie sformalizowano ich w postaci – aktualnych – standardów lub strategii, co zwiększa ryzyko, że problemy w zakresie bezpieczeństwa IT nie będą rozwiązywane spójnie w ramach tej samej EUIBA (zob. również pkt ***24***).

W szeregu EUIBA rozwiązania w zakresie cyberbezpieczeństwa nie podlegają regularnie przeprowadzanej procedurze niezależnego poświadczenia

39 Według ISACA[24] audyt wewnętrzny to obok zarządzania i zarządzania ryzykiem jedna z trzech podstawowych linii obrony w organizacji. Audyty wewnętrzne przyczyniają się do poprawy bezpieczeństwa informacji i bezpieczeństwa IT. Trybunał zbadał, jak często EUIBA uzyskują niezależne poświadczenie swoich ram bezpieczeństwa informatycznego w drodze audytów wewnętrznych lub zewnętrznych oraz poprzez proaktywne testowanie mechanizmów cyberobrony.

40 Służba Audytu Wewnętrznego Komisji (IAS) jest odpowiedzialna m.in. za przeprowadzanie audytów informatycznych w Komisji, agencjach zdecentralizowanych, wspólnych przedsięwzięciach i ESDZ. Jej mandat obejmuje 46 (70%) z 65 EUIBA, które wzięły udział w ankiecie Trybunału, a w ciągu ostatnich pięciu lat przeprowadziła ona audyty dotyczące bezpieczeństwa IT w sześciu różnych EUIBA. Ponadto DG HR jest uprawniona do przeprowadzania kontroli bezpieczeństwa IT, które obejmują techniczne aspekty bezpieczeństwa informacji[25]. Spośród pozostałych EUIBA siedem zgłosiło, że posiada własny pion audytu wewnętrznego zajmujący się również aspektami informatycznymi, a w przypadku dwunastu EUIBA odpowiedzi na ankietę Trybunału nie były wystarczające, aby stwierdzić, czy posiadają one takie zdolności w zakresie audytu wewnętrznego.

41 Zewnętrzne audyty bezpieczeństwa IT przeprowadzane przez niezależne podmioty są kolejnym sposobem na uzyskanie niezależnego poświadczenia. Pomimo szybko zmieniającego się krajobrazu cybernetycznego w okresie od początku 2015 r. do pierwszego kwartału 2021 r. 34% EUIBA nie zostało objętych wewnętrznym bądź zewnętrznym audytem bezpieczeństwa IT. Z rozbicia tych danych według rodzaju

[24] ISACA, „Auditing Cyber Security: Evaluating Risk and Auditing Controls”, 2017.

[25] Decyzja 46/2017 w sprawie bezpieczeństwa systemów teleinformatycznych w Komisji Europejskiej.

EUIBA wynika, że od 2015 r. takiemu audytowi nie zostało poddanych 75% organów UE, 66% wspólnych przedsięwzięć i 45% misji cywilnych.

42 Oprócz audytów wewnętrznych i zewnętrznych innym sposobem na uzyskanie przez organizacje poświadczenia właściwego funkcjonowania ich ram bezpieczeństwa informatycznego jest proaktywne testowanie mechanizmów cyberobrony w celu zidentyfikowania słabych punktów. Jedną z metod są testy penetracyjne (znane również jako etyczne hakowanie), polegające na symulowaniu cyberataków na poszczególne systemy komputerowe. W odpowiedzi na ankietę Trybunału 69% EUIBA stwierdziło, że w ciągu ostatnich pięciu lat przeprowadziło co najmniej jeden test penetracyjny. W 45% przypadków podmiotem przeprowadzającym takie testy był CERT-UE.

43 Ćwiczenia typu „red team” to kolejny sposób testowania mechanizmów cyberobrony. Mają one postać symulowanych ataków z wykorzystaniem najnowszych technik stosowanych w atakach rzeczywistych. Są one bardziej złożone i kompleksowe niż testy penetracyjne, ponieważ obejmują wiele systemów i potencjalnych dróg ataku. EUIBA wykonują je rzadziej: 46% z nich podało, że przeprowadziło co najmniej jedno ćwiczenie typu „red team” w ciągu ostatnich pięciu lat. 75% tych ćwiczeń przeprowadził CERT-UE. Ćwiczenia typu „red team” wymagają znacznych nakładów pracy w celu ich przygotowania i wykonania, a CERT-UE posiada obecnie zdolności do przeprowadzenia nie więcej niż pięciu do sześciu ćwiczeń rocznie.

44 Z wyłączeniem dwóch niedawno ustanowionych EUIBA, 16 (25%) EUIBA objętych ankietą nie przeprowadziło testów penetracyjnych ani ćwiczeń typu „red team” w ciągu ostatnich pięciu lat. Ogółem siedem EUIBA (10%) nie uzyskało żadnego niezależnego poświadczenia swoich rozwiązań w zakresie bezpieczeństwa IT: jedno wspólne przedsięwzięcie, jedna agencja zdecentralizowana i pięć misji cywilnych.

PODSTAWOWE DANE LICZBOWE: **Niezależne poświadczenie bezpieczeństwa IT w EUIBA w ciągu ostatnich 5 lat**

66%
EUIBA **poddano** co najmniej **jednemu wewnętrznemu lub zewnętrznemu audytowi** dotyczącemu bezpieczeństwa IT

69%
EUIBA **wykonało** co najmniej jeden **test penetracyjny**

46%
EUIBA **przeprowadziło** co najmniej jedno **ćwiczenie typu „red team"**

10%
EUIBA nie zostało **objętych niezależnym audytem ani testami** bezpieczeństwa IT

W ramach EUIBA ustanowiono mechanizmy współpracy, ale występują niedociągnięcia

45 W niniejszej sekcji omówiono podmioty i komitety ustanowione w celu promowania współpracy między EUIBA w dziedzinie cyberbezpieczeństwa, a także rozwiązania dotyczące zarządzania i koordynacji międzyinstytucjonalnej. Trybunał zbadał w szczególności dwa podmioty międzyinstytucjonalne – ENISA i CERT-UE – oraz dwa komitety międzyinstytucjonalne: Międzyinstytucjonalny Komitet ds. Transformacji Cyfrowej (ICDT), w szczególności podgrupę ds. cyberbezpieczeństwa (CSSG), oraz Komitet Doradczy ds. Technologii Informacyjno-Komunikacyjnych (ICTAC). Trybunał ocenił również, w jakim stopniu zapewniły one synergię w celu zwiększenia gotowości EUIBA w zakresie cyberbezpieczeństwa.

Ustanowiono sformalizowaną strukturę, dzięki której EUIBA koordynują swoje działania, lecz występują pewne problemy związane z zarządzaniem

46 ICDT i ICTAC to dwa najważniejsze komitety promujące współpracę w zakresie IT między EUIBA. ICDT, w skład którego wchodzą kierownicy ds. IT z instytucji i organów UE, to forum wymiany informacji i współpracy. W jego ramach utworzono podgrupę ds. cyberbezpieczeństwa (ICDT CSSG), która podlega ICDT i może zalecić podejmowanie decyzji w konkretnych kwestiach. ICTAC to natomiast podgrupa sieci agencji UE (EUAN), nieformalnej sieci utworzonej przez szefów agencji UE, która koncentruje się na współpracy między agencjami i wspólnymi przedsięwzięciami. ICDT i ICTAC pełnią jasno zdefiniowane, wzajemnie uzupełniające się role: ICTAC obejmuje agencje zdecentralizowane i wspólne przedsięwzięcia, natomiast ICDT obejmuje instytucje i organy. Już z samej swej natury ICDT i ICTAC są raczej nieformalnymi grupami doradczymi i forami wymiany informacji i najlepszych praktyk. Więcej

informacji na temat tych komitetów międzyinstytucjonalnych przedstawiono w ***załączniku II***.

EUIBA nie zawsze są odpowiednio reprezentowane na odpowiednich forach

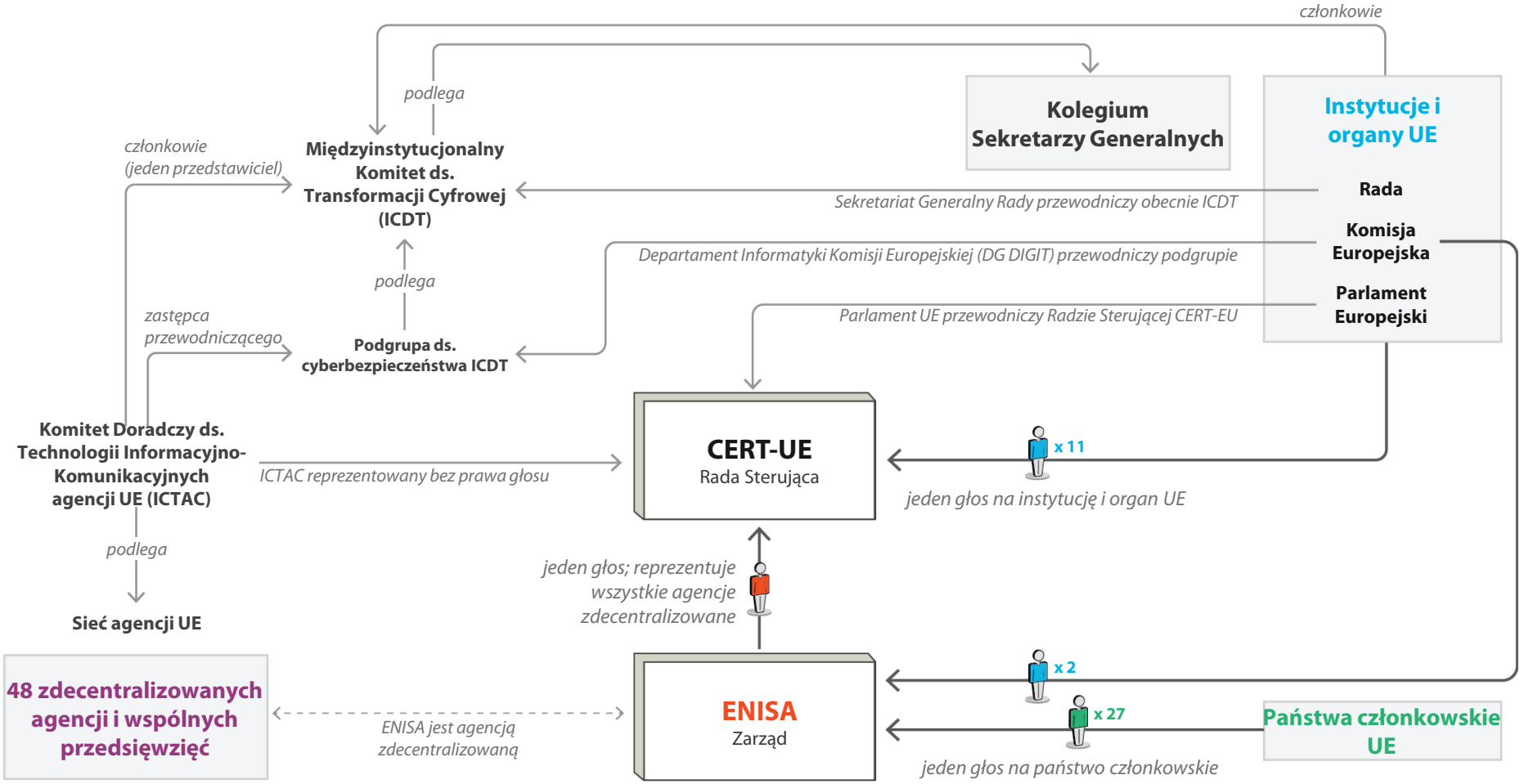
47 Chociaż struktury są jasne, nie wszystkie EUIBA uważają, że są w nich wystarczająco reprezentowane. Na pytanie w ankiecie Trybunału o opinię na temat stwierdzenia: „Moje potrzeby są w wystarczającym stopniu uwzględniane na odpowiednich forach międzyinstytucjonalnych, a moja organizacja jest odpowiednio reprezentowana w organach decyzyjnych" 42% EUIBA odpowiedziało, że się z nim nie zgadza. Niektóre z najmniejszych EUIBA stwierdziły, że nie dysponują wystarczającymi zasobami, aby aktywnie uczestniczyć w forach międzyinstytucjonalnych.

48 Rada Sterująca CERT-UE, która jest jego głównym organem decyzyjnym, nie zapewnia odpowiedniej reprezentacji wszystkich podmiotów uczestniczących. CERT-UE świadczy usługi na rzecz 87 EUIBA oraz trzech podmiotów spoza grona EUIBA. W skład jego Rady Sterującej wchodzą jednak tylko przedstawiciele 11 sygnatariuszy porozumienia międzyinstytucjonalnego (tj. siedmiu instytucji UE oraz ESDZ, Europejskiego Komitetu Ekonomiczno-Społecznego, Komitetu Regionów i Europejskiego Banku Inwestycyjnego) oraz przedstawiciel ENISA, przy czym każdy z nich dysponuje jednym głosem[26].

49 Ponad połowa podmiotów uczestniczących CERT-UE to zdecentralizowane agencje i wspólne przedsięwzięcia UE, które łącznie zatrudniają około 12 000 pracowników. Formalnie ich interesy są reprezentowane w Radzie Sterującej CERT-UE przez ENISA. Mandat ENISA do reprezentowania agencji i wspólnych przedsięwzięć UE jest jednak niewystarczający, ponieważ nie została ona przez nie bezpośrednio powołana bądź wybrana. W praktyce opinie agencji zdecentralizowanych i wspólnych przedsięwzięć są wyrażane na posiedzeniach Rady Sterującej przez przedstawiciela ICTAC, który może uczestniczyć w posiedzeniach, by wspierać ENISA w jej roli polegającej na reprezentowaniu agencji. Choć przedstawiciel ICTAC reprezentuje interesy 48 EUIBA, obecnie nie zasiada on oficjalnie w Radzie Sterującej ani nie może brać udziału w głosowaniach. W kwietniu 2021 r. ICTAC zwrócił się do przewodniczącego Rady Sterującej CERT-UE z formalnym wnioskiem o prawo głosu w Radzie. W chwili sporządzania niniejszego sprawozdania wniosek ten nie został jeszcze uwzględniony. Informacje na temat reprezentacji EUIBA w organach decyzyjnych i komitetach przedstawiono na ***rys. 6***.

[26] Art. 7 porozumienia międzyinstytucjonalnego podpisanego w dniu 20 grudnia 2017 r.

Rys. 6 – Przegląd struktur zarządzania cyberbezpieczeństwem i reprezentacji w organach decyzyjnych i komitetach



Źródło: Europejski Trybunał Obrachunkowy.

50 Międzyinstytucjonalne zarządzanie cyberbezpieczeństwem w EUIBA jest rozdrobnione i żaden pojedynczy podmiot nie dysponuje obecnie kompleksowymi informacjami na temat stopnia zaawansowania EUIBA pod względem cyberbezpieczeństwa ani uprawnieniami do odgrywania wiodącej roli bądź do egzekwowania wspólnych wiążących zasad. Zarówno ENISA, jak i CERT-UE mogą tylko „wspierać" EUIBA i „pomagać" im. Odnośne komitety nie mają uprawnień decyzyjnych i mogą jedynie formułować zalecenia pod adresem EUIBA. Ponadto jedna piąta ankietowanych EUIBA nie wie, gdzie należy się zwrócić o konkretną usługę, narzędzie lub rozwiązanie.

Istnieją protokoły ustaleń między kluczowymi podmiotami, ale jak dotąd nie przyniosły one konkretnych rezultatów

51 W maju 2018 r. podpisany został protokół ustaleń między ENISA, CERT-UE, Europejskim Centrum ds. Walki z Cyberprzestępczością Europolu (EC3) i Europejską Agencją Obrony (EDA). Skoncentrowano się w nim na pięciu obszarach współpracy: wymianie informacji, edukacji i szkoleniach, ćwiczeniach w dziedzinie cyberbezpieczeństwa, współpracy technicznej oraz kwestiach strategicznych i administracyjnych. Chociaż wspomniany protokół ustaleń mógłby pomóc uniknąć dublowania działań dzięki wspólnemu programowi prac, Trybunał nie znalazł dowodów na to, by przyniósł on konkretne rezultaty i doprowadził do podejmowania wspólnych działań.

52 W akcie o cyberbezpieczeństwie, który wszedł w życie w czerwcu 2019 r., przewidziano podpisanie nowego szczegółowego porozumienia o współpracy między CERT-UE a ENISA. Warto zauważyć, że do momentu podpisania protokołu ustaleń, co ostatecznie nastąpiło w lutym 2021 r., upłynęło ponad półtora roku. W protokole tym przewidziano ustanowienie zorganizowanej współpracy między CERT-UE a ENISA. Wskazano w nim także obszary współpracy (budowanie zdolności, współpraca operacyjna oraz wymiana wiedzy i informacji) oraz określono przybliżony podział ról: CERT-UE przejmie wiodącą rolę we wspieraniu EUIBA, a ENISA będzie ogrywać rolę wspomagającą w tych działaniach. W protokole nie określono praktycznych rozwiązań, ponieważ zostały one przedstawione w rocznym planie współpracy. Pierwszy roczny plan współpracy na 2021 r. został przyjęty przez Zarząd ENISA w lipcu 2021 r., a przez Radę Sterującą CERT-UE we wrześniu 2021 r. Jest zatem zbyt wcześnie, aby Trybunał mógł ocenić, czy plan ten przyniósł wymierne rezultaty.

53 Oba protokoły ustaleń, o których mowa w pkt ***51*** i ***52***, mają wspólne cele i obszary współpracy, takie jak szkolenia, ćwiczenia lub wymiana informacji, toteż istnieje ryzyko pokrywania się i dublowania działań.

Potencjalna synergia w ramach współpracy nie jest jeszcze w pełni wykorzystana

Podjęto pozytywne kroki w celu osiągnięcia synergii

54 W programach prac komitetów ICTAC i ICDT CSSG wskazano istotne zagadnienia, w przypadku których dzięki współpracy można osiągnąć większą wydajność. Praktyczne przykłady inicjatyw, które umożliwiły EUIBA osiągnięcie korzyści dzięki synergii, obejmują:

- międzyinstytucjonalne umowy ramowe;
- wspólny ośrodek przywracania gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej uruchomiony w 2019 r. przez Urząd Unii Europejskiej ds. Własności Intelektualnej (EUIPO) dla agencji zdecentralizowanych, umożliwiający oszczędność kosztów o co najmniej 20% w porównaniu z cenami rynkowymi (rozwiązanie to przyjęło dziewięć agencji);
- umowy między sześcioma wspólnymi przedsięwzięciami zlokalizowanymi w tym samym budynku w celu korzystania ze wspólnej infrastruktury i wspólnych ram bezpieczeństwa IT (od 2014 r.).

55 Kolejnym ważnym przykładem jest „GovSec”, czyli system, który pomaga EUIBA w przeprowadzaniu ocen ryzyka w kontekście przyjmowania rozwiązań opartych na chmurze obliczeniowej. Jak wynika z ankiety przeprowadzonej przez Trybunał, 75% EUIBA korzysta już z niektórych publicznych platform przetwarzania w chmurze, a kilka z nich, które jeszcze nie tego nie robią, planuje migrację do chmury obliczeniowej. Od 2019 r. Komisja przyjęła podejście zakładające przyjmowanie w pierwszej kolejności rozwiązań opartych na chmurze obliczeniowej, przewidując stworzenie bezpiecznej hybrydowej oferty usług opartych na wielu chmurach[27]. W kontekście umowy ramowej „Cloud II” Komisja występuje również w charakterze pośrednika usług opartych na chmurze dla wszystkich EUIBA. Zarządzanie ryzykiem związanym z bezpieczeństwem i ochroną danych na platformach chmury obliczeniowej wymaga nowych umiejętności i innego podejścia niż w przypadku tradycyjnej lokalnej infrastruktury informatycznej. Skuteczne zarządzanie ryzykiem związanym z bezpieczeństwem informacji w chmurze stanowi wspólne wyzwanie dla EUIBA, a GovSec jest przykładem rozwiązania, które może odpowiadać na potrzeby kilku, a być może wszystkich EUIBA.

[27] Komisja Europejska, „The European Commission Cloud Strategy”, 2019 r.

Współpraca i wymiana praktyk między EUIBA nadal nie jest optymalna

56 Sam fakt istnienia komitetów międzyinstytucjonalnych nie prowadzi automatycznie do synergii, a EUIBA nie zawsze dzielą się najlepszymi praktykami, wiedzą specjalistyczną, metodyką i wyciągniętymi wnioskami. Ponadto EUIBA samodzielnie decydują, w jakim stopniu zaangażować się w prace ICDT CSSG. Członkowie ICDT CSSG, mimo że uczestniczą w posiedzeniach, mogą wnosić wkład w prace komitetu jedynie w zakresie, w jakim pozwalają na to ich codzienne obowiązki w EUIBA, co spowolniło już postępy w realizacji działań uzgodnionych przez niektóre grupy zadaniowe.

57 Trybunał wskazał konkretne obszary, w których nie ma rozwiązań umożliwiających EUIBA wymianę doświadczeń i inicjatyw. Na przykład na mocy umowy ramowej dotyczącej Komórki Ochrony Sieci (NDC) EUIBA mogą wystąpić o przeprowadzenie badania w celu skonsolidowania wymogów w zakresie cyberbezpieczeństwa i znalezienia odpowiednich rozwiązań. Nie ma jednak żadnego repozytorium takich badań przeprowadzonych przez inne EUIBA lub przez nie zleconych, w związku z czym EUIBA mogą wielokrotnie występować o takie samo badanie. Ponadto EUIBA nie informują się systematycznie nawzajem, że mają podpisane umowy z konkretnymi dostawcami bądź że korzystają z danego oprogramowania. Ta luka w wiedzy może prowadzić do dodatkowych kosztów i zaprzepaszczenia możliwości synergii.

58 EUIBA nie wymieniają się także systematycznie informacjami na temat realizowanych projektów w dziedzinie cyberbezpieczeństwa, nawet jeśli takie projekty mogłyby mieć wpływ międzyinstytucjonalny. Mandat ICDT CSSG obejmuje przepis zobowiązujący EUIBA do przekazywania informacji na temat nowych projektów, które mogą mieć wpływ na cyberbezpieczeństwo innych EUIBA lub na ochronę pochodzących z nich informacji. ICDT CSSG nie jest jednak informowana o takich projektach.

59 Nowa agencja w momencie utworzenia musi od podstaw budować swoją infrastrukturę informatyczną i ramy bezpieczeństwa IT. Obecnie nie ma „katalogu usług”, zestawu narzędzi ani jasnych wytycznych/wymogów dla nowych agencji, co skutkuje znacznym zróżnicowaniem środowisk informatycznych we wszystkich EUIBA, gdyż każda organizacja może zamawiać własne oprogramowanie, sprzęt komputerowy, infrastrukturę i usługi w sposób niezależny. To samo dotyczy ram bezpieczeństwa informatycznego, co wynika z braku wspólnych wymogów i standardów. Sytuacja ta prowadzi do potencjalnego dublowania wysiłków i nieefektywnego wykorzystania

środków UE, a ponadto do większej złożoności wsparcia, jakie musi zapewniać CERT-UE.

Przy wymianie informacji szczególnie chronionych występują praktyczne niedociągnięcia

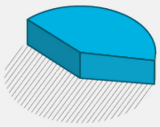
60 Niektóre EUIBA nadal nie dysponują odpowiednimi rozwiązaniami w zakresie wymiany szczególnie chronionych informacji jawnych. Te, które takimi rozwiązaniami dysponują, na ogół wdrożyły rozmaite własne produkty i systemy, co jednak oznacza, że kwestią problematyczną jest interoperacyjność. Wspólne bezpieczne platformy istnieją wyłącznie w konkretnie określonych celach, na przykład platformy CERT-UE umożliwiające wszystkim podmiotom uczestniczącym wymianę szczególnie chronionych informacji na temat incydentów, zagrożeń i słabych punktów.

61 Przykładowo ponad 20% EUIBA nie posiada zaszyfrowanej usługi poczty elektronicznej. Z kolei podmioty, które taką usługę posiadają, często borykają się z problemami z interoperacyjnością, a certyfikaty nie są wzajemnie uznawane. ICTAC i ICDT przez wiele lat omawiały możliwości wprowadzenia skalowalnego i interoperacyjnego rozwiązania w tym zakresie, a w 2018 r. przeprowadzono projekt pilotażowy. Kwestia ta nie została jednak jeszcze rozwiązana.

62 Kolejnym problemem jest brak wspólnych oznaczeń dla szczególnie chronionych informacji jawnych. Oznaczenia takie umożliwiają odpowiednią klasyfikację i wskazują posiadaczom informacji, że dane są objęte szczególnymi wymogami w zakresie ochrony. Oznaczenia te różnią się w zależności od EUIBA, co komplikuje wymianę informacji i właściwe postępowanie z nimi.

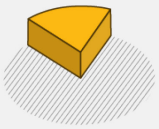
63 W 2020 r. pandemia COVID-19 zmusiła EUIBA do przyjęcia na dużą skalę narzędzi komunikacji i wideokonferencji w celu zapewnienia ciągłości działania. Trybunał zidentyfikował co najmniej 15 różnych rozwiązań w zakresie oprogramowania do wideokonferencji w poszczególnych EUIBA. Nawet w przypadku gdy poszczególne EUIBA wykorzystują to samo rozwiązanie/platformę, często nie można zapewnić interoperacyjności, mimo iż wszystkie strony korzystają z tego samego oprogramowania. Ponadto wytyczne co do tego, jakie informacje (pod względem wrażliwości) mogłyby być udostępniane lub omawiane na danej platformie, różniły się w poszczególnych EUIBA. Prowadzi to do niegospodarności i nieefektywności operacyjnej, a także może skutkować problemami w zakresie bezpieczeństwa.

PODSTAWOWE DANE LICZBOWE: **Narzędzia wymiany informacji szczególnie wrażliwych**



40%

EUIBA **nie uważa**, że posiada odpowiednie narzędzia do **wymiany (jawnych) informacji szczególnie chronionych**



20%

EUIBA **nie** posiada **zaszyfrowanej usługi poczty elektronicznej**

W EUIBA wykorzystywanych jest

ponad 15

narzędzi do wideokonferencji, a **wytyczne** dotyczące ich stosowania w odniesieniu do informacji szczególnie chronionych są **niespójne**

Zarówno w przypadku szyfrowanej poczty elektronicznej, jak i rozwiązań wideokonferencyjnych występują **problemy z interoperacyjnością**

Jak dotąd ENISA i CERT-UE nie zapewniły EUIBA wszelkiego niezbędnego wsparcia

64 W niniejszej sekcji Trybunał przeanalizował dwa główne podmioty, którym powierzono zadanie wspierania EUIBA w zakresie cyberbezpieczeństwa: ENISA i CERT-UE. Trybunał ocenił, czy wsparcie zapewniane przez te podmioty dotarło do EUIBA i czy pomogło w zaspokojeniu ich potrzeb. Wskazał także przyczyny wykrytych niedociągnięć.

ENISA jest kluczowym podmiotem w dziedzinie cyberbezpieczeństwa w UE, ale jak dotąd jej wsparcie dotarło do bardzo niewielu EUIBA

65 W czerwcu 2019 r. wszedł w życie akt o cyberbezpieczeństwie[28], który zastąpił wcześniejszą podstawę prawną ENISA[29] i wzmocnił mandat tej agencji. W szczególności akt ten stanowi, że ENISA powinna aktywnie wspierać zarówno państwa członkowskie, jak i EUIBA w zakresie cyberbezpieczeństwa poprzez budowanie zdolności, zacieśnianie współpracy operacyjnej i tworzenie synergii. W dziedzinie budowania zdolności ENISA posiada obecnie mandat do wspierania EUIBA w „ich staraniach na rzecz poprawy w zakresie zapobiegania cyberzagrożeniom i incydentom, ich wykrywania

[28] Zadania ENISA wyszczególniono w rozdziale II (art. 5–12) rozporządzenia (UE) 2019/881.

[29] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013; zadania ENISA na mocy tego rozporządzenia – zob. art. 3.

i analizowania […], w szczególności poprzez odpowiednie wsparcie CERT-UE”[30]. ENISA powinna również wspierać instytucje UE w opracowywaniu i przeglądzie strategii UE w zakresie cyberbezpieczeństwa, promując działania na rzecz upowszechniania tych strategii i śledząc postępy w ich wdrażaniu.

66 Chociaż w akcie o cyberbezpieczeństwie wyraźnie stwierdza się, że ENISA powinna wspierać EUIBA w działaniach na rzecz poprawy cyberbezpieczeństwa, nie zrealizowała ona jak dotąd żadnych planów działania w odniesieniu do celu wspierania EUIBA w zakresie budowania zdolności (szczegółowe informacje zob. ***ramka 3***).

Ramka 3

Niedostateczna harmonizacja pomiędzy celem i wynikami ENISA w odniesieniu do EUIBA

Niektóre z trzyletnich priorytetów ENISA wymienionych w wieloletnim programie prac na lata 2018–2020 w ramach celu 3.2 „Pomoc w budowaniu zdolności instytucji UE” to:

- „Zapewnienie instytucjom Unii proaktywnego doradztwa w zakresie wzmocnienia ich bezpieczeństwa sieci i informacji (określenie priorytetów dla agencji i organów UE o największych potrzebach w zakresie budowania zdolności w dziedzinie bezpieczeństwa sieci i informacji poprzez ustanowienie z nimi regularnych kontaktów (np. coroczne warsztaty) i skupienie się na tych priorytetach)”;

- „Nawiązywanie partnerstw z CERT-UE i instytucjami dysponującymi silnymi zdolnościami w zakresie bezpieczeństwa sieci i informacji z myślą o wspieraniu działań podejmowanych w ramach tego celu oraz ułatwianie im działań w zakresie bezpieczeństwa sieci i informacji”.

W programach prac ENISA na lata 2018, 2019 i 2020 istnieją tylko dwa cele operacyjne (wyniki) w ramach celu 3.2:

- „Uczestnictwo w Radzie Sterującej CERT-UE oraz reprezentowanie agencji UE korzystających z usług CERT-UE”;

- „Współpraca z odpowiednimi organami UE w zakresie inicjatyw dotyczących bezpieczeństwa sieci i informacji związanych z ich misjami (w tym EASA, CERT-UE, EDA, EC3)”.

[30] Art. 6 rozporządzenia (UE) 2019/881.

Cele operacyjne nie obejmują żadnych działań związanych z proaktywnym doradztwem. Ponadto cel, jakim jest określenie priorytetów dla agencji o największych potrzebach, nie został przełożony na działania operacyjne, ponieważ zastąpiono go innym celem, jakim jest współpraca z agencjami w celu odzwierciedlenia ich potrzeb w Radzie Sterującej CERT-UE.

67 Głównym organem decyzyjnym ENISA jest jej Zarząd, w którego skład wchodzi po jednym członku powoływanym przez każde z 27 państw członkowskich oraz dwóch członków mianowanych przez Komisję[31] (zob. ***rys. 6***). Każdy członek dysponuje jednym głosem, a decyzje są podejmowane większością głosów[32]. W rezultacie działania dotyczące państw członkowskich mogą mieć wyższy priorytet niż działania dotyczące EUIBA. Na przykład w programie prac ENISA na 2018 r. Zarząd postanowił – ze względu na brak wystarczających zasobów – nadać priorytet niektórym działaniom i zrezygnować z trzech innych, z których jedno polegało na „wsparciu na rzecz oceny istniejących polityk/procedur/praktyk dotyczących bezpieczeństwa sieci i informacji w instytucjach UE". Działanie to miało umożliwić ENISA dokonanie przeglądu praktyk EUIBA i ich orientacyjnego stanu zaawansowania pod względem cyberbezpieczeństwa, co posłużyłoby za podstawę do odpowiednio ukierunkowanych działań w przyszłości.

68 W związku z tym ambitne plany ENISA dotyczące udzielania EUIBA proaktywnej pomocy, odzwierciedlone w jej celach strategicznych, nie znalazły przełożenia na cele operacyjne lub konkretne działania. Wsparcie w obszarach budowania zdolności i współpracy operacyjnej było udzielane jedynie na żądanie i ograniczało się jak dotąd do niektórych EUIBA.

69 Akt o cyberbezpieczeństwie stanowi również, że aby pomóc EUIBA w budowaniu zdolności, ENISA powinna zapewniać odpowiednie wsparcie na rzecz CERT-UE. W momencie przeprowadzania niniejszej kontroli wsparcie takie ograniczało się do kilku konkretnych działań. Na przykład w 2019 r. ENISA przeprowadziła wzajemną ocenę CERT-UE w kontekście członkostwa w unijnej sieci CSIRT (ustanowionej na mocy dyrektywy w sprawie bezpieczeństwa sieci i informacji).

70 Jak wynika z odpowiedzi udzielonych w ankiecie, ENISA publikuje wysokiej jakości sprawozdania i wytyczne dotyczące cyberbezpieczeństwa, z których część jest wykorzystywana przez EUIBA. Brak jest jednak szczegółowych wytycznych, które byłyby skierowane do EUIBA oraz uwzględniały ich środowisko i potrzeby. EUIBA,

---

[31] Art. 14 aktu o cyberbezpieczeństwie.

[32] Art. 18 aktu o cyberbezpieczeństwie.

zwłaszcza te mniej zaawansowane w dziedzinie cyberbezpieczeństwa, potrzebują praktycznych wskazówek dotyczących nie tylko tego, co należy zrobić, ale też jakie metody przyjąć. Jak dotąd ENISA i CERT-UE zapewniały takie wsparcie w ograniczonym stopniu i w niesystematyczny sposób.

71 ENISA przeprowadziła szereg szkoleń w zakresie cyberbezpieczeństwa, które były skierowane głównie do organów państw członkowskich, ale wzięła w nich również udział niewielka liczba przedstawicieli EUIBA. Przygotowała również dwa kursy do samodzielnej nauki adresowane konkretnie do EUIBA. Na swojej stronie internetowej ENISA oferuje również materiały szkoleniowe online, do których EUIBA mają dostęp, ale do tej pory są to głównie szkolenia dla ekspertów technicznych CSIRT, w związku z czym nie były one pomocne w przypadku większości EUIBA.

72 Oprócz szkolenia ENISA może wspierać EUIBA poprzez organizację ćwiczeń w dziedzinie cyberbezpieczeństwa. W październiku 2020 r., we współpracy z CERT-UE, pomogła ona w przeprowadzeniu ćwiczenia w zakresie cyberbezpieczeństwa w ICTAC. Było to jedyne ćwiczenie zorganizowane przez ENISA specjalnie dla uczestników z EUIBA. Poza tym pomogła ona zorganizować szereg ćwiczeń na wniosek niektórych EUIBA (np. EU-LISA, EMSA, Parlamentu Europejskiego i Europolu), głównie dla zainteresowanych podmiotów w organach państw członkowskich, przy czym uczestniczyli w nich również niektórzy pracownicy EUIBA.

73 W akcie o cyberbezpieczeństwie przewidziano również nowe zadanie dla ENISA, a mianowicie wspieranie EUIBA – na zasadzie dobrowolności – przy opracowywaniu strategii dotyczących ujawniania podatności. ENISA nadal nie ma jednak pełnego obrazu sytuacji, jeśli chodzi o strategie poszczególnych EUIBA dotyczące ujawniania podatności, w związku z czym nie pomaga im w ich ustanawianiu i wdrażaniu.

CERT-UE jest wysoko ceniony przez podmioty uczestniczące, ale środki będące do jego dyspozycji są niewspółmierne do obecnych wyzwań w zakresie cyberbezpieczeństwa

74 W następstwie szeregu inicjatyw (zob. ***rys. 7***) we wrześniu 2012 r. decyzją Komisji[33] ustanowiono zespół reagowania na incydenty komputerowe (CERT-UE) jako stałą grupę zadaniową ds. EUIBA (zob. pkt ***08***).

[33] Komisja Europejska – komunikat prasowy: Większe bezpieczeństwo cybernetyczne w instytucjach unijnych – efekt udanego projektu pilotażowego.

Rys. 7 – Historia CERT-UE

Źródło: Europejski Trybunał Obrachunkowy.

75 Chociaż CERT-UE prowadzi niezależną działalność, pozostaje grupą zadaniową, która nie posiada osobowości prawnej. Pod względem administracyjnym jest on przypisany do Komisji Europejskiej (DG DIGIT), która zapewnia mu wsparcie logistyczne i administracyjne. Celem CERT-UE jest zwiększenie bezpieczeństwa infrastruktury informatycznej EUIBA poprzez poprawę ich zdolności do radzenia sobie z cyberzagrożeniami i podatnością na cyberataki oraz do zapobiegania cyberatakom, ich wykrywania i reagowania na nie. CERT-UE zatrudnia około 40 pracowników, którzy są pogrupowani w zespoły specjalistów zajmujące się na przykład analizą cyberzagrożeń, kryminalistyką cyfrową i reagowaniem na incydenty.

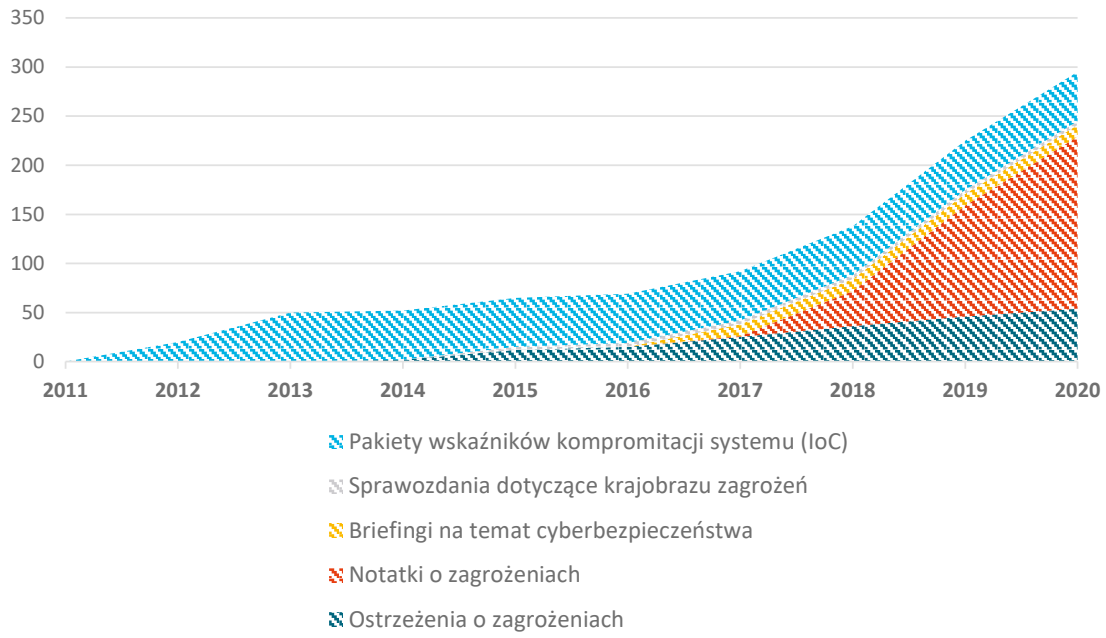
CERT-UE jest wysoce cenionym partnerem, który zmaga się z coraz większym obciążeniem pracą

76 CERT-UE zwraca się do swoich podmiotów uczestniczących o informacje zwrotne i sugestie podczas kwartalnych warsztatów i corocznych spotkań dwustronnych oraz za pośrednictwem badań poziomu zadowolenia. Jak wynika z tych badań i z ankiety przeprowadzonej przez Trybunał, podmioty uczestniczące są w dużej mierze zadowolone z usług świadczonych przez CERT-UE. To, jak zmienia się katalog usług CERT-UE, świadczy o jego wysiłkach na rzecz dostosowania się do potrzeb EUIBA.

77 Podczas gdy duże EUIBA dysponujące znacznymi zasobami wewnętrznymi wykorzystują CERT-UE głównie jako centrum wymiany informacji i źródło informacji o zagrożeniach, mniejsze EUIBA korzystają z szerszego wachlarza usług CERT-UE, takich jak monitorowanie logów, testy penetracyjne, ćwiczenia typu „red team” i wsparcie w reagowaniu na incydenty. Usługi CERT-UE są szczególnie cenne dla mniejszych EUIBA ze względu na ich ograniczoną wewnętrzną wiedzę specjalistyczną i brak korzyści skali (zob. pkt ***31*** i ***33***).

78 W ostatnich latach CERT-UE wzmocnił swoje zdolności i procedury, mając na względzie drastyczny wzrost liczby zagrożeń i incydentów. Liczba produktów informacyjnych CERT-UE, w szczególności ostrzeżeń o zagrożeniach i notatek, stale rośnie (***rys. 8***). W 2020 r. CERT-UE wydał 171 notatek o zagrożeniach i 53 ostrzeżenia o zagrożeniach (czyli znacznie więcej niż 80 notatek i 40 ostrzeżeń, które pierwotnie zamierzał wydać).

Rys. 8 – Wzrost liczby produktów umożliwiających analizę zagrożeń



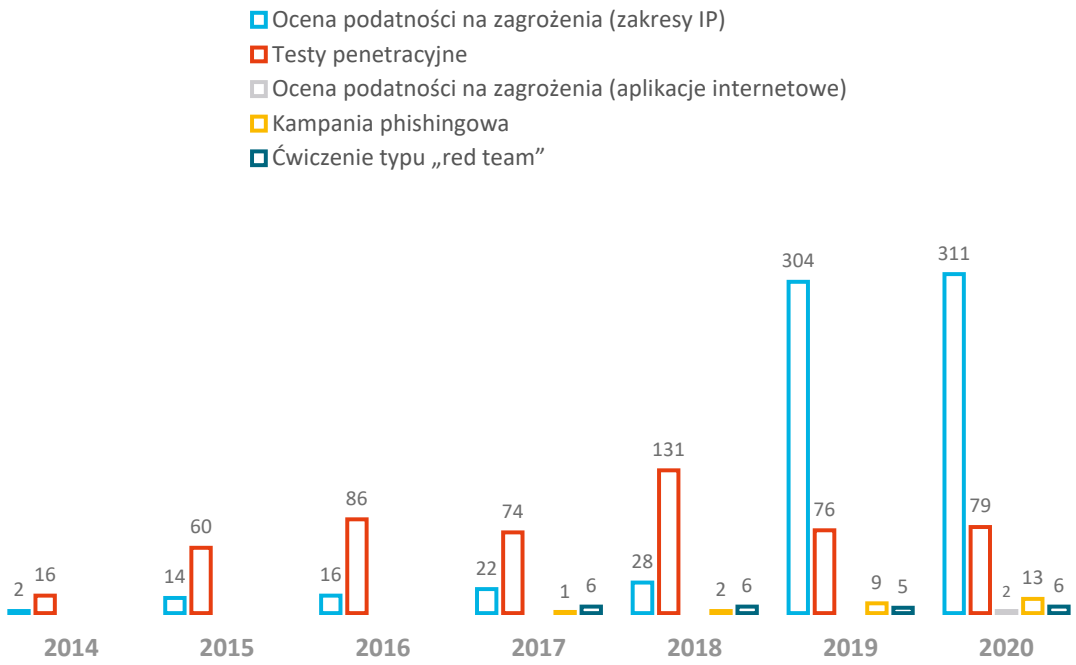
Źródło: Europejski Trybunał Obrachunkowy na podstawie danych CERT-UE.

79 CERT-UE wspiera również EUIBA w radzeniu sobie z cyberincydentami. Podczas gdy 52% EUIBA posiada wewnętrzny zespół reagowania lub przynajmniej koordynatora ds. incydentów, pozostałe 48% w przypadku wystąpienia incydentu korzysta z usług CERT-UE lub innych zewnętrznych dostawców. Nawet duże EUIBA posiadające wewnętrzne zasoby mogą jednak zwrócić się do CERT-UE o wsparcie w przypadku złożonych incydentów.

80 Całkowita liczba incydentów obsłużonych przez CERT-UE wzrosła z 561 w 2019 r. do 884 w 2020 r. W szczególności wzrosła liczba istotnych incydentów – z zaledwie jednego w 2018 r. do 13 w 2020 r. Po rekordowym pod tym względem roku 2020 liczba incydentów znowu wzrosła i w 2021 r. sięgnęła 17. Te istotne incydenty są zazwyczaj spowodowane przez bardzo wyrafinowane zagrożenia. Mogą one dotykać wielu EUIBA, obejmować kontakty z władzami, a ich zbadanie i wyeliminowanie ich skutków zajmuje zaatakowanym podmiotom i CERT-UE zazwyczaj wiele tygodni lub miesięcy.

81 CERT-UE jest również głównym podmiotem odpowiedzialnym za dokonywanie proaktywnych ocen i przeprowadzanie testów mechanizmów cyberobrony EUIBA. Na ***rys. 9*** poniżej przedstawiono podsumowanie działalności CERT-UE w tej dziedzinie. Ponadto od 2020 r. CERT-UE przeprowadza zewnętrzne skanowanie sieci.

Rys. 9 – Testy i oceny przeprowadzane przez CERT-UE



Źródło: Europejski Trybunał Obrachunkowy na podstawie danych CERT-UE.

Podmioty uczestniczące nie przekazują CERT-UE istotnych informacji w odpowiednim czasie

82 Porozumienie międzyinstytucjonalne[34] stanowi, że podmioty uczestniczące powinny informować CERT-UE o istotnych cyberincydentach. W praktyce jednak nie zawsze miało to miejsce. W porozumieniu międzyinstytucjonalnym nie przewidziano mechanizmu, by egzekwować obowiązkowe i terminowe zgłaszanie „istotnych” incydentów przez podmioty uczestniczące w CERT-UE. Ogólna definicja „istotnych incydentów” zawarta w porozumieniu pozostawia w gestii EUIBA decyzję o zgłoszeniu incydentu. Według kierownictwa CERT-UE niektóre podmioty uczestniczące nie przekazywały informacji na temat istotnych incydentów w odpowiednim czasie, co utrudnia CERT-UE pełnienie roli centrum wymiany informacji na temat cyberbezpieczeństwa i punktu koordynacji działań w odpowiedzi na incydenty dla wszystkich EUIBA. Na przykład jeden podmiot uczestniczący, stojący w obliczu bardzo wyrafinowanego zagrożenia, nie poinformował CERT-UE o tym fakcie ani nie zwrócił się do niego o wsparcie. Uniemożliwiło to CERT-UE zgromadzenie danych na potrzeby analizy zagrożeń cyberbezpieczeństwa, które byłyby przydatne w przypadku konieczności udzielenia wsparcia innym podmiotom uczestniczącym stojącym w obliczu tego samego zagrożenia. Atak ten dotknął co najmniej sześć EUIBA.

[34] Art. 3 ust. 3 porozumienia międzyinstytucjonalnego podpisanego w dniu 20 grudnia 2017 r.

83 Podmioty uczestniczące nie przekazywały również aktywnie CERT-UE aktualnych informacji na temat mających na nie wpływ zagrożeń cyberbezpieczeństwa i podatności na takie zagrożenia, mimo że na mocy porozumienia międzyinstytucjonalnego[35] były do tego zobowiązane. Zespół CERT-UE ds. kryminalistyki cyfrowej i reagowania na incydenty nie otrzymywał powiadomień o słabych punktach lub niedociągnięciach w środkach bezpieczeństwa, wykrytych poza kontekstem incydentów, w których prowadzi on aktywne prace. Podmioty uczestniczące nie przekazują proaktywnie odnośnych ustaleń z wewnętrznych lub zewnętrznych audytów bezpieczeństwa.

84 Ponadto porozumienie międzyinstytucjonalne nie nakłada na EUIBA obowiązku zgłaszania CERT-UE istotnych zmian w ich środowisku informatycznym, w związku z czym nie informowały one systematycznie CERT-UE o takich zmianach. Na przykład EUIBA nie zawsze informują CERT-UE o zmianach ich zakresu IP (tj. o zmianach w wykazie adresów internetowych w infrastrukturze EUIBA). Tymczasem CERT-UE potrzebuje aktualnego zakresu adresów IP, aby na przykład przeprowadzać skany w przypadku wykrycia poważnych luk w zabezpieczeniach. Brak poinformowania CERT-UE przez EUIBA o takich zmianach niekorzystnie wpływa na jego zdolność do wspierania EUIBA, a ponadto negatywnie odbija się na jego zdolności do monitorowania systemów i prowadzi do większego nakładu pracy w celu skorygowania nieprawidłowych danych w narzędziach monitorowania. Jak wynika z informacji udzielonych przez kierownictwo, zdarza się niekiedy, że w przypadku incydentu CERT-UE odkryje wcześniej nieznaną infrastrukturę informatyczną. Ponadto, poza konkretnymi przypadkami, CERT-UE nie dysponuje obecnie kompleksowymi informacjami na temat systemów i sieci informatycznych EUIBA.

85 Ze względu na brak mechanizmu egzekwowania w porozumieniu międzyinstytucjonalnym powiadomienia z EUIBA kierowane do CERT-UE będą w dalszym ciągu przekazywane w sposób niesystematyczny, choć stanowią one zasadniczy element w procesie tworzenia społeczności EUIBA odpowiednio przygotowanych pod kątem cyberbezpieczeństwa, w której centralną rolę odgrywa CERT-UE.

Zasoby CERT-UE są niestabilne i niewspółmierne do obecnego poziomu zagrożenia

86 Porozumienie międzyinstytucjonalne[36] stanowi, że „należy zapewnić CERT-UE stabilne finansowanie i personel, przy jednoczesnym zapewnieniu odpowiedniego

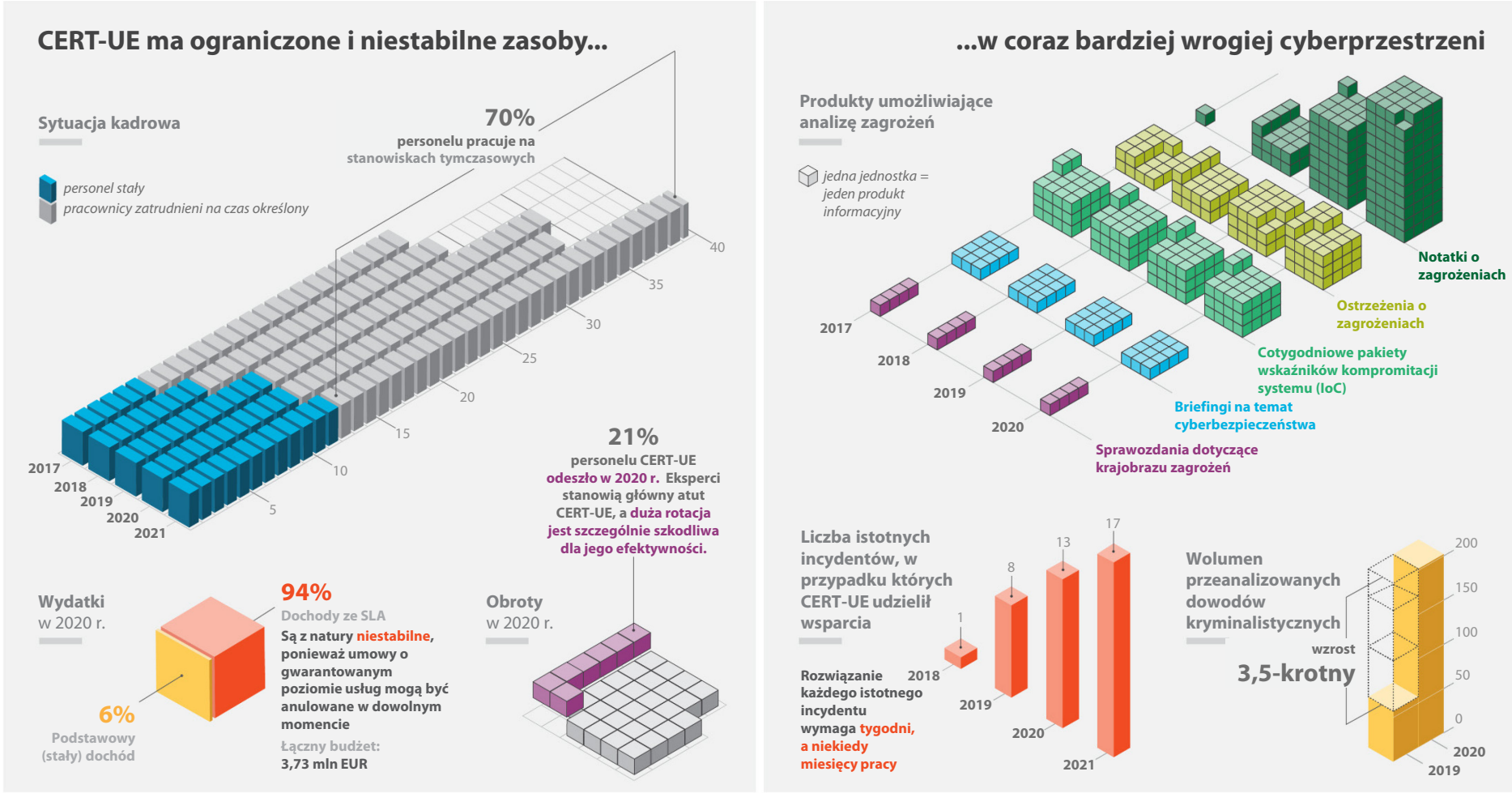
[35] Art. 3 ust. 2 porozumienia międzyinstytucjonalnego.

[36] Motyw 7 porozumienia międzyinstytucjonalnego.

wykorzystania środków finansowych, oraz odpowiedni stały personel podstawowy". Najważniejszym atutem CERT-UE jest jego wysoko wyszkolony i wyspecjalizowany personel. Na ***rys. 10*** pokazano, jak zmieniał się poziom zatrudnienia w CERT-UE od jego powstania w 2011 r. do teraz.

87 Ponad dwie trzecie pracowników CERT-UE ma umowy na czas określony. Ich wynagrodzenie nie jest bardzo konkurencyjne na rynku ekspertów w dziedzinie cyberbezpieczeństwa, a zdaniem kierownictwa CERT-UE coraz trudniej jest ich rekrutować i zatrzymać. W przypadku gdy wynagrodzenia nie są wystarczająco atrakcyjne dla kandydatów starszych stażem, CERT-UE musi zatrudniać młodszych pracowników i poświęcić czas na ich przeszkolenie. Ponadto umowy zawierane są na maksymalnie sześć lat, co oznacza, że CERT-UE musi pozwolić na odejście pracowników kontraktowych w momencie osiągnięcia przez nich najwyższego poziomu wiedzy fachowej. W 2020 r. rotacja pracowników była szczególnie wysoka: 21% pracowników opuściło CERT-UE, a nie wszystkie z tych stanowisk udało się obsadzić. Jeżeli chodzi o poprzednie lata, w 2019 r. odeszło 9% pracowników, a w 2018 r. – 13%.

Rys. 10 – Zasoby CERT-UE i stojące przed nim wyzwania



Źródło: Europejski Trybunał Obrachunkowy na podstawie danych CERT-UE.

88 Kierownictwo CERT-UE podkreśliło, że obecnie zespół ds. kryminalistyki cyfrowej i reagowania na incydenty jest często przeciążony, a inne zespoły nie są w stanie sprostać zapotrzebowaniu. W rezultacie CERT-UE został zmuszony do ograniczenia działalności. Na przykład nie przeprowadza on obecnie ocen stopnia zaawansowania swoich podmiotów uczestniczących ze względu na brak zasobów. Usługa CERT-UE polegająca na wydawaniu „ostrzeżeń przed podejrzaną aktywnością" została uruchomiona później niż oczekiwano, również ze względu na niedobór zasobów. Ponadto kilka podmiotów uczestniczących, z którymi kontrolerzy przeprowadzili wywiady, zwróciło uwagę na długi czas oczekiwania na dostęp do usług CERT-UE.

89 Z uwagi na ograniczone zasoby CERT-UE był zmuszony jak dotychczas do skoncentrowania się w szczególności na ochronie tradycyjnej lokalnej infrastruktury informatycznej przed poważnymi zagrożeniami ze strony grup (zazwyczaj wspieranych przez państwa), które stwarzają zaawansowane, trwałe zagrożenia. Niemniej, jak wynika z informacji udzielonych przez kierownictwo CERT-UE, szersza strefa bezpieczeństwa informatycznego EUIBA (obejmująca obecnie chmurę obliczeniową, urządzenia mobilne i narzędzia telepracy) wymaga ściślejszego monitorowania i ochrony, a zagrożenia niższego szczebla (takie jak cyberprzestępczość i oprogramowanie typu ransomware) również wymagają większej uwagi.

90 W porozumieniu międzyinstytucjonalnym nie przewidziano, by CERT-UE zapewniał zdolności operacyjne całodobowo przez siedem dni w tygodniu. CERT-UE nie dysponuje obecnie zasobami ani nie posiada odpowiednich ram polityki kadrowej, aby móc działać w ustrukturyzowany sposób po godzinach pracy w trybie ciągłym, mimo że cyberataki występują o różnych porach dnia i nocy. Jeśli chodzi o EUIBA objęte ankietą Trybunału, tylko 35 z 65 posiada urzędnika ds. informatyki, z którym można skontaktować się poza godzinami pracy.

91 W celu finansowania działalności CERT-UE Rada Sterująca zatwierdziła w 2012 r. model opierający się na umowach o gwarantowanym poziomie usług (SLA). Wszystkie podmioty uczestniczące otrzymują podstawowe usługi bezpłatnie i mogą zakupić dodatkowe usługi, podpisując w tym celu umowę o gwarantowanym poziomie usług. Budżet CERT-UE na 2020 r. wyniósł 3 745 000 euro, przy czym 6% pochodziło z budżetu UE, a 94% z umów o gwarantowanym poziomie usług. Podmioty uczestniczące są jednak bardzo zróżnicowane: niektóre z nich mają zaawansowane wymogi w zakresie bezpieczeństwa IT, podczas gdy inne dysponują skromnymi budżetami na kwestie IT i wykazują bardzo niski poziom zaawansowania w zakresie cyberbezpieczeństwa. Z tego względu dyskusje na temat umów o gwarantowanym poziomie usług prowadzą do sytuacji, w której pewne EUIBA mają wysokie wymogi w zakresie bezpieczeństwa, podczas gdy inne nie wykazują woli bądź nie są w stanie wnieść wkładu.

92 Ponadto umowy o gwarantowanym poziomie usług muszą być co roku indywidualnie przedłużane. Stanowi to nie tylko obciążenie administracyjne, ale stwarza również problemy z płynnością finansową, ponieważ CERT-UE nie otrzymuje jednocześnie środków finansowych ze wszystkich umów. Co więcej, agencje mogą rozwiązać umowy w dowolnym momencie. Grozi to efektem błędnego koła: ze względu na utratę dochodów CERT-UE musi ograniczać swoje usługi i nie jest w stanie sprostać zapotrzebowaniu, co z kolei może skłonić inne EUIBA do rozwiązania umów i przeniesienia się do prywatnych dostawców. W świetle powyższych rozważań obecny model finansowania nie jest idealny dla zapewnienia stabilnego i optymalnego poziomu usług.

93 W obliczu szybko zmieniającego się krajobrazu zagrożeń cyberbezpieczeństwa (zob. pkt ***06*** i ***80***) Rada Sterująca CERT-UE zatwierdziła na posiedzeniu w dniu 19 lutego 2020 r. strategiczny wniosek dotyczący rozszerzenia usług CERT-UE w zakresie cyberbezpieczeństwa i opracowania „pełnych zdolności operacyjnych”. Wnioskowi towarzyszyła analiza potrzeb kadrowych i finansowych CERT-UE. W analizie tej stwierdzono, że CERT-UE będzie potrzebował 14 dodatkowych stałych stanowisk administratorów, które będą stopniowo dodawane w latach 2021–2023. Dzięki temu od 2023 r. CERT-UE będzie mógł funkcjonować z wykorzystaniem pełni możliwości. Zgodnie z tym wnioskiem, jeśli chodzi o finansowanie, CERT-UE musiałby zwiększyć swój budżet o 7,6 mln euro w latach 2021–2023, tak aby do 2024 r. osiągnąć poziom 11,3 mln euro.

94 Pomimo zatwierdzenia wniosku strategicznego w sprawie udostępnienia dodatkowych zasobów na rzecz CERT-UE EUIBA nie osiągnęły jeszcze porozumienia w sprawie praktycznych rozwiązań, po pierwsze na okres przejściowy 2021–2023, a po drugie w długoterminowej perspektywie, po wejściu w życie przyszłego rozporządzenia w sprawie cyberbezpieczeństwa (zob. pkt ***12***).

Wnioski i zalecenia

95 Trybunał stwierdził, że instytucje, organy i agencje UE (EUIBA) nie osiągnęły poziomu gotowości w zakresie cyberbezpieczeństwa, który byłby adekwatny do zagrożeń. Wyniki prac kontrolnych Trybunału pokazują, że EUIBA są w różnym stopniu zaawansowane pod względem cyberbezpieczeństwa, a ponieważ są one często ze sobą powiązane, a także ściśle współpracują z podmiotami publicznymi i prywatnymi w państwach członkowskich, słabe punkty w jednej instytucji czy agencji lub w jednym z organów UE mogą narazić inne podmioty na zagrożenia cyberbezpieczeństwa.

96 Trybunał stwierdził, że kluczowe dobre praktyki w zakresie cyberbezpieczeństwa, w tym niektóre niezbędne środki bezpieczeństwa, nie zawsze były wdrażane. Choć należyte zarządzanie cyberbezpieczeństwem ma zasadnicze znaczenie dla bezpieczeństwa informacji i systemów IT, nie zostało ono jeszcze wprowadzone w niektórych EUIBA. W wielu przypadkach brakuje strategii i planów w zakresie bezpieczeństwa IT lub nie zostały one zatwierdzone przez kadrę kierowniczą wyższego szczebla, polityka bezpieczeństwa nie zawsze jest sformalizowana, a oceny ryzyka nie obejmują całego środowiska informatycznego. Wydatki na cyberbezpieczeństwo są nierównomierne, przy czym niektóre EUIBA przeznaczają jednoznacznie zbyt mało środków na ten cel w porównaniu z innymi podmiotami podobnej wielkości (zob. pkt ***21***–***33*** i ***37***–***38***).

97 Kluczowym elementem skutecznych ram cyberbezpieczeństwa są programy mające na celu podniesienie poziomu świadomości oraz szkolenia na ten temat. Niemniej jednak tylko 29% EUIBA zapewnia obowiązkowe szkolenia w zakresie cyberbezpieczeństwa dla kierowników odpowiedzialnych za systemy informatyczne zawierające informacje szczególnie chronione, a oferowane szkolenia są często nieformalne. W ciągu ostatnich pięciu lat 55% EUIBA zorganizowało co najmniej jedną symulowaną kampanię phishingową (lub podobne ćwiczenia). Ćwiczenia te są ważnym narzędziem szkolenia personelu i podnoszenia świadomości, ale EUIBA nie korzystają z nich systematycznie (zob. pkt ***34***–***36***). Ponadto nie wszystkie EUIBA podlegają regularnie przeprowadzanej procedurze niezależnego poświadczenia (zob. pkt ***39***–***44***).

98 CERT-UE jest wysoko ceniony przez EUIBA, które korzystają z jego usług, ale jest on przeciążony. Od 2018 r. obciążenie pracą w zakresie analizy zagrożeń i pomocy w reagowaniu na incydenty szybko rosło. Liczba istotnych cyberincydentów wzrosła ponad dziesięciokrotnie. Jednocześnie EUIBA nie zawsze przekazują w odpowiednim czasie informacje na temat istotnych incydentów, podatności na zagrożenia i istotnych zmian w swojej infrastrukturze informatycznej. Ogranicza to skuteczność działania

CERT-UE, ponieważ uniemożliwia mu powiadamianie innych EUIBA, które również mogły zostać dotknięte, a ponadto może spowodować, że istotne incydenty pozostaną niewykryte. Co więcej, zasoby CERT-UE nie są stabilne i obecnie są niewspółmierne do aktualnego poziomu zagrożenia oraz do potrzeb EUIBA. Strategiczny wniosek w sprawie zapewnienia dodatkowych zasobów potrzebnych CERT-UE został zatwierdzony przez jego Radę Sterującą w 2020 r., ale podmioty uczestniczące nie osiągnęły jeszcze porozumienia co do praktycznych warunków udostępnienia takich zasobów. W rezultacie pracownicy CERT-UE nie są w stanie sprostać zapotrzebowaniu i zostali zmuszeni do ograniczenia działalności (zob. pkt ***74–93***).

Zalecenie 1 – Zwiększenie stopnia przygotowania wszystkich EUIBA w zakresie cyberbezpieczeństwa za pomocą wspólnych wiążących zasad oraz poprzez zapewnienie większych zasobów na rzecz CERT-UE

W przyszłym wniosku dotyczącym rozporządzenia w sprawie środków na rzecz wspólnego wysokiego poziomu cyberbezpieczeństwa we wszystkich EUIBA Komisja powinna uwzględnić następujące zasady:

a) kadra kierownicza wyższego szczebla powinna ponosić odpowiedzialność za zarządzanie cyberbezpieczeństwem, zatwierdzając odnośne strategie i kluczowe polityki bezpieczeństwa oraz mianując niezależnego głównego inspektora ds. bezpieczeństwa systemów informacyjnych (lub tworząc równoważne stanowisko);

b) EUIBA powinny stworzyć ramy zarządzania ryzykiem w zakresie bezpieczeństwa IT obejmujące całą infrastrukturę informatyczną, a także przeprowadzać regularne oceny ryzyka;

c) EUIBA powinny zapewniać systematyczne szkolenia mające na celu podniesienie poziomu świadomości dla wszystkich pracowników, w tym dla kadry kierowniczej;

d) EUIBA powinny zapewniać regularne audyty i testy mechanizmów cyberobrony. Audyty powinny również obejmować adekwatność zasobów przeznaczonych na cyberbezpieczeństwo;

e) EUIBA powinny niezwłocznie zgłaszać CERT-UE istotne cyberincydenty oraz istotne zmiany w infrastrukturze informatycznej, a także informować o podatności infrastruktury na zagrożenia;

f) EUIBA powinny zwiększyć i zarezerwować w swoich budżetach zasoby na rzecz CERT-UE zgodnie z zapotrzebowaniem zgłoszonym w strategicznym wniosku zatwierdzonym przez Radę Sterującą CERT-UE;

g) w rozporządzeniu należy uwzględnić przepisy umożliwiające wyznaczenie podmiotu reprezentującego wszystkie EUIBA, który będzie dysponował odpowiednimi uprawnieniami i środkami w celu monitorowania przestrzegania przez wszystkie EUIBA wspólnych zasad cyberbezpieczeństwa i który będzie wydawał wytyczne i zalecenia oraz wzywał do podejmowania działań.

Termin realizacji: I kw. 2023 r.

99 EUIBA ustanowiły mechanizmy współpracy w dziedzinie cyberbezpieczeństwa, ale Trybunał zauważył, że potencjalna synergia w tym zakresie nie jest w pełni wykorzystywana. Istnieją sformalizowane struktury wymiany informacji, w ramach których poszczególne podmioty i komitety pełnią wzajemnie uzupełniające się role. Ze względu na ograniczone zasoby mniejszym EUIBA trudniej jest jednak uczestniczyć w pracach na forach międzyinstytucjonalnych, a agencje zdecentralizowane i wspólne przedsięwzięcia nie są w optymalny sposób reprezentowane w Radzie Sterującej CERT-UE. Trybunał stwierdził również, że EUIBA nie wymieniają się systematycznie informacjami na temat projektów związanych z cyberbezpieczeństwem bądź na temat ocen bezpieczeństwa i innych umów o świadczenie usług. Może to prowadzić do dublowania wysiłków i wzrostu kosztów. Trybunał zauważył trudności operacyjne w wymianie szczególnie chronionych informacji jawnych za pośrednictwem zaszyfrowanej poczty elektronicznej lub w trakcie wideokonferencji. Wynikały one z braku interoperacyjności rozwiązań informatycznych, niespójnych wytycznych dotyczących ich dozwolonego wykorzystywania oraz braku wspólnych oznaczeń chronionych informacji jawnych i zasad postępowania z nimi (zob. pkt ***45***–***63***).

Zalecenie 2 – Wspieranie dalszej synergii między EUIBA w wybranych obszarach

Komisja, w ramach Międzyinstytucjonalnego Komitetu ds. Transformacji Cyfrowej, powinna promować wśród EUIBA następujące działania:

a) przyjęcie rozwiązań w zakresie interoperacyjności bezpiecznych kanałów komunikacji – od zaszyfrowanej poczty elektronicznej po wideokonferencje – oraz

wspieranie przyjęcia wspólnych oznaczeń i wspólnych zasad postępowania w przypadku szczególnie chronionych informacji jawnych;

b) systematyczna wymiana informacji na temat projektów związanych z cyberbezpieczeństwem o potencjalnym wpływie międzyinstytucjonalnym, jak również na temat ocen bezpieczeństwa przeprowadzanych w odniesieniu do oprogramowania oraz obowiązujących umów z dostawcami zewnętrznymi;

c) określenie specyfikacji dla wspólnych zamówień i umów ramowych dotyczących usług w zakresie cyberbezpieczeństwa, w których mogą uczestniczyć wszystkie EUIBA, co przyniesie korzyści skali.

Termin realizacji: IV kw. 2023 r.

100 Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) i CERT-UE to dwa główne podmioty, których zadaniem jest wspieranie EUIBA w zakresie cyberbezpieczeństwa. Niemniej jednak ze względu na ograniczone zasoby i priorytetowe traktowanie innych obszarów nie były one w stanie zapewnić EUIBA wszelkiego potrzebnego wsparcia, w szczególności w zakresie budowania zdolności tych EUIBA, które wykazują mniejszy stopień zaawansowania w dziedzinie cyberbezpieczeństwa (zob. pkt ***64***–***93***).

Zalecenie 3 – Zapewnienie, by CERT-UE i ENISA koncentrowały się w większym stopniu na mniej zaawansowanych EUIBA

Trybunał zaleca, aby CERT-UE i ENISA:

a) określiły obszary priorytetowe, w których EUIBA potrzebują największego wsparcia, na przykład za pośrednictwem ocen ich zaawansowania w dziedzinie cyberbezpieczeństwa;

b) realizowały działania w zakresie budowania zdolności, zgodnie z podpisanym przez siebie protokołem ustaleń.

Termin realizacji: IV kw. 2022 r.

Niniejsze sprawozdanie zostało przyjęte przez Izbę III, której przewodniczy Bettina Jakobsen, członkini Trybunału Obrachunkowego, w Luksemburgu w dniu 22 lutego 2022 r.

W imieniu Europejskiego Trybunału Obrachunkowego

Klaus-Heiner LEHNE
Prezes

Załączniki

Załącznik I – Wykaz EUIBA objętych ankietą

Nazwa EUIBA	Rodzaj
Parlament Europejski (PE)	Instytucja (art. 13 ust. 1 TUE)
Rada Unii Europejskiej i Rada Europejska	Instytucja (art. 13 ust. 1 TUE)
Komisja Europejska (KE)	Instytucja (art. 13 ust. 1 TUE)
Trybunał Sprawiedliwości Unii Europejskiej (TSUE)	Instytucja (art. 13 ust. 1 TUE)
Europejski Bank Centralny (EBC)	Instytucja (art. 13 ust. 1 TUE)
Europejski Trybunał Obrachunkowy	Instytucja (art. 13 ust. 1 TUE)
Europejska Służba Działań Zewnętrznych (ESDZ)	Organ (art. 27 ust. 3 TUE)
Europejski Komitet Ekonomiczno-Społeczny (EKES) i Europejski Komitet Regionów (KR)[37]	Organy (art. 13 ust. 4 TUE)
Europejski Bank Inwestycyjny (EBI)	Organ (art. 308 TFUE)
Europejski Urząd ds. Pracy (ELA)	Agencja zdecentralizowana
Agencja Unii Europejskiej ds. Współpracy Organów Regulacji Energetyki (ACER)	Agencja zdecentralizowana
Urząd Organu Europejskich Regulatorów Łączności Elektronicznej (Urząd BEREC)	Agencja zdecentralizowana
Wspólnotowy Urząd Ochrony Odmian Roślin (CPVO)	Agencja zdecentralizowana
Europejska Agencja Bezpieczeństwa i Zdrowia w Pracy (EU-OSHA)	Agencja zdecentralizowana
Europejska Agencja Straży Granicznej i Przybrzeżnej (Frontex)	Agencja zdecentralizowana
Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA)	Agencja zdecentralizowana
Agencja Unii Europejskiej ds. Azylu (AUEA)	Agencja zdecentralizowana
Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego (EASA)	Agencja zdecentralizowana
Europejski Urząd Nadzoru Bankowego (EUNB)	Agencja zdecentralizowana
Europejskie Centrum ds. Zapobiegania i Kontroli Chorób (ECDC)	Agencja zdecentralizowana
Europejskie Centrum Rozwoju Kształcenia Zawodowego (Cedefop)	Agencja zdecentralizowana
Europejska Agencja Chemikaliów (ECHA)	Agencja zdecentralizowana
Europejska Agencja Środowiska (EEA)	Agencja zdecentralizowana
Europejska Agencja Kontroli Rybołówstwa (EFCA)	Agencja zdecentralizowana

[37] EKES i KR są liczone jako jeden organ.

Nazwa EUIBA	Rodzaj
Europejski Urząd ds. Bezpieczeństwa Żywności (EFSA)	Agencja zdecentralizowana
Europejska Fundacja na rzecz Poprawy Warunków Życia i Pracy (Eurofound)	Agencja zdecentralizowana
Agencja Unii Europejskiej ds. Programu Kosmicznego [zastępuje: Agencję Europejskiego GNSS – GSA] (EUSPA)	Agencja zdecentralizowana
Europejski Instytut ds. Równości Kobiet i Mężczyzn (EIGE)	Agencja zdecentralizowana
Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych (EIOPA)	Agencja zdecentralizowana
Europejska Agencja Bezpieczeństwa Morskiego (EMSA)	Agencja zdecentralizowana
Europejska Agencja Leków (EMA)	Agencja zdecentralizowana
Europejskie Centrum Monitorowania Narkotyków i Narkomanii (EMCDDA)	Agencja zdecentralizowana
Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)	Agencja zdecentralizowana
Agencja Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (CEPOL)	Agencja zdecentralizowana
Europejski Urząd Policji (Europol)	Agencja zdecentralizowana
Agencja Kolejowa Unii Europejskiej (ERA)	Agencja zdecentralizowana
Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA)	Agencja zdecentralizowana
Europejska Fundacja Kształcenia (ETF)	Agencja zdecentralizowana
Agencja Praw Podstawowych Unii Europejskiej (FRA)	Agencja zdecentralizowana
Urząd Unii Europejskiej ds. Własności Intelektualnej [znany jako UHRW do dnia 23 marca 2016 r.] (EUIPO)	Agencja zdecentralizowana
Jednolita Rada ds. Restrukturyzacji i Uporządkowanej Likwidacji (SRB)	Agencja zdecentralizowana
Agencja Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust)	Agencja zdecentralizowana
Centrum Tłumaczeń dla Organów Unii Europejskiej (CdT)	Agencja zdecentralizowana
Prokuratura Europejska (EPPO)	Agencja zdecentralizowana
Europejski Instytut Innowacji i Technologii (EIT)	Organ utworzony w ramach badań naukowych i innowacji
Wspólne Przedsięwzięcie w celu Opracowania Europejskiego Systemu Zarządzania Ruchem Lotniczym Nowej Generacji (SESAR)	Wspólne przedsięwzięcie na mocy TFUE
Wspólne Przedsięwzięcie „Podzespoły i układy elektroniczne w służbie wiodącej pozycji Europy” (ECSEL)	Wspólne przedsięwzięcie na mocy TFUE
Wspólne Przedsięwzięcie na rzecz Technologii Ogniw Paliwowych i Technologii Wodorowych 2 (FCH2)	Wspólne przedsięwzięcie na mocy TFUE
Wspólne Przedsięwzięcie na rzecz Drugiej Inicjatywy w zakresie Leków Innowacyjnych (IMI 2)	Wspólne przedsięwzięcie na mocy TFUE
Wspólne Przedsięwzięcie „Czyste Niebo 2”	Wspólne przedsięwzięcie na mocy TFUE

Nazwa EUIBA	Rodzaj
Wspólne Przedsięwzięcie na rzecz Bioprzemysłu (BBI)	Wspólne przedsięwzięcie na mocy TFUE
Wspólne Przedsięwzięcie na rzecz Wspólnej Inicjatywy Technologicznej Shift2Rail (S2R)	Wspólne przedsięwzięcie na mocy TFUE
Wspólne Przedsięwzięcie w dziedzinie Europejskich Obliczeń Wielkiej Skali (EuroHPC)	Wspólne przedsięwzięcie na mocy TFUE
Europejskie Wspólne Przedsięwzięcie na rzecz Realizacji Projektu ITER i Rozwoju Energii Termojądrowej (F4E)	Wspólne przedsięwzięcie na mocy TFUE
Misja doradcza Unii Europejskiej na Ukrainie (EUAM Ukraine)	Misja cywilna (WPBiO)
Misja Unii Europejskiej dotycząca pomocy w zintegrowanym zarządzaniu granicami w Libii (EUBAM Libya)	Misja cywilna (WPBiO)
Misja Unii Europejskiej dotycząca budowania zdolności w Nigrze (EUCAP Sahel Niger)	Misja cywilna (WPBiO)
Misja Obserwacyjna Unii Europejskiej w Gruzji (EUMM Georgia)	Misja cywilna (WPBiO)
Misja Policyjna Unii Europejskiej na Terytoriach Palestyńskich (EUPOL COPPS)	Misja cywilna (WPBiO)
Misja doradcza Unii Europejskiej w Republice Środkowoafrykańskiej (EUAM RCA)	Misja cywilna (WPBiO)
Misja doradcza Unii Europejskiej w Iraku (EUAM Iraq)	Misja cywilna (WPBiO)
Misja Unii Europejskiej ds. Szkolenia i Kontroli na przejściu granicznym w Rafah (EUBAM Rafah)	Misja cywilna (WPBiO)
Misja Unii Europejskiej dotycząca budowania zdolności w Mali (EUCAP Sahel Mali)	Misja cywilna (WPBiO)
Misja Unii Europejskiej dotycząca budowania zdolności w Somalii (EUCAP Somalia)	Misja cywilna (WPBiO)
Misja Unii Europejskiej w zakresie praworządności w Kosowie (EULEX Kosowo)	Misja cywilna (WPBiO)

Załącznik II – Dodatkowe informacje na temat najważniejszych komitetów międzyinstytucjonalnych

Międzyinstytucjonalny Komitet ds. Transformacji Cyfrowej (ICDT)

ICDT jest forum wymiany informacji i wspierania współpracy w dziedzinie IT. Został utworzony w maju 2020 r. w miejsce Międzyinstytucjonalnego Komitetu ds. IT (CII). ICDT składa się z kierowników działów IT w EUIBA. W jego ramach utworzono podgrupę ds. cyberbezpieczeństwa (ICDT CSSG), której zadaniem jest promowanie współpracy między EUIBA w zakresie cyberbezpieczeństwa, a także wspieranie wymiany informacji.

Uprawnienia decyzyjne ICDT ograniczają się do kwestii, które nie wpływają na „sposób, w jaki instytucje wypełniają swoją misję" i „nie wpływają na zarządzanie w ramach instytucji". W przypadku decyzji wykraczających poza jego kompetencje ICDT może wydawać zalecenia skierowane do kolegium sekretarzy generalnych instytucji i organów UE.

Zgodnie z mandatem ICDT jego członkami są przedstawiciele wszystkich instytucji i organów UE oraz jeden przedstawiciel wyznaczony przez agencje UE (ICTAC). Przewodnictwo w ICDT sprawuje obecnie Sekretariat Generalny Rady.

Podgrupa ICDT ds. cyberbezpieczeństwa (ICDT CSSG)

ICDT CSSG w swoim obecnym składzie została ustanowiona we wrześniu 2020 r. i zastąpiła stałą podgrupę ds. bezpieczeństwa CII. W porównaniu ze swoją poprzedniczką ICDT CSSG stosuje bardziej ustrukturyzowane i ambitne podejście zorientowane na wyniki. Jej działania są prowadzone przez grupy zadaniowe (TF), które spotykają się regularnie i koncentrują się na kluczowych wspólnych kwestiach. Grupy te to:

- TF1 „Wspólne standardy, analiza porównawcza i dojrzałość"
- TF2 „Platformy wymiany informacji na temat metod, narzędzi i umów"
- TF3 „Bezpieczeństwo chmury obliczeniowej"
- TF4 „Rozwój talentów w dziedzinie cyberbezpieczeństwa"
- TF5 „CyberAwareness"
- TF6 „Bezpieczeństwo wideokonferencji"

Zgodnie z mandatem CSSG jej sekretariat jest odpowiedzialny za regularne monitorowanie postępów prac w grupach zadaniowych i składanie sprawozdań na ten temat. Sprawozdania te, opierające się na systematycznie gromadzonych informacjach od koordynatorów grup zadaniowych, przekazywane są regularnie przewodniczącemu i wiceprzewodniczącemu podgrupy ICDT ds. cyberbezpieczeństwa. Na koniec każdego roku CSSG musi również przedstawić podsumowujące sprawozdanie z działalności.

Przewodnictwo w ICDT CSSG sprawuje obecnie Komisja, a wiceprzewodniczącym jest przedstawiciel ICTAC. Chociaż CSSG nie posiada uprawnień decyzyjnych, może zalecić ICDT podjecie decyzji w istotnych kwestiach.

Sieć agencji

Sieć agencji UE (EUAN) jest nieformalną siecią utworzoną przez szefów agencji UE w 2012 r. Składa się obecnie z 48 zdecentralizowanych agencji i wspólnych przedsięwzięć UE. Jej celem jest stworzenie platformy wymiany i współpracy dla członków sieci w dziedzinach będących przedmiotem wspólnego zainteresowania. Komitet Doradczy ds. ICT (ICTAC) jest podgrupą EUAN odpowiedzialną za promowanie współpracy w dziedzinie technologii informacyjno-komunikacyjnych, w tym w dziedzinie cyberbezpieczeństwa.

Komitet Doradczy ds. Technologii Informacyjnych i Komunikacyjnych (ICTAC)

ICTAC promuje współpracę między agencjami i wspólnymi przedsięwzięciami w dziedzinie technologii informacyjno-komunikacyjnych. Jego celem jest znalezienie realnych i oszczędnych rozwiązań wspólnych problemów, wymiana informacji i, w stosownych przypadkach, przyjęcie wspólnych stanowisk. Zgodnie z warunkami działania ICTAC dwa razy w roku odbywają się walne zgromadzenia, w których udział biorą wszyscy jego członkowie. Ponadto odbywają się regularne comiesięczne spotkania z udziałem przedstawicieli ICTAC w grupach zadaniowych CSSG, przedstawiciela ICTAC w CSSG i trojki ICTAC. W skład trojki wchodzą obecny, poprzedni i przyszły przewodniczący ICTAC (każdy przewodniczący pełni funkcję przez rok). Rolą trojki jest wspieranie obecnego przewodniczącego we wszystkich kwestiach związanych z jego funkcją, w tym zastępowanie go, jeżeli wymagają tego okoliczności.

Wykaz akronimów i skrótów

CERT-UE – zespół reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE

CISO – główny inspektor bezpieczeństwa teleinformatycznego

CSIRT – zespół reagowania na incydenty bezpieczeństwa komputerowego

DG DIGIT – Dyrekcja Generalna ds. Informatyki

DG HR – Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa

ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa

EPC – ekwiwalent pełnego czasu pracy

EUAN – sieć agencji Unii Europejskiej

EUIBA – instytucje, organy i agencje Unii Europejskiej

eu-LISA – Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości

ICDT – Międzyinstytucjonalny Komitet ds. Transformacji Cyfrowej

ICDT CSSG – podgrupa ds. cyberbezpieczeństwa działająca w ramach Międzyinstytucjonalnego Komitetu ds. Transformacji Cyfrowej

ICTAC – Komitet Doradczy ds. Technologii Informacyjno-Komunikacyjnych

ISACA – Stowarzyszenie Audytu i Kontroli Systemów Informacyjnych

ITCB – Rada ds. Technologii informacyjnej i Cyberbezpieczeństwa

NIS – bezpieczeństwo sieci i informacji

SLA – umowa o gwarantowanym poziomie usług

Glosariusz

Ataki socjotechniczne – w kontekście bezpieczeństwa informacji są to manipulacje psychologiczne mające na celu nakłonienie użytkowników do podjęcia określonych działań lub udostępnienia informacji poufnych.

Cyberbezpieczeństwo – środki mające na celu ochronę sieci i infrastruktury informatycznej oraz zawartych w nich informacji przed zagrożeniami zewnętrznymi.

Cyberprzestrzeń – globalne środowisko internetowe, w którym użytkownicy, oprogramowanie i usługi komunikują się za pośrednictwem sieci komputerów i innych urządzeń podłączonych do internetu.

Cyberszpiegostwo – czynność lub praktyka pozyskiwania tajemnic i informacji z internetu, sieci lub indywidualnych komputerów bez zezwolenia i wiedzy posiadacza informacji.

Phishing – wysyłanie e-maili, które rzekomo pochodzą z zaufanego źródła, w celu skłonienia odbiorców do otwarcia złośliwych linków lub udostępnienia danych osobowych.

„Red teaming" – realistyczna symulacja cyberataków z wykorzystaniem elementu zaskoczenia i technik obserwowanych ostatnio w świecie rzeczywistym, koncentrująca się na konkretnych celach za pomocą wielu linii ataków.

Testy penetracyjne – metoda oceny bezpieczeństwa systemu informatycznego poprzez próby naruszenia jego zabezpieczeń przy użyciu narzędzi i technik stosowanych zwykle przez przeciwników.

Zaawansowane, trwałe zagrożenie – atak polegający na tym, że nieupoważniony użytkownik uzyskuje dostęp do systemu lub sieci w celu kradzieży wrażliwych danych i pozostaje tam przez dłuższy czas.

Zespół reagowania na incydenty komputerowe w EUIBA – centrum wymiany informacji i koordynacji działań w odpowiedzi na incydenty, którego klientami („podmiotami uczestniczącymi") są instytucje, organy i agencje UE.

Odpowiedzi Komisji

https://www.eca.europa.eu/pl/Pages/DocItem.aspx?did=60922

Odpowiedzi CERT-UE i ENISA

https://www.eca.europa.eu/pl/Pages/DocItem.aspx?did=60922

Kalendarium

https://www.eca.europa.eu/pl/Pages/DocItem.aspx?did=60922

PRAWA AUTORSKIE

PDF	ISBN 978-92-847-7570-5	1977-5768	doi:10.2865/095675	QJ-AB-22-003-PL-N
HTML	ISBN 978-92-847-7573-6	1977-5768	doi:10.2865/82006	QJ-AB-22-003-PL-Q

Liczba cyberataków na instytucje, organy i agencje UE (EUIBA) gwałtownie rośnie. Jako że EUIBA są silnie ze sobą powiązane, słabe punkty w jednej instytucji, agencji lub jednym z organów UE mogą narazić pozostałe na zagrożenia bezpieczeństwa. W ramach kontroli zweryfikowano, czy EUIBA posiadają odpowiednie rozwiązania zapewniające im ochronę przed zagrożeniami cyberbezpieczeństwa. Z ustaleń kontrolerów wynika, że poziom przygotowania EUIBA jest, ogólnie rzecz biorąc, nieadekwatny do zagrożeń, a ponadto EUIBA wykazują się bardzo zróżnicowanym stopniem zaawansowania pod względem cyberbezpieczeństwa. Trybunał zaleca w związku z tym, by Komisja zwiększyła stopień przygotowania EUIBA poprzez przedłożenie wniosku w sprawie wprowadzenia wspólnych wiążących zasad w zakresie cyberbezpieczeństwa oraz zapewnienie większych zasobów na rzecz zespołu reagowania na incydenty komputerowe (CERT-UE). Komisja powinna również promować dalszą synergię pomiędzy EUIBA, a CERT-UE i Agencja Unii Europejskiej ds. Cyberbezpieczeństwa powinny wspierać przede wszystkim te EUIBA, które są mniej zaawansowane pod względem cyberbezpieczeństwa.

Sprawozdanie specjalne Europejskiego Trybunału Obrachunkowego przedstawiono na mocy art. 287 ust. 4 akapit drugi TFUE.

EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY

Urząd Publikacji Unii Europejskiej

EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY
12 rue Alcide De Gasperi
1615 Luxembourg
LUKSEMBURG

Tel.: +352 4398-1

Formularz kontaktowy: eca.europa.eu/pl/Pages/ContactForm.aspx
Strona internetowa: eca.europa.eu
Twitter: @EUAuditors