Krajobraz europejskich ISAC-ów w 2023 roku

NASK

Krajobraz europejskich ISAC-ów w 2023 roku

NASK

AUTORKI
Paulina Popow
Emilia Zalewska-Czajczyńska

RECENZJA NAUKOWA
dr hab., prof. IK Marek Pawlik

ISBN 978-83-65448-91-0
DOI: 10.60097/NASK/978-83-65448-91-0

Państwowy Instytut Badawczy NASK
ul. Kolska 12
01-045 Warszawa

NASK

Szanowni Państwo,

Z ogromną przyjemnością przekazujemy Państwu raport „Krajobraz europejskich ISAC-ów w 2023 roku" opracowany przez ekspertów z Działu Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni NASK PIB. Naszym celem jest dostarczenie Państwu kompleksowych informacji na temat funkcjonowania największych europejskich ISAC-ów, a także omówienie ich znaczenia w ekosystemie cyberbezpieczeństwa.

ISAC-i, czyli Centra Wymiany i Analizy Informacji, powstały w odpowiedzi na potrzebę współpracy oraz szybkiej wymiany informacji pomiędzy organizacjami z sektora prywatnego i publicznego. Od wielu lat stanowią jeden z fundamentów strategii ochrony przed cyberatakami w Unii Europejskiej. ISAC-i umożliwiają nie tylko wymianę danych dotyczących cyberzagrożeń pomiędzy podmiotami z sektora prywatnego i publicznego, ale także wspólne opracowywanie i wdrażanie najlepszych praktyk w zakresie cyberbezpieczeństwa.

W niniejszym raporcie przedstawiamy koncepcję ISAC oraz analizujemy ich funkcjonowanie w Europie. Zwracamy uwagę na różnorodność sektorów, które korzystają z usług ISAC, obejmujących m.in. energetykę, sektor finansowy czy transport. Podkreślamy również znaczenie międzynarodowej współpracy, która jest niezbędna do skutecznego przeciwdziałania globalnym zagrożeniom w cyberbezpieczeństwie.

W roku 2023 europejskie ISAC-i odegrały ważną rolę w koordynacji działań związanych z cyberbezpieczeństwem, czego rezultatem jest lepsza ochrona infrastruktury krytycznej oraz zwiększona świadomość zagrożeń wśród wszystkich interesariuszy.

Jeszcze raz zachęcamy Państwa do zapoznania się z treścią raportu, który, mamy nadzieję, przyczyni się do dalszego wzmacniania europejskiego ekosystemu cyberbezpieczeństwa. Słowa wdzięczności i uznania kieruję do recenzenta raportu dr hab., prof. IK Marka Pawlika, a także Autorek raportu – Emilli Zalewskiej-Czajczyńskiej i Pauliny Popow.

Paweł Zegarow

Kierownik Działu Strategii i Rozwoju
Bezpieczeństwa Cyberprzestrzeni NASK PIB

Spis treści

Wprowadzenie

ISAC-i, czyli Centra Wymiany i Analizy Informacji (Information Sharing and Analysis Centers) odgrywają coraz istotniejszą rolę w budowaniu kolektywnej odporności na cyberzagrożenia. W ostatnich latach można było zaobserwować rozwój tego typu organizacji, zarówno na poziomie krajowym, jak i międzynarodowym. Niniejsza publikacja pt. „Krajobraz europejskich ISAC-ów w 2023 roku" stanowi kompleksową analizę znaczenia i sposobów funkcjonowania ISAC-ów działających na terenie Europy oraz identyfikację szans i wyzwań, które przed nimi stoją.

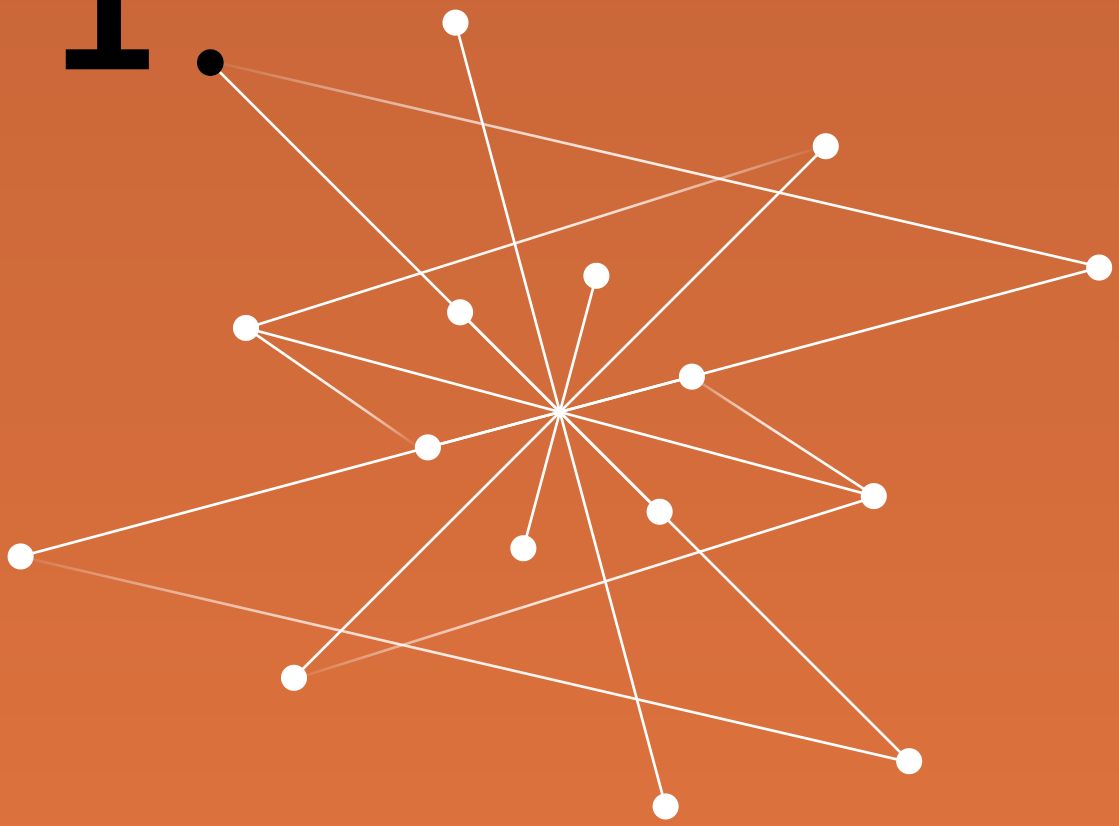
Publikacja ta składa się z trzech części. Rozpoczyna ją wstęp teoretyczny, obejmujący historię powstania ISAC-ów, ich definicję oraz omówienie podobieństw i różnic między organizacjami tego typu ze Stanów Zjednoczonych i Europy. Zawarte zostały w nim także podstawowe informacje na temat współpracy dla cyberbezpieczeństwa oraz modeli wymiany informacji.

Drugą, zasadniczą część publikacji stanowi omówienie badania z udziałem 10 europejskich ISAC-ów, które zostało przeprowadzone przez autorki w 2023 r. Przedstawione zostały sposób przeprowadzenia badania, uzyskane wyniki oraz główne wnioski. Na końcu tej części zawarto zestaw rekomendacji, sformułowanych na podstawie analizy rezultatów badania.

Publikację zamyka zestaw infografik, na których zaprezentowano szczegółowe informacje na temat wybranych, europejskich ISAC-ów.

Celem tej publikacji oraz opisanego w niej badania jest przedstawienie i przeanalizowanie krajobrazu europejskich ISAC-ów w jak najszerszym zakresie. Organizacje tego typu stanowią bowiem ważny element systemów cyberbezpieczeństwa na różnych poziomach – z tego względu warto jest zwiększać świadomość i wiedzę na ich temat. Przedstawione w publikacji przykłady działań podejmowanych przez badane ISAC-i mogą także stanowić wzór i inspirację do naśladowania dla innych organizacji działających w obszarze cyberbezpieczeństwa.

1.



O ISAC-ach – wstęp teoretyczny

W współczesność charakteryzuje się dynamicznym rozwojem technologii, co wiąże się także ze stałym wzrostem liczby oraz stopnia zaawansowania zagrożeń występujących w cyberprzestrzeni. W obliczu rosnących wyzwań podmioty sektora publicznego i prywatnego powinny stale podnosić poziom swojego bezpieczeństwa. Inicjatywą wspierającą ten proces jest tworzenie Information Sharing and Analysis Center (Centrów Wymiany i Analizy Informacji), w skrócie ISAC-ów. Głównym zadaniem organizacji tego typu jest stworzenie przestrzeni umożliwiającej dzielenie się posiadanymi informacjami, doświadczeniami oraz najlepszymi praktykami z zakresu cyberbezpieczeństwa. Dzięki temu członkowie ISAC-ów wspólnie tworzą środowisko, które jest bardziej odporne na cyberzagrożenia.

1.1 Historia powstania ISAC-ów

Pierwsze ISAC-i powstały w Stanach Zjednoczonych w latach 90. XX wieku. Do rozpoczęcia procesu ich powstawania w dużej mierze przyczyniły się dwa wydarzenia – pierwszy atak terrorystyczny na World Trade Center w 1993 r. oraz zamach w Oklahoma City w 1995 r[1]. Dostrzeżono wtedy potrzebę zwiększenia bezpieczeństwa kluczowych dla państwa zasobów. W tym celu powstała Prezydencka Komisja Ochrony Infrastruktury Krytycznej w 1996 r[2]. W ramach jej działań stworzono raport, w którym przedstawiono propozycje rozwiązań dla zwiększenia bezpieczeństwa w tym obszarze. Jednym z pomysłów było powołanie organizacji umożliwiających wymianę informacji oraz wzmacnianie współpracy między podmiotami publicznymi i prywatnymi[3]. 22 maja 1998 r. Bill Clinton, prezydent Stanów Zjednoczonych, podpisał dyrektywę dotyczącą ochrony infrastruktury krytycznej, która stworzyła grunt do wprowadzenia w życie idei tworzenia takich centrów[4]. Pierwsza organizacja tego typu, Financial Services ISAC (FS ISAC), powstała w sektorze finansowym niespełna rok od podpisania prezydenckiej dyrektywy.

---

1 European Union Agency for Cybersecurity (ENISA), *Information Sharing and Analysis Center, Cooperative models*, 2018, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models [dostęp: 15.04.2024].

2 J. Sadowski, *Ochrona Infrastruktury Krytycznej. Uregulowania prawne*, „Zeszyty Naukowe. Organizacja i Zrządzanie", 2018, nr 6, s. 1237.

3 European Union Agency for Cybersecurity (ENISA), op. cit.

4 *Presidential Decision Directive/NSC-63 – Critical Infrastructure Protection z dnia 22 maja 1998*, Critical Infrastructure Protection (PDD 63) (fas.org) [dostęp: 15.04.2024].

Aktualnie, w Stanach Zjednoczonych funkcjonuje 26 ISAC-ów, których działania od 2003 roku są koordynowane przez National Council of ISACs (Krajową Radę ISAC-ów), w skrócie NCI. Centra na bieżąco raportują Radzie podjęte działania oraz przy jej wsparciu organizują regularne spotkania i ćwiczenia. NCI aktywnie wspiera tworzenie nowych ISAC-ów, szczególnie w tych sektorach i podsektorach infrastruktury krytycznej, w których brakuje jasno ustalonych metod wymiany informacji w zakresie cyberbezpieczeństwa. Dodatkowo NCI na bieżąco prowadzi rejestr ISAC-ów działających w Stanach Zjednoczonych, który dostępny jest na stronie internetowej Rady[5].

1.2 Definicje organizacji typu ISAC

Definicja organizacji typu ISAC w Stanach Zjednoczonych

Zgodnie z definicją zaproponowaną przez NCI, ISAC-i są to organizacje non-profit, tworzone i kierowane przez swoich członków. Opierają się one na partnerstwie publiczno-prywatnym i skupiają się na potrzebach sektora, którego przedstawicieli zrzeszają. Celem ISAC-ów jest wspieranie członków organizacji poprzez inicjatywy skoncentrowane na zwiększaniu bezpieczeństwa i odporności wobec cyberzagrożeń. Szczególna uwaga skupiona jest na pomaganiu właścicielom i operatorom infrastruktury krytycznej w zapewnieniu bezpieczeństwa zarządzanych przez nich obiektów oraz zatrudnianych przez nich pracowników. Ponadto, ISAC-i, na podstawie zgromadzonych i przeanalizowanych informacji, ostrzegają swoich członków o możliwych zagrożeniach oraz zapewniają narzędzia do ochrony i wzmacniania ogólnej odporności na cyberzagrożenia[6].

Definicja organizacji typu ISAC w Europie

ENISA – European Union Agency for Cybersecurity (Europejska Agencja ds. Cyberbezpieczeństwa) definiuje ISAC jako organizację non-profit, skupioną na zbieraniu, analizowaniu i wymianie informacji o cyberzagrożeniach oraz na współpracy międzysektorowej. Celem działalności ISAC-ów jest

5 National Council of ISACs (NCI), National Council of ISACs | About NCI (nationalisacs.org) National Council of ISACs | About NCI (nationalisacs.org), [dostęp: 15.04.2024].

6 National Council of ISACs | About NCI (nationalisacs.org) Ibidem.

wzmocnienie bezpieczeństwa cyberprzestrzeni poprzez integrację sektora prywatnego i publicznego oraz wymianę wiedzy między nimi. Organizacje tego typu pełnią kluczową rolę w budowaniu odporności danego sektora gospodarki na cyberzagrożenia. Działalność ISAC-ów przyczynia się także do realizacji narodowych strategii cyberbezpieczeństwa, zgodnych z unijnymi regulacjami oraz promowania wymiany informacji i dobrych praktyk z zakresu cyberbezpieczeństwa[7].

1.3 Organizacje typu ISAC w Stanach Zjednoczonych i Europie – podobieństwa i różnice

Cele działalności

Zarówno w Stanach Zjednoczonych, jaki i w Europie, Centra Wymiany i Analizy Informacji mają taki sam cel swojego działania, czyli wspieranie budowania odporności w obszarze cyberbezpieczeństwa w różnych sektorach gospodarki. Na obydwu kontynentach, organizacje te tworzą platformy umożliwiające dzielenie się wiedzą, najlepszymi praktykami oraz ostrzeżeniami o cyberzagrożeniach.

Funkcjonowanie ogólnodostępnego rejestru

Jedną z większych różnic pomiędzy ISAC-ami europejskimi i amerykańskimi jest kwestia funkcjonowania ogólnodostępnego rejestru organizacji tego typu. Jak wspomniano wcześniej, w Stanach Zjednoczonych taki rejestr prowadzi i udostępnia publicznie na swojej stronie internetowej NCI. Zawiera on listę ISAC-ów wraz z krótkim opisem ich działalności oraz linkiem do strony internetowej. W Europie nie funkcjonuje taki rejestr, co w konsekwencji sprawia, że informacje o europejskich ISAC-ach są rozproszone i mniej dostępne.

7 European Union Agency for Cybersecurity (ENISA), op. cit.

Regulacje prawne

Zarówno w Stanach Zjednoczonych, jak i w Europie, nie ma jednego, konkretnego aktu prawnego, który regulowałby działalność ISAC-ów. Jednak na obu kontynentach istnieją regulacje, których zapisy przyczyniają się do wspierania funkcjonowania ISAC-ów.

W Stanach Zjednoczonych pierwszym takim aktem była wspomniana wcześniej prezydencka dyrektywa z 1998 r., która zachęcała do tworzenia ISAC-ów w celu ochrony infrastruktury krytycznej przed cyberzagrożeniami. Z kolei w 2015 r. przyjęty został CISA – *Cybersecurity Information Sharing Act* (Akt o wymianie informacji w cyberbezpieczeństwie), w którym, m. in., określono wytyczne dla podmiotów pozarządowych w zakresie wymiany danych o cyberzagrożeniach z instytucjami rządowymi. Akt ten nie zawiera przepisów, które wprost nakazywałby tworzenia w tym celu ISAC-ów, jednak w dużym stopniu wspiera proces wymiany informacji w ramach organizacji tego typu. CISA gwarantuje ochronę przed odpowiedzialnością firmom, które udostępniają informacje zgodnie z jego wytycznymi.

W Europie, w 2016 r. została przyjęta dyrektywa NIS w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii – pierwszy unijny akt prawny kompleksowo regulujący kwestie związane z cyberbezpieczeństwem[8]. Dyrektywa ta nie zawierała przepisów, które wprost odnosiłyby się do ISAC-ów, ale przyczyniła się do zwiększenia świadomości na temat ich znaczenia dla wymiany informacji pomiędzy różnymi podmiotami w kontekście cyberbezpieczeństwa.

W 2022 r. przyjęta została nowelizacja unijnych przepisów z obszaru cyberbezpieczeństwa – dyrektywa NIS 2[9]. Podobnie jak jej poprzednia wersja, nie zawiera ona przepisów, które bezpośrednio odnosiłyby się do ISAC-ów. Jednym z ważniejszych zapisów z punktu widzenia organizacji tego typu jest art. 29, który dotyczy mechanizmów wymiany informacji z obszaru cyberbezpieczeństwa. Państwa członkowskie zostały zobowiązane do umożliwienia podmiotom objętym zakresem NIS 2, a w stosownych przypadkach także innym podmiotom, prowadzenia dobrowolnej wymiany informacji na temat cyberbezpieczeństwa, w tym dotyczących cyberzagrożeń, podatności,

8 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

9 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.

technik i procedur. Przepis ten nakłada również na państwa członkowskie oraz na ENISA obowiązek wspierania tworzenia odpowiednich mechanizmów, aby taka wymiana informacji była prowadzona w sposób bezpieczny.

Ponadto, w motywie 9) dyrektywy NIS 2 pojawia się odniesienie do centrów analizy i wymiany informacji w kontekście wykorzystywania przez nie kodu poufności TLP (*Traffic Light Protocol*). Brak jednak doprecyzowania, czy zapis ten odnosi się konkretnie do organizacji typu ISAC, czy do jakichkolwiek organizacji prowadzących działalność polegającą na wymianie i analizie informacji.

1.4 Współpraca europejskich ISAC-ów dla cyberbezpieczeństwa

Współpraca międzynarodowa jest jednym z kluczowych elementów budowania europejskiej odporności w cyberprzestrzeni. Cyberzagrożenia nie zatrzymują się na granicach narodowych, dlatego niezbędne jest budowanie silnych międzynarodowych sojuszy w dziedzinie cyberbezpieczeństwa. Poszczególne ISAC-i gromadzą informacje na temat incydentów w reprezentowanych przez nie sektorach, takich jak np. finanse, energetyka, zdrowie, transport. Jednak w celu zwiększenia efektywności swoich działań, współpracują również ze sobą oraz z różnego rodzaju podmiotami, takimi jak instytucje unijne i stowarzyszenia branżowe.

Współpraca z instytucjami europejskimi

Unijne instytucje pełnią istotną rolę w zakresie wspierania wymiany informacji i zwiększania bezpieczeństwa cyberprzestrzeni. W kontekście działalności ISAC-ów, jedną z najważniejszych organizacji jest ENISA, która podejmuje różnorodne działania wspomagające ich tworzenie oraz funkcjonowanie. Na szczególne wyróżnienie zasługuje inicjatywa „*ISAC in a Box*" („ISAC w pudełku"), czyli kompleksowy zbiór narzędzi służących wspieraniu europejskich ISAC-ów na wszystkich etapach ich funkcjonowania[10]. Jego zakres obejmuje cztery fazy ewolucji ISAC-ów, rozpoczynając od etapu tworzenia organizacji, a kończąc na etapie jej dojrzałego działania.

10 European Union Agency for Cybersecurity (ENISA), „*ISAC in a Box*", 26.10.2020 r., ISAC in a Box – ENISA (europa.eu), [dostęp: 15.04.2024].

„ISAC in a Box" zawiera praktyczne informacje i wskazówki dotyczące m. in. ustalenia celów oraz budżetu organizacji, opracowania zasad działania, czy też pozyskiwania członków. Te kwestie są szczególnie istotne w przypadku organizacji będących w fazie budowy. Na kolejnym etapie zbiór narzędzi podpowiada, jak odpowiednio zarządzać utworzoną organizacją, budować zaufanie między członkami oraz udoskonalać proces wymiany informacji. ISAC-i, w których te elementy zostaną już wypracowane, mogą przystąpić do weryfikacji podjętych działań, oceny dynamiki rozwoju organizacji oraz określenia czynników, które wymagają zmiany. Organizacjom, które ukończą tę fazę rozwoju, „ISAC in a Box" podpowiada, jak osiągnąć dojrzałość organizacyjną, czyli zadbać o ciągły rozwój i podnoszenie poziomu zaawansowania podejmowanych działań.

ENISA podejmuje także działania w zakresie badań nad funkcjonowaniem ISAC-ów. Agencja opracowała raport, którego celem było określenie rodzajów umiejętności oraz działań organizacyjno-technicznych, niezbędnych do zapewnienia skutecznej wymiany informacji między ISAC-ami[11].

Warto zauważyć, że działania ENISA skierowane są przede wszystkim do ISAC-ów na poziomie europejskim. Jednak również krajowe ISAC-i mogą skorzystać z udostępnionych na stronie internetowej agencji dokumentów i informacji na temat tworzenia i rozwijania organizacji.

Kolejną europejską instytucją, która odgrywa ważną rolę we wspieraniu działalności ISAC-ów, jest Komisja Europejska. Jedną z jej inicjatyw jest Empowering EU-ISACs (Wzmacnianie pozycji europejskich ISAC-ów)[12]. Projekt ten ma na celu zmobilizowanie publicznych i prywatnych podmiotów do tworzenia nowych, sektorowych ISAC-ów w Unii Europejskiej, poprzez udzielanie im pomocy organizacyjnej, technicznej, prawnej oraz szkoleniowej. Ponadto, Komisja Europejska wspiera rozwój i podnoszenie poziomu dojrzałości już istniejących organizacji oraz współpracę między nimi.

Niektóre działania ISAC-ów są również wspierane przez EUROPOL (Agencję Unii Europejskiej ds. Współpracy Organów Ścigania). W 2013 r. agencja utworzyła European Cyber Crime Centre – EC3 (Europejskie Centrum ds. Walki z Cyberprzestępczością), którego głównym celem jest wspieranie organów ścigania państw członkowskich w walce z przestępstwami

11 European Union Agency for Cybersecurity (ENISA), *Cross-Sectors Exercise Requirements*, 2018, https://www.enisa.europa.eu/publications/cross-sector-exercise-requirements, [dostęp: 15.04.2024].

12 Empowering EU-ISACs, https://www.isacs.eu/, [dostęp: 15.04.2024].

popełnianymi w cyberprzestrzeni oraz wzmocnienie ochrony obywateli, przedsiębiorstw i instytucji państwowych w krajach europejskich[13]. Jednym z ważnych aspektów działalności EC3 w kontekście ISAC-ów jest współpraca z FS-ISAC w zakresie przeciwdziałania cyberprzestępstwom motywowanym finansowo, których ofiarami są banki oraz inne instytucje finansowe[14].

Jak wynika z przytoczonych wyżej przykładów, krajobraz współpracy instytucji unijnych i ISAC-ów jest bardzo różnorodny. Obejmuje m.in. wsparcie organizacyjne, prawne, techniczne, finansowe oraz doradztwo na rzecz budowania świadomości i podnoszenia wiedzy. Współpraca z instytucjami unijnymi pomaga ISAC-om dostosować się do aktualnych regulacji prawnych, rozwijać działalność, docierać do nowych członków oraz zwiększać możliwości reagowania na globalne wyzwania związane z cyberzagrożeniami.

Współpraca z innymi ISAC-ami

Europejskie ISAC-i współpracują również ze sobą nawzajem oraz z organizacjami tego typu z innych części świata. Przykładem międzykontynentalnej współpracy pomiędzy ISAC-ami jest partnerstwo organizacji działających w sektorze energetycznym – europejskiego European Energy ISAC (EE-ISAC), amerykańskiego Electricity ISAC (E-ISAC) oraz japońskiego Japan Electricity ISAC (JE-ISAC). Partnerzy podejmują działania polegające na wymianie informacji związanych regulacjami prawnymi, politykami oraz dobrymi praktykami w zakresie cyberbezpieczeństwa w sektorze energetyki. Dodatkowo, w ramach tego partnerstwa, organizowane są wspólne wydarzenia, pozwalające na nawiązywanie nowych kontaktów między regionami oraz budowanie wzajemnego zaufania między organizacjami[15].

---

13 European Cyber Crime Centre, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, [dostęp: 15.04.2024].

14 EUROPOL, *FS-ISAC and Europol Partner to Combat Cross-Border Cybercrime*, 19.09.2019 r., https://www.europol.europa.eu/media-press/newsroom/news/fs-isac-and-europol-partner-to-combat-cross-border-cybercrime, [dostęp: 15.04.2024].

15 EE-ISAC, *Japanese & European energy communities sign partnership agreement on cyber security*, 17.05.2017 r., Japanese & European energy communities sign partnership agreement on cyber security – EE-ISAC – European Energy – Information Sharing & Analysis Centre, [dostęp: 15.04.2024].

Współpraca z innymi rodzajami podmiotów

Ważnym obszarem współpracy ISAC-ów z innymi podmiotami są relacje nawiązywane z organizacjami branżowymi działającymi na poziomie europejskim i krajowym. Taka kooperacja umożliwia zwiększenie skali działań prowadzonych przez ISAC-i w obrębie danego sektora. Jako przykład może posłużyć współpraca Auto-ISAC z European Automobile Manufacturers' Association – ACEA (Europejskim Stowarzyszeniem Producentów Samochodów) oraz European Association of Automotive Suppliers – CLEPA (Europejskim Stowarzyszeniem Dostawców Motoryzacyjnych). Dzięki wsparciu ze strony organizacji branżowych, Auto-ISAC, który pierwotnie powstał i funkcjonował w Stanach Zjednoczonych, rozszerzył swoją działalność na rynek europejski oraz dotarł do potencjalnych nowych członków. Natomiast ACEA i CLEPA zyskały możliwość nawiązania kontaktów z podmiotami ze Stanów Zjednoczonych[16].

Kolejnym rodzajem podmiotów, z którymi współpracują ISAC-i, są krajowe i europejskie zespoły reagowania na incydenty bezpieczeństwa komputerowego (*Computer Emergency Response Teams*, CERTs). Odgrywają one szczególnie ważną rolę w zapewnieniu odpowiedniej reakcji na cyberzagrożenia, a ich działania obejmują m. in. monitorowanie systemów, analizę incydentów, identyfikację zagrożeń, stosowanie odpowiednich środków zaradczych oraz przywracanie właściwego funkcjonowania systemów. Dzięki sprawnej współpracy i wymianie informacji pomiędzy CERT-ami a ISAC-ami, członkowie ISAC-ów mogą szybciej i skuteczniej reagować na incydenty oraz minimalizować szkody po ich wystąpieniu. Przykładem takiej współpracy jest wymiana informacji z obszaru cyberbezpieczeństwa sektora lotniczego pomiędzy EUROCONTROL (EATM-CERT) i Aviation ISAC. Partnerstwo to obejmuje również wspólną analizę zagrożeń oraz opracowywanie dobrych praktyk i procedur, które służą budowaniu cyberodporności w globalnej sieci transportu lotniczego[17].

---

16 European Automobile Manufacturers' Association (ACEA), *European manufacturers and suppliers join with Auto-ISAC*, 12.10.2022 r., European manufacturers and suppliers join with Auto-ISAC – ACEA – European Automobile Manufacturers' Association, [dostęp: 15.04.2024].

17 EUROCONTROL, *EUROCONTROL and A-ISAC strengthen their relationship regarding air traffic management and aviation cybersecurity*, 2.10.2019 r., EUROCONTROL and A-ISAC strengthen their relationship regarding air traffic management and aviation cybersecurity | EUROCONTROL, [dostęp: 15.04.2024].

1.5 Wymiana informacji w kontekście cyberbezpieczeństwa

Wymiana informacji w kontekście cyberbezpieczeństwa może odbywać się sporadycznie – ad hoc – lub może być to stała, długoterminowa relacja. Wyróżnia się dwa modele wymiany informacji: obligatoryjny i dobrowolny. Dobór modelu odpowiedniego do danej sytuacji zależy między innymi od relacji i poziomu zaufania między stronami, celu wymiany informacji oraz obowiązujących w tej kwestii regulacji prawnych[18].

Model obligatoryjnej wymiany informacji zakłada, że jest ona wymagana przepisami prawa lub wcześniej przyjętymi przez strony uzgodnieniami (np. umownymi). Objęte zakresem obowiązku podmioty muszą więc przekazywać określone informacje, ponieważ w razie jego niedopełnienia mogą zostać ukarane wskazanymi z góry sankcjami. Ten model zazwyczaj występuje w relacji pomiędzy podmiotami podlegającymi określonym przepisom prawa a właściwymi organami państwowymi. W kontekście cyberbezpieczeństwa, jako przykład regulacji zakładającej obligatoryjną wymianę informacji, może posłużyć dyrektywa NIS 2, która nakłada na określone podmioty obowiązek zgłaszania niektórych typów incydentów.

W przypadku modelu dobrowolnej wymiany informacji, to czy informacje są udostępniane wynika z inicjatywy samych stron. To od nich zależy również zakres i forma udostępnianych danych. W przeciwieństwie do obligatoryjnego modelu wymiany informacji, w przypadku podjęcia decyzji o nieudostępnianiu określonych informacji, strony nie są narażone na sankcje. Model ten ma zastosowanie zazwyczaj w sytuacji, gdy współpracujące podmioty postanawiają o wymianie informacji między sobą, aby realizować wspólne cele.

W kontekście ISAC-ów częściej wykorzystywany jest model dobrowolnej wymiany informacji. Podmioty uczestniczące w danej organizacji dzielą się wiedzą związaną z cyberbezpieczeństwem w oparciu o wzajemne zaufanie. Udostępniane w ramach ISAC-ów dane dotyczą w szczególności takich zagadnień jak:

- **INCYDENTY** – zarówno ataki zakończone sukcesem, jak i próby ich dokonania;

18 C. Goodwin, J.P. Nicholas, *A framework for cybersecurity information sharing and risk reduction*, Journal of Cybersecurity Research, 2020, 15 (3), s. 13.

- **ZAGROŻENIA** – potencjalnie niebezpieczna aktywność, która może stwarzać ryzyko wystąpienia incydentu, np. rozpowszechnianie złośliwych plików lub oprogramowania, kradzieże adresów e-mail lub adresów IP;

- **LUKI W ZABEZPIECZENIACH** – np. w oprogramowaniu;

- **ŚRODKI NAPRAWCZE** – metody naprawy luk w zabezpieczeniach i ochrony przed zagrożeniami oraz działania po wystąpieniu incydentu;

- **WIEDZA OPERACYJNA** – umożliwiająca odpowiednie reagowanie na incydenty;

- **NAJLEPSZE PRAKTYKI** – w tym kontrole bezpieczeństwa oraz rozwój procesów reagowania na zagrożenia;

- **ANALIZY STRATEGICZNE** – dokonywane na podstawie zebranych informacji[19].

Warto jednak zwrócić uwagę na fakt, że członkowie mogą postanowić, że uprzednio uzgodnione rodzaje informacji podlegają obowiązkowemu przekazywaniu. Zastosowanie jednak w pełni obligatoryjnego modelu mogłoby zniechęcać potencjalnych członków do przystąpienia do organizacji.

19 C. Goodwin, J.P. Nicholas, *A framework for cybersecurity information sharing and risk reduction*, „Journal of Cybersecurity Research" 2020, nr 15(3), s. 13.

Wyzwania i ograniczenia w procesie wymiany informacji

Wymiana informacji pomiędzy członkami jest podstawowym zadaniem ISAC-ów. Warto podkreślić, że ten proces wymaga ścisłego przestrzegania obowiązujących regulacji prawnych. Do aktów prawnych mających realny wpływ na wymianę informacji w ramach ISAC-ów należy Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO)[20]. Obowiązuje ono od 2018 r. i ma na celu ochronę prywatności i danych osobowych obywateli Unii Europejskiej. Rozporządzenie zobowiązuje członków ISAC-ów do szczególnego zwrócenia uwagi na udostępniane informacje, tak, aby ich wymiana odbywała się w zgodzie z zasadami legalności, rzetelności, przejrzystości, minimalizacji danych oraz bezpieczeństwa przetwarzania, określonymi w art. 5 rozporządzenia. Ograniczenia dla wymiany informacji mogą być zawarte także w wewnętrznych regulaminach i politykach, które nakładają na podmioty obowiązek zachowania poufności pewnych informacji.

Innego rodzaju wyzwaniem są różnice w poziomie zaawansowania systemów informatycznych poszczególnych członków europejskich ISAC-ów. W związku z tym, trudnością może być dopasowanie metody przekazywania informacji, dostosowanej do możliwości technicznych każdego członka ISAC-a. Dodatkową kwestią jest konieczność zapewnienia bezpieczeństwa przekazywanych danych, co z kolei może wiązać się z dużymi kosztami, które nie każdy podmiot jest w stanie ponieść.

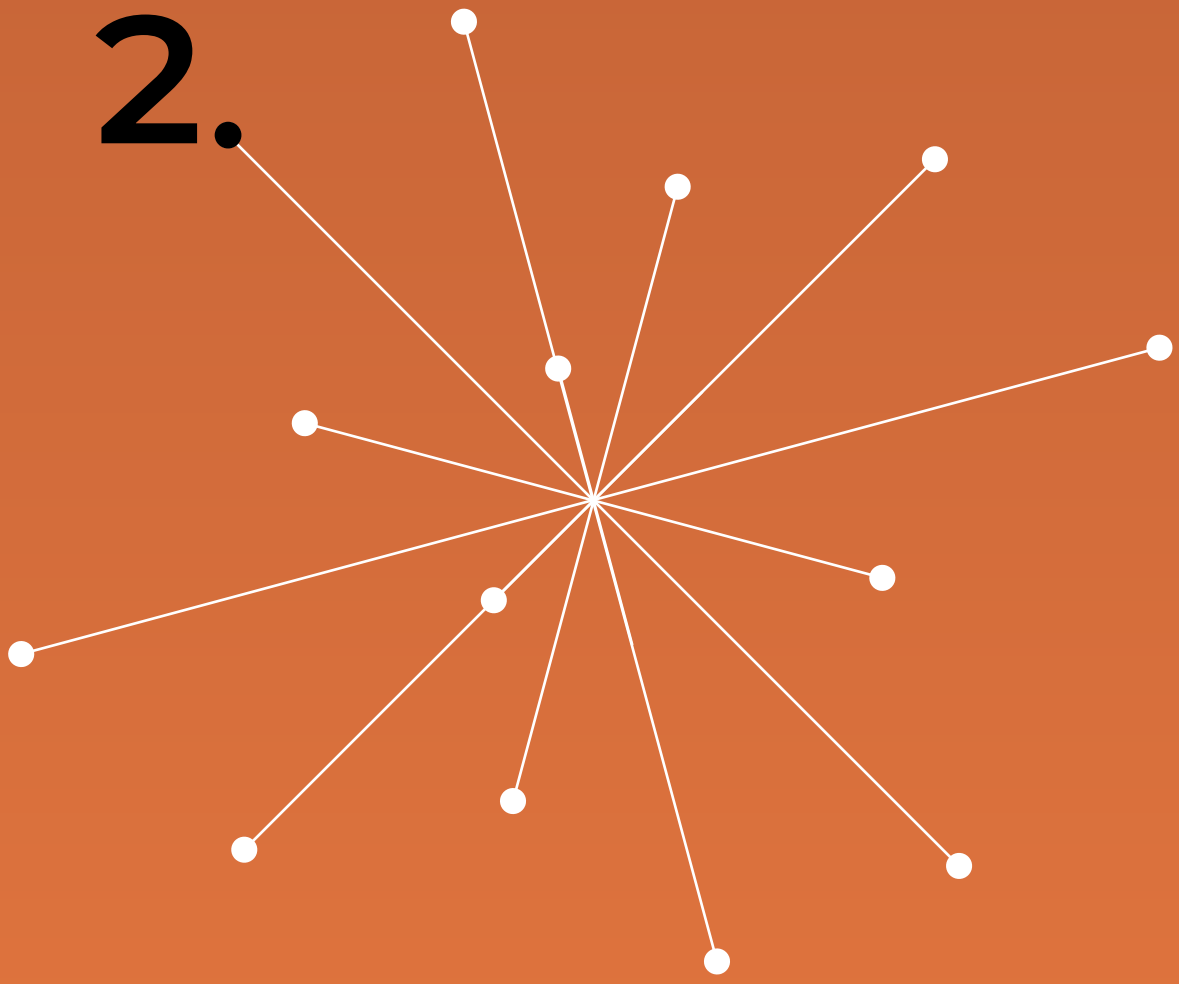
Kolejnym wyzwaniem jest zapewnienie poczucia bezpieczeństwa i zbudowanie zaufania między członkami danego ISAC-a. Organizacje zrzeszają podmioty z tej samej branży, które często konkurują ze sobą na rynku. W związku z tym, mogą się one obawiać ujawniać informacje, które mogłyby zostać wykorzystane przez konkurencję w niepożądanych celach.

Wyzwaniem może być również pochodzenie członków ISAC-ów z różnych krajów. Niesie to za sobą zróżnicowanie w podejściu do zarządzania bezpieczeństwem oraz w krajowych systemach prawnych. Ponadto komunikacja między członkami może być utrudniona przez różnice językowe i terminologiczne. Wiele specjalistycznych terminów z zakresu cyberbezpieczeństwa używanych jest jedynie w języku angielskim i nie ma odpowiednika w innych językach. Może to spowodować różnice w definiowaniu i rozumieniu danego słowa w poszczególnych krajach.

---

20 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.U.UE.L.2016.119.1 z dnia 04.05.2016.

2.



Badanie krajobrazu europejskich ISAC-ów w 2023 roku

2.1 Cel badania

W lutym 2018 r. ENISA opublikowała raport z badania „Centrum wymiany i analizy informacji (ISAC) – modele współpracy" (*Information Sharing and Analysis Center (ISACs) – Cooperative models*). Jego celem była analiza europejskich ISAC-ów, zidentyfikowanie wyzwań, z którymi się mierzą oraz wskazanie najlepszych praktyk[21]. Z kolei w sierpniu 2022 r., Komisja Europejska w ramach inicjatywy Empowering EU ISACs opublikowała „Przegląd i raport na temat europejskich inicjatyw ISAC" (*Overview and Report on EU ISAC Initiatives*), przedstawiający wybrane informacje dotyczące europejskich ISAC-ów[22].

Wspomniane prace ENISA i KE stanowiły punkt wyjścia badania, którego celem było sprawdzenie, jak kształtuje się krajobraz europejskich ISAC-ów w 2023 r. Jego intencją było zebranie szczegółowych danych, umożliwiających wyciągnięcie wniosków na temat organizacji tego typu, ich struktury, sposobów działania, aktywności oraz wyzwań, z którymi się mierzą. Ważnym celem tego projektu badawczego stanowiło także pozyskanie informacji na temat najlepszych praktyk wśród ISAC-ów oraz opracowanie listy rekomendacji na podstawie uzyskanych wyników. Dodatkowo, w ramach publikacji wyników badania chciano stworzyć przestrzeń dla zainteresowanych uczestników do indywidualnego zaprezentowania swojej organizacji.

2.2 Metodologia

Badanie zostało przeprowadzone w miesiącach czerwiec – wrzesień w 2023 r. Składało się z trzech etapów.

W pierwszej kolejności, w czerwcu, przeprowadzono wyszukiwanie informacji w publicznie dostępnych źródłach na temat organizacji typu ISAC, które są aktywne na obszarze Europy. Dodatkowo, w celu pozyskania informacji został nawiązany kontakt z przedstawicielami ENISA.

21 European Union Agency for Cybersecurity (ENISA), op. cit.

22 Empowering EU ISACs, *Empowering EU ISACs. Overview and Report on EU ISAC Initiatives*, 2022.

W wyniku tych czynności, zidentyfikowano 15 organizacji, które spełniały następujące kryteria:

a. określały się jako ISAC-i;

b. były już w pełni utworzone tj. posiadały członków i podejmowały aktywności;

c. prowadziły działalność międzynarodową i posiadały członków z więcej niż jednego kraju;

d. spełniały przesłanki wskazane w definicji ISAC-a zaproponowanej przez ENISA, czyli ich działalność nie miała charakteru zarobkowego oraz polegała na zbieraniu, analizowaniu i wymianie informacji o cyberzagrożeniach.

W przypadku trzech organizacji nie udało się wyszukać danych, które umożliwiłyby nawiązanie z nimi kontaktu. W związku z tym, zapytanie o chęć udziału w badaniu zostało przesłane do 12 ISAC-ów. Spośród nich 10 wyraziło zgodę.

W drugim etapie, do tych 10 organizacji przesłano uprzednio przygotowany kwestionariusz badawczy. Został on sporządzony w formie ankiety online, w języku angielskim i składał się z 19 pytań głównych i siedmiu pytań uszczegóławiających.

Kwestionariusz rozpoczynał się od siedmiu pytań dotyczących podstawowych informacji na temat ISAC-a: pełnej nazwy, daty założenia, siedziby, liczby członków, sektora działalności, strony internetowej oraz funkcji w ISAC-u osoby, która wypełnia kwestionariusz. Wszystkie te pytania miały charakter otwarty.

Następnie, w kwestionariuszu zawarto 12 bardziej szczegółowych pytań. Zostały one podzielone na dwie części: „Organizacja i członkostwo w ISAC-u" oraz „Działalność". Pierwsza część składała się z pięciu pytań na temat formy organizacyjnej ISAC-a, rodzaju członków, elementów struktury, źródeł finansowania i kryteriów przyjmowania nowych członków. Druga część zawierała siedem głównych pytań dotyczących celów ISAC-a, podejmowanych aktywności, metod komunikacji i wymiany informacji, sposobów promocji, wyzwań, prowadzonych inicjatyw i współprac.

Pytania w zakresie metod komunikacji oraz sposobów promocji umożliwiały wybór dowolnej liczby odpowiedzi spośród zaproponowanych.

Pozostałe wymagały wskazania maksymalnie trzech opcji, które, zdaniem wypełniającego, najbardziej pasują do jego organizacji. Celem takiego ograniczenia było skłonienie uczestnika badania do wyboru jedynie tych odpowiedzi, które stanowią rzeczywiście istotną część działalności danego ISAC-a. Instrukcje udzielania odpowiedzi zawarte były w treści każdego pytania.

Ponadto, w trzech pytaniach dotyczących rodzajów aktywności, metod komunikacji oraz współpracy, uczestnicy badania byli proszeni o odpowiedź na dodatkowe pytania uszczegółowiające. W przypadku dwóch pierwszych obszarów, pytania te dotyczyły częstotliwości podejmowanych aktywności lub stosowania danych metod komunikacji. Pytanie uszczegóławiające, dotyczące współpracy, miało zaś na celu poznanie konkretnych podmiotów, z którymi dany ISAC współpracuje.

W drugiej części kwestionariusza, pięć pytań głównych i wszystkie uszczegóławiające miały charakter zamknięty. Pytania główne zwierały jednak także opcję „inne", która umożliwiała uczestnikowi wpisanie własnej odpowiedzi. Dwa pytania dotyczące prowadzonych inicjatyw oraz tego, z jakimi podmiotami ISAC współpracuje, miały charakter otwarty.

Pełny tekst ankiety w języku angielskim stanowi Aneks 1 do tej publikacji, a wersję przetłumaczoną na język polski – Aneks 2.

Kwestionariusz badawczy został wypełniony przez wszystkie 10 podmiotów, które go otrzymały. Następnie, uczestnicy badania zostali zapytani, czy byliby zainteresowani publikacją szczegółowych danych dotyczących ich organizacji. Zgodę wyraziło sześć organizacji. Zaprezentowano je w części „Charakterystyka wybranych europejskich ISAC-ów".

2.3 Wyniki

Ogólna charakterystyka badanych ISAC-ów

Siedem ISAC-ów, które wzięły udział w badaniu, to organizacje działające tylko na obszarze Europy. Jeden ISAC ma wyodrębnione dwa oddziały – europejski oraz globalny. Dwa podmioty to ISAC-i o charakterze globalnym, które prowadzą część swojej działalności w Europie, ale nie posiadają osobnego oddziału dla tego obszaru.

Najstarszy z ankietowanych ISAC-ów został założony w 1991 r. Pozostałe powstały w 2008 r. lub później, z czego dwa w 2021 r.

Sektory działalności

Ankietowane ISAC-i wskazały, że działają w dziewięciu sektorach. Są to: telekomunikacja, transport morski, kolejowy i lotniczy (w tym lotnictwo cywilne), zdrowie, administracja publiczna na poziomie miast i regionów, motoryzacja (producenci OEM i dostawcy), energetyka, finanse.

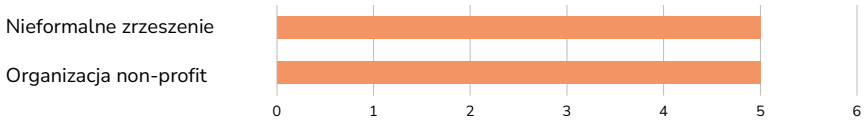
TABELA 1. **Sektory działalności badanych ISAC-ów**

Sektory działalności badanych ISAC-ów
1. Telekomunikacja
2. Transport morski
3. Transport kolejowy
4. Transport lotniczy (w tym lotnictwo cywilne)
5. Zdrowie
6. Administracja publiczna na poziomie miast i regionów
7. Motoryzacja (producenci OEM i dostawcy)
8. Energetyka
9. Finanse

Forma organizacyjna

Pięć ISAC-ów określiło swoją formę jako organizacja non-profit. Pozostałe pięć odpowiedziało, że działa jako nieformalne zrzeszenie.

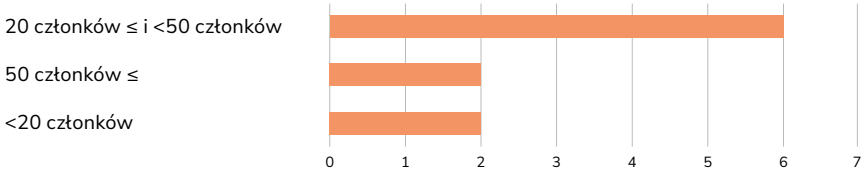
WYKRES 1. **Forma organizacyjna badanych ISAC-ów**



Członkowie organizacji

Ankietowane ISAC-i posiadają bardzo zróżnicowaną liczbę członków – najmniejsza organizacja liczy dziewięć, a największa 809 zrzeszonych podmiotów. Do dwóch organizacji należy mniej niż 20 członków (odpowiednio 9 i 15), do sześciu organizacji – między 20 a 50 członków (odpowiednio 30, 35, 37, 42, 42 i 47), a do dwóch organizacji – ponad 50 członków (odpowiednio 116 i 809).

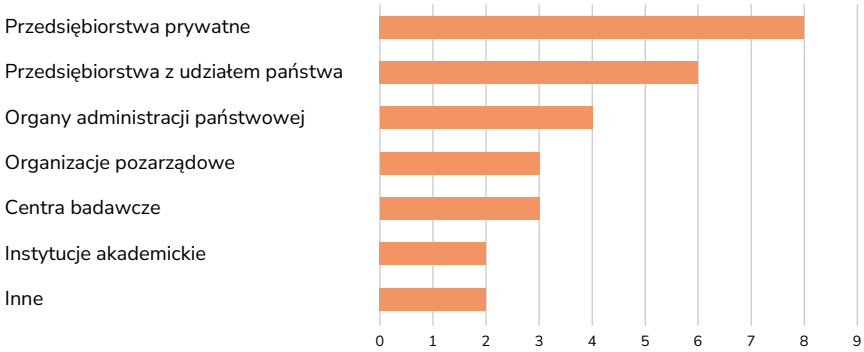
WYKRES 2. **Liczba członków badanych ISAC-ów**



Na pytanie o rodzaje podmiotów, które są ich członkami, ISAC-i mogły udzielić więcej niż jednej odpowiedzi. Z tego względu łączna liczba uzyskanych odpowiedzi jest wyższa niż liczba organizacji, które wzięły udział w badaniu.

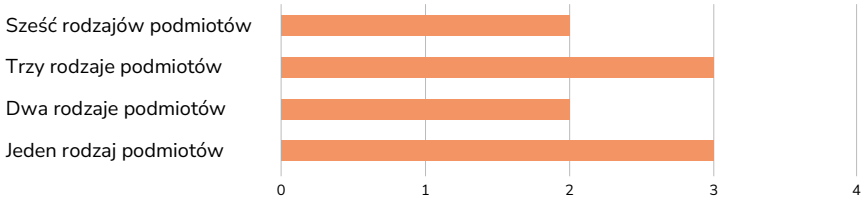
Osiem ISAC-ów wskazało, że w ich skład wchodzą przedsiębiorstwa prywatne, a sześć – że przedsiębiorstwa z udziałem państwa. Cztery ISAC-i udzieliły odpowiedzi, że ich członkami są organy administracji państwowej. Organizacje pozarządowe oraz centra badawcze uzyskały w badaniu po trzy wskazania, a instytucje akademickie – dwa wskazania. Dwa ISAC-i wybrały opcje „inne" i jako swoich członków określiły społeczność CERT-ów wraz z ich organami przedstawicielskimi oraz organy ścigania.

WYKRES 3. **Rodzaje członków badanych ISAC-ów**



Trzy ISAC-i składają się tylko z jednego rodzaju podmiotów. Dwa ISAC-i w swoim składzie mają po dwa rodzaje podmiotów, trzy ISAC-i – trzy rodzaje podmiotów, a dwa – sześć rodzajów podmiotów.

WYKRES 4. **Liczba rodzajów podmiotów, należących do badanych ISAC-ów**

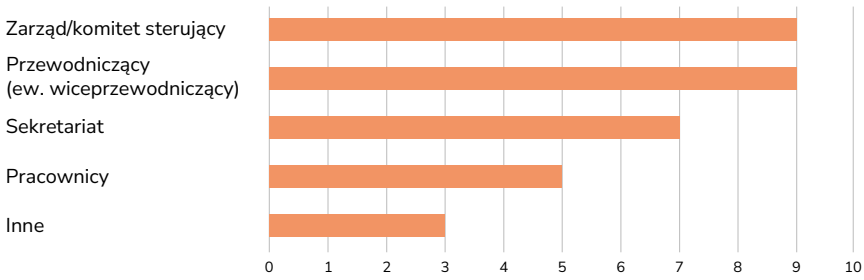


Struktura organizacyjna

Na pytanie dotyczące struktury organizacyjnej ISAC-i mogły udzielić więcej niż jednej odpowiedzi. Z tego względu łączna liczba uzyskanych odpowiedzi jest wyższa niż liczba organizacji, które wzięły udział w badaniu.

Dziewięć ISAC-ów udzieliło odpowiedzi, że ma wyznaczonego przewodniczącego oraz, ewentualnie, wiceprzewodniczącego. Dziewięć organizacji wskazało, że posiada zarząd/komitet sterujący. Siedem ISAC-ów odpowiedziało, że ma sekretariat. Pięć wskazało, że zatrudnia pracowników. Trzy ISAC-i wybrały również odpowiedź „Inne" i wskazały, że posiada takie struktury organizacyjne, jak Główna Grupa (*Core Team*), Grupa Zadaniowa (*Task Force*), Rada (*Council*) oraz grupy robocze. Pojawiła się także odpowiedź, że w ISAC-u działają wolontariusze.

WYKRES 5. **Struktura organizacyjna badanych ISAC-ów**

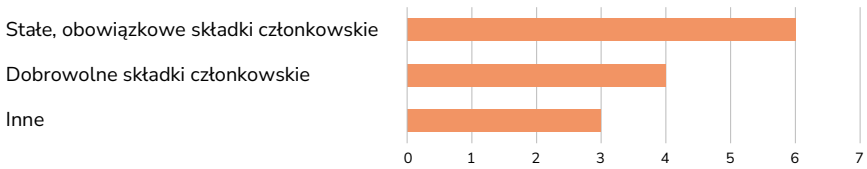


Źródła finansowania

Na pytanie o źródła finansowania ISAC-i mogły udzielić więcej niż jednej odpowiedzi. Z tego względu łączna liczba uzyskanych odpowiedzi jest wyższa niż liczba organizacji, które wzięły udział w badaniu.

Sześć ISAC-ów jako swoje źródło finansowania wskazało stałe, obowiązkowe składki członkowskie. Cztery organizacje odpowiedziały, że ich źródłem finansowania są dobrowolne składki członkowskie. Trzy organizacje wybrały opcję „inne" i w ramach niej jako źródła finansowania wskazały wsparcie sponsorskie oraz wsparcie niepieniężne, w tym w postaci wolontariatu.

WYKRES 6. **Źródła finansowania badanych ISAC-ów**

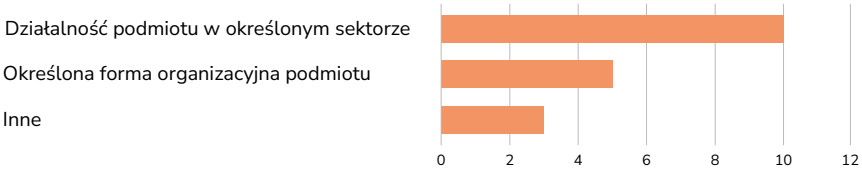


Kryteria przyjmowania nowych członków

Na pytanie o kryteria przyjmowania nowych członków ISAC-i mogły udzielić więcej niż jednej odpowiedzi. Z tego względu łączna liczba uzyskanych odpowiedzi jest wyższa niż liczba organizacji, które wzięły udział w badaniu.

Wszystkie dziesięć badanych ISAC-ów wskazało, że kryterium przyjęcia do ich organizacji jest prowadzenie przez zainteresowany podmiot działalności w określonym sektorze. Pięć ISAC-ów odpowiedziało również, że takim kryterium jest posiadanie przez podmiot określonej formy organizacyjnej. Ponadto, trzy ISAC-i wybrały odpowiedź „inne" i jako kryteria wskazały: posiadanie siedziby/prowadzenie działalności na obszarze UE, uzyskanie poparcia przynajmniej jednego dotychczasowego członka, prowadzenie określonego typu działalności oraz zobowiązanie się do przestrzegania karty członkostwa. Żaden z ISAC-ów nie wybrał zaproponowanej w ankiecie odpowiedzi, że kryterium przyjęcia jest wielkość zainteresowanego podmiotu.

WYKRES 7. **Kryteria przyjmowania nowych członków do badanych ISAC-ów**



Główne cele i aktywności

Na pytanie o główne cele i aktywności ISAC-i mogły udzielić więcej niż jednej odpowiedzi. Z tego względu łączna liczba uzyskanych odpowiedzi jest wyższa niż liczba organizacji, które wzięły udział w badaniu.

Wszystkie dziesięć badanych ISAC-ów udzieliło odpowiedzi, że jednym z ich głównych celów działalności jest wymiana informacji i analiza ryzyk. Ponadto, dziewięć organizacji jako swój cel wskazało promowanie najlepszych praktyk w dziedzinie cyberbezpieczeństwa. Cztery organizacje odpowiedziały, że do głównych celów ich działalności należy prowadzenie treningów i edukacji w zakresie cyberbezpieczeństwa. Po jednym wskazaniu uzyskały odpowiedzi dotyczące celów działalności, takich jak koordynowania reakcji na incydenty i udzielanie technicznego wsparcia i doradztwa. Dwa ISAC-i wybrały opcję „inne" i jako cele swojej działalności wskazały budowanie relacji opartych na zaufaniu, tworzenie platformy do dyskusji między członkami i organizację wydarzeń.

WYKRES 8. **Główne cele realizowane przez badane ISAC-i**

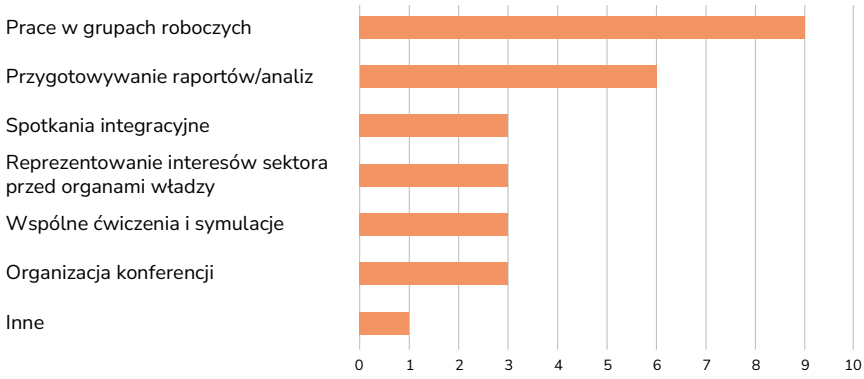
Dziewięć ISAC-ów udzieliło odpowiedzi, że jedną z ich głównych aktywności są prace w grupach roboczych. Sześć organizacji wskazało, że takie prace podejmowane są raz w miesiącu lub częściej, trzy – że raz na kwartał i jedna – że raz na sześć miesięcy.

Sześć ISAC-ów jako jedną ze swoich głównych aktywności wskazało przygotowywanie raportów lub analiz. Cztery z nich podało, że podejmują tę aktywność raz w miesiącu lub częściej, jeden – że raz na kwartał i jeden – że raz na rok.

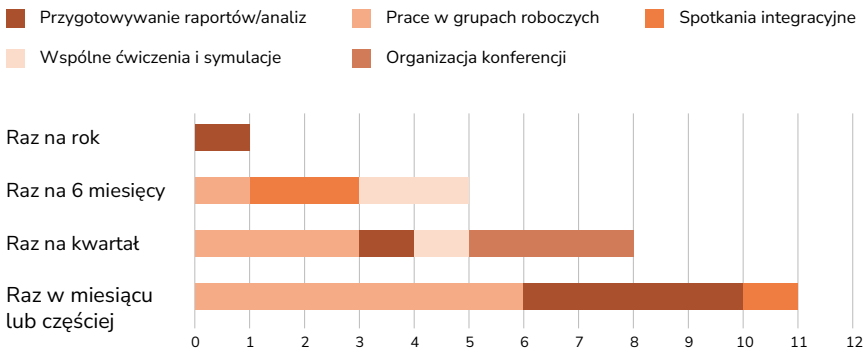
Po trzy wskazania w ankiecie uzyskały cztery rodzaje aktywności: organizacja konferencji; przeprowadzanie wspólnych ćwiczeń i symulacji; reprezentowanie interesów sektora przed organami władzy publicznej oraz organizacja spotkań integracyjnych. Wszystkie ISAC-i, które wybrały odpowiedź dotyczącą organizowania konferencji, podały, że robią to raz na kwartał. W przypadku aktywności w postaci przeprowadzania wspólnych ćwiczeń i symulacji, dwie organizacje wskazały, że podejmują ją raz na sześć miesięcy, a jedna, że raz na kwartał. Spotkania integracyjne są organizowane przez dwa ISAC-i raz na sześć miesięcy, a przez jeden – raz na miesiąc lub częściej. W przypadku aktywności polegającej na reprezentowaniu interesów sektora przed organami władzy publicznej, nie zostało zadane pytanie o częstotliwość ze względu na ciągły charakter tego typu działania.

Jeden z ISAC-ów dodatkowo, w ramach odpowiedzi „inne", wskazał, że jedną z jego głównych aktywności jest dokonywanie przeglądu przepisów prawnych i standardów.

WYKRES 9. **Główne aktywności badanych ISAC-ów – rodzaj**



WYKRES 10. **Główne aktywności badanych ISAC-ów – częstotliwość**



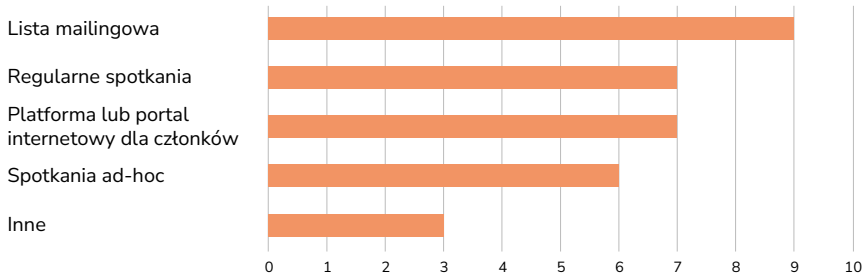
Metody komunikacji i wymiany informacji

Na pytanie o metody komunikacji i wymiany informacji ISAC-i mogły udzielić więcej niż jednej odpowiedzi. Z tego względu łączna liczba uzyskanych odpowiedzi jest wyższa niż liczba organizacji, które wzięły udział w badaniu.

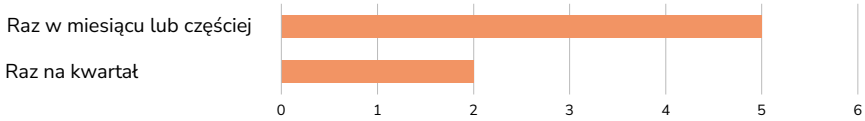
Dziewięć ISAC-ów udzieliło odpowiedzi, że do komunikacji i wymiany informacji wykorzystują listę mailingową. Siedem organizacji wskazało, że posługują się w tym celu także platformą lub portalem internetowym dla członków. Również siedem z nich podało, że komunikuje się i wymienia informacjami w ramach regularnych spotkań, z czego pięć wskazało, że spotyka się w tym celu raz w miesiącu lub częściej, a dwa – że raz na kwartał. Sześć ISAC-ów odpowiedziało, że ich formą komunikacji i wymiany informacji są spotkania ad-hoc.

Dodatkowo, w ramach opcji „inne" udzielone zostały trzy odpowiedzi, w których organizacje określiły konkretne narzędzia i kanały, które wykorzystują do komunikacji i wymiany informacji.

WYKRES 11. **Metody komunikacji i wymiany informacji badanych ISAC-ów**

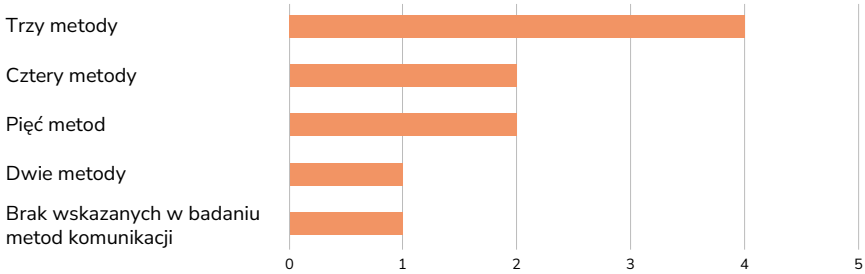


WYKRES 12. **Regularne spotkania – częstotliwość**



Cztery ISAC-i podały, że wykorzystują trzy metody komunikacji i wymiany informacji. Po dwie badane organizacje udzieliły odpowiedzi, że stosują odpowiednio pięć i cztery takie metody. Jeden ISAC wykorzystuje dwie metody, a jeden nie zadeklarował stosowania jakiejkolwiek metody komunikacji i wymiany informacji.

WYKRES 13. **Ilość stosowanych metod komunikacji i wymiany informacji w badanych ISAC-ach**



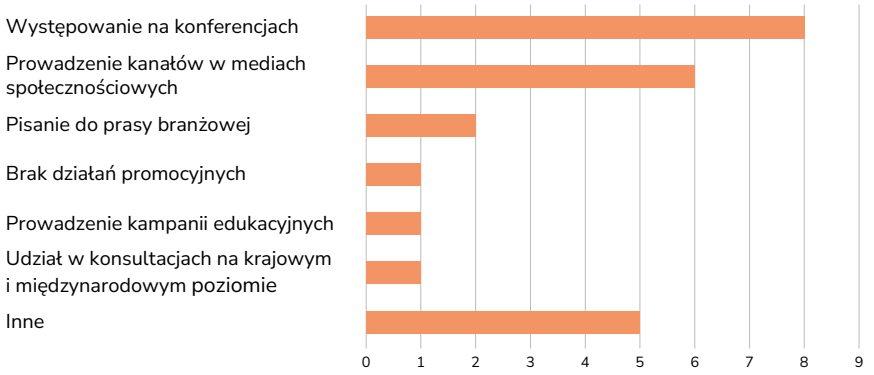
Metody międzynarodowej promocji działalności

Na pytanie o metody międzynarodowej promocji działalności ISAC-i mogły udzielić więcej niż jednej odpowiedzi. Z tego względu łączna liczba uzyskanych odpowiedzi jest wyższa niż liczba organizacji, które wzięły udział w badaniu.

Osiem ISAC-ów wskazało, że promuje swoją działalność na arenie międzynarodowej poprzez udział ich przedstawicieli w charakterze prelegentów na konferencjach. Sześć organizacji podało, że do celów promocyjnych wykorzystuje kanały w mediach społecznościowych. Dwa ISAC-i odpowiedziały, że promują swoją działalność na arenie międzynarodowej poprzez pisanie do prasy branżowej. Po jednym zaznaczeniu uzyskały odpowiedzi dotyczące udziału w konsultacjach na krajowym i międzynarodowym poziomie oraz prowadzenia kampanii edukacyjnych.

Pięć organizacji wybrało także odpowiedź „inne". W ramach niej wskazały, że stosują takie metody międzynarodowej promocji, jak wysyłanie maili do podmiotów, które mogłyby być zainteresowane członkostwem, przekazywanie informacji „pocztą pantoflową", zgłaszanie się do projektów finansowanych przez UE, aktywne angażowanie się w organizacje/stowarzyszenia sektorowe oraz zamieszczanie informacji o ISAC-u na stronach internetowych członków. Jeden ISAC wskazał, że nie prowadzi żadnych działań promocyjnych.

WYKRES 14. **Metody międzynarodowej promocji działalności badanych ISAC-ów**

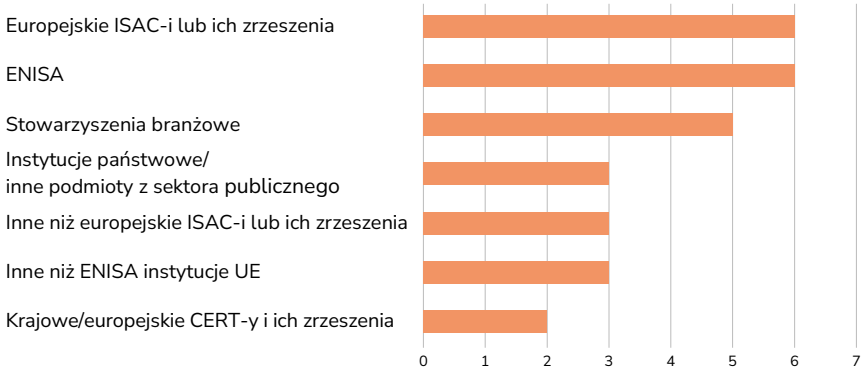


Współpraca z innymi podmiotami

Na pytanie o współpracę z innymi podmiotami ISAC-i mogły udzielić więcej niż jednej odpowiedzi. Z tego względu łączna liczba uzyskanych odpowiedzi jest wyższa niż liczba organizacji, które wzięły udział w badaniu.

Wszystkie dziesięć badanych ISAC-ów udzieliło odpowiedzi, że podejmuje współpracę z innymi podmiotami. Sześć z nich wskazało, że współpracuje z ENISĄ, a trzy – że z inną europejską instytucją. Sześć ISAC-ów udzieliło odpowiedzi, że współpracuje z europejskimi ISAC-ami lub ich zrzeszeniami, a trzy – że z ISAC-ami lub ich zrzeszeniami innymi niż europejskie. Pięć organizacji wskazało, że współpracuje ze stowarzyszeniami branżowymi. Trzy ISAC-i zadeklarowały, że współpracują z instytucjami państwowymi lub innymi podmiotami z sektora publicznego. Dwie organizacje wskazały na współpracę z krajowymi lub europejskimi CERT-ami i ich zrzeszeniami.

WYKRES 15. **Współpraca badanych ISAC-ów z innymi podmiotami**



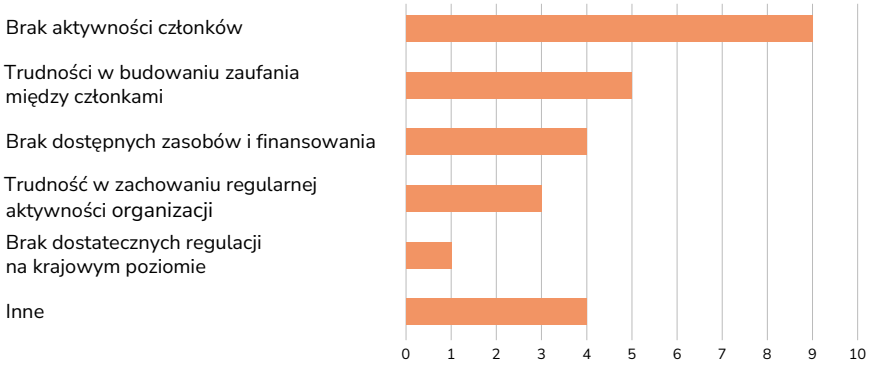
Wyzwania dla działalności ISAC-ów

Na pytanie o wyzwania dla działalności ISAC-i mogły udzielić więcej niż jednej odpowiedzi. Z tego względu łączna liczba uzyskanych odpowiedzi jest wyższa niż liczba organizacji, które wzięły udział w badaniu.

Dziewięć ISAC-ów wskazało, że jednym z głównych wyzwań dla ich działalności jest brak aktywności członków. Pięć organizacji wybrało odpowiedź, że napotyka trudności w budowaniu zaufania między członkami. Cztery ISAC-i podały, że wyzwaniem jest brak dostępnych zasobów i finansowania. Trzy wskazania uzyskała odpowiedź dotycząca trudności w zachowaniu regularnej aktywności organizacji. Jeden z podmiotów wskazał również, że problem stanowi brak dostatecznych regulacji na krajowym poziomie. Żadna z badanych organizacji nie wybrała zaproponowanej w ankiecie odpowiedzi, że wyzwaniem jest występowanie konkurencji między członkami.

Ponadto, cztery ISAC-i zaznaczyły opcję „inne". W ramach niej, jako trudności dla prowadzenia swojej działalności podały brak powszechnej świadomości na temat roli ISAC-ów, brak ich rozpoznawalności w UE oraz brak dostatecznych regulacji na poziomie europejskim.

WYKRES 16. **Wyzwania dla działalności badanych ISAC-ów**



2.4 Wnioski

Wyniki przedstawione w tym raporcie oparte są na odpowiedziach uzyskanych od relatywnie niewielkiej liczby respondentów, co wynika ze specyfiki przedmiotu badania. Dotyczy ono bowiem jedynie 10 organizacji. Zgromadzone dane pozwalają jednak na sformułowanie pewnych wstępnych wniosków dotyczących charakterystyki i działalności ankietowanych ISAC-ów.

Większość z dziesięciu podmiotów, które wzięły udział w badaniu, powstało w ciągu ostatnich 10 lat, z czego aż cztery w 2019 r. i później. Liczby te wskazują na to, że rozwój ISAC-ów w Europie zaczął się stosunkowo niedawno, w szczególności w porównaniu do Stanów Zjednoczonych. Jednocześnie te z badanych organizacji, które zadeklarowały w ankiecie wyższą liczbę członków, w większości działają zarówno w Europie, jak i w Stanach Zjednoczonych.

Sektory działalności

W pytaniu o obszary działalności wszystkie ankietowane ISAC-i wskazały na aktywność tylko w jednym sektorze. Oznacza to, że żaden z nich nie uważa swojej działalności za międzysektorową. Dodatkowo, aktywność w określonym sektorze jest dla wszystkich ISAC-ów kryterium przyjęcia do ich organizacji. Można z tego wyciągnąć wniosek, że przynależność do określonego sektora stanowi ważny element charakterystyki wszystkich ankietowanych podmiotów.

Poniżej przedstawione zostało zestawienie obszarów, do których przynależność zadeklarowały badane ISAC-i z sektorami, które objęto regulacjami dyrektyw NIS i NIS 2[23]. Warto podkreślić, że jest ono wykonane w uproszczeniu, ponieważ opiera się na samodzielnej identyfikacji ISAC-ów jako wchodzących w zakres danego sektora lub podsektora. Bardziej precyzyjne określenie przynależności tych organizacji do poszczególnych obszarów wymagałoby szerszej analizy ich składu członkowskiego, co znaczenie przekraczałoby zakres tego badania. W związku z tym, poniższe zestawienie ma charakter orientacyjny i służy poglądowemu zarysowaniu części wspólnych pomiędzy deklarowanymi obszarami działalności badanych ISAC-ów a sektorami wchodzącymi w zakres regulacji NIS i NIS 2.

TABELA 2. **Zestawienie sektorów objętych dyrektywami NIS i NIS 2, a obszarów działalności wskazanych przez ISAC-i**

NIS – sektory i podsektory	NIS 2 – sektory i podsektory	Obszary działalności ISAC-ów – wg odpowiedzi
Energetyka: • energia elektryczna • ropa naftowa • gaz	Energetyka: • energia elektryczna • system ciepłowniczy lub chłodniczy • ropa naftowa • gaz • wodór	Energetyka
Transport: • transport lotniczy • transport kolejowy • transport wodny • transport drogowy	Transport: • transport lotniczy • transport kolejowy • transport wodny • transport drogowy	Transport: • transport lotniczy • transport kolejowy • transport morski
Bankowość	Bankowość	Sektor finansowy
Infrastruktura rynków finansowych	Infrastruktura rynków finansowych	Sektor finansowy
Służba zdrowia	Opieka zdrowotna	Zdrowie
Zaopatrzenie w wodę pitną i jej dystrybucja	Woda pitna	
Infrastruktura cyfrowa	Infrastruktura cyfrowa	
	Ścieki	

23 Odpowiednio Załącznik I do dyrektywy NIS oraz Załącznik I i Załącznik II do dyrektywy NIS 2.

NIS – sektory i podsektory	NIS 2 – sektory i podsektory	Obszary działalności ISAC-ów – wg odpowiedzi
	Zarządzanie usługami ICT (między przedsiębiorstwami)	
	Podmioty administracji publicznej – centralnej i regionalnej	Administracja publiczna na poziomie miast i regionów
	Przestrzeń kosmiczna	
	Usługi pocztowe i kurierskie	
	Gospodarowanie odpadami	
	Produkcja, wytwarzanie i dystrybucja chemikaliów	
	Produkcja, przetwarzanie i dystrybucja żywności	
	Produkcja: • produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro • produkcja komputerów, wyrobów elektronicznych i optycznych • produkcja urządzeń elektrycznych • produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana • produkcja pojazdów samochodowych, przyczep i naczep • produkcja pozostałego sprzętu transportowego	Sektor motoryzacyjny (producenci oryginalnego wyposażenia (OEM) i dostawcy)
Dostawcy usług cyfrowych	Dostawcy usług cyfrowych	
	Badania naukowe	
		Telekomunikacja

Zestawiając obszary, w których badane ISAC-i umiejscowiły swoją działalność z sektorami i podsektorami wskazanymi w dyrektywach NIS i NIS 2, można zauważyć, że część ISAC-ów jest aktywna w obrębie całych sektorów zdefiniowanych w dyrektywach, część – w podsektorach, a pozostałe – w części sektorów lub podsektorów.

Sektory, które ISAC-i wskazały jako swoje obszary działania, pokrywają się, przynajmniej częściowo, z pięcioma sektorami objętymi dyrektywą NIS i siedmioma objętymi dyrektywą NIS 2. W przypadku dwóch sektorów – transportu i produkcji – zakres działalności badanych ISAC-ów pokrywa się nie z całym sektorem, a z poszczególnymi podsektorami. Jedna organizacja biorąca udział w badaniu wskazała na działalność w sektorze telekomunikacji, który nie jest wyodrębniony jako osobny sektor ani w dyrektywie NIS, ani w dyrektywie NIS 2. Mimo to, niektóre podmioty działające w jego obrębie mogą wchodzić w zakres innych sektorów objętych obowiązywaniem dyrektyw.

Ponieważ powyższe zestawienie oparte jest o ogólne wskazania samych respondentów, nie można wykluczyć, że w rzeczywistości organizacje te i ich członkowie nie wpisują się wyłącznie w te sektory i podsektory, do których zostały przypisane w Tabeli nr 2. Mimo to, analiza przywołanego zestawienia pozwala zauważyć, że o ile europejskie ISAC-i działają, przynajmniej częściowo, w większości sektorów i podsektorów, które są wymienione w dyrektywie NIS, to inaczej jest w przypadku jej znowelizowanej wersji. NIS 2 obejmuje bowiem wiele nowych obszarów, w których – zgodnie z wynikami przeprowadzanego wyszukiwania – takie organizacje jeszcze nie funkcjonują.

Wyjątkami są tutaj nowododane w dyrektywie NIS 2 sektory: podmiotów administracji publicznej (centralnej i regionalnej) oraz produkcji. Istnieją bowiem dwa ISAC-i, których zakres działalności częściowo pokrywa się z tymi dwoma obszarami. W przypadku jednej z organizacji, zakres podmiotowy jest nawet szerszy niż ten wskazany w dyrektywie. Mianowicie, obejmuje on także administrację publiczną na poziomie miast, czyli dotyczy szczebla lokalnego, który, zgodnie z NIS 2, jest objęty regulacjami jedynie fakultatywnie, jeżeli państwo członkowskie tak zadecyduje.

W 2023 r. zapowiedziane zostało utworzenie europejskiego ISAC-a, który będzie działał w sektorze dodanym przez dyrektywę NIS 2 – przestrzeni kosmicznej[24]. Być może rozszerzony zakres podmiotowy NIS 2 w stosunku do poprzedniej wersji dyrektywy będzie zachęcał organizacje z nowo uregulowanych sektorów do tworzenia kolejnych ISAC-ów. Funkcjonowanie społeczności do wymiany najlepszych praktyk oraz wzmacniania ogólnej odporności danego sektora może bowiem ułatwiać podmiotom wypełnianie obowiązków nałożonych przez nowe przepisy.

---

24 Zob. szerzej: https://www.euspa.europa.eu/opportunities/isac, [dostęp: 13.05.2024].

Struktura ISAC-ów

W skład ankietowanych ISAC-ów najczęściej wchodzą prywatne przedsiębiorstwa, a najrzadziej instytucje akademickie. Analiza tego, ile rodzajów podmiotów należy do organizacji, wskazuje, że cechują się one zróżnicowaną strukturą członkostwa. Połowa ankietowanych organizacji składa się z dwóch lub trzech rodzajów podmiotów. Druga połowa wybrała dwie skrajne odpowiedzi – trzy ISAC-i wskazały, że mają w swoim składzie tylko jedną kategorię podmiotów członkowskich, a dwie – że sześć różnych kategorii podmiotów. Zróżnicowanie w liczbie rodzajów członków może wynikać ze specyfiki sektorów lub podsektorów, w których działają poszczególne organizacje – niektóre z nich mogą być zdominowane przez określony rodzaj podmiotów, np. przedsiębiorstwa z udziałem państwa.

W zakresie struktury wewnętrznej badanych ISAC-ów z zebranych odpowiedzi wynika, że w każdym z nich jest wyznaczona przynajmniej jedna osoba lub grupa osób pełniąca funkcje kierownicze – czy to przewodniczący, ewentualnie wiceprzewodniczący, czy też zarząd. W zdecydowanej większości organizacji sprawowane są obydwie funkcje. W większości ISAC-ów ustanowiony jest także sekretariat, a połowa z nich zadeklarowała, że zatrudnia pracowników. Tylko jedna organizacja wskazała, że posiada w swojej strukturze wyłącznie jeden organ – przewodniczącego/wiceprzewodniczącego.

Powyższe informacje pozwalają stwierdzić, że wszystkie badane ISAC-i posiadają ustaloną wewnętrzną strukturę i w przypadku większości z nich jest ona rozbudowana.

Finansowanie ISAC-ów

Do ciekawych wniosków prowadzi analiza odpowiedzi ISAC-ów w zakresie źródeł finansowania. Prawie wszystkie organizacje wskazały, że są nimi składki członkowskie – obowiązkowe, dobrowolne lub jednocześnie obydwa te rodzaje. Tylko jedna organizacja zadeklarowała, że nie dysponuje środkami finansowymi i polega wyłącznie na dobrowolnym wsparciu niepieniężnym od swoich członków.

Oznacza to, że wszystkie badane organizacje opierają swoją działalność przede wszystkim na wsparciu finansowym i pozafinansowym swoich członków. Pozyskiwanie dodatkowego, zewnętrznego wsparcia finansowego zostało wspomniane przez wyłącznie jeden ISAC, który wskazał, że jego aktywności wspomagane są przez sponsorów. Żadna organizacja

nie zaznaczyła zaproponowanej w ankiecie odpowiedzi, że otrzymuje środki finansowe od państwa.

Warto przy tym zauważyć, że w pytaniu o wyzwania, jakie ISAC-i dostrzegają dla swojej działalności, odpowiedź „brak dostępnych zasobów i finansowania" została wybrana przez prawie połowę respondentów. Może to wskazywać na to, że w niektórych przypadkach, wsparcie wyłącznie przez członków, okazuje się niewystarczające. Brak dostatecznych możliwości pozyskania zewnętrznego finansowania lub wsparcia w innej formie może stanowić czynnik hamujący rozwój ISAC-ów. Niewystarczające zasoby mogą uniemożliwiać organizacjom podejmowanie określonych rodzajów aktywności (np. przeprowadzania realistycznych symulacji) lub rozwój struktury (np. zatrudnienie pracowników).

Cele i aktywności ISAC-ów

Celem działalności, który łączy wszystkie badane ISAC-i, jest wymiana informacji i analiza ryzyka. Nie jest to zaskakujący wynik, jeśli weźmie się pod uwagę, że na ten rodzaj aktywności wskazuje sama nazwa takich organizacji. Dziewięć ISAC-ów wskazało również, że jednym z ich głównych celów jest promowanie najlepszych praktyk w dziedzinie cyberbezpieczeństwa. Można wysunąć przypuszczenie, że te kierunki działalności łączą się ze sobą, ponieważ opracowywanie i promowanie najlepszych praktyk w danym sektorze możliwe jest dzięki wnioskom wyciągniętym z analizy ryzyk i informacji. Jest to spójne także z następnym najczęściej wskazywanym celem działalności ISAC-ów, czyli treningiem i edukacją w zakresie cyberbezpieczeństwa.

Z kolei koordynacja odpowiedzi na incydenty oraz udzielanie technicznego wsparcia i doradztwa okazały się być najrzadziej wybieranymi, przez badane organizacje, odpowiedziami – uzyskały one tylko po jednym wskazaniu. Może to oznaczać, że w przeważającej części członkowie realizują te cele poza ISAC-ami – np. przy pomocy zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT).

W zakresie podejmowanych aktywności, prawie wszystkie ISAC-i wskazały, że prowadzą prace w grupach roboczych. Czynność ta, zgodnie z wynikami ankiety, najczęściej wykonywana jest przynajmniej raz na miesiąc. Jednocześnie żadna z organizacji nie wskazała, aby wykonywała ją rzadziej niż raz na pół roku. Dodatkowo te ISAC-i, które zadeklarowały, że prowadzą prace w grupach roboczych rzadziej niż raz w miesiącu – czyli przynajmniej raz na kwartał lub raz na pół roku – przy innych aktywnościach

wskazały, że wykonują je jeszcze rzadziej. Na tej podstawie można więc wnioskować, że praca w grupach roboczych to podstawowa, najbardziej regularna forma aktywności badanych ISAC-ów.

Wśród innych odpowiedzi, zaproponowanych do pytania o aktywności, w drugiej kolejności najczęściej wybieraną była „przygotowywanie raportów i analiz". Wszystkie pozostałe odpowiedzi uzyskały taką samą, mniejszą liczbę wskazań. Nasuwa się z tego wniosek, że aktywności podejmowane przez ISAC-i są dość różnorodne, z przewagą jednak pracy w grupach roboczych i przygotowywania raportów i analiz.

Odpowiedzi badanych ISAC-ów dotyczące częstotliwości podejmowanych aktywności wskazują, że prowadzą one swoje działania raczej regularnie. Najczęściej wybieraną przez organizacje opcją było „raz w miesiącu", a w drugiej kolejności „raz na kwartał". Odpowiedź „raz na rok" została wybrana wyłącznie przez jedną organizację dla jednej aktywności, a odpowiedź „rzadziej niż raz na rok" – ani razu.

Metody komunikacji i wymiany informacji w ISAC-ach

Z badania wynika, że zdecydowana większość ISAC-ów stosuje przynajmniej trzy lub więcej metod komunikacji i wymiany informacji pomiędzy członkami. Najpopularniejszą z nich jest lista mailingowa – jej wykorzystanie zadeklarowały prawie wszystkie ankietowane organizacje. Drugim najczęściej wskazywanym kanałem komunikacji są platforma lub portal internetowy dla członków.

Ponadto, niemal wszystkie ISAC-i udzieliły odpowiedzi, że komunikują się i wymieniają informacjami w ramach spotkań – regularnych lub ad hoc. Oznacza to, że dziewięć z dziesięciu ankietowanych ISAC-ów przekazuje informacje zarówno poprzez narzędzia komunikacyjne (listę mailingową i ew. platformę/portal dla członków), jak i w ramach spotkań w czasie rzeczywistym.

Dodatkowo, większość ISAC-ów, które wskazały, że organizują regularne spotkania, określiła ich częstotliwość jako przynajmniej raz na miesiąc. Pozostałe odpowiedziały, że spotykają się przynajmniej raz na kwartał. Wynika z tego, że taka forma komunikacji i wymiany informacji w ISAC-ach jest stosowana regularnie.

Promocja działalności ISAC-ów

Niemalże wszystkie ankietowane ISAC-i stosują różne metody i kanały promocji swojej działalności na arenie międzynarodowej. Metody te mają dwojaki charakter. Z jednej strony, organizacje promują się w ogólnodostępnych kanałach – poprzez występy przedstawicieli organizacji na konferencjach i prowadzenie profili w mediach społecznościowych. Z drugiej strony, niektóre z nich przekazują informacje o swojej działalności poprzez indywidualny kontakt z potencjalnymi zainteresowanymi lub „pocztą pantoflową". W przypadku jednego ISAC-a jest to jedyna stosowana forma promocji.

Dodatkowo, niektóre ISAC-i wskazały, że budują swoją rozpoznawalność także poprzez aktywne angażowanie się w projekty unijne oraz działania w obrębie swojego sektora. Zestawiając to z pozostałymi wynikami, można wyróżnić kolejny podział na dwa rodzaje promocji stosowanej przez ISAC-i – promocję poprzez indywidualną aktywność (m. in. profile w mediach społecznościowych, nawiązywanie kontaktu z potencjalnymi członkami) oraz promocję poprzez zaangażowanie w działania innych podmiotów oraz współpracę z nimi (np. występowanie na konferencjach, udział w projektach unijnych).

Współpraca ISAC-ów z innymi podmiotami

Wszystkie ISAC-i wskazały, że współpracują z innymi podmiotami – najczęściej z więcej niż jednym. Wskazuje to na to, że prowadzenie współpracy nie tylko wewnętrznej, ale i zewnętrznej, stanowi ważny element funkcjonowania organizacji tego typu.

Z uzyskanych wyników wyłania się bardzo różnorodny krajobraz takich współprac. Wśród podmiotów, których dotyczą, znajdują się zarówno stowarzyszenia branżowe, jak instytucje państwowe lub inne podmioty powiązane z państwem i krajowe zespoły CERT. Zdecydowanie jednak największa część odpowiedzi ISAC-ów w tym zakresie dotyczyła kooperacji na poziomie Unii Europejskiej, w szczególności z ENISA, na współpracę z którą wskazała ponad połowa respondentów. Wśród odpowiedzi pojawiły się także inne instytucje unijne oraz europejskie zespoły CERT i ich zrzeszenia.

Ponadto, wyniki badania wskazują na to, że ankietowane ISAC-i prowadzą współpracę z innymi organizacjami tego typu zarówno z Europy, jak i innych części świata, w tym ze Stanów Zjednoczonych i Japonii. Najczęściej wskazywaną platformą do współpracy ISAC-ów w Europie była Europejska Rada ISAC-ów.

Wyzwania dla działalności ISAC-ów

Wśród wyzwań dla działalności wskazanych przez ISAC-i w badaniu, na prowadzenie zdecydowanie wysuwają się te związane z ich członkami. Prawie wszystkie organizacje wskazały, że problemem jest brak aktywności ich członków, a połowa z nich – że są nim trudności w budowaniu zaufania między członkami. Obydwie te kwestie mogą stanowić poważne wyzwanie dla sprawnego funkcjonowania organizacji, która z założenia opiera się właśnie na tych dwóch filarach – aktywnej społeczności oraz poczuciu wzajemnego zaufania. Brak zaangażowania członków może wiązać się również z innym wyzwaniem, które zostało wskazane przez część respondentów, a mianowicie trudności w zachowaniu regularności w działaniach organizacji.

Jednocześnie jednak żaden badany podmiot nie wybrał zaproponowanej w ankiecie odpowiedzi, że wyzwaniem jest konkurencja pomiędzy jego członkami. Jest to ciekawa informacja, zważając na to, że z odpowiedzi na inne pytania wynika, że do ankietowanych ISAC-ów należą podmioty działające w jednym sektorze, w tym często prywatne przedsiębiorstwa, które najprawdopodobniej na co dzień ze sobą konkurują. Może to oznaczać, że wspólne cele realizowane w ramach ISAC-ów przeważają nad chęcią realizacji przez poszczególnych członków własnych interesów, wynikających z działalności prowadzonej poza tymi organizacjami.

Jak zostało już wspomniane, kilka podmiotów wskazało, że wyzwaniem jest brak finansowania. Ten problem może stanowić jedną z przyczyn innych trudności zgłoszonych przez ISAC-i w odpowiedzi na to pytanie, takich jak brak dostatecznej aktywności członków. Jeżeli bowiem działania na rzecz organizacji są wykonywane przez nich nieodpłatnie, może to zniechęcać ich do poświęcenia na nie większej ilości czasu lub wysiłku. Ponadto, brak funduszy może również wpływać negatywnie na skalę działalności ISAC-ów – bez dostatecznych środków nie są one bowiem w stanie wykonywać bardziej skomplikowanych aktywności, które wymagają zakupu sprzętu lub zatrudnienia personelu.

Jako wyzwanie wskazany został także brak powszechnej świadomości na temat istnienia ISAC-ów oraz roli, którą pełnią. Zdaniem jednego z respondentów, utrudnia to organizacjom tego typu pozyskiwanie nowych członków oraz zdobywanie finansowania.

Brak rozpoznawalności ISAC-ów może wiązać się także z innym wyzwaniem zasygnalizowanym przez nie w badaniu, czyli brakiem dostatecznej regulacji ich działalności na poziomie unijnym. Nie ma aktualnie przepisów,

które wprost dotyczyłyby działalności takich organizacji (dyrektywa NIS 2 jedynie pośrednio dotyka tej kwestii poprzez zapisy na temat dobrowolnej wymiany informacji). Brak wyraźnego, unijnego uregulowania działalności ISAC-ów może przyczyniać się do tego, że państwa i inne rodzaje podmiotów nie zauważają ich roli w budowaniu cyberodporności i koncentrują się na wzmacnianiu innych rodzajów organizacji, wskazanych w aktach prawnych dotyczących cyberbezpieczeństwa.

Ponadto, jak zasygnalizował jeden z respondentów, brak przepisów dotyczących wymiany informacji w ramach ISAC-ów stanowi utrudnienie dla jego członków w prowadzeniu takiej działalności bez narażania się na odpowiedzialność z tego tytułu. Wskazuje to na to, że podmioty uczestniczącego w takim ISAC-u mogą mieć poczucie działania w stanie niepewności prawnej, co może z kolei zniechęcać je do pełnego zaangażowania się w dzielenie się informacjami.

2.5 Rekomendacje

1. Tworzenie europejskich ISAC-ów w nowych sektorach i podsektorach

Tworzenie nowych, europejskich ISAC-ów może stanowić istotny element wzmacniania cyberbezpieczeństwa w poszczególnych obszarach gospodarki. W szczególności należy skupić uwagę na sektorach i podsektorach, które zostały objęte zakresem obowiązywania dyrektywy NIS 2. Ponieważ nowe przepisy mają zastosowanie do znacznie większej liczby podmiotów niż w przypadku poprzedniej wersji dyrektywy, część z nich po raz pierwszy będzie musiała dostosować się do unijnych wymagań w obszarze cyberbezpieczeństwa. Tym samym, może to stanowić dla nich ogromne wyzwanie. Aby mu sprostać, takie podmioty będą potrzebowały wsparcia, które może im zapewnić udział w organizacjach typu ISAC. Pozwalają one bowiem nie tylko na wzmacnianie odporności poszczególnych członków poprzez dzielenie się informacjami o zagrożeniach, ale także na wymianę doświadczeń i najlepszych praktyk oraz uczenie się od siebie nawzajem.

2. Budowanie platform do współpracy między ISAC-ami z różnych sektorów

Wiele incydentów dotyka kilku sektorów jednocześnie. Rozwijanie platform do współpracy między ISAC-ami może umożliwić szybsze identyfikowanie i odpowiednie reagowanie na cyberzagrożenia, które występują w więcej niż jednym obszarze gospodarki. Ponadto, przedstawiciele różnych sektorów posiadają odmienne doświadczenia i wiedzę, których wymiana pomiędzy ISAC-ami może przyczyniać się do wspólnego opracowania najskuteczniejszych metod zwalczania incydentów o zróżnicowanym charakterze.

3. Opracowanie narzędzi do wymiany informacji między ISAC-ami

Współpraca między ISAC-ami może zostać ułatwiona poprzez stworzenie odpowiednich narzędzi do komunikacji i przepływu wiedzy. Dzięki nim, organizacje mogłyby przekazywać sobie informacje o incydentach oraz na bieżąco je aktualizować. Pozwoliłoby to także na stworzenie wspólnej bazy danych o incydentach i zagrożeniach, która umożliwiałaby wszystkim zrzeszonym ISAC-om stały dostępu do informacji. Takie narzędzia do komunikacji mogłyby także posłużyć do organizacji różnego rodzaju spotkań z udziałem przedstawicieli ISAC-ów, w tym poświęconych dzieleniu się wiedzą i najlepszymi praktykami w zakresie różnych aspektów funkcjonowania ISAC-ów.

4. Wzmacnianie współpracy między ISAC-ami o różnym stopniu dojrzałości

Aby stworzyć nowe ISAC-i w sektorach na ten moment niezagospodarowanych, istotne jest zapewnienie im wsparcia ze strony już rozwiniętych ISAC-ów. Mogą one bowiem podzielić swoimi doświadczeniami i wypracowanymi praktykami w zakresie tworzenia i usprawniania działania organizacji tego typu, dzięki czemu nowe podmioty mogłyby np. uniknąć popełnienia określonych błędów. Taka współpraca mogłaby przynieść korzyści również dojrzałym ISAC-om, które miałyby możliwość poznania nowej perspektywy, prezentowanej przez świeżo utworzone organizacje.

5. Wzmacnianie współpracy pomiędzy europejskimi a krajowymi ISAC-ami

Wypracowanie kanałów do regularnej komunikacji między krajowymi i europejskimi ISAC-ami mogłoby przynieść korzyści obydwu stronom. Krajowe ISAC-i dzięki kooperacji z europejskimi organizacjami zyskałyby dostęp do informacji pochodzących od ich członków z innych państw. Z kolei europejskie ISAC-i mogłyby zwiększyć swoją wiedzę na temat specyfiki różnych aspektów związanych z cyberbezpieczeństwem na gruncie poszczególnych krajów. Dzięki temu, obydwa rodzaje ISAC-ów poszerzyłyby zasób posiadanych informacji, co mogłoby pozytywnie wpłynąć na wypracowywane przez nie praktyki w zakresie budowania odporności na różne rodzaje zagrożeń.

6. Zapraszanie różnorodnych podmiotów do członkostwa w ISAC-ach

Zwiększanie różnorodności podmiotów, które tworzą ISAC-i, może mieć korzystny wpływ na rozwój zasobów posiadanej wiedzy oraz poszerzenie zakresu możliwych do podjęcia aktywności. Warto rozważyć włączanie do organizacji na przykład instytucji akademickich oraz centr badawczych, które mogą wesprzeć je w wielu aspektach, m. in.:

- prowadzenia zaawansowanych badań z zakresu cyberbezpieczeństwa, w tym analizy zagrożeń oraz opracowywania metod ochrony;
- przeprowadzenia kursów i szkoleń z zakresu cyberbezpieczeństwa dla pozostałych członków ISAC-a;
- angażowania ekspertów i naukowców z różnych dziedzin;
- edukowania społeczeństwa na temat działalności ISAC-a.

Każdy nowy rodzaj podmiotu w ISAC-u wnosi odmienny rodzaj wiedzy, doświadczeń i zasobów. Może na przykład udostępnić organizacji infrastrukturę oraz narzędzia, do których nie miałaby dostępu bez takiego członka. Ponadto, zaangażowanie przedstawicieli różnorodnych podmiotów z danego sektora może pozytywnie wpłynąć na szersze upowszechniania się w jego obrębie świadomości na temat funkcjonowania i roli ISAC-ów.

7. Budowanie systemów wsparcia finansowego ISAC-ów

Finansowanie stanowi jeden z kluczowych aspektów dla sprawnego działania ISAC-ów. Dzięki środkom finansowym organizacje mogą pozyskać i utrzymać odpowiednie zasoby, takie jak narzędzia i infrastrukturę, oraz zapewniać szkolenia i warsztaty swoim członkom. Brak dostatecznego finansowania ogranicza ISAC-om możliwości rozwoju. Dlatego zalecane jest rozwijanie programów wsparcia finansowego, z których organizacje tego typu mogłyby skorzystać. Same ISAC-i mogą również zwiększyć promocję swojej działalność oraz dzielić się jej efektami i osiągnięciami, aby dotrzeć do jak najszerszego grona potencjalnych podmiotów, mogących pomóc im finansowo.

8. Stworzenie ogólnodostępnego rejestru ISAC-ów

Aktualnie informacje na temat poszczególnych europejskich ISAC-ów znajdują się w różnych miejscach i niejednokrotnie ich odnalezienie wymaga długiego wyszukiwania. Dlatego warto rozważyć stworzenie ogólnodostępnego rejestru europejskich ISAC-ów, który zbierałby w jednym miejscu podstawowe informacje na ich temat, takie jak reprezentowane sektory gospodarki, krótki opis działalności, dane kontaktowe organizacji oraz adresy stron internetowych. Taki rejestr ułatwiłby odnalezienie informacji na temat poszczególnych ISAC-ów lub skontaktowanie się z nimi. Byłby on również pomocny dla podmiotów, które potencjalnie chciałyby zostać członkami takich organizacji. Rejestr pozwalałby także na zapewnienie ISAC-om szerszej rozpoznawalności.

9. Promowanie działalności ISAC-ów w obrębie sektorów i podsektorów

ISAC-i mogą podejmować działania dedykowane promowaniu swojej działalności w obrębie sektora lub podsektora, w którym są aktywne. Przykładem może być organizowanie szkoleń, warsztatów i webinariów. Sprzyjałoby to podnoszeniu poziomu rozpoznawalności ISAC-ów w danym sektorze lub podsektorze oraz umożliwiałoby nawiązywanie kontaktów z nowymi, potencjalnymi członkami. Skutecznym narzędziem dotarcia do szerszego grona podmiotów z danej branży może być również regularne

publikowanie rezultatów pracy ISAC-ów w postaci raportów, analiz czy zaleceń. Dodatkowo, mogłyby być one prezentowane na konferencjach oraz innych wydarzeniach sektorowych.

10. Zwiększanie powszechnej świadomości na temat ISAC-ów

Podnoszenie świadomości na temat organizacji typu ISAC wymaga podjęcia działań w kilku obszarach jednocześnie. Ważnym elementem w docieraniu do szerszego grona odbiorców jest posiadanie przez ISAC-i przejrzystej strony internetowej. Powinna ona zawierać podstawowe informacje o danym ISAC-u, takie jak opis działalności, kryteria dołączenia oraz dane kontaktowe. Kolejnym, ważnym aspektem promowania świadomości na temat ISAC-ów są media społecznościowe, w których organizacje te mogą na bieżąco dzielić się podejmowanymi działaniami, wydarzeniami oraz publikacjami. Kanały te służą również budowaniu społeczności wokół ISAC-ów, a tym samym promują aktywny udział w organizacjach.

3.

Charakterystyka wybranych europejskich ISAC-ów

Na poniższych grafikach zaprezentowane zostały dane dotyczące sześciu europejskich ISAC-ów. Są to podmioty, które po udziale w badaniu wyraziły dodatkową zgodę na opublikowanie w tym raporcie ich szczegółowej charakterystyki.

Auto-ISAC Europe*

Pełna nazwa

Auto Information Sharing and Analysis Centre Europe

Data założenia

2021

Siedziba

Stuttgart, Niemcy

Liczba członków

42

Sektor działalności

sektor motoryzacyjny (producenci OEM i dostawcy)

Forma organizacyjna

organizacja non-profit

Rodzaje podmiotów członkowskich

przedsiębiorstwa prywatne

Kryteria członkostwa

- aktywność w określonym sektorze
- określona forma organizacji

Główne działania

- wspólne ćwiczenia i symulacje – raz na kwartał
- przygotowywanie raportów/analiz – raz w miesiącu lub częściej
- działania w grupach roboczych – raz w miesiącu lub częściej

Metody komunikacji

- regularne spotkania – raz w miesiącu lub częściej
- spotkania ad hoc
- platforma/portal internetowy dla członków
- lista mailingowa
- warsztaty
- coroczny szczyt

Pozostałe działania

- stworzenie programu edukacyjnego w zakresie cyberbezpieczeństwa w branży motoryzacyjnej Automotive Cybersecurity Training (ACT)
- udział w opracowywaniu najlepszych praktyk, opisanych w dokumencie Amerykańskiego urzędu ds. bezpieczeństwa ruchu drogowego (NHTSA) „Najlepsze praktyki w zakresie cyberbezpieczeństwa dla bezpieczeństwa nowoczesnych pojazdów" (Cybersecurity Best Practices for the Safety of Modern Vehicles) z września 2022 r.

Strona internetowa

https://automotiveisac.com/europe

https://www.linkedin.com/company/auto-isac/

@AutoISAC

* Część ogólnoświatowego Auto-ISAC, założonego w 2015 roku, z siedzibą w Waszyngtonie, w Stanach Zjednoczonych.

Aviation ISAC

Pełna nazwa

Aviation Information Sharing and Analysis Center

Data założenia

2014

Siedziba

Annapolis, Stany Zjednoczone*

Liczba członków

122**

Sektor działalności

transport lotniczy

Forma organizacyjna

organizacja non-profit

Rodzaje podmiotów członkowskich

- przedsiębiorstwa prywatne
- przedsiębiorstwa z udziałem państwa

Kryteria członkostwa

- aktywność w określonym sektorze

Główne działania

- przygotowywanie raportów/analiz – raz w miesiącu lub częściej
- działania w grupach roboczych – raz w miesiącu lub częściej
- organizowanie konferencji – raz na kwartał

Metody komunikacji

- regularne spotkania – raz w miesiącu lub częściej
- platforma/portal internetowy dla członków
- lista mailingowa

Pozostałe działania

- organizacja spotkań na poziomie regionalnym i globalnym
- organizacja Tabletop Exercises (TTX)
- organizacja zawodów typu „zdobądź flagę" (Capture the Flag, CTF)
- przygotowywanie codziennych, cotygodniowych i comiesięcznych raportów i analiz

Strona internetowa

https://www.a-isac.com/

* Siedziba globalnego ISAC-a

** Liczba członków globalnego ISAC-a.

ECCSA

Pełna nazwa

European Centre for Cybersecurity in Aviation

Data założenia

2017

Siedziba

–

Liczba członków

42

Sektor działalności

cywilny transport lotniczy

Forma organizacyjna

nieformalne zgromadzenie

Rodzaje podmiotów członkowskich

- przedsiębiorstwa prywatne
- organy administracji państwowej
- organizacje pozarządowe

Kryteria członkostwa

- aktywność w określonym sektorze
- określona forma organizacji
- przestrzeganie Karty Członkostwa ECCSA

Główne działania

- przygotowywanie raportów/analiz – raz w miesiącu lub częściej
- działania w grupach roboczych – raz na pół roku
- spotkania integracyjne – raz na pół rokuraz w miesiącu lub częściej

Metody komunikacji

- spotkania ad hoc
- lista mailingowa

Pozostałe działania

- wsparcie dla ujawniania podatności
- wydawanie alertów ECCSA
- wydawanie miesięcznego raportu o zagrożeniach ECSSA
- wydawania ostrzeżeń o zagrożeniach technicznych ECCSA

Strona internetowa

https://www.easa.europa.eu/en/eccsa

EE-ISAC

Pełna nazwa

European Energy Information Sharing and Analysis Center

Data założenia

2015

Siedziba

Bruksela, Belgia

Liczba członków

35

Sektor działalności

energetyka

Forma organizacyjna

organizacja non-profit

Rodzaje podmiotów członkowskich

- przedsiębiorstwa prywatne
- przedsiębiorstwa z udziałem państwa
- organizacje pozarządowe
- instytucje akademickie
- ośrodki badawcze

Kryteria członkostwa

- aktywność w określonym sektorze
- określona forma organizacji

Główne działania

- przygotowywanie raportów/analiz – raz na kwartał
- działania w grupach roboczych – raz w miesiącu lub częściej
- reprezentowanie interesów sektora wobec władz publicznych

Metody komunikacji

- platforma/portal internetowy dla członków
- lista mailingowa

Pozostałe działania

- opracowanie EE-ISAC MISP – wersji platformy dedykowanej dla członków EE-ISAC
- organizacja corocznej konferencji dla sektora energetyki na temat cyberbezpieczeństwa sieci energetycznych (*Conference on Power Grids Cybersecurity*) we współpracy z ENISA, EU DSO, E.DSO i ENCS
- zawarcie trójstronnego porozumienia z amerykańskim E-ISAC i JE-ISAC w celu promowania międzynarodowej współpracy i wymiany informacji poprzez partnerstwo publiczno-prywatne

Strona internetowa

https://www.ee-isac.eu/

FI-ISAC

Pełna nazwa

European Financial Institutes – Information Sharing and Analysis Center

Data założenia

2008

Siedziba

–

Liczba członków

30

Sektor działalności

sektor finansowy

Forma organizacyjna

nieformalne zrzeszenie

Rodzaje podmiotów członkowskich

- przedsiębiorstwa prywatne
- CERT-y i ich organy przedstawicielskie
- organy ścigania

Kryteria członkostwa

- aktywność w określonym sektorze

Główne działania

- spotkania integracyjne – raz na pół roku
- reprezentowanie interesów sektora wobec władz publicznych

Metody komunikacji

–

Pozostałe działania

–

Strona internetowa

https://fi-isac.eu

ETIS

Pełna nazwa

ETIS – European Telco Information Sharing and Analysis Center

Data założenia

1991

Siedziba

Bruksela, Belgia

Liczba członków

47

Sektor działalności

telekomunikacja

Forma organizacyjna

organizacja non-profit

Rodzaje podmiotów członkowskich

- przedsiębiorstwa prywatne
- przedsiębiorstwa z udziałem państwa
- ośrodki badawcze

Kryteria członkostwa

- aktywność w określonym sektorze
- określona forma organizacji

Główne działania

- wspólne ćwiczenia i symulacje – raz na pół roku
- działania w grupach roboczych – raz w miesiącu lub częściej
- organizowanie konferencji – raz na kwartał

Metody komunikacji

- regularne spotkania – raz w miesiącu lub częściej
- spotkania ad hoc
- lista mailingowa
- platforma/portal internetowy dla członków

Pozostałe działania

- uczestnictwo w opracowywaniu raportu Telco IT Benchmarking (TeBIT) oraz krajobrazu bezpieczeństwa telekomunikacyjnego
- łączenie ekspertów ds. bezpieczeństwa operatorów telekomunikacyjnych z organizacjami, które opracowują coroczne wskaźniki (benchmarki) w zakresie bezpieczeństwa telekomunikacyjnego
- organizacja corocznego Telco Security Landscape we współpracy z TNO

Strona internetowa

www.etis.org

kalendarz wydarzeń ETIS: https://www.etis.org/events

EU City ISAC

Pełna nazwa

EU City Information Sharing and Analysis Center

Data założenia

2021

Siedziba

Brema, Niemcy

Liczba członków

37

Sektor działalności

administracja publiczna miast i regionów

Forma organizacyjna

nieformalnie zrzeszenie

Rodzaje podmiotów członkowskich

organy administracji państwowej

Kryteria członkostwa

- aktywność w określonym sektorze
- określona forma organizacji

Główne działania

- wspólne ćwiczenia i symulacje – raz na pół roku
- działania w grupach roboczych – raz w miesiącu lub częściej
- spotkania integracyjne – raz w miesiącu lub częściej

Metody komunikacji

- regularne spotkania – raz w miesiącu lub częściej
- spotkania ad hoc
- lista mailingowa

Pozostałe działania

- przeprowadzanie ćwiczeń w formie symulacji wspólnej obrony przed zagrożeniami, podobnych do „Locked Shields", organizowanych przez NATO

Strona internetowa

https://isac4cities.eu/

4.

Podsumowanie

Niniejszy raport stanowi próbę spojrzenia na europejskie ISAC-i z lotu ptaka. Taka perspektywa pozwoliła na zarysowanie krajobrazu tych organizacji i zebranie podstawowych danych na temat ich charakterystyki. Wyłonił się z nich obraz różnorodnych podmiotów, z których każdy posiada swoją unikalną specyfikę, choć jednocześnie, istnieją pewne obszary wspólne.

Przyjęta metoda badawcza posiada oczywiście pewne ograniczenia. Zbieranie informacji za pośrednictwem kwestionariusza nie pozwoliło na dodatkowe dopytanie respondentów o interesujące wątki poruszone w ich odpowiedziach. Dominujący w ankiecie typ pytań zamkniętych również mógł ograniczyć ilość informacji przekazanych przez organizacje. W pierwszej kolejności zależało nam jednak na zebraniu uporządkowanych danych na temat badanych organizacji, które umożliwiają ich analizę pod kątem ilościowym. Z tego względu, metoda kwestionariuszowa została wybrana jako najlepiej spełniająca ten cel.

Obraz europejskich ISAC-ów przedstawiony w raporcie nie zawiera więc szczegółowego wglądu w ich strukturę i wewnętrzne funkcjonowanie, a raczej mapuje pewne obszary w tym zakresie. Autorki mają nadzieję, że to badanie będzie stanowić dobry punkt wyjścia do dalszych, pogłębionych analiz wybranych aspektów działania organizacji tego typu. Bez wątpienia, dalsze wysiłki badawcze mogą przynieść jeszcze wiele ciekawych wniosków, które mogą okazać się przydatne zarówno z punktu widzenia samych ISAC-ów, jak i podmiotów, które chciałyby je wspierać.

Temat szans i ryzyk dla rozwoju ISAC-ów z pewnością nie straci w najbliższym czasie na aktualności. Krajobraz wyzwań w obszarze cyberbezpieczeństwa podlega bowiem ciągłej zmianie. Z jednej strony, na skutek czynników takich jak rozwój technologii czy zmiany w sytuacji geopolitycznej, pojawiają się nowe typy zagrożeń w cyberprzestrzeni. Z drugiej strony, wyzwaniem są także zmiany prawne, które nakładają nowe obowiązki na kolejne grupy podmiotów. Przemianom tym towarzyszą także nowe oczekiwania społeczne w zakresie bezpieczeństwa, które organizacje muszą uwzględniać. To wszystko sprawia, że rośnie znaczenie platform takich jak ISAC-i, które służą wzajemnemu wspieraniu się podmiotów w sprostaniu tym wyzwaniom.

Zapewnienie takim inicjatywom odpowiednich warunków do rozwoju powinno być traktowane jako ważny element strategii dla cyberbezpieczeństwa na poziomie krajowym oraz unijnym. W tym celu niezbędne jest budowanie świadomości na temat znaczenia ISAC-ów dla wzmacniania powszechnej odporności na zagrożenia.

Bibliografia

1. *Decision Directive/NSC-63 – Critical Infrastructure Protection* z dn, 22 maja 1998, Critical Infrastructure Protection (PDD 63) (fas.org) [dostęp: 15.04.2024].

2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

3. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.

4. EE-ISAC, *Japanese & European energy communities sign partnership agreement on cyber security*, 17.05.2017 r. Japanese & European energy communities sign partnership agreement on cyber security – EE-ISAC – European Energy – Information Sharing & Analysis Centre.

5. Empowering EU-ISACs, https://www.isacs.eu/ [dostęp: 15.04.2024].

6. European Union Agency for Cybersecurity (ENISA), „ISAC in a Box", ISAC in a Box – ENISA (europa.eu) [dostęp: 15.04.2024].

7. European Union Agency for Cybersecurity (ENISA), Cross-Sectors Exercise Requirements, 2018, https://www.enisa.europa.eu/publications/cross-sector-exercise-requirements, [dostęp: 15.04.2024].

8. European Cyber Crime Centre, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, [dostęp: 15.04.2024].

9. EUROPOL, FS-ISAC and Europol Partner to Combat Cross-Border Cybercrime, 19.09.2019 r., https://www.europol.europa.eu/media-press/newsroom/news/fs-isac-and-europol-partner-to-combat-cross-border-cybercrime, [dostęp: 15.04.2024].

10. European Automobile Manufacturers' Association (ACEA), European manufacturers and suppliers join with Auto-ISAC, 12.10.2022 r., European manufacturers and suppliers join with Auto-ISAC – ACEA – European Automobile Manufacturers' Association, [dostęp: 15.04.2024].

11. EUROCONTROL, *EUROCONTROL and A-ISAC strengthen their relationship regarding air traffic management and aviation cybersecurity*, 2.10.2019 r., EUROCONTROL and A-ISAC strengthen their relationship regarding air traffic management and aviation cybersecurity | EUROCONTROL, [dostęp: 15.04.2024].

12. European Union Agency for Cybersecurity (ENISA), *Information Sharing and Analysis Center, Cooperative models*, 2018, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs--cooperative-models [dostęp: 15.04.2024].

13. National Council of ISACs (NCI), National Council of ISACs | About NCI (nationalisacs.org) National Council of ISACs | About NCI (nationalisacs.org), [dostęp: 15.04.2024].

14. Goodwin C., Nicholas J. P., *A framework for cybersecurity information sharing and risk reduction*, „Journal of Cybersecurity Research" 2020, nr 15(3).

15. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.U.UE.L.2016.119.1 z dnia 04.05.2016.

16. Sadowski J., Ochrona Infrastruktury Krytycznej. Uregulowania prawne, „Zeszyty Naukowe. Organizacja i Zarządzanie" 2018, nr 6.

Aneks 1

Ankieta w języku angielskim

(wersja wypełniona przez uczestników badania)

On behalf of the Polish National Research Institute NASK, we thank you for your interest in participating in our survey. The collected data will serve to conduct research on the landscape of ISACs functioning in Europe. The results will be published in the form of a report in English and Polish. An additional aim of the report will be to promote the activities of the ISACs participating in the survey. Hence, we encourage you to answer all questions, including the open ones so that the work of your ISAC could be comprehensively presented in the publication. Thank you for your time! Cybersecurity Strategy and Development Department at NASK.

INFORMATIONAL DATA ON ISAC

1. Full name of the ISAC: .....

2. Founding date of the ISAC: .....

3. Headquarters of the ISAC (if applicable): .....

4. Current number of the ISAC members: .....

5. Sector(s) to which the ISAC members belong: .....

6. The ISAC's website/social media: .....

7. Role in the ISAC of a person filling in the survey: .....

I. ORGANISATION AND MEMBERSHIP OF ISAC

1. What is the organisational form of your ISAC (for ex. a non-profit organisation, an agency, an informal gathering)?

.....

2. What types of entities are members of your ISAC? (please indicate all matching answers)

- **a.** state administrative bodies
- **b.** state-owned companies
- **c.** private companies
- **d.** academic institutions
- **e.** research centres
- **f.** non-governmental organisations
- **g.** other (please specify): .....

3. What elements of the organisational structure does the ISAC have? (please indicate all matching answers)

- **a.** chair (alternatively vice-chair)
- **b.** management board/steering committee
- **c.** secretariat
- **d.** employees
- **e.** other (please specify): .....

4. How the ISAC's activities are funded? (please indicate all matching answers)

- **a.** fixed, mandatory membership fee
- **b.** voluntary membership contributions
- **c.** state funding
- **d.** other (please specify): .....

5. What criteria must be met to become a member of your ISAC? (please indicate all matching answers)

- **a.** activity in a specific sector
- **b.** the form of organisation specified by the ISAC
- **c.** the size of the organisation specified by the ISAC
- **d.** other (please specify): .....

II. ACTIVITY

6. What are the objectives pursued by your ISAC?
(please choose up to 3 answers that suits best to the ISAC's focus areas)

- **a.** information exchange and risk analysis
- **b.** incident response coordination
- **c.** provision of technical support and advice
- **d.** training and education on cybersecurity
- **e.** promotion of best practices in the area of cybersecurity
- **f.** other (please specify): .....

7. What activities are undertaken within the ISAC?
(please choose up to 3 answers that suits best to the ISAC's focus areas)

- **a.** organising conferences (if selected, then question 7a)
- **b.** joint exercises and simulations (if selected, then question 7b)
- **c.** preparing reports/analyses (if selected, then question 7c)
- **d.** representing the interests of the sector towards public authorities
- **e.** integration meetings (if selected, then question 7e)
- **f.** activities in working groups (if selected, then question 7f)
- **g.** other (please specify): .....

7a. How often does the ISAC organise conferences?

- **a.** once a month or more often
- **b.** once a quarter
- **c.** once in six months
- **d.** once a year
- **e.** less than once a year

7b. How often does the ISAC organise joint exercises and simulations?

- **a.** once a month or more often
- **b.** once a quarter
- **c.** once in six months
- **d.** once a year
- **e.** less than once a year

7c. How often does the ISAC prepare reports/analyses?

- **a.** once a month or more often
- **b.** once a quarter
- **c.** once in six months
- **d.** once a year
- **e.** less than once a year

7d. How often does the ISAC organise integration meetings?

- **a.** once a month or more often
- **b.** once a quarter
- **c.** once in six months
- **d.** once a year
- **e.** less than once a year

7e. How often does the ISAC conduct activities in working groups?

- **a.** once a month or more often
- **b.** once a quarter
- **c.** once in six months
- **d.** once a year
- **e.** less than once a year

8. What are the methods of communication and information exchange within your ISAC? (please indicate all matching answers)

- **a.** regular meetings (if selected, then question 8a)
- **b.** ad-hoc meetings
- **c.** an online platform or portal for members
- **d.** mailing list
- **e.** other (please specify): .....

8a. How often does the ISAC organise regular meetings?

- **a.** once a month or more often
- **b.** once a quarter
- **c.** once in six months
- **d.** once a year
- **e.** less than once a year

9. How does your ISAC promote its activities internationally? (please choose up to 3 answers that suits best to the ISAC's focus areas)

- **a.** social media channels
- **b.** speaking at conferences
- **c.** participation in consultations on national and international level
- **d.** running educational campaigns
- **e.** writing for the trade press
- **f.** other (please specify): .....

10. What challenges do you see for the ISAC's activities (please choose up to 3 answers that you find most relevant to your ISAC's experience)

- **a.** inactivity of members
- **b.** difficulties in building trust between members
- **c.** difficulties in maintaining regularity in ISAC activities
- **d.** competition between members
- **e.** lack of available resources and funding
- **f.** lack of sufficient regulation at national level
- **g.** other (please specify): .....

11. Does the ISAC have any initiatives that you would particularly like to share? Please provide their names and brief descriptions (3–4 sentences).

.....

12. Does the ISAC cooperate with other organisations, including European or national ISACs?

- **a.** Yes (if selected, then question 12a)
- **b.** No

12a. Please list the organisations the ISAC cooperates with and give a brief description of the cooperation.

.....

Thank you for filling in the survey!

Aneks 2

Ankieta w języku polskim

(tłumaczenie oryginalnej wersji angielskiej)

W imieniu Państwowego Instytutu Badawczego NASK dziękujemy za zainteresowanie udziałem w naszym badaniu. Zebrane dane posłużą do przeprowadzenia badań na temat krajobrazu ISAC-ów działających w Europie. Wyniki zostaną opublikowane w formie raportu w języku polskim i angielskim. Dodatkowym celem raportu będzie promocja działalności ISAC-ów biorących udział w badaniu. Zachęcamy zatem do udzielenia odpowiedzi na wszystkie pytania, również te otwarte, aby działalność Państwa ISAC-a mogła zostać kompleksowo zaprezentowana w publikacji. Dziękujemy za poświęcony czas! Dział Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni NASK.

PODSTAWOWE INFORMACJE O ISAC-U

1. Pełna nazwa ISAC-a: .....

2. Data założenia ISAC-a: .....

3. Siedziba (jeśli dotyczy):.....

4. Aktualna liczba członków ISAC-a: .....

5. Sektor/sektory, do których należą członkowie ISAC-a: .....

6. Strona internetowa/kanały w mediach społecznościowych: .....

7. Funkcja w ISAC-u pełniona przez osobę wypełniającą ankietę: .....

I. ORGANIZACJA I CZŁONKOSTWO W ISAC-u

1. Jaka formę organizacyjna ma ISAC? (np. organizacja non-profit, agencja, nieformalne zgromadzenie)?

.....

2. Jakie rodzaje podmiotów są członkami ISAC-a?
(proszę zaznaczyć wszystkie pasujące odpowiedzi)

- **a.** organy administracji państwowej
- **b.** przedsiębiorstwa z udziałem państwa
- **c.** przedsiębiorstwa prywatne
- **d.** instytucje akademickie
- **e.** ośrodki badawcze
- **f.** organizacje pozarządowe
- **g.** inne (proszę podać): .....

3. Jakie elementy struktury organizacyjnej posiada ISAC?
(proszę zaznaczyć wszystkie pasujące odpowiedzi)

- **a.** przewodniczący (ewentualnie wiceprzewodniczący)
- **b.** zarząd/komitet sterujący
- **c.** sekretariat
- **d.** pracownicy
- **e.** inne (proszę podać): .....

4. W jaki sposób finansowana jest działalność ISAC-a?
(proszę zaznaczyć wszystkie pasujące odpowiedzi)

- **a.** stała, obowiązkowa opłata członkowska
- **b.** dobrowolne wpłaty członków ISAC
- **c.** finansowanie przez państwo
- **d.** inne (proszę podać): .....

5. Jakie warunki należy spełnić, aby zostać członkiem ISAC-a?

- **a.** działalność w określonym sektorze
- **b.** forma organizacji określona przez ISAC-a
- **c.** wielkość organizacji określona przez ISAC-a
- **d.** inne (należy określić): .....

II. DZIAŁALNOŚĆ ISAC

6. Jakie cele są realizowane przez ISAC-a?
(proszę zaznaczyć 3 najbardziej pasujące odpowiedzi)

- **a.** wymiana informacji i analiza zagrożeń
- **b.** koordynacja działań w przypadku incydentów
- **c.** zapewnienie wsparcia technicznego i doradztwa
- **d.** szkolenia i edukacja w zakresie cyberbezpieczeństwa
- **e.** promowanie najlepszych praktyk w dziedzinie cyberbezpieczeństwa
- **f.** inne (proszę podać): .....

7. Jakie działania prowadzone są w ramach ISAC-a?
(proszę zaznaczyć 3 najbardziej pasujące odpowiedzi)

- **a.** organizacja konferencji (jeśli wybrano, to pytanie 7a)
- **b.** wspólne ćwiczenia i symulacje (jeśli wybrano, to pytanie 7b)
- **c.** przygotowywanie raportów/analiz (jeśli wybrano, to pytanie 7c)
- **d.** reprezentowanie interesów sektora przed organami państwowymi
- **e.** spotkania integracyjne (jeśli wybrano, to pytanie 7e)
- **f.** praca w grupach roboczych (jeśli wybrano, to pytanie 7f)
- **g.** inne (należy określić): .....

7a. Jak często ISAC organizuje konferencje?

- **a.** raz w miesiącu lub częściej
- **b.** raz na kwartał
- **c.** raz na sześć miesięcy
- **d.** raz w roku
- **e.** rzadziej niż raz w roku

7b. Jak często ISAC organizuje wspólne ćwiczenia i symulacje?

- **a.** raz w miesiącu lub częściej
- **b.** raz na kwartał
- **c.** raz na sześć miesięcy
- **d.** raz w roku
- **e.** rzadziej niż raz w roku

7c. Jak często ISAC przygotowuje raporty/analizy?

- **a.** raz w miesiącu lub częściej
- **b.** raz na kwartał
- **c.** raz na sześć miesięcy
- **d.** raz w roku
- **e.** rzadziej niż raz w roku

7e. Jak często ISAC organizuje spotkania integracyjne?

- **a.** raz w miesiącu lub częściej
- **b.** raz na kwartał
- **c.** raz na sześć miesięcy
- **d.** raz w roku
- **e.** rzadziej niż raz w roku

7f. Jak często ISAC prowadzi prace w grupach roboczych?

- **a.** raz w miesiącu lub częściej
- **b.** raz na kwartał
- **c.** raz na sześć miesięcy
- **d.** raz w roku
- **e.** rzadziej niż raz w roku

8. Jakie są metody komunikacji i wymiany informacji w ramach ISAC-a? (proszę zaznaczyć wszystkie pasujące odpowiedzi)

- **a.** regularne spotkania (jeśli wybrano, to pytanie 8a)
- **b.** spotkania ad-hoc
- **c.** platforma internetowa lub portal dla członków
- **d.** lista mailingowa
- **e.** nne (należy określić):.....

8a. Jak często ISAC organizuje regularne spotkania?

- **a.** raz w miesiącu lub częściej
- **b.** raz na kwartał
- **c.** raz na sześć miesięcy
- **d.** raz w roku
- **e.** rzadziej niż raz w roku

9. W jaki sposób ISAC promuje swoją działalność?
(proszę zaznaczyć 3 najbardziej pasujące odpowiedzi)

- **a.** kanały w mediach społecznościowych
- **b.** wystąpienia przedstawicieli na konferencjach
- **c.** udział w konsultacjach na poziomie krajowym i unijnym
- **d.** prowadzenie kampanii edukacyjnych
- **e.** przygotowywanie artykułów do prasy branżowej
- **f.** inne (proszę podać): .....

10. Jakie wyzwania dostrzegają Państwo dla działalności ISAC-a?
(proszę zaznaczyć 3 najbardziej pasujące odpowiedzi)

- **a.** brak aktywności członków
- **b.** trudności w budowaniu zaufania między członkami
- **c.** trudność w utrzymaniu regularności w działaniu ISAC
- **d.** konkurencja między członkami
- **e.** brak dostępnych zasobów i finansowania
- **f.** brak dostatecznych uregulowań prawnych na poziomie krajowym
- **g.** inne (proszę podać): .....

11. Czy ISAC prowadzi jakieś inicjatywy, którymi w szczególności chcieliby się Państwo pochwalić? Prosilibyśmy o podanie ich nazw i krótkich opisów (3–4 zdania).

.....

.....

12. Czy ISAC współpracuje z innymi organizacjami, w tym z europejskimi lub krajowymi ISAC?

- **a.** Tak (jeśli wybrano, to pytanie 12a)
- **b.** Nie

12a. Prosimy o wymienienie organizacji, z którymi współpracuje ISAC i podanie krótkiego opisu te współpracy.

.....

.....

Podziękowania

Dziękujemy bardzo wszystkim ISAC-om, które zgodziły się na udział w badaniu. To dzięki ich zaangażowaniu mogła powstać ta publikacja. Szczególne podziękowania kierujemy również do naszego recenzenta, dr hab., prof. IK Marka Pawlika za cenne uwagi i wskazówki. Ogromnym wsparciem była dla nas także pomoc dr hab. prof. ucz. Aleksandry Gasztold i Katarzyny Nakoniecznej z Wydawnictwa NASK.

O NASK

NASK jest Państwowym Instytutem Badawczym, którego misją jest opracowywanie i wdrażanie rozwiązań służących rozwojowi sieci teleinformatycznych w Polsce oraz poprawie ich efektywności i bezpieczeństwa. Realizuje on projekty badawczo-rozwojowe oraz projekty mające na celu poprawę bezpieczeństwa polskiej cyberprzestrzeni cywilnej. Ważnym obszarem działalności Instytutu jest także edukacja użytkowników i promowanie idei społeczeństwa informacyjnego, przede wszystkim w celu ochrony dzieci i młodzieży przed zagrożeniami płynącymi z nowych technologii.

O Dziale Rozwoju Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni

Dział Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni monitoruje zmiany zachodzące w krajowych i międzynarodowych regulacjach dotyczących cyberbezpieczeństwa i nowych technologii. Prowadzi działania zmierzające do rozpoznawania trendów mających bezpośredni wpływ na ekosystem cyberbezpieczeństwa oraz identyfikuje strategiczne kierunki rozwoju tej dziedziny. Misją Działu Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni jest także doradztwo na poziomie strategicznym oraz wspieranie podmiotów krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa. Dział Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni rozwija serwis informacyjny cyberpolicy.nask.pl będący kompendium wiedzy i dobrych praktyk na temat strategicznych, regulacyjnych i organizacyjnych aspektów cyberbezpieczeństwa.

Dział Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni prowadzi również współpracę z ośrodkami akademickimi, sektorem publicznym i organizacjami międzynarodowymi.

NASK