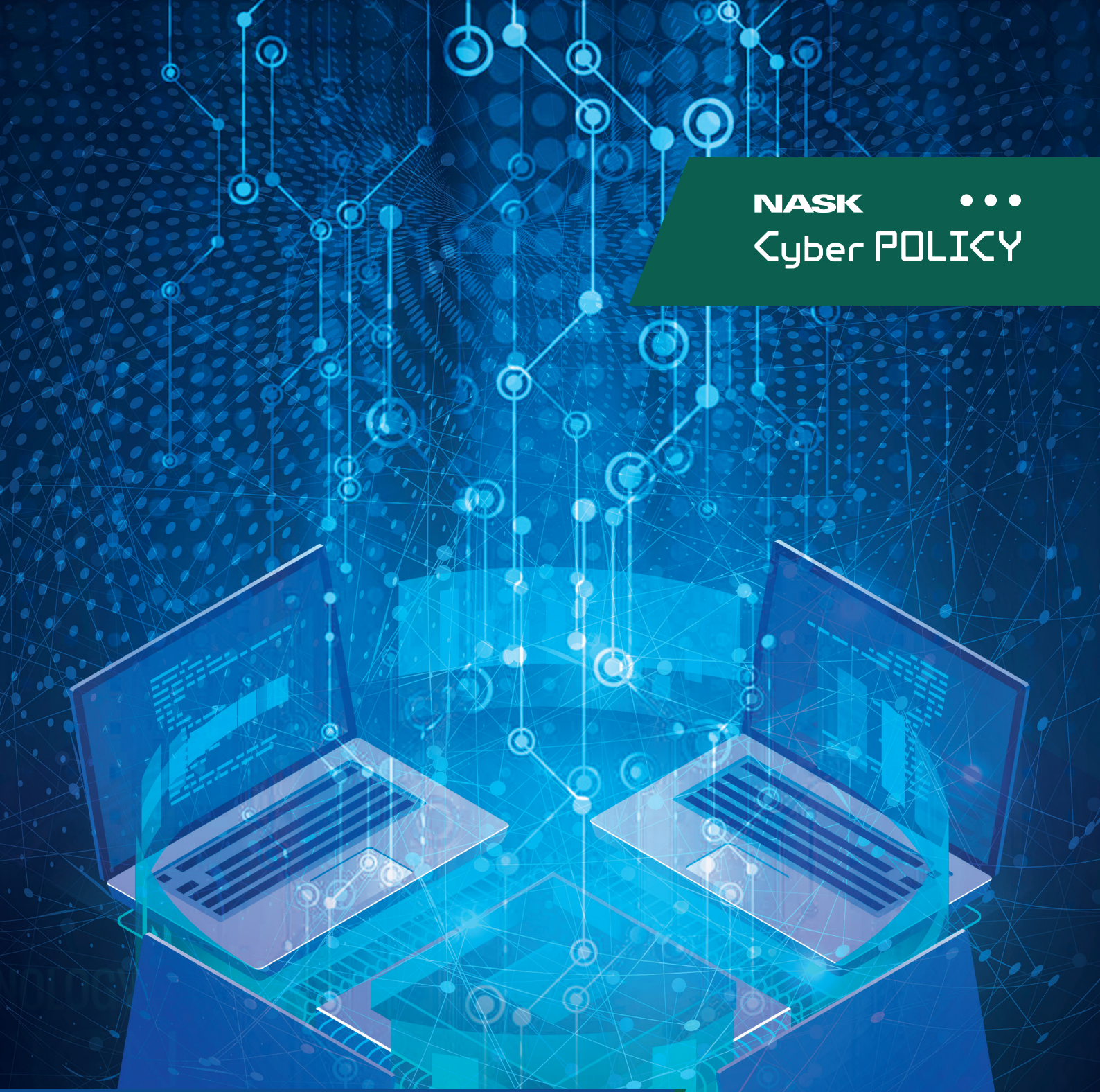
NASK

Cyber POLICY



ISAC

(Centra Wymiany i Analizy Informacji) w kontekście sektorowych centrów cyberbezpieczeństwa

Publikacja przygotowana we współpracy z Narodowym Centrum Cyberbezpieczeństwa w Holandii

NASK Cyber POLICY

SPIS TREŚCI

Ustawa o krajowym systemie cyberbezpieczeństwa umożliwia powołanie sektorowego zespołu cyberbezpieczeństwa. Ta struktura na ogół jest utożsamiana z sektorowym CSIRT. Tymczasem w sektorach mogą istnieć różne formy wspierające cyberbezpieczeństwo. Bardzo ciekawą i godną uwagi formułą jest sektorowy ISAC – Centrum Wymiany i Analizy Informacji.

Poniższa publikacja jest swego rodzaju poradnikiem na temat tego jak powołać ISAC.

Dedykowana jest przede wszystkim organom właściwym ds. cyberbezpieczeństwa i operatorom usług kluczowych.

Zapraszam do lektury!

Krzysztof Silicki, Zastępca Dyrektora NASK ds. Cyberbezpieczeństwa i Innowacji

NASK
Cyber POLICY

Czym jest ISAC?

ISAC to akronim angielskiego **Information Sharing and Analysis Center**, tłumaczony na język polski, jako **Centra Wymiany i Analizy Informacji**. To centra wymiany wiedzy i doświadczeń dotyczących incydentów cyberbezpieczeństwa w danym sektorze gospodarki (np. finansowym, energetyki czy lotnictwa).

ISAC jest formą partnerstwa publiczno-prywatnego (PPP) rozumianego, jako długookresowe porozumienie przynajmniej dwóch przedstawicieli sektora prywatnego lub publicznego[1]. Partnerstwo publiczno-prywatne jest często rozumiane, jako współpraca sektora prywatnego i publicznego, tymczasem chodzi także o budowanie relacji pomiędzy różnymi sektorami gospodarki oraz pomiędzy różnymi instytucjami publicznymi. PPP wydaje się być szczególnie istotne w zakresie cyberbezpieczeństwa, ponieważ operatorzy usług kluczowych to przede wszystkim prywatne przedsiębiorstwa[2]. Dodatkowo zagrożenia teleinformatyczne rzadko dotyczą tylko jednej instytucji, a nawet jednego sektora. Dlatego dobra współpraca i właściwa wymiana wiedzy może znacznie podnieść poziom cyberbezpieczeństwa. Nie tylko z uwagi na wymianę informacji o samych incydentach, czy też zagrożeniach, ale także możliwość uczenia się od siebie nawzajem. Z danych zebranych przez Europejską Agencję Bezpieczeństwa Sieci i Informacji (ENISA) wynika, że rozwinięcie systemu partnerstw publiczno-prywatnych w dziedzinie cyberbezpieczeństwa, a w szczególności powstanie ISAC, wyraźnie przyczyniło się do zwiększenia ogólnego poziomu wiedzy na temat zagrożeń w danym państwie, a także do wzrostu kompetencji poszczególnych firm i instytucji w przeciwdziałaniu zagrożeniom[3].

[1] Public Private Partnership (PPP). Coooperative models. Listopad 2017, ENISA, dostęp na dzień 31.01.2019; https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models

[2] Zgodnie z Ustawą o krajowym systemie cyberbezpieczeństwa operatorzy usług kluczowych to firmy i instytucje świadczące usługi o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej w sektorach: energetycznym, transportowym, bankowym i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną (wraz z dystrybucją) i infrastruktury cyfrowej. Usługa kluczowa jest zależna od systemów informatycznych.

[3] ISAC (Information Sharing and Analysis Center) - Centra Wymiany i Analizy Informacji; CyberPolicy; dostęp na dzień 4.01.2019 r; link: https://cyberpolicy.nask.pl/cp/dobre-praktyki/isac/69,ISAC-Information-Sharing-and-Analysis-Center-Centra-Wymiany-i-Analizy-Informacji.html

Krótka lekcja historii…

Pierwsze ISACs powstały w latach 90. po atakach terrorystycznych w Nowym Jorku i Oklahoma City[4], kiedy to prezydent Bill Clinton powołał Prezydencką Komisję do spraw Zabezpieczania Infrastruktury Krytycznej (ang. President's Commision on Critical Infrastructure Protection – PCCIP). Zadaniem Komisji było przygotowanie raportu rekomendującego działania zabezpieczające amerykańską infrastrukturę krytyczną w przyszłości. W raporcie, jako jedno z największych zagrożeń, komisja wskazała Internet i systemy teleinformatyczne. Eksperci zalecali przede wszystkim wzmocnienie współpracy pomiędzy agencjami rządowymi i operatorami infrastruktury krytycznej oraz dzielenie się informacjami na temat potencjalnych zagrożeń. Zalecenie to miało być realizowane właśnie poprzez powołanie ISAC.

Komisja podkreśliła także konieczność inwestowania w badania i rozwój nowoczesnych technologii. W odpowiedzi na rekomendacje Komisji stworzono pierwsze centra ISACs, a dwa lata później, zgodnie z prezydencką Dyrektywą 63, uchwalono obowiązek utworzenia ISAC w każdym z sektorów infrastruktury krytycznej. Organizacją zrzeszającą zespoły ISACs ze wszystkich sektorów jest Narodowa Rada ISAC (ang. National Council of ISACs). Do jej obowiązków należy wzmacnianie współpracy i wymiana informacji międzysektorowych[5]. Obecnie w Stanach Zjednoczonych działa ponad 20 organizacji ISAC.

W Europie pierwsze ISACs powstały w sektorze finansowym i energetycznym. Warto podkreślić, że organizacje europejskie mają odmienną specyfikę od ich amerykańskich odpowiedników. Powstały później, zostały zbudowane na innym gruncie kulturowym i są znacznie bardziej nakierowane na wsparcie rządowe, a nie tylko współpracę sektorową. Wynika to z głęboko zakorzenionego w kulturze europejskiej przekonania, że państwo powinno zapewniać bezpieczeństwo zarówno sektora publicznego, jak i prywatnego. Europejskie ISACs, w porównaniu do amerykańskich odpowiedników, są zdecydowanie bardziej sformalizowane, głównie za sprawą większego wpływu organów rządowych na ich funkcjonowanie. Koncentrują się przede wszystkim na budowaniu partnerstwa i zaufania. Zgodnie z nomenklaturą przyjętą przez Europejską Agencję Bezpieczeństwa Sieci i Informacji (ENISA), w Europie wyróżnia się 3 modele ISAC: krajowe, sektorowe i międzynarodowe. Każdy z tych modeli ma swoją charakterystykę i specyfikę. Obecnie w Europie działa ponad 20 ISACs, m.in. w Hiszpanii, Portugalii, Polsce, Holandii, Litwie, Węgrzech, Grecji, Irlandii, Francji, Estonii, Austrii, Belgii i Bułgarii[6].

[4] W 1993 r. pod północną wieżą World Trade Center eksplodowała ciężarówka, zabijając 6 osób i raniąc ponad 1000. Natomiast w 1995 r. terroryści zaatakowali budynek federalny w Oklahoma City. Był to największy atak terrorystyczny w USA do czasu zamachów z 11 września 2001.

[5] ISAC (Information Sharing and Analysis Center) - Centra Wymiany i Analizy Informacji; CyberPolicy; dostęp na dzień 4.01.2019r; link: https://cyberpolicy.nask.pl/cp/dobre-praktyki/isac/69,ISAC-Information-Sharing-and-Analysis-Center-Centra-Wymiany-i-Analizy-Informacji.html

[6] Information Sharing and Analysis Centres (ISACs) Cooperative models, Listopad 2018, ENISA; dostęp na dzień 7.01.2019; file:///C:/Users/justynab/Documents/ISAC/WP2017%20O-3-1-3%202%20Information%20Sharing%20and%20Analysis%20Center%20-ISACs-%20Cooperative%20models.pdf

ISAC a sektorowe zespoły cyberbezpieczeństwa

Ustawa o krajowym systemie cyberbezpieczeństwa wprowadza pojęcie **sektorowego zespołu cyberbezpieczeństwa**, który zgodnie z art. 44 może być powołany przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora wymienionego w załączniku do ustawy[7].

Sektorowy zespół cyberbezpieczeństwa:

- przyjmuje zgłoszenia o incydentach poważnych i pomaga w obsłudze tych incydentów,
- wspiera operatorów usług kluczowych w wykonywaniu obowiązków ustawowych,
- analizuje incydenty poważne[8], wyszukuje powiązania pomiędzy incydentami oraz opracowuje wnioski z obsługi incydentu,
- współpracuje z właściwym zespołem CSIRT poziomu krajowego w zakresie koordynowania obsługi incydentów poważnych,
- może przeprowadzić audyt operatorów usług kluczowych, jeśli audytorzy spełniają kryteria wskazane w ustawie,
- ma możliwość wymiany informacji o incydentach poważnych z innymi krajami UE[9].

[7] Ustawodawca wymienia 6 sektorów. Są to: energia, transport, bankowość i infrastruktura rynków finansowych, ochrona zdrowia, zaopatrzenie w wodę pitną i jej dystrybucja, infrastruktura cyfrowa.

[8] Incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej (Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. art. 2, ust. 7). Progi uznania danego incydentu za poważny zostały określone w Rozporządzeniu Rady Ministrów w sprawie progów uznania incydentu za poważny z dnia 31.10.2018 r.

[9] Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. art. 44, ust. 1,2,3,4.

Powołanie sektorowego zespołu cyberbezpieczeństwa może być cennym wsparciem zarówno dla operatorów usług kluczowych w danym sektorze, właściwego CSIRT, jak i organów właściwych.

Zalety sektorowych zespołów cyberbezpieczeństwa:

- Duże zrozumienie specyfiki danego sektora, potrzeb i wyzwań stojących przed operatorami usług kluczowych.
- Wiedza o możliwych ryzykach, występujących incydentach i sposobach ich skutecznej obsługi.
- Utworzenie platformy wymiany dobrych praktyk i budowania zdolności reagowania na zagrożenia w ramach sektora.
- Możliwość gromadzenia i pogłębiania wiedzy na temat sektora, nie tylko ze źródeł krajowych, ale również zagranicznych.
- Nawiązywanie współpracy międzynarodowej z analogicznymi podmiotami z danego sektora.
- Najlepsza forma monitoringu aktualnego stanu cyberbezpieczeństwa w danym sektorze.

W ogólnym dyskursie sektorowy zespół cyberbezpieczeństwa jest utożsamiany z sektorowym CERT lub CSIRT. Tymczasem w sektorach mogą istnieć różne formy wspierające cyberbezpieczeństwo. Bardzo ciekawą i godną uwagi formułą jest sektorowy ISAC.

ISAC stanowi bardzo dobrą formę gromadzenia wiedzy na temat aktualnych zagrożeń i ryzyka, głównie dlatego, że składa się ze specjalistów, którzy znają specyfikę sektora i mają najbardziej aktualne informacje na temat zagrożeń. Taki stan wiedzy może być trudny do osiągnięcia dla organów właściwych. Jednocześnie ISAC może być dobrą platformą współpracy i wymiany informacji dla operatorów usług kluczowych. W obliczu incydentu nie zawsze konieczny jest zespół typu CERT/CSIRT działający w systemie 24/365. Czasem wystarczy wiedzieć gdzie i do kogo w sektorze zadzwonić, żeby uzyskać potrzebne informacje i wsparcie – np. od organu właściwego lub innego przedsiębiorstwa z sektora. Takie działania, wraz ze wsparciem właściwego CSIRT poziomu krajowego, mogą okazać się wystarczające.

Wydawać by się mogło, że utworzenie centrum jest złożonym i kosztownym przedsięwzięciem. Nic bardziej mylnego! Wystarczy kilku specjalistów z zakresu cyberbezpieczeństwa, którzy zaczną wymieniać się informacjami oraz doświadczeniami. Warto też zaznaczyć, że każdy sektor ma odmienną specyfikę i dlatego każdy ISAC może być odmienny. Dla przykładu: funkcjonujące już w Europie ISAC w sektorze finansowym koncentrują się przede wszystkim na współpracy z organami ścigania w celu zwalczania cyberprzestępczości, podczas gdy te działające w sektorze energetyki koncentrują się przede wszystkim na aspektach badawczych i rozwojowych (R&D). Uruchomienie sektorowego ISAC powinno być poprzedzone analizą potrzeb i wyzwań stojących przed danym sektorem. Kolejne kroki zostały opisane w dalszej części publikacji.

Jakie korzyści stwarza uruchomienie ISAC?

Dla sektora publicznego:

Informacje na temat poziomu bezpieczeństwa w kluczowych sektorach gospodarki

Członkostwo w ISAC daje sektorowi publicznemu dostęp do wiedzy na temat poziomu cyberbezpieczeństwa w kluczowych sektorach gospodarki. Poprzez systematyczne interakcje z przedstawicielami sektora prywatnego, przedstawiciele sektora publicznego zyskują większą świadomość na temat zagrożeń i incydentów. Dzięki temu łatwiej tworzyć standardy sektorowe i regulacje prawne, które wspierają rzeczywiste działania oraz przyczyniają się do zwiększenia ogólnego poziomu bezpieczeństwa teleinformatycznego w danym sektorze gospodarki.

Lepsze zrozumienie potrzeb sektora prywatnego

Dzięki ścisłej współpracy z przemysłem, podmioty publiczne lepiej rozumieją sektor prywatny, co jest bardzo przydatne podczas tworzenia nowego prawodawstwa i sektorowej strategii cyberbezpieczeństwa.

Możliwość ustanowienia jednego punktu koordynacji

Członkostwo w ISAC umożliwia sektorowi publicznemu utworzenie jednego punktu koordynacji współpracy z sektorem prywatnym. Ułatwia to administracji realizację zadań organów właściwych[10] powierzonych w Ustawie o krajowym systemie cyberbezpieczeństwa.

[10] Organy właściwe ds. cyberbezpieczeństwa sprawują nadzór nad każdym z kluczowych sektorów gospodarki. 11 sektorów, wymienionych w Ustawie o krajowym systemie cyberbezpieczeństwa, podlega ministrom właściwym dla konkretnych działów administracji. Organy właściwe decydują, które podmioty z ich sektora otrzymają status operatora usługi kluczowej. Poza tym przygotowują rekomendacje działań, które wzmacniają cyberbezpieczeństwo sektora.

Dla sektora prywatnego:

Uczenie się od siebie nawzajem

Celem ISAC jest dzielenie się wiedzą oraz doświadczeniem, żeby zwiększyć odporność na cyberzagrożenia nie tylko w konkretnej organizacji, ale również w całym sektorze. Ucząc się na incydentach z różnych organizacji, można podjąć kroki, które zapobiegną podobnym zdarzeniom w innym miejscu pracy. Obowiązuje, więc zasada: „Ty będziesz uczył się od innych, a inni od Ciebie". Jest to szczególnie korzystne dla tych organizacji, które mają mniej rozwinięte kompetencje w zakresie cyberbezpieczeństwa.

Poprawa poziomu cyberbezpieczeństwa

Wymieniając się informacjami w sektorze, można znacznie szybciej pozyskiwać informacje o możliwych zagrożeniach. Większa świadomość zagrożeń może umożliwić wykrycie ataku, którego inaczej nikt by nie zauważył. Taka współpraca pomaga również lepiej szacować ryzyko i efekty planowanych działań. Dzięki temu wzrasta poziom bezpieczeństwa w całym sektorze, w myśl zasady, że system jest na tyle odporny na zagrożenia, na ile odporne jest jego najsłabsze ogniwo.

Zmniejszenie kosztów

W każdej organizacji zakłócenie procesów operacyjnych ma wymierne koszty finansowe. Wspólne podejście do problemów kosztuje znacznie mniej czasu i pieniędzy. Być może nie będzie trzeba samemu wymyślać rozwiązania, które ktoś opracował już wcześniej? ISAC umożliwia także wspólny zakup usług bezpieczeństwa, co stanowi realną oszczędność finansową.

Poprawa wizerunku

Uczestnictwo w ISAC jest jasnym sygnałem, pokazującym klientom oraz innym współpracującym organizacjom, że firma bardzo poważnie podchodzi do bezpieczeństwa informacji oraz ochrony swoich danych. Dzięki współpracy można również zapobiec incydentom, które mogłyby spowodować spadek reputacji organizacji.

Przewodzenie poprzez działanie

Działanie na rzecz poprawy cyberbezpieczeństwa często stanowi element polityki społecznej odpowiedzialności biznesu danej organizacji.

Co jest potrzebne, żeby ustanowić ISAC?[11]

Zaufanie

Zaufanie jest kluczem do współpracy. Konieczna jest pewność, że informacje, którymi dzielą się uczestnicy, nie ukażą się w jutrzejszych gazetach ani nie zostaną przekazane dalej bez ich zgody. Dlatego dobrym wyjściem będzie stworzenie wytycznych członkostwa, które określą, z kim i w jaki sposób można dzielić się informacjami. W późniejszym okresie warto wykorzystać reguły Traffic Light Protocol (TLP)[12].

Budowaniu zaufania służy również wyznaczenie stałych reprezentantów. Ponieważ ISAC funkcjonuje w oparciu o systematyczne interakcje (m.in. spotkania) warto, aby przy stole wciąż zasiadali ci sami ludzie. Warto inwestować w relacje, być odpowiedzialnym, dotrzymywać słowa i dawać dobry przykład.

Wspólne interesy

Od początku należy być szczerym i jasno komunikować swoje motywacje. Tylko takie podejście pozwoli odkryć, jakie wspólne interesy mają uczestnicy oraz ich organizacje, a także ustalić priorytety dla działania ISAC. Nie można zapominać, że na bezpieczeństwo sektora składa się suma bezpieczeństwa należących do niego organizacji.

Organizacje tworzące ISAC mogą mieć różne interesy, o ile zostały one przedyskutowane i nie leżą w sprzeczności do siebie. Każdy konflikt interesów szybko zakończy owocną pracę ISAC, bo spowoduje utratę zaufania jego członków.

Równość

Udana współpraca wymaga tego, aby uczestnicy ISAC byli sobie równi. Nie powinno się tworzyć hierarchicznych relacji. Jeśli organizacje są podległe jedna drugiej poza ISAC, zapewne nie będą przygotowane na to, aby dzielić się informacjami wewnątrz grupy. Trudno dzielić się wiedzą, która w przyszłości może zostać wykorzystana przeciw Tobie.

[11] Starting an ISAC: Sectoral collaboration. Guide, National Cyber Security Centtre of the Netherlands, https://www.ncsc.nl/english/cooperation/_collaboration/sectoral-cooperation-isac.html, s. 3-4

[12] Traffic Light Protocol jest to zestaw reguł, pogrupowanych w 4 kategorie, używanych w celu lepszego zdefiniowania grupy odbiorców wrażliwych informacji. Dla ułatwienia kategorie opisywane są czterema kolorami (czerwony, pomarańczowy, zielony oraz biały). Zakwalifikowanie do odpowiedniej kategorii leży po stronie organizacji, z której pochodzą informacje. Jeśli odbiorca chciałby podzielić się uzyskanymi informacjami z szerszym gronem, musi uzyskać odpowiednią akceptację od autora wiadomości.

Jak uruchomić ISAC?[13]

Proces uruchamiania ISAC składa się z trzech faz: poszukiwania, budowania i kontynuacji.

Faza 1 – Poszukiwanie

Najważniejsze jest znalezienie osób, które myślą podobnie. Początki nie muszą być spektakularne. Czasem najlepiej jest zacząć od kilku entuzjastycznie nastawionych oficerów bezpieczeństwa informacji. Pozwoli to stworzyć nieformalną grupę współpracy i wzajemnie się poznać. Warto też na samym początku zastanowić się nad wspólnymi celami, zmapować podobieństwa i różnice.

Faza 2 – Budowanie

Ważnym elementem jest organizacja oficjalnego otwarcia ISAC. Wspólny wybór przewodniczącego, wiceprzewodniczącego oraz sekretarza. Da im to jasną legitymizację do dalszych działań. Dodatkowo niezwykle istotne jest uzgodnienie częstotliwości spotkań i sposobu komunikacji, a także wytycznych dotyczących członkowstwa i przekazywania informacji. Warto od razu spisać to w formie MoU (memorandum of understanding), bo dzięki temu wszystkie zasady będą jasne i dostępne dla wszystkich członków (zarówno obecnych, jak i przyszłych).

Faza 3 – Kontynuacja

Warto być krytycznym, jeśli chodzi o uczestnictwo w ISAC, stworzyć przestrzeń do oceny i podsumowania swoich działań. ISAC jest pewnego rodzaju „żywym organizmem", który powinien ewoluować wraz ze zmianą potrzeb jego członków. Ważne tylko, aby te zmiany odbywały się w sposób transparentny, za zgodą wszystkich członków.

[13] Starting an ISAC: Sectoral collaboration. Guide, National Cyber Security Centtre of the Netherlands, https://www.ncsc.nl/english/cooperation/_collaboration/sectoral-cooperation-isac.html, s. 6-10

Faza 1 – Poszukiwanie

Warto znaleźć w sektorze osoby, które myślą podobnie, są skłonne do współpracy i szukają rozwiązań, aby podnieść poziom cyberbezpieczeństwa w swoich organizacjach. Początki nie muszą być spektakularne, wystarczy, że chęć współpracy wyrażą przedstawiciele trzech do pięciu firm. Mała grupa ułatwi budowę zaufania oraz określenie tego, jak powinna wyglądać współpraca. Doświadczenie pokazuje, że w ISAC może być maksymalnie dwadzieścia pięć organizacji. Większa grupa znacznie utrudnia umawianie spotkań, a uczestnicy są mniej chętni, aby dzielić się informacjami.

Dobrym momentem uruchomienia ISAC może być incydent we własnej organizacji lub inny poważny incydent, który spowodował zainteresowanie mediów. Punktem startu mogą być też regularne spotkania z kolegami z sektora. Takie spotkania i tak mają miejsce przy okazji różnych okoliczności (np. konferencje czy szkolenia), więc decyzja o założeniu ISAC może być naturalnym, kolejnym krokiem.

Gdy już znajdzie się grupa osób o podobnych interesach z różnych organizacji, która będzie miała przekonanie o konieczności rozpoczęcia współpracy, w pierwszej kolejności warto zorganizować nieformalną grupę roboczą. Niezwykle ważna jest tu uczciwość oraz wypracowywanie porozumienia. Poniżej przedstawiamy listę pytań, na które warto sobie odpowiedzieć w momencie rozpoczęcia współpracy.

Pytania, które warto sobie zdać w pierwszej fazie formowania ISAC:

Kim jesteśmy i co mamy ze sobą wspólnego?

Być może pracujecie na takich samych systemach, mierzycie się z podobnymi wyzwaniami lub incydentami?

Jaki jest nasz wspólny cel?

Chcecie wymieniać się informacjami o zagrożeniach i incydentach? Ułatwić sobie współpracę w zakresie realizacji zadań i obowiązków ustawowych? A może ustanowić standardowe procedury operacyjne dla organizacji w danym sektorze lub dyskutować o nowych trendach?

Czy potrzebujemy jeszcze innych organizacji, aby osiągnąć nasz cel?

Używajcie nawzajem swojej wiedzy i kontaktów. Celem może być oczywiście włączenie do prac ISAC jak największej liczby organizacji, lecz ważne, aby wcześniej zapewnić solidny fundament.

Jakimi informacjami chcielibyśmy się dzielić?

Rozważcie różne poziomy informacji (operacyjny, taktyczny, strategiczny), ich typy (cyberbezpieczeństwo, prywatność, wyłudzenia) oraz ważne tematy (bezpieczeństwo chmury, zarządzanie ryzykiem, wiedza o cyberzagrożeniach). Wykorzystajcie te aspekty do ustalenia, kto w ramach danej organizacji powinien dołączyć do ISAC.

Czy jesteśmy właściwymi osobami do uczestnictwa w ISAC?

Być może w danej organizacji są inni pracownicy, którzy powinni uczestniczyć w ISAC? Warto tak dobierać osoby, które biorą udział w pracach grupy, aby każdy członek miał odpowiednią wiedzę, która umożliwi mu aktywne uczestnictwo.

Faza 2 – Budowanie

Organizacja oficjalnego rozpoczęcia działalności sektorowego ISAC.

Zapoznanie

Wprawdzie uczestnicy mogą się już znać, ale być może nie na tyle dobrze, aby w pełni sobie zaufać. Warto poświęcić czas, podczas wydarzenia rozpoczynającego działalność, aby lepiej się poznać. Można na przykład zorganizować sesję, podczas której wszyscy członkowie będą mieli okazję porozmawiać ze sobą nie tylko o służbowych, ale również prywatnych sprawach. Kolejną możliwością jest zorganizowanie wspólnego wyjścia na lunch lub obiad.

Ustanowienie ról

Wspólne wybranie przewodniczącego, wiceprzewodniczącego oraz sekretarza.

Przewodniczący nie tylko prowadzi spotkania, ale również jest siłą napędową stojącą za całym ISAC. Zachęca członków do dzielenia się informacjami oraz do aktywnej współpracy. Każda komunikacja na zewnątrz grupy, dotycząca działalności ISAC, to również jego odpowiedzialność. Warto, żeby była to osoba rozpoznawalna i ciesząca się autorytetem w środowisku.

Wiceprzewodniczący zastępuje przewodniczącego oraz bierze udział w przygotowaniu agendy spotkań. Razem z przewodniczącym jest również pierwszym punktem kontaktowym dla organizacji, które chciałyby dołączyć do grupy.

Sekretarz pełni niezwykle istotną rolę przed oraz po spotkaniach. Zapewnia, że uczestnicy przestrzegają uzgodnionych porozumień i procedur. Jego zadaniem jest również dopilnowanie, aby wszyscy zapoznali się z wytycznymi członkostwa. Dba także o organizację spotkań, wysyła zaproszenia, program oraz krótkie podsumowania.

Częstotliwość spotkań

Należy uzgodnić jak często warto się spotykać: raz na miesiąc, a może raz na kwartał? Najczęściej spotkania ISAC odbywają się od czterech do ośmiu razy w roku. Ważne jest również, aby ustalić miejsce oraz czas trwania spotkań. Dobrym pomysłem jest zaplanowanie dat na cały rok. Taki krok pozwoli uczestnikom zarezerwować czas oraz zapewni kontynuację dyskusji

nad podjętymi tematami. Spotkania mogą odbywać się rotacyjnie w siedzibach członków ISAC. Stworzy to możliwość lepszego zapoznania się z działalnością poszczególnych organizacji.

Komunikacja

Dobrym rozwiązaniem jest przygotowanie listy mailingowej. Ważne, aby była to bezpieczna komunikacja. Dobrze, kiedy jest szyfrowana. Dbanie o należytą poufność to absolutna konieczność, która przyczynia się do wzrostu zaufania pomiędzy członkami ISAC. Z czasem użyteczne może okazać się stworzenie bezpiecznej przestrzeni (np. forum lub repozytorium), gdzie będzie można dzielić się wiedzą.

Wytyczne członkostwa

Przygotowanie wytycznych wymaga dużo czasu i rozwagi, ponieważ to one formują podstawy ISAC. Dokument nie jest jednak aktem prawnym, z którego wywodzą się prawa i obowiązki członków, lecz nieformalnym porozumieniem.

Wytyczne zawierają kryteria przyjęcia nowych organizacji oraz ich przedstawicieli czy też zakres współpracy. Powinny znaleźć się w nich również tematy takie jak opracowywanie umów dotyczących przyjmowania nowych organizacji i ich przedstawicieli, a także sposób ewentualnej zmiany wytycznych. Ważne też, żeby dokument opisywał uzgodnione sposoby postępowania z informacjami, którymi członkowie dzielą się w ramach ISAC.

Faza 3 – Kontynuacja

Nie należy przestawać pracować nad budową zaufania.

Program

Przewodniczący, jego zastępca i sekretarz przygotowują program na następne spotkanie i rozsyłają go do uczestników z dwu lub trzytygodniowym wyprzedzeniem. Dobrym pomysłem jest zaproponowanie konkretnych tematów, zostawiając jednocześnie czas na bieżące zagadnienia oraz pytania. Program powinien być przedstawiony do wiadomości wszystkim członkom ISAC.

Plan roczny

Podczas pierwszego spotkania w danym roku, warto zastanowić się nad rocznym planem działania. Należy wybrać tematy do omówienia, a następnie przypisać im właścicieli, którzy zadbają, aby dane zagadnienie było regularnie poruszane. Można też zaplanować tematy z wyprzedzeniem, przypisując je do konkretnych dat spotkań. Ponownie obowiązuje zasada, że plan roczny powinien być znany i akceptowany przez wszystkich członków.

Raport roczny

W rocznym raporcie można opisać, z czym mierzył się ISAC, a także jaki miał wkład w budowę cyfrowej odporności poszczególnych organizacji oraz całego sektora. Taki raport może też pomóc wytłumaczyć potrzebę uczestnictwa w ISAC oraz wykazać korzyści z tego płynące.

Kwestie praktyczne

Warto pamiętać o kwestiach praktycznych. Zarezerwować miejsce spotkania, sprzęt do prezentacji, przygotować listę obecności, a w miarę możliwości zadbać również o napoje i przekąski. Można spotykać się w jednym miejscu lub organizować posiedzenia ISAC na zmianę. Wówczas uczestnik, który jest gospodarzem, może zaprezentować jak wygląda dany temat w jego organizacji.

Aktywne uczestnictwo

Sukces współpracy zależy od tego, jak aktywne będzie uczestnictwo w ISAC i jak dobrze członkowie będą przygotowani do spotkań. Warto aktywnie pozyskiwać informacje o zagrożeniach, incydentach czy wyciągniętych wnioskach, które mogą być wartościowe dla pozostałych uczestników.

„Red Round", czyli czerwona runda

Incydent w jednej organizacji może zapobiec podobnemu zdarzeniu w następnej. Wrażliwe informacje mogą być wymieniane w ramach TLP:RED w trakcie tzw. czerwonej rundy. Żadna z rzeczy, która zostanie powiedziana na takim spotkaniu, nie powinna być w żaden sposób komunikowana na zewnątrz. Uczestnicy nie robią żadnych notatek. Jeśli uznają za konieczne wykorzystanie informacji z „Red Round", muszą zawsze skonsultować to ze źródłem informacji.

Nowi członkowie

Gdy ISAC zacznie już działać, coraz więcej organizacji będzie chciało dołączyć do grupy. Wymaga to jednomyślnej zgody uczestników – zarówno, jeśli chodzi o zgodę na przyjęcie nowej organizacji, jak i jej wyznaczonego przedstawiciela. Jednomyślność jest konieczna, aby utrzymać poziom zaufania wewnątrz ISAC. Gdy jej zabraknie, członkowie mogą mniej chętnie dzielić się informacjami. Warto wyznaczyć procedurę przyjęcia w wytycznych członkostwa.

Znajome twarze

Znajome twarze przy stole budują zaufanie. Dlatego ważne jest, aby z jednej organizacji był wyznaczony jeden, maksymalnie dwóch przedstawicieli. Jeśli uczestnicy wyrażą zgodę na zastępstwo, powinni ustalić jak często dany reprezentant może uczestniczyć w spotkaniach, aby utrzymać zaufanie w grupie.

Wewnętrzne spojrzenie

W następstwie spotkań członkowie ISAC mogą przekazywać punkt widzenia swoich organizacji na dany temat. Dowiadując się, które procesy są istotne dla danej organizacji, można zrozumieć, dlaczego konkretne tematy są ważne dla uczestników.

Wyzwania[14]

Zaufanie

Poziom zaufania rośnie powoli i wymaga ciągłego podtrzymywania. Brak zaufania narazi całe przedsięwzięcie na niepowodzenie.

Zaangażowanie

Uczestnictwo w ISAC jest dobrowolne, co nie znaczy, że pozbawione zobowiązań. Ważne, aby wszyscy członkowie grupy zapewniali wartość dodaną. Każdy powinien krytycznie przyglądać się swojemu uczestnictwu i zaangażowaniu, biorąc pod uwagę wkład w pracę grupy oraz to, ile z nich wynosi.

Konkurencja

Współpraca w ramach ISAC może oznaczać, że organizacje będą wymieniać wrażliwe informacje ze swoimi konkurentami. Jeśli model biznesowy organizacji nie opiera się na zapewnieniu cyberbezpieczeństwa, dobrym pomysłem będzie ustalenie, że członkowie nie konkurują ze sobą w tym względzie.

Jeśli jednak organizacje konkurują również na tym polu, trzeba rozważyć dopuszczenie do prac ISAC jedynie osób odpowiedzialnych ściśle za cyberbezpieczeństwo. Nie należy wówczas przyjmować osób, które odpowiadają w swoich firmach za komercjalizację czy sprzedaż.

[14] Starting an ISAC: Sectoral collaboration. Guide, National Cyber Security Centtre of the Netherlands, https://www.ncsc.nl/english/cooperation/_collaboration/sectoral-cooperation-isac.html , s. 10-11

Samozadowolenie

Samozadowolenie jest zawsze niebezpieczne. Należy pamiętać o krytycznym podejściu oraz dyskusji o rzeczach, które budzą frustracje. Dobrym pomysłem jest ustalanie celów oraz stałe adaptowanie ich do zmieniającej się sytuacji. Dobrym narzędziem do tego jest roczny plan działania.

Międzysektorowa wymiana informacji

Poważną wartość dodaną może stanowić wymiana informacji oraz współpraca ISAC na poziomie krajowym, europejskim, a nawet globalnym. Zwłaszcza, jeśli chodzi o sektory, które mają podobną dojrzałość, wspólne zależności i używają tych samych systemów bądź procedur. Ciągle wzrasta liczba europejskich ISAC, w których członkowie mogą uczestniczyć, aby zebrać informacje dla swojego ISAC.

NASK

Cyber POLICY