ISAC – „zaufana platforma” współpracy, organizacji i wymiany informacji dla cyberbezpieczeństwa. Praktyczne doświadczenia i rekomendacje.

Wstęp

Cyberbezpieczeństwo jest obecnie jednym z kluczowych obszarów w funkcjonowaniu każdej organizacji. Planujemy, budujemy wewnętrzne struktury bezpieczeństwa, monitorujemy i reagujemy na zagrożenia. Poświęcamy na to czas i budżet, jednak czasami dochodzi do przykrych sytuacji w których nikt nie chciałby się znaleźć. Cyberatak i jego konsekwencje są poważnym w skutkach wydarzeniem, z którym należy właściwie postępować. Dobrze „uczyć się na błędach" innych lub wykorzystywać unikalną wiedzę w zarządzaniu incydentem, którą mogą się podzielić z nami inne firmy. Możemy też otrzymać wsparcie w czasie kryzysu lub odpowiednie wskazówki do budowy odporności, aby jakikolwiek atak nie był klasyfikowany jako incydent poważny, ale zdarzenie, na które organizacja jest przygotowana i może spokojnie kontynuować swoja działalność. W organizacji naszej odporności, w dzieleniu się wiedza i doświadczeniami może nam pomóc wiele organizacji czy systemów współpracy a jednym z nich jest ISAC.

Budowa i współpraca z ISAC

Organizacje jakimi są ISAC (Infomation Sharing and Analysis Center – Centra Wymiany i Analizy Informacji) są znane na całym świecie, zarówno wśród osób zajmujących się cyberbezpieczeństwem, ale nie tylko[1]. Początek tych organizacji oraz funkcjonowania przypada na czas prezydentury Billa Clintona, który po atakach terrorystycznych m.in. w Nowym Jorku powołał komisję do wypracowania rekomendacji m.in. dla bezpieczeństwa systemów infrastruktury krytycznej. W raporcie znajdziemy rekomendacje do wzmocnienia tego obszaru poprzez współpracę i wymianę informacji na temat zagrożeń, dobrych praktyk zwiększających poziom bezpieczeństwa. Jednakże ISAC nie powoływane są tylko dla tego, ale również mają historię dostarczania usług operacyjnych – minimalizacji ryzyka, bądź też odpowiedzi na incydenty bezpieczeństwa.

Na bazie tych rekomendacji oraz późniejszych aktów prawnych powstały pierwsze ISAC. Obecnie w USA praktycznie w każdym sektorze jest utworzona taka organizacja a zrzesza je wszystkie narodowa rada ISAC, koordynująca wzmacnianie współpracy z innymi podmiotami m.in. federalnymi oraz zagranicznymi.

Na gruncie europejskim ISAC pojawiły się stosunkowo niedawno jako bardziej sformalizowane organizacje ukierunkowane na wsparcie rządowe. Głównym obszarem działalności ISAC jest budowa zaufania i partnerstwa a także umożliwianie współpracy pomiędzy podmiotami publicznymi i prywatnymi będącymi członkami poszczególnych ISAC.
W Europie znane są m.in. EE-ISAC (European Energy – ISAC) wspierająca działanie sektora elektroenergetycznego[2], czy Rail ISAC będący społecznością zrzeszającą europejskich operatorów kolejowych Natomiast FS – ISAC (Financial Services ISAC) zbudowana została dla sektora finansowego i jej działanie skupia się wokół tych organizacji[3]. Europejska Agencja Bezpieczeństwa Sieci i Informacji ENISA opublikowała na stronie internetowej różne

[1] https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Poradnik-NASK-na-temat-tworzenia-ISAC.pdf - dostęp: 18.05.2023 r.
[2] https://www.ee-isac.eu/ - dostep:18.05.2023 r.
[3] https://www.fsisac.com/ - dostęp: 18.05.2023 r.

materiały dot. ISAC, w tym przewodnik dot. ISAC, ich modeli oraz zasad funkcjonowania, który może być pomocny przy podejmowaniu decyzji o utworzeniu takiej struktury[4]. Naczelną zasadą, jaka przewija się wśród założeń dobrej i efektywnej współpracy, jest: *„One key success factor for an ISAC is trust. Without trust between the members, the ISAC will not fill its purpose, to share sensitive information."*

Analizując podstawy tworzenia i funkcjonowania ISAC należałoby dodać najnowszy akt prawny UE – dyrektywę NIS2, zmieniającą obowiązujący akt NIS, w którym to dokumencie, w rozdziale VI, art. 29, wskazane są mechanizmy wymiany informacji na temat cyberbezpieczeństwa[5]. Nie ulega wątpliwości, że w realizacji tych zapisów idealnym rozwiązaniem i „partnerem", chociażby w zakresie dobrowolnej wymiany informacji na temat cyberbezpieczeństwa, będą właśnie ISAC. Państwa członkowskie, jak wynika z zapisów w NIS2, mają wręcz zapewnić, aby wymiana informacji odbywała się w społecznościach podmiotów kluczowych (dostawców usług zaufania, publicznych sieci łączności i innych zgodnie z załącznikiem I) oraz ważnych (podmioty z załącznika I i II, które nie kwalifikują się jako podmioty kluczowe)[6], ale także w przypadkach związanych z ich dostawcami lub usługodawcami (bezpieczeństwo łańcucha dostaw).

Przechodząc na grunt Polskich doświadczeń oraz organizacji ISAC, można zauważyć, że tego typu rozwiązania nie znalazły na razie szerokiego zastosowania. Obecnie funkcjonują dwie organizacje: ISAC - Kolej w sektorze transportu[7]. Natomiast dla sektora wydobywczo-energetycznego powstało Centrum Wymiany i Analizy Informacji ISAC- GIG[8]. Z posiadanych przez CISO #Poland informacji wynika, iż jest w trakcie tworzenia kolejna organizacja ISAC w sektorze transportu, której uruchomienie zostanie oficjalnie potwierdzone w najbliższym czasie.

Wspominane przepisy dyrektyw NIS2 na pewno zwiększą zainteresowanie ISAC i możliwościami współpracy oraz integracji w poszczególnych sektorach, tym bardziej że będzie to idealne miejsce do swobodnej współpracy w relacjach partnerstwa publiczno - prywatnego.

Z praktycznego punktu widzenia, na bazie obecnych doświadczeń funkcjonujących ISAC warto przypomnieć podstawowe „zasady", dobre praktyki związane z tworzeniem, uruchomieniem i początkowym funkcjonowaniem takiej struktury.

ISAC-Kolej

Zagrożenia związane z cyberbezpieczeństwem na kolei dotyczą infrastruktury stacjonarnej (systemy sterowania ruchem kolejowym, radiołączność), nowoczesnych pojazdów kolejowych oraz klasycznych systemów IT cechujących się jednak potrzebą wysokiej dostępności np. systemy sprzedaży biletów, systemy planowania i realizacji rozkładów jazdy itp. Należy wskazać, że na Polskim rynku kolejowym funkcjonuje kilkuset przedsiębiorców pełniących

[4] https://www.enisa.europa.eu/enisa-search#/?SearchableText=ISAC – dostęp: 19.05.2023 r.
[5] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555 – dostęp: 19.05.2023 r.
[6] https://eur-lex.europa.eu/eli/dir/2022/2555 – dostęp: 05.06.2023 r.
[7] https://isac-kolej.pl/ - dostęp: 19.05.2023 r.
[8] https://isac.gig.eu/ - dostęp: 19.05.2023 r.

różne role: zarządcy infrastruktury, użytkownika bocznicy kolejowej, przewoźnika, producentów czy podmioty odpowiedzialne za utrzymanie pojazdów kolejowych. Każdy z nich odpowiada zgodnie z ustawą o transporcie kolejowym za bezpieczeństwo ruchu kolejowego. Postępująca informatyzacja procesów na kolei spowodowała wzrost zagrożeń związanych z cyberbezpieczeństwem i niewątpliwie kreuje potrzebę zaangażowania wszystkich uczestników rynku kolejowego w działania związane z cyberbezpieczeństwem. Utworzenie ISAC-Kolej jest częścią realizowanego projektu „Polityki współpracy w sferze IT i telekomunikacji w Grupie PKP i PKP PLK". To krok w stronę tworzenia specjalistycznego zespołu do reagowania na sytuacje kryzysowe związane z bezpieczeństwem cyfrowym w transporcie kolejowym. Jednym z głównych założeń tej polityki jest potrzeba standaryzacji i wprowadzenia ogólnych reguł zarządzania cyberbezpieczeństwem w branży kolejowej, zabezpieczenia wszystkich aspektów przestrzeni cyfrowej oraz aktywne wsparcie dla tworzenia Krajowego Systemu Cyberbezpieczeństwa.

ISAC-Kolej jest organizacją, do której mogą należeć określone podmioty związane z sektorem kolejowym. Aby zostać członkiem ISAC-Kolej podmiot musi posiadać status przedsiębiorstwa prowadzącego działalność gospodarczą zgodnie z ustawą o transporcie kolejowym na albo podmiotu publicznego zajmującego się bezpośrednio lub pośrednio sprawami cyberbezpieczeństwa, bezpieczeństwa ruchu kolejowego lub posiadający status państwowego instytutu badawczego.

Kluczowym obszarem działania ISAC-Kolej jest wymiana informacji o ryzykach, incydentach i strategiach zarządzania nimi. W ramach ISAC-Kolej dystrybuowane są codziennie informacje o zagrożeniach w sieci Internet a także informacje o podatnościach wybranych technologii informatycznych. Dodatkowymi obszarami opisanymi w Regulaminie ISAC Kolej są ambitne cele wypracowania standardów w zakresie cyberbezpieczeństwa w podsektorze kolejowym czy udział w tworzeniu standardów dla podsektora kolejowego i regulacji prawnych, które wspierają działania oraz przyczyniają się do zwiększenia poziomu bezpieczeństwa teleinformatycznego w podsektorze kolejowym.

Wadą obecnego ISAC-Kolej jest ograniczony krąg podmiotów uczestniczących w przedsięwzięciu. Brakuje bowiem kluczowych uczestników rynku niepochodzących z Grupy PKP. Istotne jest, aby kluczowi producenci wyrobów kolejowych zaangażowali się w proces dostarczania informacji o podatnościach dostarczanych elementów czy systemów OT. Niemniej jednak pozytywnie należy ocenić utworzenie pierwszego w Polsce ISACa w tak ważnej dla funkcjonowania państwa branży.

H-ISAC

Health-ISAC jest społecznością zrzeszającą właścicieli i operatorów krytycznej infrastruktury w sektorach związanych z ochroną zdrowia. Mówimy tutaj o szpitalach, firmach biotechnologicznych, laboratoriach, ubezpieczycielach zdrowotnych, producentach urządzeń medycznych itp. Społeczność ta jest w dużej mierze skupiona na udostępnianiu informacji dotyczących zagrożeń, incydentów i podatności, które zawierają np. IoC, taktyki, techniki i procedury (TTP) atakujących, ale również porady i dobre praktyki jak się przed nimi bronić.

Materiały te są udostępniane zarówno w formie „newsletterów", czy szkoleń, ale również pomiędzy członkami społeczności.

H-ISAC dba o pielęgnowanie relacji pomiędzy członkami organizacji organizując spotkania „networkingowe" czy seminaria edukacyjne. W ramach organizacji istnieje kilka wyspecjalizowanych podgrup (Ransomware, Szczepionki, Covid-19), które angażują się we współpracę w celu ustalenia wyspecjalizowanych standardów pracy, bądź produkcji białych ksiąg udostępnianych publicznie.

H-ISAC dba o nawiązywanie strategicznych relacji nie tylko w ramach społeczności, ale również z organizacjami ze szczebla rządowego, organami ścigania czy innymi stowarzyszeniami skupiającymi podmioty z branży ochrony zdrowia.

Wśród plusów (wynikających z formy płatnego członkostwa) H-ISAC możemy wyróżnić forum wymiany wiedzy i doświadczeń dla zarejestrowanych członków, warsztaty organizowane w siedzibach organizacji partycypujących dotyczących istotnych zagadnień (ryzyka firm trzecich, bezpieczeństwo AI), tygodniowe i miesięczne newslettery, czy rokroczne spotkania.

Niewątpliwą przeszkodą dla niektórych organizacji, które chciałyby przystąpić do stowarzyszenia jest element finansowy, jednak jak już zostało to wspomniane składka zależy od wielkości podmiotu a narzędzia oraz wiedza dostarczana wraz z członkostwem bardzo często przewyższają jego koszt.

ISAC powstaje w celu wsparcia danego sektora, firm lub organizacji, których działalność jest ze sobą powiązana lub na tyle zbliżona, iż dzielenie się doświadczeniem lub informacjami o sposobach zabezpieczenia jest potencjalnym pozytywnym powodem do rozpoczęcia współpracy. Przykładowe ISAC w Polsce powstały w sektorze transportu, czy górnictwie. Polskie firmy współpracują w ramach ISAC międzynarodowych na poziomie europejskim m.in. EE_ISAC (europejska energetyczna ISAC), F-ISAC (ISAC o dla organizacji z sektora finansowego), czy wspomniany już H-ISAC (ISAC dla organizacji z sektora ochrony zdrowia).

Jak założyć „własny" ISAC?

Dla tych co planują lub zastanawiają się nad kwestią organizacji, współpracy lub zasad działania ISAC kilka praktycznych rad.

1. **Zorganizuj grupę „wsparcia" lub „budowniczych".**
   Osoby z firm, które widzą potrzebę nawiązania współpracy w ramach ISAC, powinny wyznaczyć osoby, które będą w ścisłym gronie pracować w celu utworzenia organizacji. To dobre rozwiązanie ze względu na praktyczny wymiar takiej ISAC. Oczywiście możemy się spotkać z "poleceniem" utworzenia ISAC, która w danym sektorze może być podyktowana potrzebami innego rodzaju niż zwiększenie współpracy w zakresie cyberbezpieczeństwa, ale jeżeli na bazie takiego formatu powstaje realna współpraca i organizacje wspierają się i pracują na rzecz wspólnego cyberbezpieczeństwa, powód powstania jest kwestią pomijalną.

2. **Rozpocznij od podstaw, wyznaczaj „małe cele", osiągalne w krótkich terminach.** Powodzenie każdej inicjatywy, zwłaszcza w obszarze tak specyficznym jak

cyberbezpieczeństwo jest uzależniona od pozytywnego nastawienia, „sukcesów" które odnosi się już na początku, a to przekłada się na przekonanie o właściwej decyzji o utworzeniu ISAC. Dlatego planujmy, wyznaczajmy proste cele, np. utworzenie umowy o współpracy, porozumienia o współpracy, zasad współpracy. Grupa „budowniczych" powinna już na tym etapie spotykać się regularnie i pracować z uwzględnieniem planu oraz wyznaczonych terminów.

3. **Wyznacz cele długoterminowe i stałe, tak żeby mieć plan i „uzasadnienie" dla swojej działalności.**
   Planowanie działań w ISAC wymaga sporo konsultacji, uzgodnień oraz zaangażowania. Uczestnicy ISAC współpracują ze sobą (niekiedy biorąc na siebie dodatkowe obowiązki poza bieżącą organizacją) organizując różnego rodzaju wydarzenia czy też nawet bieżącą współpracę. Jednak całość musi mieć cel, który powinien być jasno zdefiniowany a poszczególne działania monitorowane, poddawane ocenie skuteczności i efektywności realizacji.

4. **Monitoruj, wspieraj, mierz wszystkie elementy działania ISAC.**
   Jak w każdej działalności, żeby wiedzieć, jak działa dana organizacja, system musi być mierzony. Nie ulega wątpliwości, że ISAC też tego wymaga. Spotykaj się z grupa „budowniczych" rozmawiaj o celach i stopniu ich realizacji. Wprowadzaj korekty i eliminuj rzeczy, które okazały się nietrafione lub zbędne. To tylko pochłania czas i niczego nie wnosi.

5. **Rozbuduj ISAC o nowych członków, buduj współpracę na zewnątrz, nawiązuj nowe kontakty i relacje.**
   ISAC z założenia to centrum współpracy i wymiany informacji. Chcąc wpłynąć na zwiększenie skuteczności działania, zasięg a przez to wzmocnienie danego sektora organizacja musi pozyskiwać nowych członków, starać się o pozyskanie wiedzy i kompetencji z zewnątrz np. nawiązanie współpracy z innymi ISAC a także powinna starać się o zwiększenie swojego zasięgu kontaktów. Instytucje naukowe, jednostki akademickie to potencjalny partner do współpracy. Organizacje tj. fundacje lub stowarzyszenia wspierające dany obszar są naturalnym kandydatem do współpracy. Nie zapominajmy o zasięgu nie tylko krajowym, ale również międzynarodowym. Obecnie funkcjonują ISAC na poziomie EU lub międzynarodowym, skupującym nie tylko firmy, ale również ISAC z danego sektora. Pierwsza i podstawowa „wartość dodana" to dostęp do wiedzy, kompetencji i doświadczenie osób z różnych firm, które mogą tymi „zasobami" z nami się dzielić. Np. bazy zawierające „wnioski z incydentów", aktualne informacje o akcje phishingowe[9]. Bardzo często na potrzeby ISAC

[9] https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y - dostęp: 04.06.2023 r.

sektorowych powstają dedykowane instancje MISP[10] w celu wymiany IoC[11] dla danego sektora.

6. **Zadbaj i zapewnij kanały do komunikacji dla członków ISAC.**
   Nic tak pozytywnie nie wpływa na współpracę, jak możliwość bieżącej wymiany informacji. Wymiana pomysłów, planów, informacji o postępach prac, to element kluczowy dla powodzenia funkcjonowania nie tylko ISAC, ale każdej działalności. Pamiętajmy o tym, żeby wymianie informacji towarzyszyły odpowiednio zdefiniowane zasady ochrony informacji, związane np. z systemem TLP[12] a także z umową o współpracy ISAC, w której takie zasady, w tym ochrona informacji wrażliwych muszą być określone wprost dla wszystkich.

7. **Powołaj „radę", „zarząd" – ktoś musi o to dbać.**
   ISAC jako organizacja wymaga stałego zarządzania, monitorowania działalności, realizacji celów. Ktoś za to musi odpowiadać, wspierać, koordynować czy też w momentach ważnych podejmować decyzje o właściwym kierunku działania całej organizacji. Co najmniej raz do roku, „rada" musi sporządzić raport z działalności ISAC. Co osiągnęliśmy, jakie mamy plany, stopień realizacji, bieżące problemy to m.in. tematy jakie powinny znaleźć się w raporcie.

8. **Finansowanie działalności ISAC.**
   Ten temat nie został specjalnie pozostawiony na końcu, bo jest „niewygodny" i powoduje różne spory, ale dlatego że jest bardzo ważny. Bez finansowania ISAC może działać, ale ta działalność jest ograniczana do pewnych „podstawowych" kwestii. Często, zależnie od organizacji uczestniczących i chcących „dzielić" się z innymi uczestnikami ISAC swoimi zasobami np. informacyjnymi, nie musimy za to ponosić kosztów. Jednak nie wszystkie ISAC działają w ten sposób – te większe bazują na donacjach członków, w których składka różni się w zależności od wielkości i zasobności portfela podmiotu. Prace poszczególnych osób, realizujących swoje zadania w ramach zadań organizacji uczestniczących, też możemy pominąć. Wyzwaniem może być stworzenie innych produktów lub usług ISAC które na co dzień nie są dostępne w ramach organizacji np. wspólna instancja MISP, uczestnictwo w konferencjach, warsztatach.

[10] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing/isacs-toolkit/further-reading/misp-2013-malware-information-sharing-platform-threat-sharing – dostęp: 04.06.2023r.
[11] https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/ - dostep: 04.06.2023 r.
[12] https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage - dostęp: 04.06.2023 r.

Podsumowanie.

Na co warto wskazać przy okazji omawiania ISAC, to wartość jaką daje współpraca w ramach takiej struktury. Funkcjonowanie jest ważne nie tylko dla organizacji, które uczestniczą w jej tworzeniu, ale przede wszystkim dla osób uczestniczących w jej pracach, spotkaniach, konferencjach. Wymiana wiedzy, doświadczeń oraz informacji przybiera nowy wymiar. Problemy, które stanowiły wyzwanie mogą być rozwiązane przy udziale większej liczby osób. Czasami też problem jest rozwiązywalny na podstawie wcześniejszych doświadczeń innych osób.

Warto stawiać też na współpracę ISAC z innymi podmiotami, partnerami ISAC, których udział może być limitowany ze względu na zakres wymienianych informacji „wewnątrz" organizacji. Zwiększa to znacznie zasób wiedzy i informacji, a także przynosi dodatkowe możliwości w relacji wspólnych projektów np. z obszaru R&D. Takim naturalnym partnerem ISAC są jednostki naukowe i akademickie, ale też start-upy. Rozwiązanie polegające na przyjmowaniu członków stowarzyszonych w postaci takich jednostek przyjęła EE-ISAC. Głównym celem było wypracowywanie różnego rodzaju zaleceń na bazie analiz naukowych, czy też badań, których celem ma być wzmocnienie sektora elektroenergetycznego w obszarze cyberbezpieczeństwa.

Na zakończenie warto dodać, iż tego typu inicjatywy, jak każda inna organizacja, powinny być poddawane regularnej ocenie w zakresie swojej skuteczności oraz efektywności. To, jak bardzo satysfakcjonująca jest współpraca dla poszczególnych członków – uczestników, przekłada się później na ich zaangażowanie i pracę na rzecz całej ISAC.