Zadanie
„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Konferencja naukowa
„Wzmacnianie odporności szkół wyższych
na cyberataki przez podnoszenie kompetencji cyfrowych”

ISAC jako instrument wzmacniania cyberbezpieczeństwa

Prelegent: Maciej Siciarek – CSIRT NASK

Ministerstwo Edukacji i Nauki

UKSW Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

CLTC Centrum Liderów Transformacji Cyfrowej

Czym jest ISAC?

- Ang. *Information Sharing and Analysis Center*
- Centrum wymiany wiedzy i doświadczeń dot. incydentów i zagrożeń cyberbezpieczeństwa w danym sektorze gospodarki
- **Współpraca**
  - Podmiotów mających podobne procesy i usługi, a zatem posiadających podobne systemy i rozwiązania ICT, zbiory danych… wyzwani i problemy,
  - asektora prywatnego i publicznego oraz **budowanie relacji** pomiędzy różnymi sektorami gospodarki i instytucjami publicznymi
- **Cel: znaczące podniesienie poziomu cyberbezpieczeństwa**

CyberPOLICY NASK

ISAC – co to jest?

https://cyberpolicy.nask.pl/model-dojrzalosci-isac-poradnik/

References

- Information Sharing and Analysis Centers (ISACs) webpage
- Cross-sector Exercise Requirements
- ISAC in a Box
- EU Agency for Cybersecurity launches ISAC in a Box Toolkit
- Study - Effective Collaborative models for ISACs
- Opinion paper - ISAC Cooperation
- ENISA Incident Reporting webpage
- European Electronic Communications Code
- NIS Directive – ENISA topic
- press (at) enisa.europa.eu

Show 2 more

„Prawne i pozaprawne instrumenty wzmacniania cyberodporności uczelni”

ISAC – instrument prawny czy pozaprawny?

Nowelizacja ustawy o KSC…

3) art. 2 otrzymuje brzmienie: / „Art. 2. Użyte w ustawie określenia oznaczają:

(…) 22) ISAC – centrum wymiany i analizy informacji na temat podatności, cyberzagrożeń i incydentów funkcjonujące w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa;

Dyrektywa NIS II

art 10 ustęp 4 4.: CSIRT współpracują z **sektorowymi i międzysektorowymi społecznościami podmiotów**

kluczowych i ważnych oraz, w odpowiednich przypadkach, wymieniają z nimi stosowne informacje

ISAC – instrument prawny czy poza prawny?

Dyrektywa NIS II cd…

(120) Należy zachęcać podmioty do wspólnego wykorzystywania ich indywidualnej wiedzy i praktycznego doświadczenia na szczeblu strategicznym, taktycznym i operacyjnym – a państwa członkowskie powinny im w tym pomagać – w celu wzmocnienia zdolności podmiotów w zakresie odpowiedniego zapobiegania incydentom, wykrywania ich, reagowania na nie lub przywracania normalnego działania lub łagodzenia skutków incydentów. **Należy zatem umożliwić powstawanie na poziomie Unii mechanizmów dobrowolnej wymiany informacji o cyberbezpieczeństwie.** W tym celu państwa członkowskie powinny aktywnie wspierać podmioty, takie jak podmioty świadczące usługi i prowadzące badania w zakresie cyberbezpieczeństwa, jak również odpowiednie podmioty nieobjęte zakresem niniejszej dyrektywy, i zachęcać je do uczestnictwa w takich mechanizmach wymiany informacji o cyberbezpieczeństwie.

Filary działania ISAC

Zaufanie

Wspólne interesy

Równość

Filary działania ISAC

Zaufanie

- pewność, że informacje, którymi dzielą się uczestnicy, nie zostaną przekazane dalej bez ich zgody
- budowane m. in. poprzez stworzenie dot. wytycznych członkostwa, z kim i w jaki sposób można dzielić się informacjami
- tworzenie relacji między uczestnikami

Wspólne interesy

- szczera i jasna komunikacja swoich motywacji
- ustalenie celów i priorytetów dla działania ISAC
- namierzanie konfliktów interesów i przeciwdziałanie im

Równość

- równość uczestników ISAC – brak hierarchicznych relacji

Etapy powoływania ISAC

Poszukiwanie

- Podobne potrzeby i wyzwania
- Kontakty wewnątrzsektorowe
- Od małej grupy do większej
- Wstępne ustalenia – kto, w jakim celu, jakie informacje

Budowanie

- Rozpoczęcie oficjalnej działalności
- Podpisanie MoU
- Ustanowienie ról
- Uzgodnienie częstotliwości spotkań
- Określenie kanałów komunikacji
- Wytyczne członkostwa

Kontynuacja

- Przygotowanie planu rocznego działalności
- Organizacja spotkań
- Raporty roczne
- Aktywne uczestnictwo
- Budowanie relacji
- Nowi członkowie

Kluczowe obszary dojrzałości ISAC

Budowa zaufania

Zarządzanie i organizacja

Wymiana informacji

Usługi (narzędzia IT, analizy, budowanie zdolności)

Działania zewnętrzne

Uczenie się od siebie nawzajem

- wymiana wiedzy i najlepszych praktyk między uczestnikami
- nauka na doświadczeniach innych uczestników – możliwość wypracowania skuteczniejszych metod reagowania na incydenty

Poprawa poziomu cyberbezpieczeństwa

- wymiana informacji w sektorze = szybsze pozyskiwanie wiedzy o potencjalnych zagrożeniach
- wzrost świadomości i bezpieczeństwa w całym sektorze

Zmniejszenie kosztów

- wspólne opracowywanie rozwiązań problemów – zmniejszenie kosztów, które wygenerowałoby ich samodzielne rozwiązywanie
- możliwość wspólnego zakupu usług bezpieczeństwa

Budowa wizerunku

- sygnał dla klientów i podmiotów współpracujących, że instytucja/ firma poważnie podchodzi do bezpieczeństwa informacji i ochrony danych
- zapobieganie incydentom, które mogłyby spowodować spadek reputacji

Przywództwo w działaniu

- działania na rzecz poprawy cyberbezpieczeństwa mogą stanowić element polityki społecznej odpowiedzialności firmy
- budowanie pozycji lidera w zakresie działań na rzecz bezpieczeństwa sektora

Międzysektorowa wymiana informacji

- współpraca na poziomie krajowym, europejskim i globalnym
- możliwość dołączania do europejskich ISAC

Wyzwania

Zaufanie

- wymaga ciągłego podtrzymywania
- jego brak może spowodować niepowodzenie całego przedsięwzięcia

Zaangażowanie

- każdy uczestnik powinien stanowić wartość dodaną dla grupy
- konieczność krytycznego przyglądania się swojemu wkładowi w prace grupy

Konkurencja

- potencjalna wymiana wrażliwych informacji ze swoją konkurencją
- konieczność zastanowienia się, w jaki sposób zapewnić, aby członkowie ISAC nie konkurowali ze sobą na tym polu

Samozadowolenie

- konieczność krytycznego podejścia do swoich działań
- monitorowanie realizacji programu rocznego i ujętych w nim celów

Co oferuje NASK?

Bieżące wsparcie ekspertów

Szkolenia i warsztaty

Ocena dojrzałości ISAC

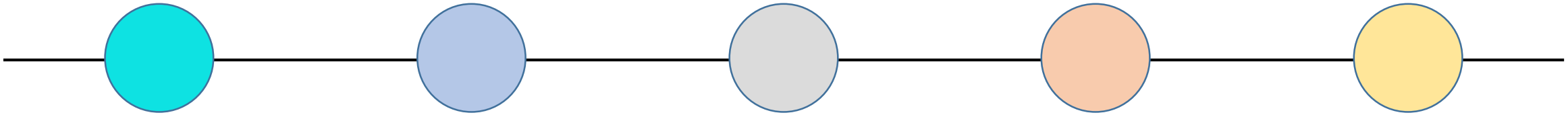
Dziękuję za uwagę

CyberPOLICY
NASK

Maciej.Siciarek@nask.pl

Pięć poziomów dojrzałości ISAC

Kluczowe obszary dojrzałości ISAC – budowa zaufania

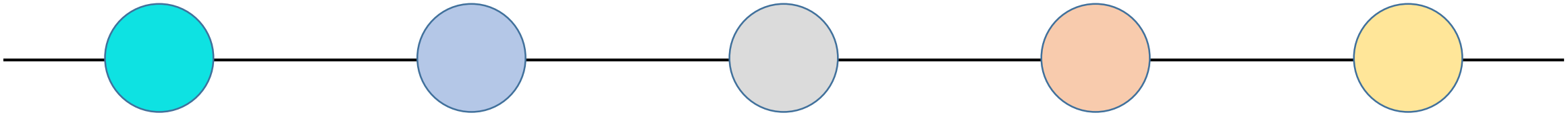


Poziom 1	Poziom 2	Poziom 3	Poziom 4	Poziom 5
Spotkania ad hoc, na których podejmowane są doraźne decyzje	Systematyczne spotkania bezpośrednie	Spotkania integracyjne	Różne statusy członków (w zależności od stażu w organizacji)	Utarte sposoby komunikacji bezpośredniej (wysoki poziom zaufania)
Stali przedstawiciele reprezentujący członków na spotkaniach ISAC		Kontakty robocze (pomiędzy spotkaniami ISAC)		Członkowie wymieniają się informacjami zgodnie ze zdefiniowanym statusem członkostwa i zapotrzebowaniem
Członkowie zaangażowani w zależności od potrzeb danej organizacji		Wzrost aktywności członków ISAC		

Kluczowe obszary dojrzałości ISAC – zarządzanie i organizacja

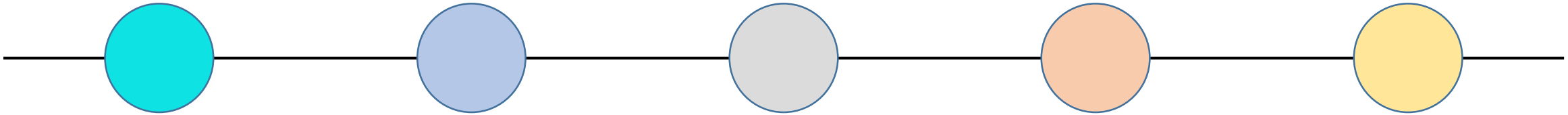
Poziom 1	Poziom 2	Poziom 3	Poziom 4	Poziom 5
Porozumienie określające zasady współpracy oraz zasady członkostwa i regulamin ISAC	Funkcjonuje oficjalny sekretariat ISAC	Grupy robocze dedykowane konkretnym tematom	Długoterminowy plan działalności organizacji, weryfikowany na spotkaniach rocznych	Osobowość prawna
Jedna z organizacji sprawuje nieoficjalną funkcję przewodniczącego i sekretariatu	Przewodniczący i wiceprzewodniczący wybrani zgodnie z regulaminem	Doraźny budżet na wybrane projekty	Wyodrębniony zarząd, który nadzoruje realizację celów	Osobna struktura, z własnym sekretariatem
	Ustrukturyzowane spotkania, zgodnie z zaakceptowaną wcześniej agendą		Ustrukturyzowane, tematyczne grupy robocze	Pracownicy zatrudnieni przez ISAC
	Ustalony i przyjęty roczny plan ISAC		Stały budżet, tworzony ze składek członkowskich	Siedziba, w której odbywają się spotkania zarządu i grup roboczych
			Roczne spotkanie podsumowujące działalność ISAC	Ustrukturyzowany budżet centralny

Kluczowe obszary dojrzałości ISAC – wymiana informacji



Poziom 1	Poziom 2	Poziom 3	Poziom 4	Poziom 5
Wymiana dobrych praktyk	Na spotkaniach omawiane są ciekawe przykłady zagrożeń i incydentów	Wymiana informacji o incydentach post factum	Współpraca w czasie obsługi incydentów	Wymiana informacji wrażliwych i poufnych
Stopniowe poznawanie organizacji, które biorą udział w ISAC	Doraźna wymiana ostrzeżeń i informacji o incydentach (poprzez szyfrowaną listę mailingową)	Wymiana analiz na temat incydentów	Wymiana informacji o incydentach w czasie rzeczywistym	Wspólna koordynacja kryzysu i dużych incydentów (także wspólne komunikaty prasowe)
	Informacje wymienianie są zgodnie z zasadami TLP	Wymiana informacji o podatnościach		

Kluczowe obszary dojrzałości ISAC – usługi



Poziom 1	Poziom 2	Poziom 3	Poziom 4	Poziom 5
Lista mailingowa	Szyfrowana lista mailingowa	Platforma do wymiany informacji	Zaufany i bezpieczny chat do rozmów bezpośrednich w czasie rzeczywistym	Zaufana platforma z systemem monitorowania zagrożeń
		Wspólne ćwiczenia *table top* dla członków ISAC	Wspólne ćwiczenia techniczne dla członków ISAC	Przygotowywanie raportów i analiz dla uczestników ksc
		Organizowanie szkoleń i warsztatów dla członków ISAC	Przygotowywanie raportów i analiz dla członków ISAC	Organizacja ćwiczeń, szkoleń i warsztatów dla podmiotów ksc
			Organizowanie szkoleń i warsztatów dla całego sektora (także dla podmiotów nie będących członkami ISAC)	

Kluczowe obszary dojrzałości ISAC – działania zewnętrzne

Poziom 1	Poziom 2	Poziom 3	Poziom 4	Poziom 5
Pozyskanie patronatu ministra właściwego dla danego sektora lub podsektora	Doraźne uczestnictwo przedstawicieli administracji publicznej w spotkaniach ISAC	Jasno określone zasady współpracy z administracją	ISAC ma zaplanowaną działalność zewnętrzną (komunikacja i współpraca z organizacjami trzecimi)	ISAC uczestniczy w budowaniu wyższego poziomu cyber. w całym ksc, a nie tylko w sektorze
Współpraca z CSIRT poziomu krajowego	Doraźne uczestnictwo przedstawicieli CSIRT sektorowych, innych ISAC oraz firm świadczących usługi z zakresu cyber. w spotkaniach ISAC	Jasno określone zasady współpracy z CSIRT sektorowymi, innymi ISAC oraz firmami świadczącymi usługi z zakresu cyber.	ISAC reprezentuje interesy sektora przed organami właściwymi ds. cyber. oraz sektorowymi CSIRT i krajowymi CSIRT	ISAC organizuje własne konferencje, warsztaty i spotkania w których mogą brać udział podmioty zewnętrzne
Wstępne rozmowy o współpracy z przedstawicielami administracji publicznej		Jasno określone zasady współpracy z przedstawicielami sektora/ podsektora którzy nie są członkami ISAC	Istnieje polityka rozwoju ISAC i pozyskiwania nowych członków	ISAC dostępnia swoje analizy i raporty podmiotom zewnętrznym
Wstępne rozmowy współpracy z przedstawicielami CSIRT sektorowych, innych ISAC oraz firmami świadczącymi usługi z zakresu cyber.			Członkowie zarządu reprezentują ISAC w wydarzeniach zewnętrznych (konferencje, warsztaty)	ISAC organizuje szkolenia i warsztaty dla podmiotów zewnętrznych
			Regularna i ustrukturyzowana współpraca z członkami ksc	