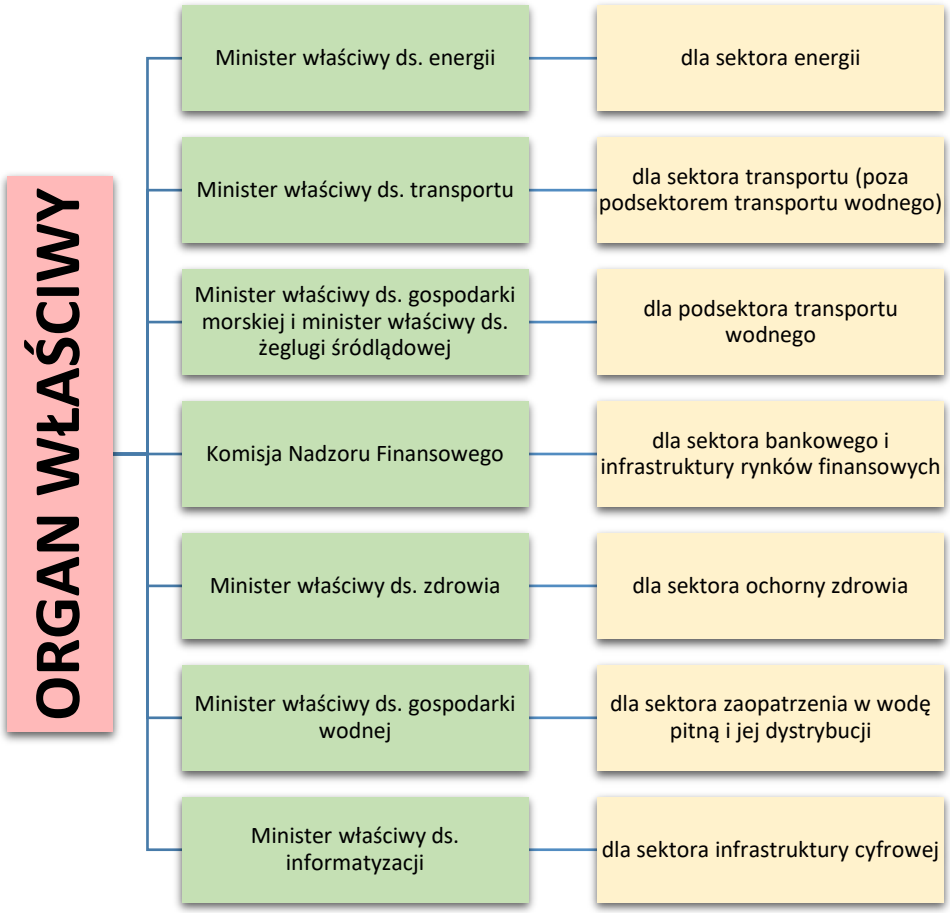
ORGAN WŁAŚCIWY – kto kim jest?



ZADANIA ORGANU WŁAŚCIWEGO (OW)

- ✓ Na bieżąco prowadzi analizę podmiotów w danym sektorze lub podsektorze pod katem uznania ich za operatora usługi kluczowej.
- ✓ Wydaje decyzje o uznaniu podmiotu za operatora usługi kluczowej.
- ✓ Przygotowuje rekomendacje działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące działania incydentów (współpraca z CSIRT NASK, CSIRT GOV, CSIRT MON i sektorowymi zespołami cyberbezpieczeństwa).
- ✓ Prowadzi kontrole operatorów usług kluczowych i dostawców usług cyfrowych (monitoruje stosowanie przez nich przepisów ustawy).
- ✓ Na wniosek CSIRT NASK, CSIRT GOV LUB CSIRT MON wzywa operatorów usług kluczowych lub dostawców usług cyfrowych do usunięcia w wyznaczonym terminie podatności które doprowadziły lub mogły doprowadzić do incydentu poważnego, istotnego lub krytycznego.
- ✓ Uczestniczy w ćwiczeniach w zakresie cyberbezpieczeństwa organizowanych w RP lub UE.
- ✓ Dla danego sektora lub podsektora może ustanowić, sektorowy zespół cyberbezpieczeństwa (SCZ to opcjonalne zadanie OW, tylko one decydują jak je ustanawiają i w jakiej formie prawnej.

RODZAJE INCYDENTÓW

Incydent krytyczny - incydent, skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi.

Incydent poważny - incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości działania świadczonej usługi kluczowej; Incydent istotny- incydent, który ma istotny wpływ na świadczenie usługi cyfrowej.

Incydent o podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.
Incydent zwykły - zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo – ten incydent nie podlega zgłoszeniu, ale też należy go obsługiwać.

SEKTOROWY ZESPOŁ CYBERBEPIECZEŃSTWA (SCZ)

- ✓ przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w ich obsłudze;
- ✓ wspieranie operatorów usług kluczowych w wykonywaniu obowiązków;
- ✓ analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowywanie wniosków z ich obsługi;
- ✓ współpraca z właściwym CSIRT NASK, CSIRT GOV, CSIRT MON w zakresie koordynowania obsługi incydentów poważnych;
- ✓ SZC może przekazywać do innych państw i przyjmować od nich informacje o incydentach poważnych, w tym dot. dwóch lub większej liczby państw członkowskich UE;
- ✓ SZC może otrzymywać zgłoszenia incydentu poważnego z innego państwa członkowskiego UE, dot. dwóch lub większej liczby państw. Takie zgłoszenia przekazuje do właściwego CSIRT NASK, CSIRT GOV, CSIRT MON oraz PPK.

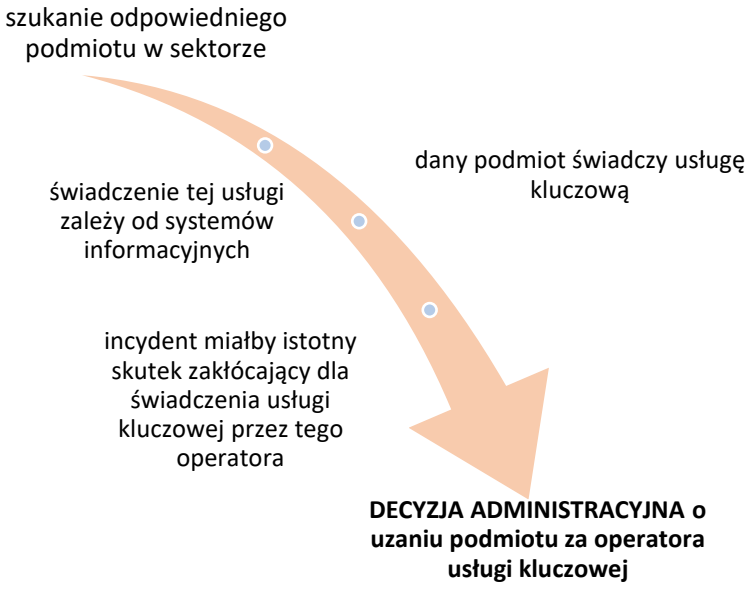
Przy Ministrze Cyfryzacji działa, Pojedynczy Punkt Kontaktowy (PPK) który jest odpowiedzialny m.in. za:

- ✓ tworzenie ram prawnych funkcjonowania obszaru cyberbezpieczeństwa RP, w tym czuwanie nad ich spójnością;
- ✓ pełnienie funkcji łącznika w celu zapewnienia współpracy podmiotami odpowiedzialnymi za cyberbezpieczeństwo;
- ✓ gromadzenie i przetwarzanie informacji otrzymanych od m.in. operatorów usług kluczowych;
- ✓ kontrolowanie spełniania przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa wymagań organizacyjnych i technicznych;
- ✓ przekazywanie na wniosek właściwego CSIRT, zgłoszenia incydentu poważnego lub incydentu istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych innych państwa członkowskich UE;
- ✓ zapewnienie reprezentacji RP w Grupie Współpracy;
- ✓ zapewnienie współpracy z Komisją Europejską w dziedzinie cyberbezpieczeństwa;
- ✓ koordynację współpracy między organami właściwymi ds. cyberbezpieczeństwa RP z odpowiednimi organami w państwa członkowskich UE.

Współpraca PPK z innymi organami:

1. W uzasadnionych przypadkach współpracują z organami ścigania i organem właściwym do spraw ochrony danych osobowych;
2. W przypadku gdy podmiot świadczy usługę kluczową w innych państwach członkowskich UE, organ właściwy w toku postępowania administracyjnego, za pośrednictwem Pojedynczego Punktu Kontaktowego, prowadzi konsultacje z tymi państwami w celu ustalenia, czy ten podmiot został uznany w tych państwach za operatora usługi kluczowej.

Organ właściwy wydaje decyzję o uznaniu podmiotu za operatora usługi kluczowej jeżeli:



Schemat zawierający poszczególne organy właściwe wraz z przypisanymi im sektorami. Od pola „ORGAN WŁAŚCIWY” odchodzą rozgałęzienia prowadzące do kolejnych pól, opisujące organy właściwe oraz podległe im sektory (pole 1 do 7).

Treść pola 1: Minister właściwy ds. energii dla sektora energii

Treść pola 2: Minister właściwy ds. transportu dla sektora transportu (poza podsektorem transportu wodnego)

Treść pola 3: Minister właściwy ds. gospodarki morskiej i minister właściwy ds. żeglugi śródlądowej

dla podsektora transportu wodnego

Treść pola 4: Komisja Nadzoru Finansowego dla sektora bankowego i infrastruktury rynków finansowych

Treść pola 5: Minister właściwy ds. zdrowia dla sektora ochrony zdrowia

Treść pola 6: Minister właściwy ds. gospodarki wodnej dla sektora zaopatrzenia w wodę pitną i jej dystrybucji

Treść pola 7: Minister właściwy ds. informatyzacji dla sektora infrastruktury cyfrowej

Schemat w postaci strzałki, od której odchodzą punkty opisujące działania organu właściwego przy wydawaniu decyzji o uznaniu podmiotu jako OUK (punkty od 1 do 5). Poszczególne punkty są kolejnymi krokami koniecznymi do zrealizowania zamierzonego celu, jakim jest decyzja administracyjna o uznaniu podmiotu za OUK.

Treść punktu nr 1: szukanie odpowiedniego podmiotu w sektorze;

Treść punktu nr 2: świadczenie tej usługi zależy od systemów informacyjnych

Treść punktu nr 3: dany podmiot świadczy usługę kluczową

Treść punktu nr 4: incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora

Treść punktu nr 5: DECYZJA ADMINISTRACYJNA o uzaniu podmiotu za operatora usługi kluczowej