

KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Celem systemu jest zapewnienie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych. Obejmuje on swoim zasięgiem szereg podmiotów, m.in.:



**OPERATORZY
USŁUG
KLUCZOWYCH**



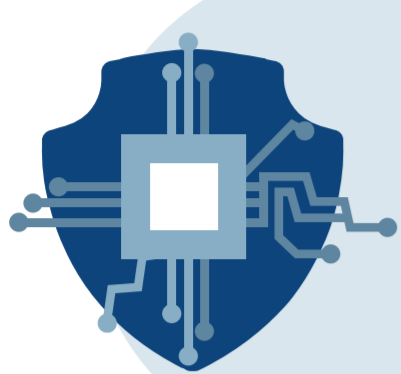
**DOSTAWCY
USŁUG
CYFROWYCH**

Świadczący usługi w sektorach:

- Energia
- Transport
- Bankowość i infrastruktura rynków finansowych
- Ochrona zdrowia
- Zaopatrzenie w wodę pitną i jej dystrybucja
- Infrastruktura cyfrowa

Są nimi:

- Internetowe platformy handlowe
- Dostawcy rozwiązań chmurowych
- Wyszukiwarki internetowe



**ZESPOŁY REAGOWANIA
NA INCYDENTY
BEZPIECZEŃSTWA
KOMPUTEROWEGO (CSIRT).**



**PEŁNOMOCNIK
RZĄDU DS.
CYBERBEZPIECZEŃSTWA**

1) CSIRT GOV – prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego

2) CSIRT NASK – prowadzony przez Naukową i Akademicką Sieć Komputerową

3) CSIRT MON – prowadzony przez Ministra Obrony Narodowej

Ustawa wskazuje także możliwość tworzenia sektorowych zespołów cyberbezpieczeństwa.

- Koordynuje działania i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w RP
- Powoływany przez Prezesa Rady Ministrów
- Zgodnie z aktualnym rozporządzeniem Rady Ministrów z dn. 16 marca 2018 r. Pełnomocnikiem jest sekretarz stanu albo podsekretarz stanu w Ministerstwie Obrony Narodowej



**KOLEGIUM
DO SPRAW
CYBERBEZPIECZEŃSTWA**



**POJEDYNCZY PUNKT
KONTAKTOWY
DO SPRAW
CYBERBEZPIECZEŃSTWA**

- Działa przy Radzie Ministrów jako organ opiniotwórczo-doradczy w sprawach cyberbezpieczeństwa
- W skład Kolegium wchodzi m.in.: Premier, wybrani ministrowie, szef BBN
- W posiedzeniach uczestniczą także m.in.: Dyrektor RCB, Szef ABW, Szef SKW, Dyrektor NASK

- Prowadzony przez Ministerstwo Cyfryzacji
- Zapewnia wymianę informacji o incydentach z innymi Krajami Członkowskimi UE
- Odpowiada za współpracę na poziomie UE, zarówno z Komisją Europejską jak i w ramach Grupy Współpracy



**PODMIOTY ŚWIADZĄCE
USŁUGI Z ZAKRESU
CYBERBEZPIECZEŃSTWA**

Wyspecjalizowane firmy zabezpieczające infrastrukturę operatorów usług kluczowych oraz zapewniające obsługę incydentów w ich sieciach na podstawie zawartych umów.

USTAWA ZAKŁADA PODZIAŁ OBSŁUGI INCYDENTÓW BEZPIECZEŃSTWA W CYBERPRZESTRZENI RP POMIĘDZY TRZY ZESPOŁY:



CSIRT GOV



CSIRT NASK



CSIRT MON

CYBERPRZESTRZEŃ RP

CSIRT NASK

- Obywatele
- Firmy
- Administracja samorządowa
- Uczelnie publiczne
- Pozostałe podmioty sektora publicznego i prywatnego

CSIRT MON

Podmioty podległe lub nadzorowane przez MON oraz przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym

CSIRT GOV

- Infrastruktura Rządowa oraz jednostek podległych
- Infrastruktura Krytyczna
- Infrastruktura NBP, BGK, ZUS, NFZ, NIK, RPO, KRRTV, sądów i trybunałów

KLASYFIKACJA INCYDENTÓW

W RAMACH KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

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
- Klasyfikowany przez właściwy CSIRT

INCYDENT POWAŻNY

- Incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej
- Klasyfikowany przez operatora usługi kluczowej

INCYDENT ISTOTNY

- Incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r.
- Klasyfikowany przez dostawcę usługi cyfrowej



INSTYTUT KOŚCIUSZKI