NASK

Cyber POLICY

Ustawa o Krajowym Systemie Cyberbezpieczeństwa

AGENDA

- **NASK PIB**
- **USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZCEŃSTWA**
- **PYTANIA**

NASK Cyber POLICY

NASK PIB

- W **1992 r**. powstał NASK podłączając Polskę do Internetu.
- W **1996 r.** powstał pierwszy w Polsce zespół reagowania na zagrożenia w sieci – CERT Polska.
- W **2003 r.** jako jeden z pierwszych rejestrów na świecie wprowadził obsługę domen ze znakami narodowymi.
- Od **2010 r**. jest instytutem badawczym.
- NASK jest polskim koordynatorem Europejskiego Miesiąca Cyberbezpieczeństwa.
- Od 24 lat NASK organizuje konferencję SECURE dot. bezpieczeństwa teleinformatycznego.

Ustawa o Krajowym Systemie Cyberbezpieczeństwa

Ustawa o **Krajowym Systemie Cyberbezpieczeństwa** to **pierwszy akt prawny**, który implementuje do polskiego porządku prawnego **dyrektywę NIS** Parlamentu Europejskiego i Rady (UE) **2016/1148**.

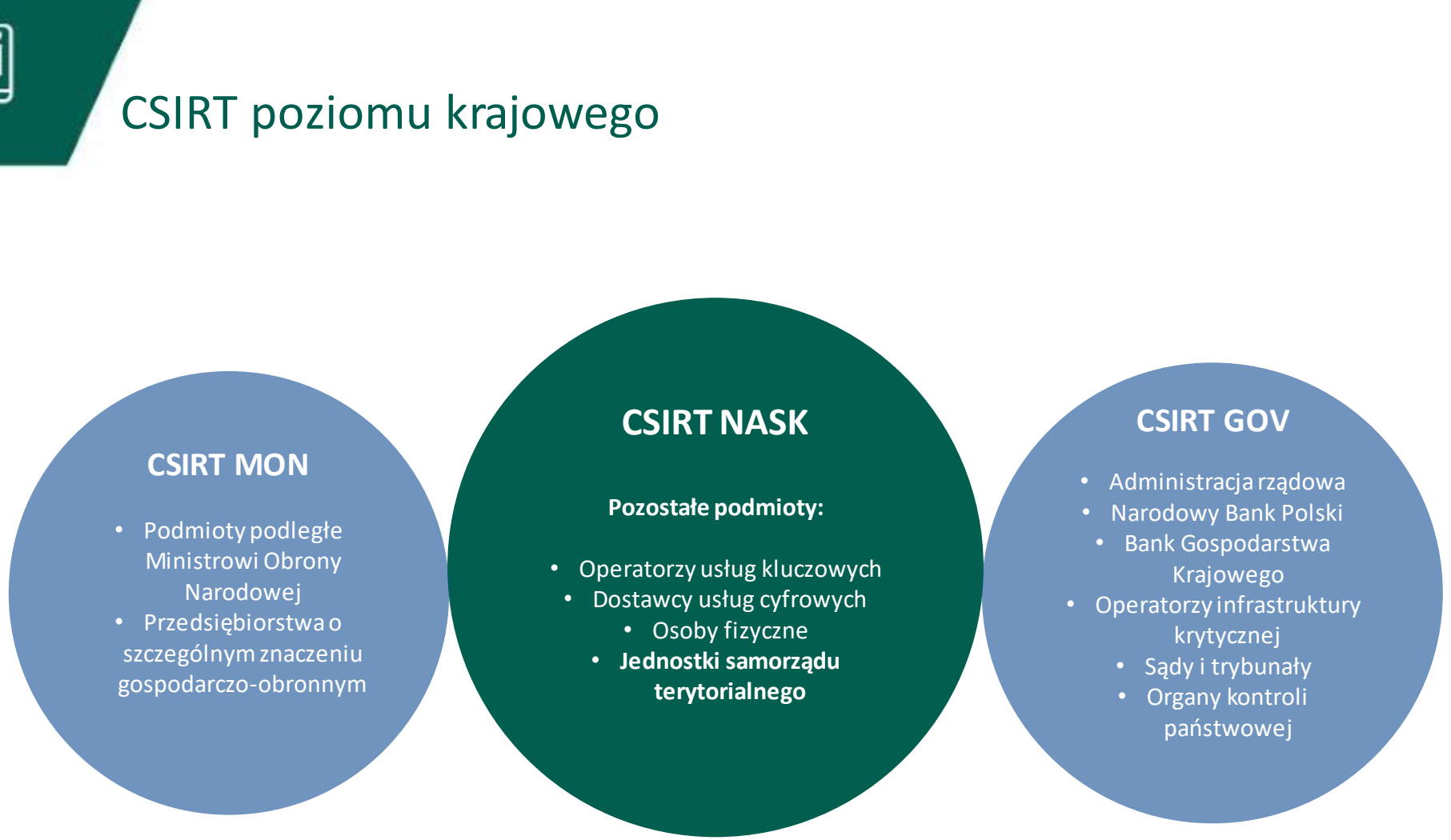
Ustawa weszła w życie 28 sierpnia 2018 roku.

Ustawa o Krajowym Systemie Cyberbezpieczeństwa

Co nowego wprowadza ustawa?

- podział obowiązków pomiędzy poszczególnymi CSIRT poziomu krajowego;
- nadzór w zakresie cyberbezpieczeństwa (organy właściwe, wprowadzenie kar finansowych);
- ramy zarządzania cyberbezpieczeństwem w Polsce (Strategia Cyberbezpieczeństwa RP, powołanie Pełnomocnika i Kolegium ds. Cyberbezpieczeństwa).

CSIRT poziomu krajowego



Zadania CSIRT

- **Monitorowanie** zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym
- **Szacowanie** ryzyka w skali kraju
- **Przekazywanie** informacji na temat incydentów i ryzyk
- **Wydawanie** komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa
- **Reagowanie** na zgłoszone incydent
- **Koordynowanie** obsługi incydentów krytycznych

W uzasadnionych przypadkach CSIRT może zapewnić wsparcie w obsłudze incydentu, albo przekazać informacje o podatnościach i sposobach ich usunięcia

Zadania CSIRT NASK

CSIRT NASK

- **CERT Polska** prowadzi działania operacyjne, takie jak: monitorowanie zagrożeń cyberbezpieczeństwa, reagowanie na zgłoszone incydenty i koordynacja ich obsługi oraz przeciwdziałanie zagrożeniom cyberbezpieczeństwa.

- **Dyżurnet.pl** reaguje na zgłoszenia dotyczące nielegalnych i szkodliwych treści, w tym materiałów przedstawiających seksualne wykorzystywanie dzieci.

- **NASK CyberPolicy** prowadzi analizy i opracowuje standardy, rekomendacje oraz dobre praktyki w zakresie cyberbezpieczeństwa, a także wspiera podmioty krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa.

- **Partnerstwo dla Cyberbezpieczeństwa** zapewnia wsparcie dla różnego rodzaju podmiotów na poziomie: technicznym, strategicznym i kompetencyjnym. Celem jest budowanie zaufania oraz sieci kontaktów.

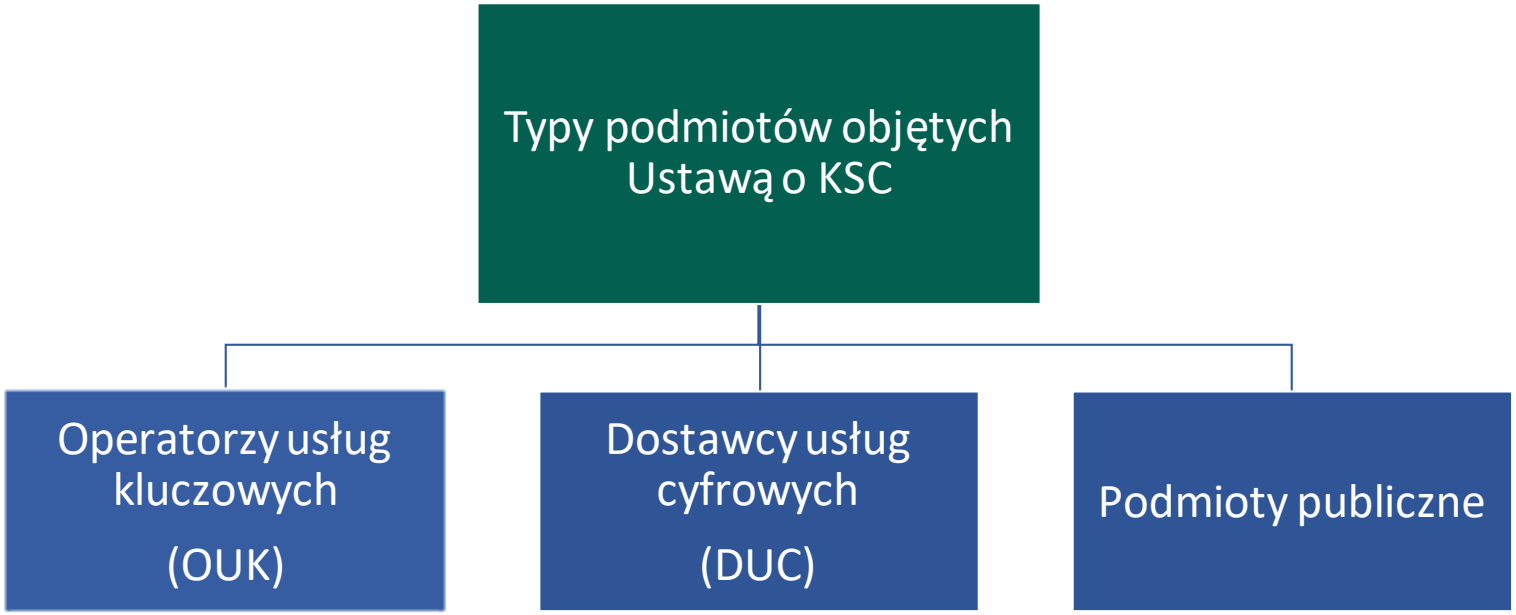
Organy właściwe

Organami właściwymi są ministrowie właściwi dla konkretnych działów administracji, którzy na podstawie porozumienia **mogą powierzyć realizację niektórych zadań jednostkom podległym lub nadzorowanym** (jeśli w danym sektorze funkcjonuje regulator sektorowy, może realizować funkcje organu właściwego, zamiast ministra).

Zadania organu właściwego:

- wydawanie decyzji, który z podmiotów może otrzymać status OUK (Operatora Usług Kluczowych);
- przygotowanie rekomendacji działań, które wzmocnią cyberbezpieczeństwo sektora;
- przeprowadzanie kontroli podległych operatorów.

Organ właściwy ds. cyberbezpieczeństwa	Sektor/podsektor
Minister właściwy ds. energii	Energia
Minister właściwy ds. transportu	Transport
Minister właściwy ds. gospodarki morskiej i minister właściwy ds. żeglugi śródlądowej	Transport wodny
Komisja Nadzoru Finansowego	Bankowy, Infrastruktura rynków finansowych
Minister właściwy ds. zdrowia	Ochrona zdrowia
Minister właściwy ds. gospodarki wodnej	Zaopatrzenie w wodę pitną i jej dystrybucja
Minister właściwy ds. informatyzacji	Infrastruktura cyfrowa
	Dostawcy usług cyfrowych
Minister Obrony Narodowej (podmioty podległe MON oraz przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym)	Ochrona zdrowia
	Infrastruktura cyfrowa
	Dostawcy usług cyfrowych


Typy podmiotów objętych Ustawą o KSC
Operatorzy usług kluczowych (OUK)
Dostawcy usług cyfrowych (DUC)
Podmioty publiczne

Operatorzy usług kluczowych (OUK)

Operatorzy usług kluczowych to przedsiębiorstwa lub instytucje, które świadczą usługi zależne od systemu teleinformatycznego o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej i gospodarczej państwa.

Ustawa wskazuje następujące sektory, w których funkcjonują operatorzy usług kluczowych:

- Sektor energetyczny
- Sektor transportowy
- Sektor bankowy i infrastruktury rynków finansowych
- Sektor ochrony zdrowia
- Sektor zaopatrzenia w wodę pitną (wraz z dystrybucją)
- Sektor infrastruktury cyfrowej

Operatorzy usług kluczowych (OUK)

Organy właściwe identyfikują operatorów na podstawie**:**

- świadczenia usługi kluczowej w jednym ze wskazanych sektorów;
- pełniącej usługi, która musi zależeć od systemów informatycznych;
- wystąpienie incydentu ma istotny skutek zakłócający dla świadczenia tej usługi.

Kryteria przy ustalaniu progów istotności skutku zakłócającego – OUK (Rozdział 2, art. 6 ust. 2 pkt a-g)

Dla każdej z wymienionych w wykazie usług określono próg istotności skutku zakłócającego, który pozwala zakwalifikować usługę jako kluczową.

Progi zostały określone z uwzględnieniem następujących kryteriów:

- liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot;
- zależność innych sektorów gospodarki od usługi świadczonej przez podmiot;
- wpływ, jaki mógłby mieć incydent, ze względu na jego skalę i czas trwania na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne;
- udział podmiotu świadczącego usługę kluczową w rynku;
- zasięg geograficzny obszaru, którego mógłby dotyczyć incydent;
- zdolność podmiotu do utrzymywania wystarczającego poziomu świadczenia usługi kluczowej, przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia;
- inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują.

Obowiązki operatorów usług kluczowych (OUK)

- **Wdrożenie systemu zarządzania bezpieczeństwem** (systematyczne szacowanie ryzyka i dostosowanie do niego środków bezpieczeństwa).
- **Stworzenie wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo** lub zawarcie umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa.
- **Obsługa i zgłaszanie incydentów (niezwłocznie, nie później niż 24h od wykrycia incydentu).**
- **Przeprowadzanie audytu bezpieczeństwa systemu** informacyjnego wykorzystywanego do świadczenia usługi kluczowej **raz na 2 lata** (przy czym pierwszy w ciągu roku od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej).

Obsługa i zgłaszanie incydentów przez operatorów usług kluczowych (OUK)

- **Klasyfikacja incydentu** na podstawie kryteriów określonych przez Radę Ministrów w drodze rozporządzenia.
- W przypadku **zakwalifikowania incydentu jako poważny - zgłoszenie do właściwego CSIRT nie później niż w ciągu 24 godzin** od momentu wykrycia.
- Współdziałanie z CSIRT w ramach **obsługi incydentu** wraz z zapewnieniem odpowiedniego **dostępu do informacji.**
- **Usunięcie podatności systemu.**

obsługa incydentu – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie i przyznanie pierwszeństwa obsługi, a także podejmowanie działań naprawczych i ograniczenie skutków incydentu

zarządzanie incydentem – obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowanie wniosków z obsługi incydentu;

Dostawcy usług cyfrowych (DUC)

Dostawca usługi cyfrowej - podmiot świadczący usługę cyfrową w rozumieniu ustawy o świadczeniu usług drogą elektroniczną.

- **Internetowe platformy handlowe**
- **Usługi przetwarzania w chmurze**
- **Wyszukiwarki internetowe**

Dostawcy usług cyfrowych (DUC)

Obowiązki:

- **zapewnienie bezpieczeństwa systemów informacyjnych i obiektów;**
- **przekazanie informacji o incydencie do właściwego CSIRT nie później niż 24h od wykrycia;**
- **prowadzenie rejestru, analiz i klasyfikacji incydentów;**
- **zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej;**
- posiadanie aktualnego stanu wiedzy w tym **zgodność z normami międzynarodowymi;**
- **monitorowanie, audyt i testowanie.**

Podmioty publiczne

W skład krajowego systemu cyberbezpieczeństwa wchodzą również podmioty publiczne takie jak:

- Jednostki sektora finansów publicznych,
- Narodowy Bank Polski,
- Bank Gospodarstwa Krajowego,
- Urząd Dozoru Technicznego,
- Polska Agencja Żeglugi Powietrznej,
- Polskie Centrum Akredytacji,
- Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej,
- instytuty badawcze i spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej, których celem jest bieżące i nieprzerwane zaspokajanie zbiorowych potrzeb ludności w drodze świadczenia usług powszechnie dostępnych.

Obowiązki podmiotów publicznych

Podmiot publiczny realizujący zadanie publiczne zależne od systemu informacyjnego:

- **zapewnia zarządzanie incydentem w podmiocie publicznym;**
- **zgłasza incydent niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT;**
- **przekazuje zgłoszenie w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej, przy użyciu innych dostępnych środków komunikacji;**

Obowiązki podmiotów publicznych

Podmiot publiczny realizujący zadanie publiczne zależne od systemu informacyjnego:

- **zapewnia obsługę incydentu w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRT, przekazując niezbędne dane, w tym dane osobowe.**
- **wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami KSC w zakresie zadań publicznych zależnych od systemów informacyjnych.**

Klasyfikacja zgłaszanych incydentów

Poziom incydentu	Definicja	Nadawanie klasyfikacji	Konieczność raportowania
Poziom pierwszy	**incydent** zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo	brak	brak
Poziom drugi	**incydent poważny** powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej	operator usługi kluczowej	CSIRT GOV – operatorzy infrastruktury krytycznej CSIRT MON – podmioty podległe RON **CSIRT NASK** – pozostałe podmioty
	incydent istotny ma istotny wpływ na świadczenie usługi cyfrowej	dostawca usługi cyfrowej	**CSIRT NASK**
	incydent w podmiocie publicznym **powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego**	podmiot publiczny	CSIRT GOV **CSIRT NASK** CSIRT MON
Poziom trzeci	**incydent krytyczny** skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi	CSIRT MON CSIRT GOV **CSIRT NASK**	tak, ale właściwy CSIRT poziomu krajowego zadecyduje o klasyfikacji incydentu

Przydatne strony internetowe

cyberpolicy.nask.pl

www.cert.pl/ouch

www.cert.pl

Kontakt

Zespół Ćwiczeń i Szkoleń

Marcin Napiórkowski
Kamil Kuć

cwiczenia@nask.pl