Ministerstwo Cyfryzacji

Tu tworzymy przyszłość

# Nowy wymiar bezpieczeństwa cyfrowego

## Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa

# Wdrożenie dyrektywy NIS 2

Cele:

- skuteczniejsza ochrona przed cyberzagrożeniami
- zwiększenie bezpieczeństwa usług, z których korzystają obywatele
- lepsza ochrona danych

# Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC)

- wzmocnione kompetencje organów
- nowe podmioty objęte KSC
- sektorowe zespoły CSIRT
- sprawniejsze zgłaszanie incydentów
- możliwość identyfikacji dostawców wysokiego ryzyka

# Wzmocnione kompetencje organów

## Organy właściwe ds. cyberbezpieczeństwa

- ostrzeżenia
- monitoring realizacji obowiązków przez podmioty kluczowe i ważne
- nakazy - ocena bezpieczeństwa systemu, audyt bezpieczeństwa

## Minister Cyfryzacji

- polecenia zabezpieczające
- identyfikacja dostawców wysokiego ryzyka
- działania edukacyjne
- rozwój systemu S46

## Pełnomocnik Rządu ds. Cyberbezpieczeństwa

- rekomendacje
- żądanie informacji od organów
- zlecanie wykonania badań
- zakup oprogramowania dla uczestników posiedzeń PCOC

# Cyberbezpieczeństwo bez luk:

## nowe sektory ze wzmocnioną ochroną

### Sektory kluczowe

- zbiorowe odprowadzanie ścieków
- zarządzanie usługami ICT
- przestrzeń kosmiczna

### Sektory ważne

- usługi pocztowe
- inwestycje energetyki jądrowej
- produkcja i dystrybucja chemikaliów oraz żywności
- produkcja – ogólnie
- dostawcy usług cyfrowych
- badania naukowe
- gospodarowanie odpadami

# Podmioty kluczowe i ważne

## nowe obowiązki

- wzmocnione zarządzanie ryzykiem dla bezpieczeństwa sieci i systemów IT
- odpowiedzialność kierownika za cyberbezpieczeństwo
- zgłaszanie incydentów **za pomocą systemu S46** do zespołów CSIRT
- rejestracja w wykazie

# Dostawcy wysokiego ryzyka

## schemat postępowania

1. **WSZCZĘCIE POSTĘPOWANIA PRZEZ MINISTRA CYFRYZACJI**
   z urzędu lub na wniosek Przewodniczącego Kolegium ds. Cyberbezpieczeństwa

2. **ZAWIADOMIENIE STRON**
   oraz Prokuratora Generalnego

3. **STANOWISKA ORGANIZACJI SPOŁECZNYCH**
   termin: 14 dni

4. **OPINIA KOLEGIUM DS. CYBERBEZPIECZEŃSTWA**
   termin: 3 miesiące

5. **DECYZJA MINISTRA CYFRYZACJI**
   w sprawie uznania danego dostawcy za dostawcę wysokiego ryzyka

6. **MOŻLIWOŚĆ ZŁOŻENIA SKARGI DO SĄDU ADMINISTRACYJNEGO**

7. **WYKONANIE DECYZJI**
   obowiązek wycofania z użycia konkretnych typów sprzętu i oprogramowania wskazanych w decyzji – co do zasady w ciągu 7 lat

8. **KONTROLA WYKONANIA**
   monitorowanie wykonania decyzji przez organy właściwe ds. cyberbezpieczeństwa

Ministerstwo Cyfryzacji

Tu tworzymy przyszłość

# Nowy wymiar bezpieczeństwa cyfrowego

## Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa