#cyberbezpieczeństwo

Projekt ustawy o krajowym systemie cyberbezpieczeństwa

Wdrożenie dyrektywy NIS 2

#cyberbezpieczeństwo

Tło nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa

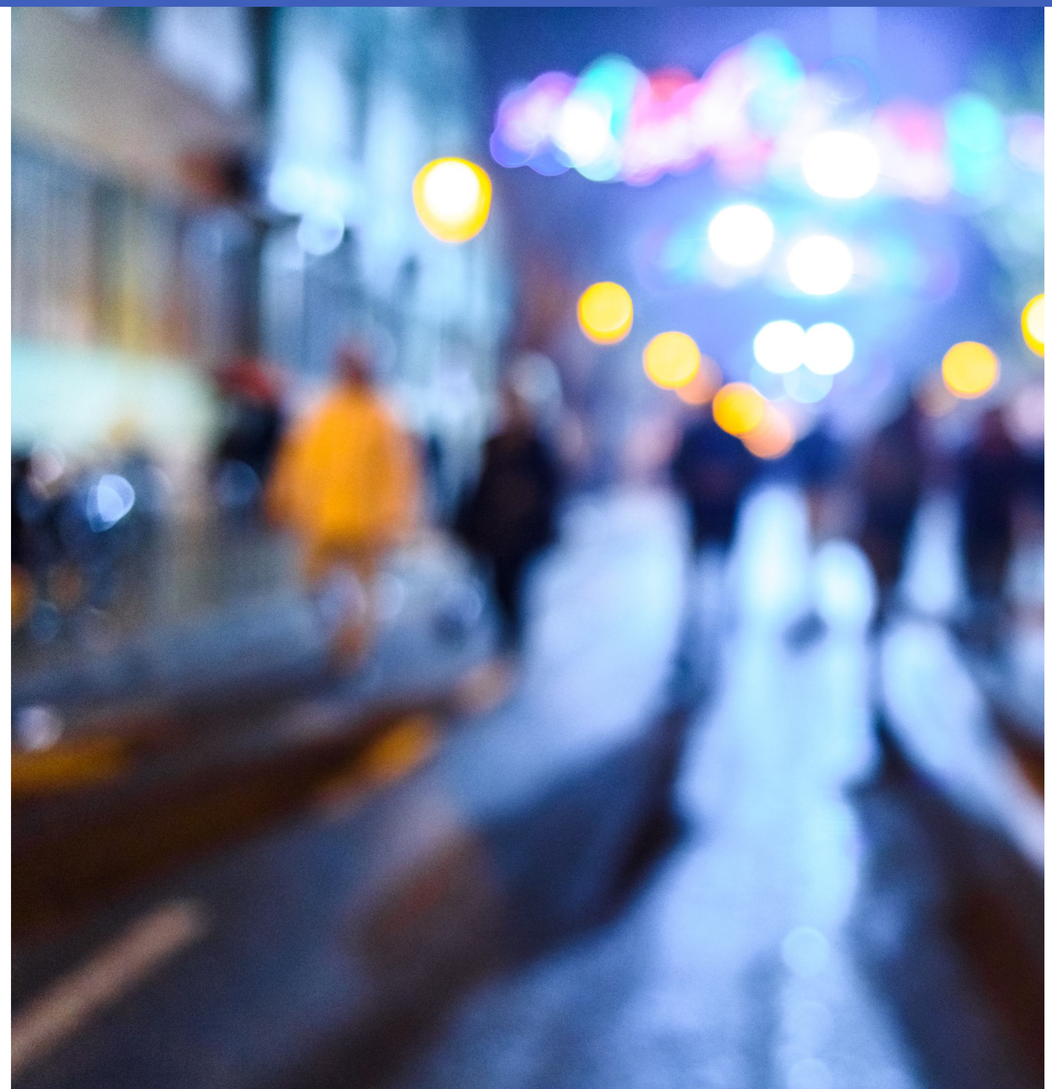
- **Dyrektywa NIS 2**
- **Toolbox 5G** (zestaw środków dot. minimalnej harmonizacji i standaryzacji na poziomie UE rozwiązań cyberbezpieczeństwa sieci 5G)
- **Krajowy Plan Odbudowy i Zwiększania Odporności**

MC

#cyberbezpieczeństwo

Najważniejsze zmiany

- Przepisy ogólne
- Podmioty kluczowe i podmioty ważne
- CSIRT sektorowe
- Ocena bezpieczeństwa
- System S46 i Pojedynczy Punkt Kontaktowy
- Dostawca Wysokiego Ryzyka
- Polecenie zabezpieczające
- Nadzór i środki egzekwowania przepisów
- Kary pieniężne
- Strategia Cyberbezpieczeństwa RP i Krajowy Plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie



MC

#cyberbezpieczeństwo

Podmioty kluczowe i ważne

- Status podmiotu kluczowego lub ważnego nabywany jest z mocy prawa w przypadku spełnienia warunków
- Obowiązek rejestracji w wykazie podmiotów kluczowych i ważnych
- Operatorzy usług kluczowych zostaną automatycznie wpisani do wykazu
- Szczególny tryb uznania za podmiot kluczowy lub ważny – decyzja administracyjna

MC

#cyberbezpieczeństwo

Podmioty kluczowe i ważne - obowiązki

1

Podejście oparte na ryzyku dla tysięcy nowych podmiotów

2

Nowe zasady zgłaszania incydentów do jednostek CSIRT

3

Obowiązek przeprowadzania audytów bezpieczeństwa

MC

#cyberbezpieczeństwo

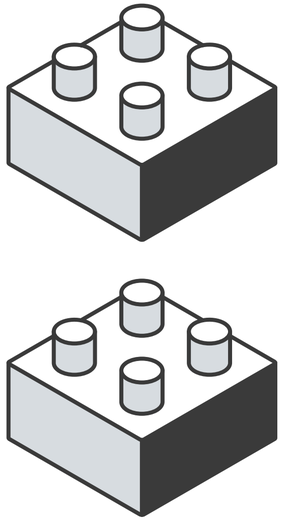
Terminy - projekt

1

miesiąc od dnia ogłoszenia – wejście w życie

6

miesięcy okresu dostosowawczego do nowych obowiązków dla podmiotów kluczowych i podmiotów ważnych



#cyberbezpieczeństwo

Zespoły CSIRT

Powołanie CSIRT sektorowych
Rozszerzenie zadań zespołów CSIRT poziomu krajowego w szczególności:

- doprecyzowanie kompetencji zespołów do badania produktów ICT
- prowadzenie oceny bezpieczeństwa
- CSIRT NASK będzie pełnił rolę koordynatora na potrzeby skoordynowanego ujawniania podatności

MC

#cyberbezpieczeństwo

Ocena bezpieczeństwa

Przeprowadza
CSIRT MON, CSIRT
NASK, CSIRT GOV
lub CSIRT sektorowy

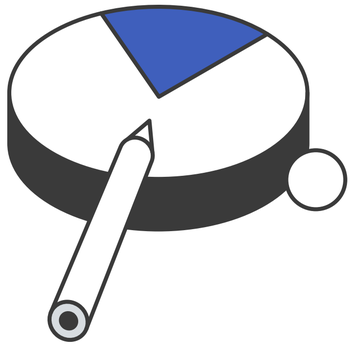
Minimalizacja
zakłócenia pracy
systemu

Prowadzona:

- za zgodą podmiotu KSC

lub

- na zlecenie organu właściwego ds. cyberbezpieczeństwa



Identyfikacja
podatności tego
systemu

#cyberbezpieczeństwo

System S46 i Pojedynczy Punkt Kontaktowy

System S46
= Główny Środek Komunikacji Pomiędzy Podmiotami KSC

Rezygnacja z zawierania porozumienia o dołączeniu do systemu

Cloud First Policy w zakresie S46

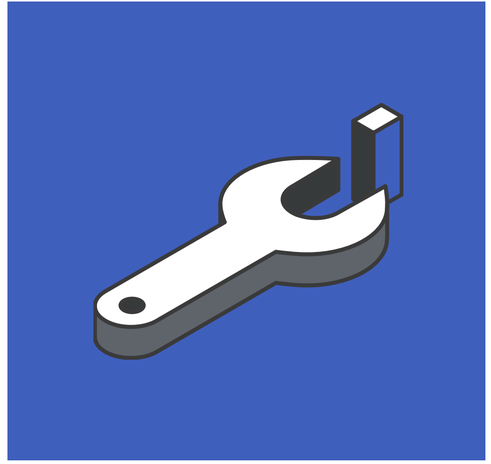
3 miesięczny termin na wdrożenie minimalnych wymagań technicznych i funkcjonalnych podłączenia do systemu

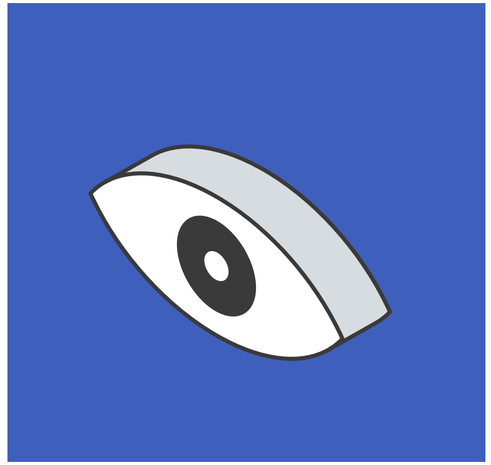
Pojedynczy punkt kontaktowy

MC

#cyberbezpieczeństwo

Nadzór i środki egzekwowania przepisów





- Ostrzeżenia, nakazy i decyzje administracyjne nakazujące podjęcie lub zaniechanie określonego działania
- Nadzór prewencyjny i następczy nad podmiotami kluczowymi oraz nadzór wyłącznie następczy nad podmiotami ważnymi
- Rozbudowanie systemu nadzoru i środków egzekwowania przepisów i wyposażenie organów nadzorczych w szerokie kompetencje
- Uprawnienie do zwracania się do właściwych organów o zawieszenie lub cofnięcie zezwolenia czy koncesji, a nawet zakazanie pełnienia określonej funkcji
- Metodyki nadzoru i hierarchia priorytetów działań nadzorczych jako ułatwienie dla organów nadzorczych i efektywniejsze sprawowanie nadzoru

MC

#cyberbezpieczeństwo

Minister właściwy do spraw informatyzacji - kompetencje

1

Prowadzenie wykazu podmiotów kluczowych i ważnych

2

Przygotowywanie i monitorowanie wykonania Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę

3

Organ odpowiedzialny za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze cywilnym

MC

#cyberbezpieczeństwo

Pełnomocnik Rządu ds. Cyberbezpieczeństwa

- Bezpośrednie wskazanie, kto może zostać Pełnomocnikiem Rządu ds. Cyberbezpieczeństwa
- Zlecanie przeprowadzenia badań i ekspertyz
- Tworzenie zespołów roboczych
- Koordynacja Połączonego Centrum Operacji w Cyberprzestrzeni i współpraca z innymi organami państwowymi

MC

#cyberbezpieczeństwo

Kolegium ds. Cyberbezpieczeństwa

- Rozbudowa składu Kolegium ds. Cyberbezpieczeństwa
- Rozbudowa zakresu zadań Kolegium ds. Cyberbezpieczeństwa
- Rozbudowa kompetencji przewodniczącego Kolegium
- Usprawnienie funkcjonowania Kolegium

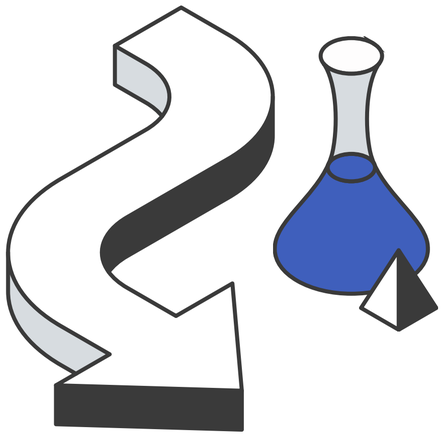
MC

#cyberbezpieczeństwo

Dostawca wysokiego ryzyka (HRV)

Nadzwyczajny środek służący ochronie kluczowych rodzajów działalności

7 lat lub 4 lata na wycofanie ze swoich systemów sprzętów produktów dostawcy wysokiego ryzyka



Wskazanie dostawcy Wysokiego Ryzyka odbywa się w drodze decyzji administracyjnej Ministra Cyfryzacji

MC

#cyberbezpieczeństwo

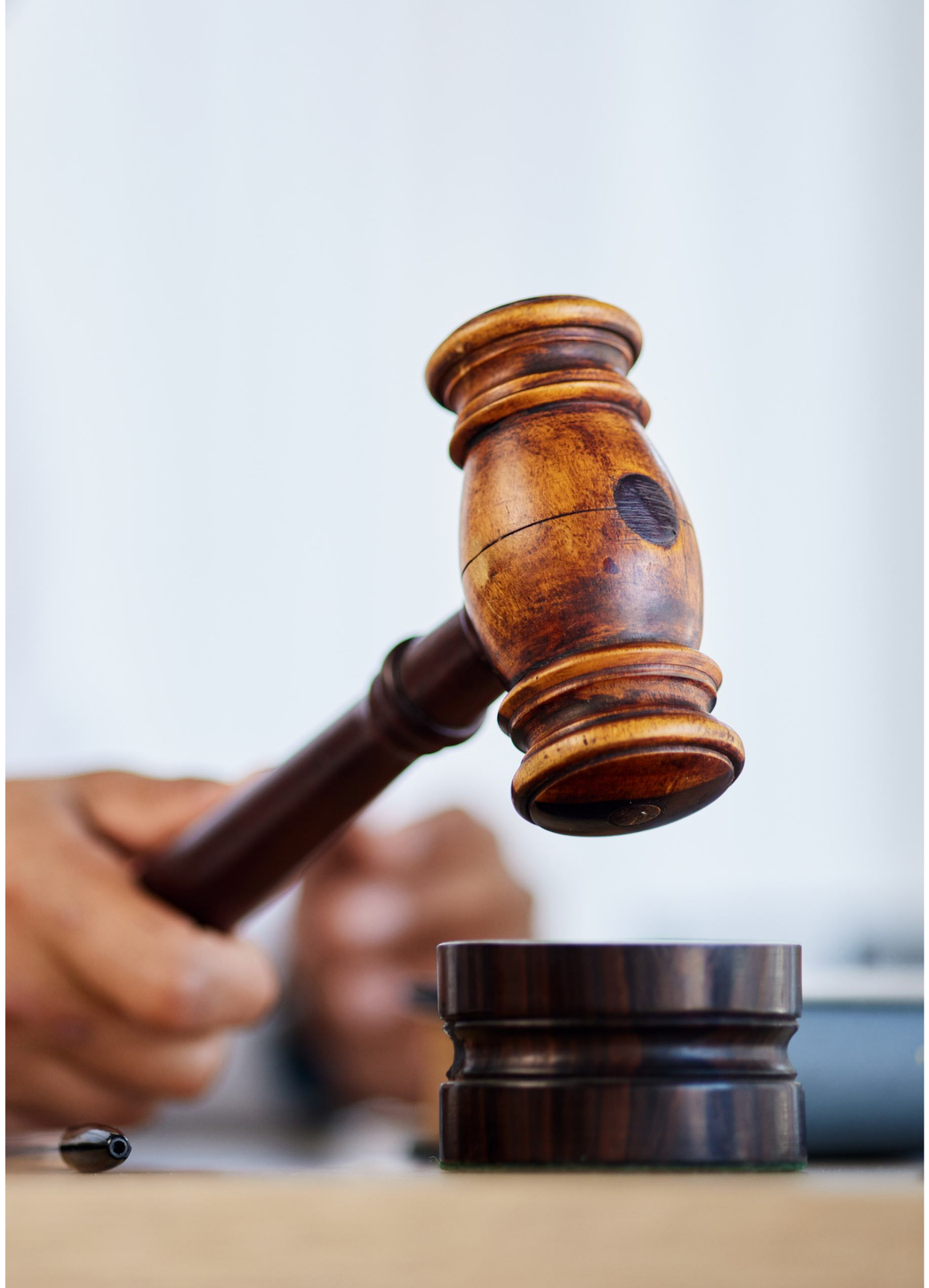
Polecenie zabezpieczające

- Wydawane przez Ministra Cyfryzacji w drodze decyzji
- Publikowane w Dz. Urz. Ministra Cyfryzacji oraz informacyjnie w BIP
- Nadzwyczajny środek, możliwy do zastosowania tylko w przypadku wystąpienia incydentu krytycznego
- Określa rodzaje podmiotów do których jest skierowane oraz zachowanie jakie należy podjąć dla przeciwdziałania skutkom incydentu krytycznego
- Wydawane na czas koordynacji obsługi incydentu krytycznego

#cyberbezpieczeństwo

Kary pieniężne

- Kary adekwatne, proporcjonalne i odstraszające
- Rozbudowany katalog przypadków określających kiedy podmioty kluczowe i ważne podlegają karze pieniężnej
- Kary pieniężne nakładane na kierownika podmiotu kluczowego lub ważnego
- Nowe formy i procedury wymierzania kar pieniężnych
- Okresowe kary pieniężne w celu przymuszenia podmiotu kluczowego lub ważnego do realizacji nałożonych na niego obowiązków



MC

#cyberbezpieczeństwo

Strategia Cyberbezpieczeństwa RP i Krajowy Plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie

- Rozszerzenie i uszczegółowienie treści Strategii
- możliwość uzyskiwania informacji przez Ministra Strategii na temat realizacji strategii od innych podmiotów zaangażowanych w jej realizację
- Zespoły CSIRT I Organy Właściwe Ds. Cyberbezpieczeństwa będą corocznie informować ministra o postępach we wdrażaniu strategii
- Plan Działań do Strategii
- Krajowy Plan Reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę

MC

#cyberbezpieczeństwo

Projekt ustawy o krajowym systemie cyberbezpieczeństwa

Wdrożenie dyrektywy NIS 2