NIS2

Dyrektywa Parlamentu Europejskiego i Rady (UE)
2022/2555 z dnia **14 grudnia 2022 r.**
w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii,
zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972
oraz uchylająca dyrektywę (UE) **2016/1148**

Łukasz Wojewoda

Co musimy osiągnąć?

Implementacja krajowa

do 17 października 2024

Ustanowienie wykazu podmiotów kluczowych i ważnych, a także podmiotów świadczących usługi rejestracji nazw domen

do 17 kwietnia 2025

Dlaczego implementacja będzie wyzwaniem

Brak noweli uKSC	Zwiększony zakres podmiotowy	Zwiększony zakres przedmiotowy
Nowe aspekty wymagane do rozważenia (np. łańcuch dostaw)	Kary	Finansowanie….?

Jak musimy wdrożyć NIS2?

Minimalna harmonizacja

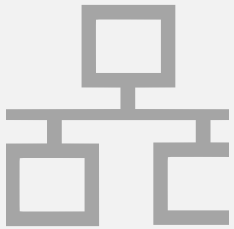
Dyrektywa nie uniemożliwia państwom członkowskim przyjęcia lub utrzymania przepisów zapewniających wyższy poziom cyberbezpieczeństwa, pod warunkiem że takie przepisy są spójne z obowiązkami państw członkowskich, ustanowionymi w prawie Unii.

Co muszą zrobić podmioty?

Wprowadzić odpowiednie i proporcjonalne
środki **techniczne, operacyjne i organizacyjne**
w celu **zarządzania ryzykiem** dla bezpieczeństwa sieci i systemów informatycznych
wykorzystywanych przez te podmioty do
prowadzenia działalności lub świadczenia usług oraz
w celu **zapobiegania wpływowi incydentów** na
odbiorców ich usług lub na **inne usługi** bądź
minimalizowania takiego wpływu

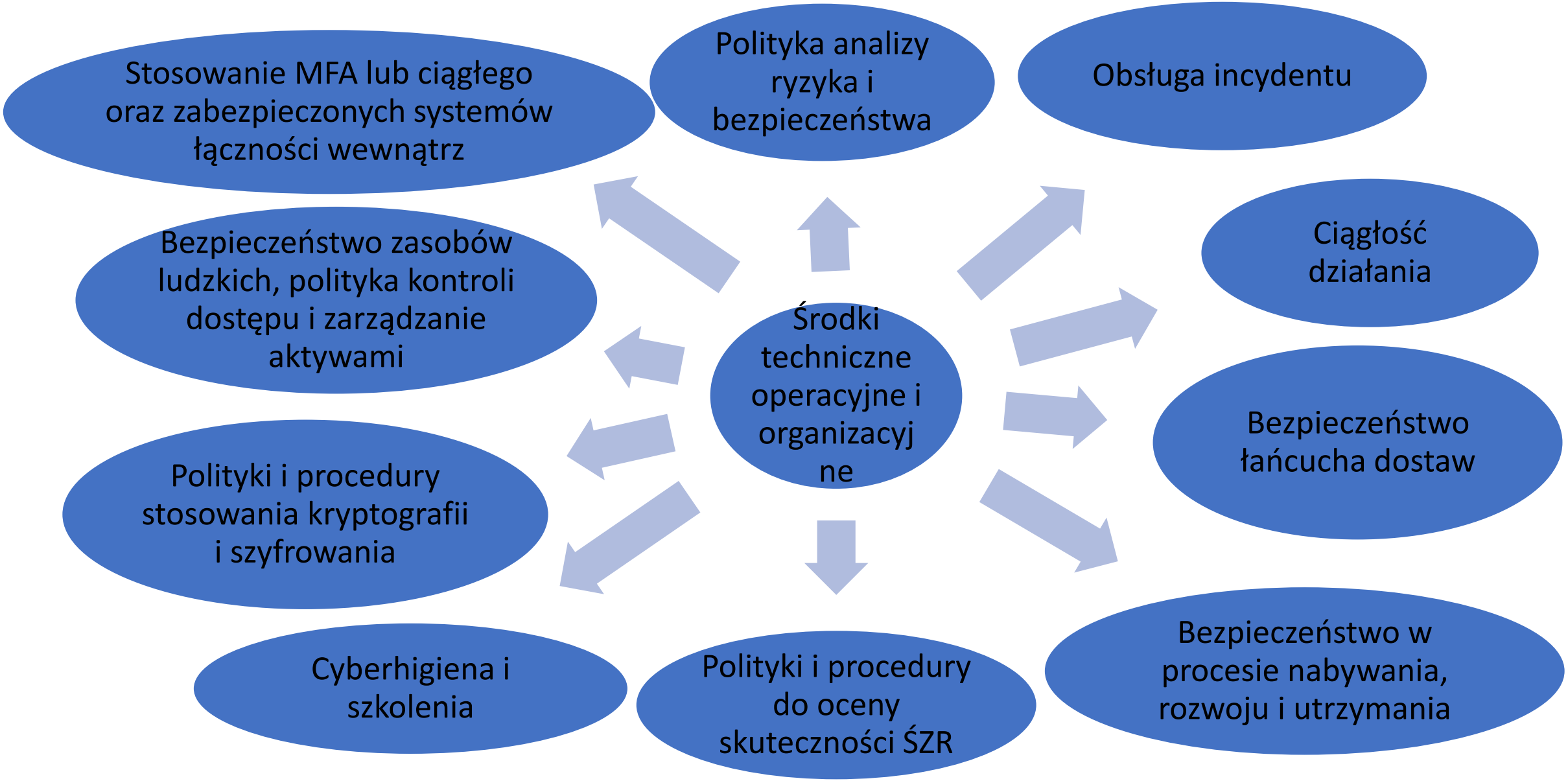
Co uwzględniają odpowiednie i proporcjonalne środki?

wszystkie zagrożenia



podejście mające na celu **ochronę sieci i systemów informatycznych** oraz **środowiska fizycznego tych systemów** przed incydentami

Co obejmują


Środki techniczne operacyjne i organizacyjne
Polityka analizy ryzyka i bezpieczeństwa
Obsługa incydentu
Ciągłość działania
Bezpieczeństwo łańcucha dostaw
Bezpieczeństwo w procesie nabywania, rozwoju i utrzymania
Polityki i procedury do oceny skuteczności ŚZR
Cyberhigiena i szkolenia
Polityki i procedury stosowania kryptografii i szyfrowania
Bezpieczeństwo zasobów ludzkich, polityka kontroli dostępu i zarządzanie aktywami
Stosowanie MFA lub ciągłego oraz zabezpieczonych systemów łączności wewnątrz

Skoordynowane Szacowanie Ryzyka

Podmioty będą musiały uwzględniać wyniki **skoordynowanych oszacowań ryzyka** dla bezpieczeństwa **krytycznych łańcuchów dostaw**

Grupa Współpracy we współpracy z Komisją i ENISA może przeprowadzać skoordynowane szacowanie ryzyka dla bezpieczeństwa określonych krytycznych łańcuchów dostaw usług ICT, systemów ICT lub produktów ICT, z uwzględnieniem **technicznych** i, w stosownych przypadkach, **pozatechnicznych** czynników ryzyka

Zakres przedmiotowy

- Obowiązek ustanowienia w każdym państwie krajowego planu reagowania na incydenty i kryzysy
- Umocowanie European Cyber Crisis Liaison Organisation Network (CyCLONe)
- Zmiany w krajowej strategii cyberbezpieczeństwa:
  - obowiązek ustanowienia polityki koordynacji między organami właściwymi w sprawach zarządzania kryzysowego a organami realizującymi zadania z NIS 2.0
- Peer Review
- Zwiększenie kompetencji nadzorczych np.:
  - możliwość wydawania wiążących instrukcji dla podmiotów kluczowych
  - możliwość nakazania przeprowadzenia *security scan* wobec *podmiotów ważnych*

Zakres podmiotowy – podmioty kluczowe

[…]

✓inne podmioty:

- ➢podmiot jest jedynym w danym państwie członkowskim dostawcą usługi, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej;
- ➢zakłócenie usługi świadczonej przez podmiot mogłoby mieć znaczący wpływ na porządek publiczny, bezpieczeństwo publiczne lub zdrowie publiczne;
- ➢zakłócenie usługi świadczonej przez podmiot mogłoby prowadzić do powstania poważnego ryzyka systemowego

Zgłaszanie incydentów

podmioty kluczowe i ważne bez zbędnej zwłoki zgłaszają swojemu właściwemu CSIRT […], incydent mający istotny wpływ na świadczenie przez nie usług, […](poważny incydent)

w stosownych przypadkach dane podmioty bez zbędnej zwłoki **powiadamiają odbiorców swoich usług** o poważnych incydentach, które **mogą mieć niekorzystny wpływ na świadczenie tych usług**.

Incydent poważny

spowodował lub może spowodować dotkliwe zakłócenia operacyjne usług lub straty finansowe dla danego podmiotu

wpłynął lub jest w stanie wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe i niemajątkowe

Motyw (101)

[…] Wskaźniki takie jak

- zakres skutków dla funkcjonowania usługi,
- czas trwania incydentu lub
- liczba dotkniętych nim odbiorców usług

mogą odegrać ważną rolę w ustaleniu, czy zakłócenie operacyjne usługi jest dotkliwe

Czas na zgłaszanie incydentów

bez zbędnej zwłoki,
a w każdym razie w ciągu
24 godzin od powzięcia
wiedzy o poważnym
incydencie – wczesne
ostrzeżenie

bez zbędnej zwłoki,
a w każdym razie w ciągu
72 godzin od powzięcia
wiedzy o poważnym
incydencie – zgłoszenie
incydentu

CSIRT

- każdy CSIRT ma dysponować odpowiednią, bezpieczną i odporną infrastrukturą teleinformatyczną służącą wymianie informacji z podmiotami kluczowymi i ważnymi
- CSIRT współpracują z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych i ważnych oraz, w odpowiednich przypadkach, wymieniają z nimi stosowne informacje
- CSIRT mogą prowadzić aktywne, nieinwazyjne skanowanie publicznie dostępnych sieci i systemów podmiotów kluczowych i ważnych

Kary

Kary pieniężne nakładane na podmioty kluczowe i ważne za naruszenie obowiązków określonych w dyrektywie mają być skuteczne, proporcjonalne i odstraszające

Podmioty kluczowe/ważne naruszające obowiązki podlegają administracyjnym karom pieniężnym w maksymalnej wysokości co najmniej 10/7 mln EUR lub 2/1,4 % łącznego rocznego światowego obrotu

Co dalej?

warsztaty / spotkania

konferencje / fora / dedykowane aktywności

prowizorium zapisów regulacyjnych

formalny proces legislacyjny

Dziękuję za uwagę.