NASK

Dyrektywa NIS 2

Czy JST mają się czego bać?

nask.pl

Monika Stachoń
Dział Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni

Dyrektywa NIS 2 – główne zmiany

Nowe sektory (lub rozszerzenie wcześniej objętych działaniem NIS sektorów).

Wielkość podmiotu jako jednolite kryterium.

W niektórych przypadkach stosowanie dyrektywy także do **małych i mikro przedsiębiorstw**.

Podział na **podmioty kluczowe i ważne** w miejsce OUK i DUZ.

Zwiększone i uelastycznione obowiązki podmiotów.

Wzmocniony **nadzór**.

Rozszerzone **obowiązki CSIRT**.

Rozszerzony zakres **krajowych strategii cyberbezpieczeństwa**.

Skoordynowane ujawnianie podatności.

Krajowe ramy **zarządzania kryzysowego** w cyberbezpieczeństwie.

Sektory kluczowe i ważne

Sektory kluczowe:

- **Energetyka (Energia elektryczna, Centralne ogrzewanie i chłodzenie, Ropa naftowa, Gaz, Wodór)**
- Transport (lotniczy, kolejowy, wodny, lądowy)
- Bankowość
- Infrastruktura rynków finansowych
- **Zdrowie**
- Woda pitna
- **Ścieki**
- **Infrastruktura cyfrowa**
- **Zarządzanie usługami ICT**
- **Administracja publiczna**
- **Przestrzeń kosmiczna**

Sektory ważne:

- **Usługi pocztowe i kurierskie,**
- **Gospodarowanie odpadami,**
- **Produkcja, wytwarzanie i dystrybucja chemikaliów,**
- **Produkcja, przetwarzanie i dystrybucja żywności,**
- **Produkcja (wyroby medyczne i wyroby medyczne do diagnostyki in vitro, produkty komputerowe, elektroniczne i optyczne; urządzenia elektryczne; maszyny i urządzenia; pojazdy samochodowe, przyczepy i naczepy; inny sprzęt transportowy)**
- Dostawcy usług cyfrowych,
- **Badania naukowe.**

Podmioty kluczowe

Co do zasady **za podmioty kluczowe uznaje się podmioty z sektorów kluczowych** przekraczające pułapy dla średnich przedsiębiorstw.

Za **podmioty kluczowe dodatkowo** uznaje się:

- kwalifikowanych **dostawców usług zaufania** i **rejestry nazw domen najwyższego poziomu**, a także **dostawców usług DNS**, niezależnie od ich wielkości;
- **dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej**, które kwalifikują się jako średnie przedsiębiorstwa;
- **podmioty administracji publicznej**
- jeżeli państwo członkowskie tak postanowi, podmioty, które to państwo członkowskie wskazało przed wejściem w życie NIS2 jako **operatorów usług kluczowych**
- podmioty wskazane jako **podmioty krytyczne** na podstawie przepisów dyrektywy o odporności podmiotów krytycznych (CER)

NASK

Podmioty ważne

Podmiotami ważnymi są podmioty z sektorów kluczowych i ważnych, które nie kwalifikują się jako podmioty kluczowe.

NASK

Podmioty kluczowe i ważne – dodatkowe kryterium

podmioty, o których mowa w załączniku I lub II, które **zostaną uznane przez państwo członkowskie** jako kluczowe (lub ważne), **niezależnie od ich wielkości:**

- **jedyny dostawca usługi kluczowej** dla utrzymania krytycznej działalności społecznej lub gospodarczej;
- znaczący wpływ zakłócenia świadczonej usługi na **porządek publiczny, bezpieczeństwo publiczne lub zdrowie publiczne**;
- **Poważne ryzyko systemowe o wpływie transgranicznym** spowodowane zakłóceniem świadczonej usługi;
- **szczególne znaczenie** na poziomie krajowym lub regionalnym dla sektora, rodzaju usługi lub współzależnych sektorów;

Jakie podmioty z sektora administracji publicznej będą objęte NIS 2?

- **na poziomie rządu centralnego**, zdefiniowanym przez państwo członkowskie, zgodnie z prawem krajowym

- **na poziomie regionalnym**, zdefiniowanym przez państwo członkowskie zgodnie z prawem krajowym, który zgodnie z oceną opartą na analizie ryzyka świadczy usługi, których zakłócenie mogłoby mieć znaczący wpływ na krytyczną działalność społeczną lub gospodarczą

NASK

Obowiązki podmiotów kluczowych i ważnych

Proporcjonalne środki zarządzania ryzykiem w cyberbezpieczeństwie

Zgłaszanie incydentów poważnych do odpowiedniego CSIRT/właściwego organu;

Obowiązkowe **szkolenia** dla kadry kierowniczej oraz zalecane dla pracowników

W stosownych wypadkach **powiadamianie odbiorców usług** o poważnych incydentach oraz środkach zaradczych

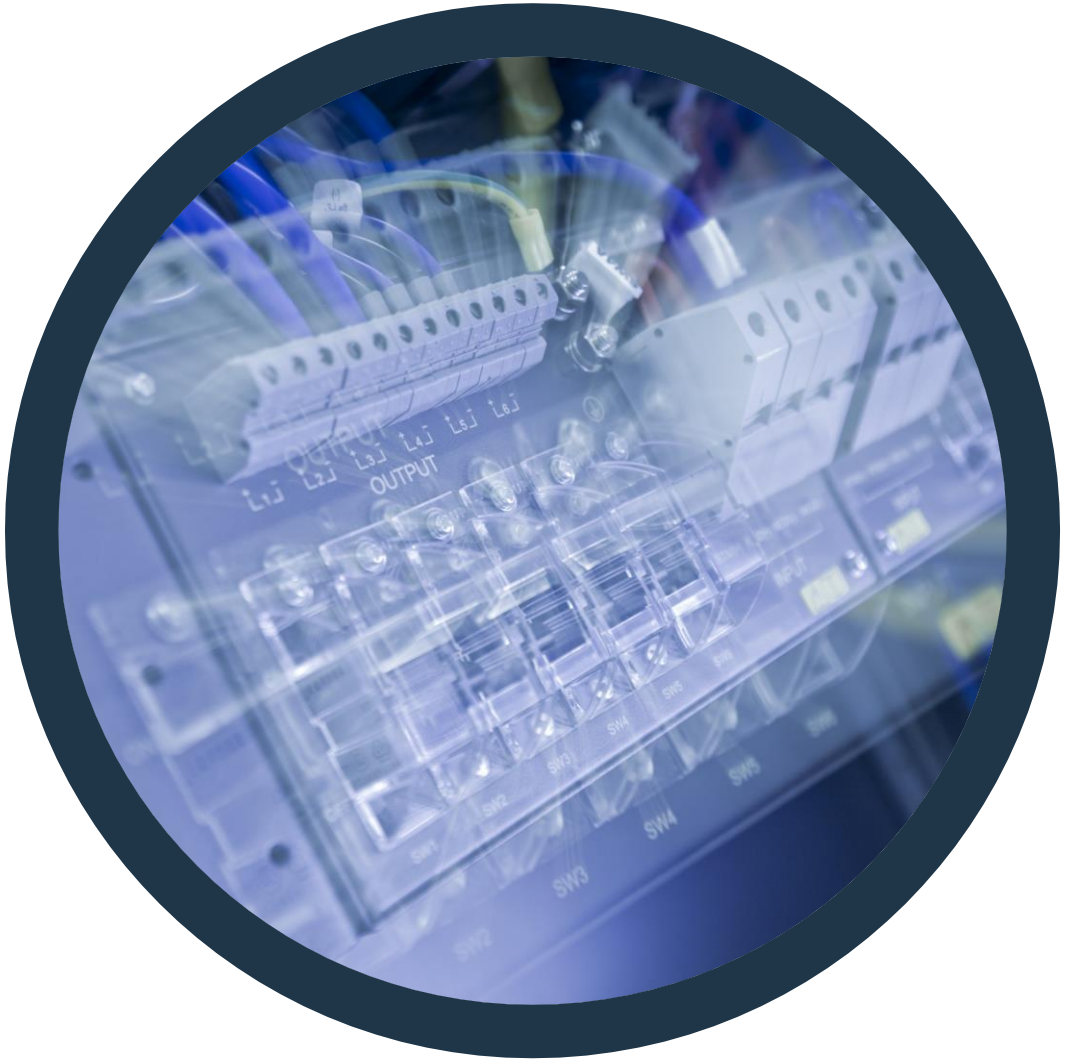
Stosowanie własnych lub nabytych **certyfikowanych produktow, usług i procesów.**

Zalecane **korzystanie z kwalifikowanych usług zaufania**

Zawiadamianie o **uczestnictwie w mechanizmach wymiany informacji**

Środki zarządzania ryzykiem

- polityka **analizy ryzyka** i bezpieczeństwa systemów informatycznych;
- **obsługa incydentu**;
- zapewnienie **ciągłości działania**, w tym zarządzanie kryzysowe;
- **bezpieczeństwo łańcucha dostaw**;
- bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym **postępowanie w przypadku podatności i ich ujawnianie**;
- polityki i procedury służące **ocenie skuteczności środków zarządzania ryzykiem** w cyberbezpieczeństwie;
- podstawowe praktyki **cyberhigieny** i szkolenia w zakresie cyberbezpieczeństwa;
- stosowanie **kryptografii** i, w stosownych przypadkach, szyfrowania;
- **bezpieczeństwo zasobów ludzkich**, polityka kontroli dostępu i zarządzanie aktywami;
- w stosownych przypadkach – **stosowanie 2FA**, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności w sytuacjach nadzwyczajnych.



Środki nadzoru i egzekwowania przepisów

- Środki nadzoru i egzekwowania prawa **powinny być**
  - ✓ skuteczne,
  - ✓ proporcjonalne,
  - ✓ odstraszające i
  - ✓ nakładane stosownie do indywidualnego przypadku.

✓ Istnieją różnice w środkach nadzoru i egzekwowania przepisów w stosunku do podmiotów kluczowych i ważnych.

✓ **Każda osoba fizyczna** odpowiedzialna za podmiot kluczowy lub działająca w charakterze przedstawiciela prawnego tego podmiotu **może być pociągnięta do odpowiedzialności** za niewywiązanie się z obowiązku zapewnienia przestrzegania niniejszej dyrektywy.

Administracyjne kary pieniężne

Wysokość kar administracyjnych to **maksymalnie**:

Podmioty kluczowe	Podmioty ważne
Co najmniej 10 000 000 EUR lub co najmniej 2% rocznego światowego obrotu	Co najmniej 7 000 000 EUR lub co najmniej 1,4% rocznego światowego obrotu

NASK