Dzień IOD 2024

# NIS2

- 80% nadal musi odpowiednio zabezpieczyć swoje łańcuchy dostaw
- 76% musi ocenić skuteczność istniejących środków cybernetycznych
- 74% musi dodać nowe środki zarządzania ryzykiem
- 76% musi wdrożyć zabezpieczenia HR
- 72% nadal musi zapewnić pracownikom szkolenia z zakresu cyberbezpieczeństwa

# Dlaczego NIS2?

·niewystarczający poziom cyberodporności przedsiębiorstw działających w UE

·niespójna odporność w poszczególnych państwach członkowskich i sektorach

·niewystarczające wspólne zrozumienie głównych zagrożeń i wyzwań przez państwa członkowskie

·brak wspólnego reagowania kryzysowego

· **Źródło:** https://www.infosecurity-magazine.com/news/third-organizations-comply-nis2/

# Załącznik I

## Sektory kluczowe

- Energetyka
- Transport
- Bankowość
- Infrastruktura rynków finansowych
- Opieka zdrowotna
- Woda pitna
- Ścieki
- Infrastruktura cyfrowa
- Zarządzanie usługami ICT (między przedsiębiorstwami)
- Podmioty administracji publicznej
- Przestrzeń kosmiczna

# Załącznik II

## Sektory ważne

- Usługi pocztowe i kurierskie
- Gospodarowanie odpadami
- Produkcja, wytwarzanie i dystrybucja chemikaliów
- Produkcja, przetwarzanie i dystrybucja żywności
- Produkcja
- Dostawcy usług cyfrowych
- Badania naukowe

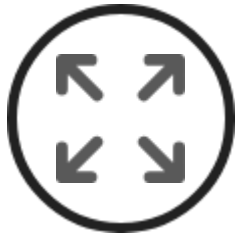
**średnie i duże** przedsiębiorstwa w powyższych sektorach będą objęte dyrektywą NIS 2

NIS2

# Podmioty kluczowe

NIS2

# Podmioty kluczowe



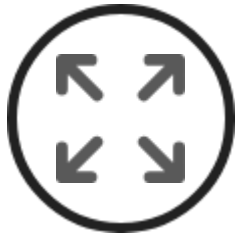
## a)

Podmioty w rodzaju tych, o których mowa w **załączniku I, przekraczające pułapy dla średnich przedsiębiorstw**

NIS2

# Podmioty kluczowe

[...]



## a)

Podmioty w rodzaju tych, o których mowa w **załączniku I, przekraczające pułapy dla średnich przedsiębiorstw**

## b)

kwalifikowany dostawca usług zaufania i rejestry nazw domen najwyższego zaufania a także dostawców usług DNS, niezależnie od ich wielkości;

## c)

dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej, które kwalifikują się jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia 2003/361/WE;

## e)

inne podmioty w rodzaju tych, o których mowa w załączniku I lub II, które zostały wskazane przez państwo członkowskie jako podmioty kluczowe zgodnie z art. 2 ust. 2 lit. b)–e);

NIS2

# Podmioty ważne

NIS2

# Podmioty ważne

podmioty w rodzaju tych, o których **mowa w załączniku I lub II**, które **nie kwalifikują** się jako podmioty kluczowe [...], uznaje się za podmioty ważne

# Podmioty ważne

podmioty w rodzaju tych, o których **mowa w załączniku I lub II**, które **nie kwalifikują** się jako podmioty kluczowe […], uznaje się za podmioty ważne

podmioty wskazane w NIS2, jako ważne (wymieniono je w art. 2 ust. 2 lit. b-e NIS2)

# **CEL:** zapewnienie bezpieczeństwa **sieci i systemów informatycznych**

**„sieci i systemy informatyczne”**

a) **sieć łączności elektronicznej** zdefiniowaną w art. 2 pkt 1 dyrektywy (UE) 2018/1972
b) **urządzenie** lub **grupę wzajemnie połączonych lub powiązanych urządzeń,** z których co najmniej jedno, na podstawie programu, **automatycznie** przetwarza dane cyfrowe; lub
c) **dane cyfrowe** przechowywane, przetwarzane, pobierane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użycia, ochrony i utrzymania

**art. 6 pkt.1**

**CEL:** zapewnienie bezpieczeństwa **sieci i systemów informatycznych**

**„bezpieczeństwo sieci i systemów informatycznych”**

**odporność sieci i systemów informatycznych**, przy danym poziomie zaufania, na **wszelkie zdarzenia**, które mogą **naruszyć dostępność**, **autentyczność**, **integralność** lub **poufność** przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem

**art. 6 pkt.2**

**CEL:**
zapewnienie bezpieczeństwa sieci i systemów informatycznych

**podmioty ważne i kluczowe**

**analiza ryzyka**

**odpowiednie i proporcjonalne środki**

- techniczne
- operacyjne
- organizacyjne

# PROPORCJONALNOŚĆ ŚRODKÓW

•stopień narażenia podmiotu na ryzyko

•krytyczność podmiotu

•wielkość podmiotu

•prawdopodobieństwo wystąpienia incydentów

•dotkliwość incydentu, w tym skutki społeczne i gospodarcze

# FIZYCZNE I ŚRODOWISKOWE BEZPIECZEŃSTWO sieci i systemów informatycznych

## ochrona przed:

- kradzieżą
- pożarem
- powodzią
- awarią telekomunikacyjną
- awarią zasilania
- nieuprawnionym dostępem fizycznym do infrastruktury
- uszkodzeniem infrastruktury
- ingerencją w infrastrukturę

# WYMOGI BEZPIECZEŃSTWA

•polityka analizy ryzyka bezpieczeństwa informatycznego

•obsługa incydentu

•ciągłość działania

•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

•cyberhigiena i szkolenia

•polityki i procedury stosowania kryptografii

•bezpieczeństwo zasobów ludzkich, polityka kontroli dostępu i zarządzanie aktywami

# ORGANY ZARZĄDZAJĄCE

## podmiotów ważnych i kluczowych

•zatwierdzają środki zarządzania ryzykiem w cyberbezpieczeństwie

•nadzorują wdrażania środków zarządzania ryzykiem w cyberbezpieczeństwie

•odpowiedzialność

•obowiązkowe i regularne szkolenia

•wiedza i umiejętności pozwalające rozpoznać ryzyko i stosowanie praktyki zarządzania ryzykiem w cyberbezpieczeństwie

# ZGŁASZANIE INCYDENTÓW

## Co zgłaszamy?

# ZGŁASZANIE INCYDENTÓW

**Co zgłaszamy? ⟶ poważny incydent**

# ZGŁASZANIE INCYDENTÓW

**Co zgłaszamy?** → **poważny incydent**

↓

**ma istotny wpływ na świadczenie usług**

- spowodował lub może spowodować dotkliwe zakłócenia operacyjne
- straty finansowe dla danego podmiotu
- wpłynął lub jest w stanie wpłynąć na inne osoby fizyczne lub prawne powodując znaczne szkody majątkowe i niemajątkowe

# ZGŁASZANIE INCYDENTÓW

**Co zgłaszamy?** ⟶ **poważny incydent**

**Komu?**

# ZGŁASZANIE INCYDENTÓW

**Co zgłaszamy? ⟶ poważny incydent**

**Komu? ⟶ CSIRT / właściwy organ**

# ZGŁASZANIE INCYDENTÓW

**Co zgłaszamy?** ⟶ **poważny incydent**

**Komu?** ⟶ **CSIRT / właściwy organ**

**Kiedy?** ⟶

# ZGŁASZANIE INCYDENTÓW

**Co zgłaszamy?** ⟶ **poważny incydent**

**Komu?** ⟶ **CSIRT / właściwy organ**

**Kiedy?** ⟶ **24 godziny –**
wstępne ostrzeżenie

# ZGŁASZANIE INCYDENTÓW

**Co zgłaszamy?** ⟶ **poważny incydent**

**Komu?** ⟶ **CSIRT / właściwy organ**

**Kiedy?** ⟶ **24 godziny –**
wstępne ostrzeżenie

- czy incydent spowodowany **czynem niezgodnym** z **prawem** lub popełniony **w złym zamiarze**
- czy incydent może mieć wpływ **transgraniczny**

# ZGŁASZANIE INCYDENTÓW

**Co zgłaszamy?** ⟶ **poważny incydent**

**Komu?** ⟶ **CSIRT / właściwy organ**

**Kiedy?** ⟶ **24 godziny –**
wstępne ostrzeżenie

**72 godziny –**
zgłoszenie incydentu

# ZGŁASZANIE INCYDENTÓW

**Co zgłaszamy?** → **poważny incydent**

**Komu?** → **CSIRT / właściwy organ**

**Kiedy?** →

**24 godziny –**
wstępne ostrzeżenie

**72 godziny –**
zgłoszenie incydentu

**1 miesiąc –**
sprawozdanie końcowe

# ZGŁASZANIE INCYDENTÓW

**Co zgłaszamy?** ⟶ **poważny incydent**

**Komu?** ⟶ **CSIRT / właściwy organ**

**Kiedy?** ⟶

**24 godziny –**
wstępne ostrzeżenie

**72 godziny –**
zgłoszenie incydentu

**1 miesiąc –**
sprawozdanie końcowe

- w stosownych przypadkach powiadomienie bez zbędnej zwłoki odbiorców usług o poważnym incydencie, który mieć **niekorzystny wpływ** na świadczenie usług

# SPRAWOZDANIE KOŃCOWE

- szczegółowy opis incydentu
  - w tym jego dotkliwości i skutków
  - rodzaj zagrożenia lub pierwotną przyczynę, która prawdopodobnie była źródłem incydentu
- zastosowane i wdrażane środki ograniczające ryzyko
- w stosownych przypadkach, transgraniczny wpływ tego incydentu.

# NIS2 a RODO

- **Współpraca pomiędzy organem ochrony danych osobowych a organami z NIS 2**

Jeżeli w czasie nadzoru lub egzekwowania przepisów właściwe **organy powzięły wiedzę**, że naruszenie przez podmiot kluczowy lub ważny obowiązków określonych w art. 21 i 23 niniejszej dyrektywy **może pociągać za sobą naruszenie ochrony danych osobowych** zdefiniowane w art. 4 pkt 12 rozporządzenia (UE) 2016/679, które podlega zgłoszeniu na podstawie art. 33 tego rozporządzenia, **bez zbędnej zwłoki informują o tym organy nadzorcze**, o których mowa w art. 55 i 56 tego rozporządzenia.

**art. 35 ust. 1**

# NIS2 a RODO

- **Współpraca pomiędzy organem ochrony danych osobowych a organami z NIS 2**
- **Przetwarzanie danych osobowych w zakresie koniecznym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i systemów informatycznych**

# NIS2 a RODO

- **Współpraca pomiędzy organem ochrony danych osobowych a organami z NIS 2**
- **Przetwarzanie danych osobowych w zakresie koniecznym i proporcjonalnym do zapewnienia <u>bezpieczeństwa sieci i systemów informatycznych</u>**
  - uzasadniony interes – art. 6 ust. 1 lit. f RODO

[...] gdy takie przetwarzanie jest niezbędne w związku **z mechanizmami wymiany informacji o cyberbezpieczeństwie** lub do dobrowolnego zgłaszania odpowiednich informacji zgodnie z niniejszą dyrektywą.

# Motyw 121 NIS2

- środki związane z **zapobieganiem incydentom**, ich wykrywaniem i identyfikacją, ograniczaniem ich zasięgu i ich analizowaniem oraz reagowaniem na nie,
- środki zwiększające świadomość konkretnych cyberzagrożeń, **wymianę informacji** w kontekście usuwania oraz skoordynowanego **ujawniania podatności**,
- **dobrowolną wymianę** informacji na temat tych incydentów, a także na temat cyberzagrożeń i podatności, oznak naruszenia integralności systemu, taktyk, technik i procedur, ostrzeżeń dotyczących cyberbezpieczeństwa i narzędzi konfiguracji

**mogą wymagać przetwarzania pewnych kategorii danych osobowych**, takich jak adresy IP, ujednolicone formaty adresowania zasobów (URL), nazwy domen, adresy poczty elektronicznej oraz znaczniki czasu, w przypadku gdy ujawniane są w nich dane osobowe.

# NIS2 a RODO

- **Współpraca pomiędzy organem ochrony danych osobowych a organami z NIS 2**
- **Przetwarzanie danych osobowych w zakresie koniecznym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i systemów informatycznych**
- **Różne terminy powiadamiania organów**

# Kary

Państwa członkowskie zapewniają, by **podmioty kluczowe** dokonujące naruszeń **art. 21 lub 23** podlegały zgodnie z ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w maksymalnej wysokości co najmniej **10 000 000 EUR** lub co najmniej **2 % łącznego rocznego światowego obrotu** w poprzednim roku obrotowym przedsiębiorstwa, do którego należy podmiot kluczowy, przy czym zastosowanie ma kwota wyższa.

**art. 34 ust. 4**

# Kary

Państwa członkowskie zapewniają, by **podmioty ważne** dokonujące naruszeń art. 21 lub 23 podlegały zgodnie z ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w maksymalnej wysokości co najmniej **7 000 000 EUR** lub **1,4 % łącznego rocznego światowego obrotu** w poprzednim roku obrotowym przedsiębiorstwa, do którego należy podmiot ważny, przy czym zastosowanie ma kwota wyższa.

**art. 34 ust. 5**