trecom | cisco Partner

NIS 2
BAZA WIEDZY

NIS 2 i UoKSC -
aktualizacja
i najważniejsze informacje.

Prezentacja autorstwa **Tomasza Matuły**

dyrektywanis2.trecom.pl

NIS 2 i UKSC – aktualizacja i przypomnienie najważniejszych informacji

NIS 2 i UKSC – aktualizacja i przypomnienie najważniejszych informacji

Spis treści

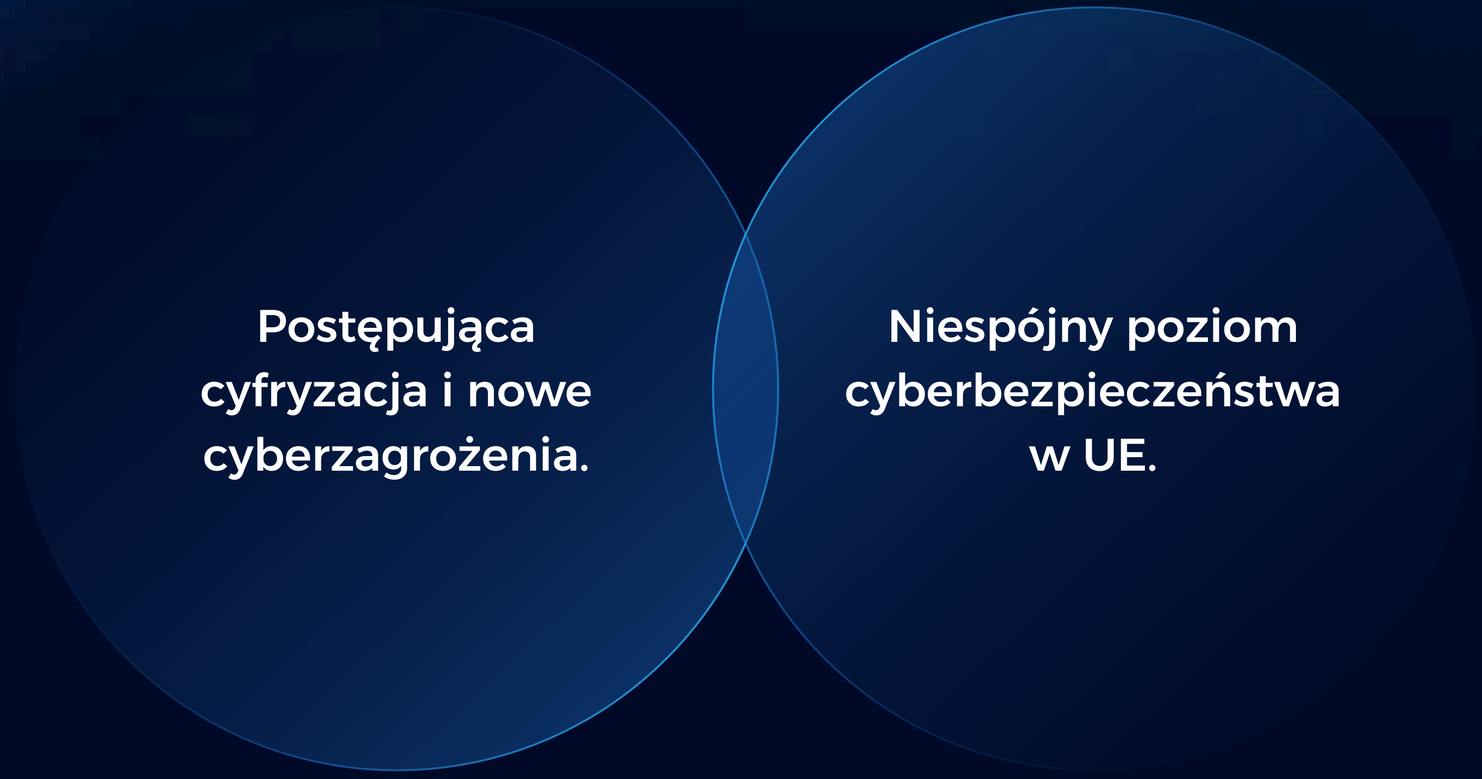
Stan na 09.2025

- Bazujemy na projekcie nowelizacji z 08.2025.
- Ten projekt zawiera już poprawki wprowadzone po konsultacjach społecznych.

trecom

Skąd pomysł na NIS 2?

- 2016 NIS
- Przeglądy i kontrole wykazały dwa główne powody do wdrożenia nowej dyrektywy:



trecom

NIS 2 – mit pierwszy

Polska może wdrożyć wyłącznie wybrane fragmenty dyrektywy NIS 2.

Nieprawda

NIS 2 określa i wprowadza minimalne wymagania i obowiązki, które każdy z krajów członkowskich UE musi wdrożyć.

trecom

Harmonogram – mit drugi

17.10.2024

Polskie podmioty muszą spełniać obowiązki od 17.10.2024 niezależnie od tego, kiedy formalnie wejdzie w życie znowelizowana ustawa o KSC.

Nieprawda

Nowelizacja ustawy trafi do sejmu w 2025r.

UKSC prawdopodobnie formalne wejdzie w życie w maju 2025.

1 miesiąc vacatio legis + 6 miesięcy na dostosowanie się podmiotów.

UKSC prawdopodobnie zacznie obowiązywać we wrześniu lub październiku 2025.

trecom

Harmonogram wprowadzania zmian

6 miesięcy na dostosowanie

Miesiąc vacatio legis

2016

6 lipca 2016

Wejście w życie Dyrektywy NIS

2020

16 grudnia 2020

Publikacja projektu nowelizacji Dyrektywy NIS przez Komisję Europejską

2022

13 maja 2022

Wstępne porozumienie Rady i Parlamentu Europejskiego

14 grudnia 2022

Podpisanie Dyrektywy NIS 2

27 grudnia 2022

Publikacja w Dzienniku Urzędowym UE

2024

18 października 2024

NIS 2 wchodzi w życie w UE

2025

grudzień 2025/ styczeń 2026

Nowelizacja UKSC zatwierdzona

2026

??? 2026

Przekazanie do KE listy podmiotów objętych NIS 2 i nowelizacją UKSC

Q3 2026

Nowelizacja UKSC wchodzi efektywnie w życie

trecom

Kogo dotyczy NIS 2?

Około 40 tyś. podmiotów z czego ok 28 tysięcy to podmioty publiczne.

Podmioty działające w obszarach uznanych przez UE jako istotne

i równocześnie...

...przekraczające określoną wielkość (size cap rule*): 50 pracowników i roczny obrót > 10 mln EUR.

*** Wyjątki od size cap rule:**

- Dostawcy usług zaufania
- Jednostki administracji publicznej
- Jedyny dostawca usługi w kraju
- Dostawcy usług zarządzania w zakresie cyberbezpieczeństwa

trecom

Podmioty kluczowe

Kogo dotyczy **NIS 2/UKSC** - **sektory kluczowe**

> 250 pracowników i roczny obrót >50mln EUR

- **Energia**
  - Wydobywanie kopalin
  - Energia elektryczna
  - Centralne ogrzewanie i chłodzenie
  - Ropa i paliwa
  - Gaz, wodór, jądrowa
- **Ochrona zdrowia**
  - Świadczenia i zdrowie publiczne
  - Produkcja i dystrybucja
- **Infrastruktura cyfrowa**
  - Data Center
  - Usługi łączności elektronicznej
  - Dostawcy usług chmurowych
  - Dostawcy uslug DNS
- **Transport**
  - Lotniczy
  - Kolejowy
  - Wodny
  - Drogowy
- **Woda pitna - zaopatrzenie i dystrybucja**
- **Zbiorowe odprowadzanie ścieków**
- **Administracja publiczna***
- **Przestrzeń kosmiczna**
- **Zarządzanie usługami ICT**
  - Dostawcy Usług Zarządzanych
  - Dostawcy Usług Zarządzanych w zakresie bezpieczeństwa

*z wyłączeniem podmiotów ważnych-publicznych (kolejny slajd)

Podmioty ważne

Kogo dotyczy **NIS 2/UKSC** - **sektory ważne**

> 50 pracowników i roczny obrót >10mln EUR

Usługi pocztowe i kurierskie

Badania naukowe

Gospodarowanie odpadami

- Zbieranie odpadów
- Transport odpadów
- Przetwarzanie odpadów
- Sprzedaż lub pośrednictwo

Dostawcy usług cyfrowych

- Wyszukiwarki sieciowe
- Platformy e-commerce
- Platformy sieci społecznościowych

Administracja publiczna

- Samorządowe jednostki budżetowe
- Samorządowe zakłady budżetowe
- Samorządowe instytucje kultury
- Spółka prawa handlowego wykonująca zadania o charakterze użyteczności publicznej (w rozumieniu ustawy o gospodarce komunalnej) przy wykorzystaniu systemów informacyjnych

Produkcja

- Produkcja, wytwarzanie i dystrybucja chemikaliów
- Produkcja, wytwarzanie i dystrybucja żywności
- Wyroby medyczne
- Wyroby medyczne do diagnostyki in vitro
- Produkty komputerowe
- Produkty elektroniczne i optyczne
- Sprzęt elektroniczny
- Maszyny i urządzenia
- Pojazdy samochodowe, przyczepy i naczepy

Kary finansowe

Podmioty kluczowe:

do **10 000 000 EUR** lub **2 %** całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego, przy czym zastosowanie będzie mieć kwota wyższa, jednak nie mniej niż 20 000 PLN.

Podmioty ważne:

do **7 000 000 EUR** lub **1,4 %** całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego, jednak nie mniej niż 15 000 PLN.

trecom

Dodatkowe kary w UKSC

Do **100 000 000 PLN,** dla podmiotów kluczowych i ważnych, jeżeli podmiot naruszy przepisy ustawy i spowoduje bezpośrednie, ekstremalnie poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, życia i zdrowia ludzi, wywołania poważnej szkody majątkowej itp.

Zawieszenie certyfikacji/zezwoleń na świadczenie usługi.

Kierownik podmiotu - mit trzeci

Prezes czy dyrektor generalny to nie kierownik podmiotu.

W ustawie chodzi o kierownika IT czy security.

Nieprawda

Kim jest **KIEROWNIK PODMIOTU** definiuje ustawa o rachunkowości.

Zgodnie z nią kierownikiem podmiotu zależnie od formy prawnej i rodzaju podmiotu jest prezes, dyrektor generalny, rektor, dyrektor szpitala, starosta, wójt itd.

trecom

Kierownik podmiotu - mit czwarty

Kierownik podmiotu może zdelegować odpowiedzialność związaną z cyberbezpieczeństwem na inną osobę w organizacji np. szefa IT, CISO.

✕ Nieprawda

Obowiązki kierownika podmiotu

Ocena ryzyk cybernetycznych i ich wpływu na działalność podmiotu.

Zatwierdzanie środków zarządzania ryzykiem cyberbezpieczeństwa.

Regularne szkolenia (co najmniej raz w roku) umożliwiające:

- identyfikację zagrożeń i ocenę ryzyk cybernetycznych,
- ocenę praktyk zarządzania ryzykiem cyberbezpieczeństwa,
- ich wpływu na działalność podmiotu.

Sankcje dla kierownika podmiotu

Publiczne oświadczenie określające osobę fizyczną i prawną odpowiedzialną za naruszenie oraz charakter tego naruszenia.

Czasowy zakaz pełnienia funkcji kierowniczych w podmiocie na poziomie dyrektora generalnego, przedstawiciela prawnego.

Kara pieniężna do 300% średniego miesięcznego wynagrodzenia danego kierownika podmiotu - nie średnia krajowa!

Zakres obowiązków dla podmiotów

- Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji
- Analiza ryzyka i polityki bezpieczeństwa systemów informatycznych
- Zarządzanie incydentami cyberbezpieczeństwa i informowanie o nich
- Plany ciągłości działania i zarządzanie kryzysowe
- Bezpieczeństwo łańcucha dostaw
- Polityki i procedury służące ocenie skuteczności środków zarządzania
- Podstawowe praktyki z zakresu cyberhigieny i szkoleń
- Bezpieczeństwo w pozyskiwaniu, rozwijaniu i utrzymywaniu sieci oraz systemów informatycznych
- Stosowanie kryptografii i szyfrowania
- Uwierzytelnianie wieloskładnikowe lub ciągłe

trecom

SZBI

Systematyczne szacowanie ryzyka wystąpienia incydentów oraz zarządzanie tym ryzykiem.

Wdrożenie odpowiednich środków technicznych i organizacyjnych, które są proporcjonalne do oszacowanego ryzyka.

Opracowanie i aktualizacja dokumentacji dotyczącej bezpieczeństwa systemów informacyjnych używanych w procesie świadczenia usług.

Regularne przeglądy i audyty systemu, które pomagają w ocenie skuteczności SZBI oraz identyfikacji obszarów do poprawy.

W oparciu o dowolny framework!

Załącznik do ustawy – mapowanie obowiązków na wybrane normy np. ISO czy NIST.

Podmioty ważne-publiczne wdrażają uproszczone SZBI - szczegóły w załączniku 4 do projektu ustawy.

trecom

Zarządzanie ryzykiem

Prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem.

Posiadania przez każdą organizację udokumentowanych, aktualizowanych analiz i ewaluacji ryzyk:

- określenie ryzyk, ich poziomu i ich priorytetyzacja (wybranie tych najważniejszych)
- posiadanie planu postępowania (mitygacji) z cyber ryzykami oraz zarządzanie nimi

trecom

Zapewnienie ciągłości i zarządzanie kryzysowe

Posiadanie planów ciągłości działania i zarządzania kryzysowego.

Obowiązkowe, cykliczne testowanie.

Zarządzanie kopiami zapasowymi (w tym testowanie).

Przywracanie działania po wystąpieniu sytuacji nadzwyczajnej.

Zarządzanie incydentami bezpieczeństwa

Wczesne ostrzeżenie – do 24h od zdobycia wiedzy o poważnym incydencie.

- Czy wywołany działaniem bezprawnym?
- Czy wywołany działaniem w złym zamiarze?
- Czy ma wpływ transgraniczny?

Zarządzanie incydentami bezpieczeństwa

Zgłoszenie incydentu – do 72h od zdobycia wiedzy o poważnym incydencie.

- Aktualizacja wcześniejszych informacji.
- Wstępna ocena dotkliwości i skutków.
- Wskaźniki integralności systemów (jeśli dotyczy).

Podmioty ważne-publiczne obowiązuje wyłącznie zgłaszanie incydentu w ciągu 72h.

trecom

Zarządzanie incydentami bezpieczeństwa

Raport końcowy – do miesiąca od zdobycia wiedzy o poważnym incydencie.

- Szczegółowy opis incydentu – waga, wpływ, dotkliwość i skutki.
- Rodzaj zagrożenia, pierwotna przyczyna incydentu.
- Zastosowane i wdrażane środki zaradcze ograniczające ryzyko.
- Transgraniczne skutki (jeśli dotyczy).

Gdzie i jak zgłaszać incydenty?

Incydenty i raporty musimy zgłosić do odpowiedniego, obsługującego nas CSIRT sektorowego.

Za pomocą systemu S46 (komunikacja dwustronna).

Definicja łańcucha dostaw

Firmy, z którymi współpracujemy w szczególności podwykonawcy i usługodawcy.

Biblioteki i pakiety oprogramowania typu open-source lub innych firm, które są wymagane do funkcjonowania naszych aplikacji i operacji.

Infrastruktura czy serwisy firm trzecich.

Zewnętrzni dostawcy zarządzanych usług bezpieczeństwa np. SOC.

Obowiązki związane z łańcuchem dostaw

Ocena ryzyka (risk assesment) dla bezpośrednich dostawców i podwykonawców (Tier 1)

- Badanie i dokumentowanie cyber ryzyk związanych z współpracą.
- Sposoby minimalizacji tych ryzyk.

Aktywny monitoring bezpieczeństwa współpracy

- Wykrywanie incydentów i reagowanie na nie.
- Pentesty (tam gdzie potrzeba).
- Audyty bezpieczeństwa (tam gdzie potrzeba).

Ważne - ustandaryzowane wymagania względem partnerów i dostawców.

trecom

Efekt domina

Firma nieobjęta NIS 2 czy nowelą UKSC a będąca dostawcą firmy objętej NIS 2 będzie zmuszona w dużym stopniu dostosować się do obowiązków.

Ocena skuteczności środków zarządzania ryzykiem

Testowanie planów ciągłości działania i zarządzania kryzysowego.

Cykliczne wykonywanie testów penetracyjnych czy audytów bezpieczeństwa.

W przypadku dużych organizacji np. ciągłe testowanie pipelinie CI/CD.

Cykliczny audyt bezpieczeństwa – tylko podmioty kluczowe, raz na 3 lata.

trecom

Cyberhigiena i szkolenia

Szkolenia dla pracowników wszystkich szczebli.

Opracowanie i wdrażanie modułów szkoleniowych security awareness dostosowanych do specyfiki organizacji.

Szkolenie dla zarządu/kierownika podmiotu – ocena ryzyka cybernetycznego, praktyki zarządzania ryzykiem, ich wpływ na działalność podmiotu – minumum raz w roku.

Rozwiązania technologiczne

"Kluczowe i ważne podmioty podejmują odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykiem stwarzanym dla bezpieczeństwa systemów sieciowych i informatycznych, z których podmioty te korzystają przy świadczeniu swoich usług."

trecom

Rozwiązania technologiczne

Grupa 1:

Kryptografia i szyfrowanie.

Uwierzytelnianie wieloskładnikowe lub ciągłe.

Grupa 2:

Bezpieczeństwo w pozyskiwaniu, rozwijaniu i utrzymywaniu sieci i systemów informatycznych, w tym ujawnianie i zarządzanie podatnościami.

Rozwiązania technologiczne

Utrzymanie i bezpieczna eksploatacja systemu informacyjnego, bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu.

Stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym.

Rozwiązania technologiczne

Objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym.

Zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usług.

trecom

Rozwiązania technologiczne

Regularne przeprowadzanie aktualizacji oprogramowania: stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji.

trecom

Rozwiązania technologiczne

Niezwłoczne podejmowanie działań po dostrzeżeniu podatności.

trecom

Kontrole

Nadzór następczy:

- Po incydencie bezpieczeństwa.
- W podmiotach kluczowych i ważnych.

Nadzór prewencyjny (proaktywny):

- Cykliczna kontrola stanu spełnienia obowiązków.
- W podmiotach kluczowych.

Kontrole

Kontrole doraźne:

- Przeprowadzane m.in. po zgłoszeniu przez tzw. urzędnika monitorującego.
- Podmiot zostanie powiadomiony wcześniej.

Kto będzie wykonywał kontrole?

Wyznaczone z właściwego dla podmiotu ministerstwa ze wsparciem CSIRT sektorowych i poziomu krajowego.

trecom

Chcesz wiedzieć więcej? Wyceń projekt lub umów się na konsultację.

Jan Bręczewski

jan.breczewski@trecom.pl

+48 727 990 111

trecom

Chcesz wiedzieć więcej?

www.trecom.pl

trecom

Chcesz wiedzieć więcej?

edyta.jedynak@trecom.pl

576 421 500

trecom

Chcesz wiedzieć więcej?

rafal.ziolek@trecom.pl

660 679 885