RBR

🛡️ Dyrektywa NIS 2 w pytaniach i odpowiedziach

❓ Co to jest dyrektywa NIS 2?

Dyrektywa NIS 2 (Network and Information Security Directive 2) to unijne przepisy mające na celu wzmocnienie cyberbezpieczeństwa w UE. Zastępuje wcześniejszą dyrektywę NIS i wprowadza bardziej rygorystyczne wymagania dla firm i instytucji w zakresie zarządzania ryzykiem i reagowania na incydenty.

🏛️ Kogo dotyczy dyrektywa NIS 2?

Dyrektywa NIS2 obejmuje szeroki zakres firm i instytucji działających w Unii Europejskiej, które świadczą usługi kluczowe lub ważne dla funkcjonowania gospodarki i społeczeństwa.

🔑 Podmiot kluczowy

osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy	**co najmniej średni przedsiębiorca (zatrudniający 50-250 pracowników i osiągający roczny obrót o wartości 50 mln euro)**
przedsiębiorca komunikacji elektronicznej	**co najmniej średni przedsiębiorca**
dostawca usług zarządzanych w zakresie cyberbezpieczeństwa	**co najmniej średni przedsiębiorca**
dostawca usług DNS i podmiot świadczący usługi rejestracji domen	**niezależnie od wielkości**
kwalifikowany dostawca usług zaufania	**niezależnie od wielkości**
część podmiotów publicznych	**Niezależnie od wielkości**
podmiot krytyczny	**niezależnie od wielkości**
podmiot zidentyfikowany jako podmiot kluczowy	**niezależnie od wielkości**

RBR

Podmiot ważny

osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 lub 2 do ustawy, która nie jest podmiotem kluczowym	co najmniej średni przedsiębiorca (zatrudniający 50-250 pracowników i osiągający roczny obrót o wartości 50 mln euro)
niekwalifikowany dostawca usług zaufania	mikro, mały lub średni przedsiębiorca
przedsiębiorca komunikacji elektronicznej	mikro, mały lub średni przedsiębiorca
podmiot zidentyfikowany jako podmiot ważny na podstawie poszczególnych przepisów ustawy	
podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 2	
część podmiotów publicznych	

Jakie są główne obowiązki?

Obowiązki dotyczą firm działających w UE, które są co najmniej średnimi przedsiębiorstwami, a w określonych przypadkach także mniejszych firmy, jeśli ich działalność ma krytyczne znaczenie.

RBR

Obszar	Wymagania
1. Zarządzanie ryzykiem cyberbezpieczeństwa	Wdrożenie systemu zarządzania ryzykiem obejmującego identyfikację, ocenę i minimalizację zagrożeń; regularne oceny ryzyka; wdrażanie polityk bezpieczeństwa, segmentacji sieci, szyfrowania danych i zarządzania incydentami.
2. Wdrożenie środków technicznych, operacyjnych i organizacyjnych	Stosowanie odpowiednich środków technicznych i organizacyjnych, takich jak aktualizacje oprogramowania, mechanizmy poufności, integralności, dostępności, autentyczności danych, kryptografia, uwierzytelnianie wieloskładnikowe.
3. Zgłaszanie incydentów cyberbezpieczeństwa	Obowiązek szybkiego zgłaszania poważnych incydentów do właściwych organów (np. CSIRT) w ciągu 24 godzin; prowadzenie rejestru incydentów i współpraca z organami państwowymi.
4. Monitorowanie i ochrona łańcucha dostaw	Ocena i monitorowanie ryzyka związanego z dostawcami i podwykonawcami, aby zapewnić bezpieczeństwo całego łańcucha dostaw.
5. Audyty i szkolenia	Regularne audyty bezpieczeństwa (np. co 3 lata) oraz organizowanie szkoleń z zakresu cyberbezpieczeństwa dla pracowników.
6. Wyznaczenie punktu kontaktowego ds. cyberbezpieczeństwa	Wyznaczenie osoby lub zespołu odpowiedzialnego za kontakt z organami nadzorczymi w sprawach cyberbezpieczeństwa.
7. Współpraca z organami państwowymi i CSIRT-ami	Obowiązek współpracy z krajowymi zespołami reagowania na incydenty oraz innymi organami odpowiedzialnymi za cyberbezpieczeństwo.
8. Utrzymanie ciągłości działania i zarządzanie kryzysowe	Posiadanie planów ciągłości działania i procedur zarządzania kryzysowego na wypadek poważnych incydentów.
9. Certyfikacja i dokumentacja	Zachęta do korzystania z europejskich systemów certyfikacji cyberbezpieczeństwa oraz prowadzenie dokumentacji potwierdzającej zgodność z wymogami NIS2.

Typ podmiotu	Przykłady sektorów
Podmioty kluczowe	Energetyka, transport, bankowość, infrastruktura cyfrowa, opieka zdrowotna
Podmioty ważne	Usługi pocztowe, gospodarka odpadami, produkcja żywności, usługi cyfrowe

RBR

📅 Jakie są terminy zgłaszania incydentów?

Etap	Termin
Wstępne zgłoszenie	Do 24 godzin od wykrycia incydentu
Wstępny raport	Do 72 godzin od wykrycia
Końcowy raport	Do 1 miesiąca od wykrycia

🕵️ Jakie są sankcje za nieprzestrzeganie przepisów?

Typ podmiotu	Maksymalna kara
Podmioty kluczowe	10 mln euro lub 2% rocznego obrotu
Podmioty ważne	7 mln euro lub 1,4% rocznego obrotu

🛠️ Jakie działania powinny podjąć firmy?

- Przeprowadzić analizę ryzyka i wdrożyć odpowiednie środki bezpieczeństwa.
- Opracować procedury reagowania na incydenty.
- Przeszkolić personel w zakresie cyberbezpieczeństwa.
- Regularnie aktualizować polityki i procedury bezpieczeństwa.

Jesteśmy Partnerem: SoDA ABSL fintech CENTRAL POLAND