C & C solution partner

NIS 2: Kluczowe założenia, obowiązki i wymagania

Cyberbezpieczeństwo – nowe obowiązki firm w Dyrektywie NIS2

Dyrektywa NIS2 z 2022 roku ma przeciwdziałać cyberprzestępczości. Sprawdź, jakie obowiązki wynikają z niej dla małych i średnich przedsiębiorców.

- Od kiedy firmy będą miały nowe obowiązki
- Kto będzie stosował NIS2
- Które sektory są objęte NIS2
- Którzy przedsiębiorcy nie są objęci NIS2
- Kiedy NIS2 obowiązuje niezależnie od wielkości firmy
- Kiedy NIS2 obowiązuje MŚP
- Rejestr podmiotów ważnych i kluczowych
- Obowiązki firm objętych Dyrektywą NIS2
- Zgłaszanie incydentów cyberbezpieczeństwa
- Dobrowolne zgłaszanie incydentów lub cyberzagrożeń

Od kiedy firmy będą miały nowe obowiązki

Datę wejścia w życie nowych obowiązków w zakresie cyberbezpieczeństwa określi ustawa, która dostosuje polskie przepisy do Dyrektywy NIS2.
Rząd pracuje nad tą ustawą. Jej przyjęcie wstępnie zaplanowano na październik 2024 roku.

Kto będzie stosował NIS2

Dyrektywa NIS2 nakłada szereg obowiązków z zakresu cyberbezpieczeństwa na większych przedsiębiorców określanych jako **podmioty kluczowe**.
Część obowiązków dotyczy również małych i średnich przedsiębiorców oraz mikroprzedsiębiorców.

Dyrektywa NIS2 dzieli przedsiębiorców na:

- podmioty kluczowe
- podmioty ważne.

Te grupy różnią się poziomem nadzoru, tym w jaki sposób są egzekwowane wymagania z zakresu cyberbezpieczeństwa oraz wysokością kar.

Które sektory są objęte NIS2

Dyrektywa NIS2 dotyczy głównie **średnich i dużych firm**, które działają w sektorach o wysokim stopniu krytyczności, czyli:

- energia

- energia elektryczna, w tym systemy produkcji, dystrybucji i przesyłu oraz punkty ładowania
- ciepłownictwo i chłodnictwo
- ropa naftowa, w tym rurociągi produkcyjne, magazynowe i przesyłowe
- gaz, w tym systemy dostaw, dystrybucji i przesyłu oraz magazynowanie
- wodór
- transport lotniczy, kolejowy, wodny i drogowy
- infrastruktura bankowa i rynku finansowego, jak instytucje kredytowe, operatorzy systemów obrotu i partnerzy centralni
- zdrowie, w tym podmioty świadczące opiekę zdrowotną, producenci podstawowych produktów farmaceutycznych i wyrobów medycznych o krytycznym znaczeniu oraz laboratoria referencyjne UE
- woda pitna
- ścieki
- infrastruktura cyfrowa, w tym dostawcy usług centrów danych, usług przetwarzania w chmurze, publicznych sieci łączności elektronicznej i publicznie dostępnych usług łączności elektronicznej
- usługi zarządzane przez TIK (między przedsiębiorstwami)
- przestrzeń.

NIS2 obejmuje także firmy **z innych sektorów krytycznych**, tak jak:

- usługi pocztowe i kurierskie
- gospodarka odpadami
- produkcja, wytwarzanie i dystrybucja chemikaliów
- produkcja, przetwarzanie i dystrybucja żywności
- produkcja, w szczególności wyrobów medycznych, komputerowych, elektronicznych i optycznych, niektórych rodzajów sprzętu elektrycznego i maszyn, pojazdów silnikowych i innego sprzętu transportowego
- dostawcy usług cyfrowych w zakresie internetowych platform handlowych, wyszukiwarek i sieci społecznościowych.

Którzy przedsiębiorcy nie są objęci NIS2

Dyrektywy NIS2 nie stosują:

- przedsiębiorcy, którzy świadczą usługi **wyłącznie na rzecz podmiotów administracji publicznej,** prowadzący działania w obszarach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, w tym zapobiegania przestępstwom, prowadzenia postępowań w ich sprawie, wykrywania ich i ścigania

- przedsiębiorcy, którzy **zostaną zwolnieni** z obowiązków ustanowienia środków zarządzania ryzykiem w cyberbezpieczeństwie lub zgłaszania incydentów w odniesieniu do prowadzonych przez siebie działań lub świadczonych usług.
- przedsiębiorców, którzy zostali zwolnieni ze stosowania **DORA**.

Kiedy NIS2 obowiązuje niezależnie od wielkości firmy

Zgodnie z Dyrektywą NIS2:

- przedsiębiorcy, którzy świadczą określone usługi cyfrowe z sektora infrastruktury cyfrowej są objęci obowiązkami wynikającymi z NIS2, **niezależnie od wielkości.**

Przedsiębiorcy objęci NIS2 niezależnie od wielkości to:

- dostawcy usług TLD (top level domain)
- dostawcy usług DNS (domain name server)
- dostawcy kwalifikowanych usług zaufania
- dostawcy publicznych sieci łączności elektronicznej
- dostawcy publicznie dostępnych usług łączności elektronicznej
- **małe lub średnie** firmy, który zostaną zakwalifikowane przez właściwe organy krajowe jako **podmiot krytyczny** (zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE).

Kiedy NIS2 obowiązuje MŚP

Dyrektywa NIS 2 obowiązuje mikro, małe i średnie firm, które spełniają **jeden z dwóch** warunków:

- świadczą **usługi w sektorze objętym NIS2** na terenie UE i **nie zostały sklasyfikowane** jako podmioty kluczowe
- albo
    - są dostawcą usługi, która ma w Polsce kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej
    - zakłócenie usługi, którą świadczą, mogłoby mieć znaczący wpływ na porządek publiczny, bezpieczeństwo publiczne lub zdrowie publiczne
    - zakłócenie usługi, którą świadczą mogłoby prowadzić do powstania poważnego ryzyka systemowego, w szczególności w sektorach, w których takie zakłócenie mogłoby mieć wpływ transgraniczny
    - zakłócenie usługi, którą świadczą, mogłoby prowadzić do powstania poważnego ryzyka systemowego, w szczególności w sektorach, w których takie zakłócenie mogłoby mieć wpływ transgraniczny

- mają charakter krytyczny ze względu na ich szczególne znaczenie na poziomie krajowym lub regionalnym dla konkretnego sektora lub rodzaju usługi lub dla innych współzależnych sektorów w kraju.

Dodatkowo Ministerstwo Cyfryzacji może zdecydować, że określone **małe przedsiębiorstwa i mikroprzedsiębiorstwa** będą objęte obowiązkami wynikającymi z NIS2 i zostaną zakwalifikowane jako **podmiot kluczowy albo podmiot ważny**, jeżeli spełnią szczególne kryteria. Taka kwalifikacja może wynikać z oceny roli firmy dla społeczeństwa, gospodarki, konkretnych sektorów lub rodzajów usług.

Podmioty kluczowe i ważne, aby zwiększyć swoją odporność na cyberzagrożenia, muszą wprowadzić odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych. Środki te obejmują **bezpieczeństwo łańcucha dostaw -** pomioty kluczowe i ważne mają obowiązek kontroli swych dostawców lub klientów biznesowych, nawet jeśli ci dostawcy lub klienci nie są objęci Dyrektywą NIS2.

W konsekwencji, jeśli firmy z łańcucha dostaw będą chciały utrzymać współpracę z podmiotem ważnym albo z podmiotem kluczowym, jako poddostawcy, kontrahenci, klienci biznesowi, muszą wdrożyć odpowiednie środki bezpieczeństwa i spełniać wymagania z zakresu cyberbezpieczeństwa wynikające z Dyrektywy NIS2.
Łańcuch dostaw to sieć organizacji, ludzi, działań, informacji i zasobów, które współpracują ze sobą, aby dostarczyć produkt lub usługę z początkowego etapu do rąk konsumenta końcowego/końcowego odbiorcy biznesowego. W łańcuchu dostaw uczestniczą firmy, które dostarczają komponenty podmiotom kluczowym lub ważnym niezbędne w danym produkcie bądź usłudze.

Uwaga! Komisja Europejska planuje opublikować wytyczne dotyczące wdrażania kryteriów mających zastosowanie do **mikroprzedsiębiorstw i małych przedsiębiorstw.** Wytyczne pomogą ocenić, czy firm mikro i małe są objęte NIS2.

Rejestr podmiotów ważnych i kluczowych

To przedsiębiorca musi samodzielnie określić, czy jest średnim przedsiębiorcą i czy świadczy usługę lub usługi w sektorze objętym dyrektywą NIS2. Jest to mechanizm samoidentyfikacji.

Jeżeli jesteś podmiotem objętym NIS2, masz obowiązek wpisać się do **rejestru podmiotów kluczowych i ważnych,** prowadzonego przez Ministra Cyfryzacji. Wniosek o wpis do wykazu przekażesz elektronicznie, w terminie określonym przez Ministra.

Obowiązki firm objętych Dyrektywą NIS2

Zgodnie z NIS2 przedsiębiorca ważny (średni, mały lub mikro) musi:

- wdrożyć odpowiednie i proporcjonalne **środki techniczne, operacyjne i organizacyjne** w firmie
- **zgłaszać incydenty** cyberbezpieczeństwa.

Wdrożenie odpowiednich środków w firmie

Dyrektywa NIS2 nie określa, jakie konkretnie środki zarządzania ryzykiem w cyberbezpieczeństwie powinien wdrożyć przedsiębiorca. Wskazuje jednak, że mają one być:

- proporcjonalne
- uwzględniające stopień narażenia podmiotu na ryzyko
- uwzględniające wielkość podmiotu
- uwzględniające prawdopodobieństwo wystąpienia incydentów oraz ich dotkliwość, w tym skutki społeczne i gospodarcze.

To oznacza, że firmy same muszą zdefiniować właściwe środki, zgodnie ze swoją specyfiką i wdrożyć je bez zbędnej zwłoki. Takie podejście pozwala przedsiębiorcom zachować elastyczność.

Jednocześnie firmy objęte NIS2 powinny co najmniej zapewnić:

- politykę analizy ryzyka i bezpieczeństwa systemów informatycznych
- obsługę incydentu
- ciągłość działania, na przykład zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej, i zarządzania kryzysowego
- bezpieczeństwo łańcucha dostaw, w tym aspektów związanych z bezpieczeństwem dotyczących stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami
- bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowania w przypadku podatności i ich ujawniania
- polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie
- podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa
- polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania
- bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu i zarządzania aktywami

- w stosownych przypadkach – stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.

Ważne! Przedsiębiorca ma obowiązek zgłosić **osoby lub organy zarządzające w firmie**, które zatwierdzają środki zarządzania ryzykiem w cyberbezpieczeństwie, nadzorują ich wdrażanie i ponoszą odpowiedzialność za ewentualne naruszenia dyrektywy NIS2. Te osoby lub organy powinny odbywać **regularne szkolenia**, które pozwolą im zdobyć wiedzę wystarczającą do prawidłowego rozpoznania i oceny praktyki zarządzania ryzykiem w cyberbezpieczeństwa oraz ich wpływu na usługi świadczone przez firmę. Osoby lub organy zarządzające w firmie powinny oferować podobne szkolenia pracownikom (ale nie mają takiego obowiązku).

Zgłaszanie incydentów cyberbezpieczeństwa

Przedsiębiorca ma obowiązek:

- zgłosić bez zbędnej zwłoki, właściwemu Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego - CSIRT lub innemu organowi właściwemu (który zostanie określony w ustawie wdrażającej dyrektywę NIS2) incydent mający istotny wpływ na świadczenie przez nie usług (poważny incydent)
- zgłosić informacje umożliwiające ustalenie transgranicznego wpływu incydentu
- powiadomić odbiorców usług o poważnych incydentach, które mogą mieć niekorzystny wpływ na świadczenie usług, z których korzystają
- poinformować odbiorców usług, których potencjalnie dotyczy poważne cyberzagrożenie, o środkach zaradczych i innych środkach, które ci odbiorcy mogą zastosować w reakcji na to zagrożenie; w stosownych wypadkach również należy ich poinformować o samym poważnym cyberzagrożeniu.

Incydent jest **poważny**, jeżeli:

- 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.

Przedsiębiorca informuje o poważnym incydencie:

- bezzwłocznie (maksymalnie w ciągu 24 godzin) – **wczesne ostrzeżenie** ze wskazaniem, czy poważny incydent został przypuszczalnie wywołany działaniem bezprawnym lub działaniem w złym zamiarze lub czy mógł wywrzeć wpływ transgraniczny

- bezzwłocznie (maksymalnie 72 godziny) – **zgłoszenie incydentu** z ewentualną aktualizacją informacji przekazanych w ramach wczesnego ostrzeżenia i wstępną oceną poważnego incydentu, w tym jego dotkliwości i skutków, a w stosownych przypadkach także wskaźników integralności systemu.

Uwaga! Dostawca **usług zaufania** zgłasza poważne incydenty bez zbędnej zwłoki, maksymalnie w ciągu 24 godzin od pozyskania informacji o takim poważnym incydencie.

Na wniosek CSIRT lub, jeżeli ma to zastosowanie, właściwego organu – podmiot składa:

- **sprawozdanie okresowe** na temat aktualizacji statusu
- **sprawozdanie końcowe** - nie później niż **miesiąc** po zgłoszeniu incydentu (dokonanego w ciągu 72 godzin).

Sprawozdanie końcowe zawiera następujące elementy:

- 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 transgraniczne skutki incydentu.

Jeżeli incydent nie zakończył się w terminie składania sprawozdania końcowego, firmy przedstawiają w tym terminie sprawozdanie z postępu prac, a sprawozdanie końcowe – w ciągu **miesiąca** od zakończenia przez nich obsługi incydentu.
Jeżeli poważny incydent dotyczy co najmniej dwóch państw członkowskich UE, CSIRT, właściwy organ lub pojedynczy punkt kontaktowy bez zbędnej zwłoki informują o tym nim pozostałe państwa członkowskie, których incydent dotyczy, a także ENISA.

Po otrzymaniu wczesnego ostrzeżenia CSIRT lub właściwy organ odpowiada przedsiębiorcy zgłaszającemu, w tym:

- przekazuje mu wstępne informacje zwrotne na temat poważnego incydentu
- przekazuje wytyczne lub porady operacyjne dotyczące wdrożenia możliwych środków ograniczających ryzyko (na wniosek przedsiębiorcy)
- zapewnia dodatkowe wsparcie techniczne (na wniosek przedsiębiorcy).

Jeśli poważny incydent miał **cechy przestępstw**a, CSIRT lub właściwy organ informują również organy ścigania.

Na wniosek CSIRT lub właściwego organu pojedynczy punkt kontaktowy przekazuje zgłoszenia incydentów transgranicznych lub międzysektorowych, pojedynczym punktom kontaktowym w innych państwach członkowskich, których dotyczy incydent.

Niektórzy przedsiębiorcy, między innymi dostawcy usług DNS, rejestrów nazw TLD, usług chmurowych, zostaną objęte aktami wykonawczymi doprecyzowującymi incydenty poważne w ich zakresie.

Dobrowolne zgłaszanie incydentów lub cyberzagrożeń

Zgłoszenia do CSIRT lub właściwych organów mogą **dobrowolnie** przekazywać:

- podmioty kluczowe i ważne, w przypadku incydentów, cyberzagrożeń i potencjalnych zdarzeń dla cyberbezpieczeństwa
- inne podmioty, niezależnie od tego, czy są objęte NIS2, w odniesieniu do poważnych incydentów, cyberzagrożeń oraz potencjalnych zdarzeń dla cyberbezpieczeństwa.

Dobrowolne zgłoszenia są rozpatrywane zgodnie z procedurą przewidzianą do rozpatrywania zgłoszeń poważnych incydentów , przy czym zgłoszenia obowiązkowe mogą być traktowane **priorytetowo.**

W razie potrzeby zgłoszenia są przekazywane do pojedynczych punktów kontaktowych, z zachowaniem poufności i ochrony informacji przekazanych przez zgłaszającego. Zgłoszenie nie nakłada dodatkowych obowiązków na zgłaszającego.