Czym jest dyrektywa NIS2?

W dzisiejszej erze cyfrowej cyberbezpieczeństwo jest głównym problemem dla osób fizycznych i organizacji ze względu na rosnącą częstotliwość cyberataków. Uznając to, Komisja Europejska wprowadziła w 2016 r. dyrektywę w sprawie bezpieczeństwa sieci i informacji (NIS) w celu zwiększenia cyberbezpieczeństwa w całej Unii Europejskiej. Dyrektywa nie wskazywała jednak podmiotów ponoszących odpowiedzialność, co skłoniło Komisję do zastąpienia jej bardziej solidną dyrektywą NIS2.

Dyrektywa NIS2 zobowiązuje przedsiębiorstwa do wdrożenia kluczowych środków cyberbezpieczeństwa, w tym bezpieczeństwa łańcucha dostaw, kryptografii i szyfrowania (art. 18). Artykuł 89 kładzie nacisk na przyjęcie podstawowych praktyk higieny cybernetycznej, takich jak zasady zerowego zaufania, aktualizacje oprogramowania, konfiguracja urządzeń, segmentacja sieci oraz zarządzanie tożsamością i dostępem dla kluczowych i ważnych podmiotów.

NIS a NIS2 - co się zmieniło?

Istnieją pewne istotne różnice między starą a nową dyrektywą:

- Nowy wniosek usuwa rozróżnienie między operatorami usług kluczowych (OES) i dostawcami usług cyfrowych (DSP), zamiast tego klasyfikując podmioty jako kluczowe lub ważne.
- Zakres dyrektywy został rozszerzony, aby objąć nowe sektory w oparciu o ich krytyczne znaczenie dla gospodarki i społeczeństwa, w tym wszystkie średnie i duże przedsiębiorstwa w tych sektorach. Państwa członkowskie mogą również zidentyfikować mniejsze podmioty o profilu wysokiego ryzyka.
- Zaproponowano utworzenie europejskiej sieci organizacji łącznikowych ds. kryzysów cybernetycznych (EU-CyCLONe) w celu wspólnego przygotowywania i wdrażania planów szybkiego reagowania kryzysowego, na przykład w przypadku incydentu lub kryzysu cybernetycznego na dużą skalę.
- Zwiększona koordynacja w zakresie ujawniania nowych luk w zabezpieczeniach wykrytych w całej Unii. Ustanowiono wykaz sankcji administracyjnych (podobnych do tych przewidzianych w RODO), w tym grzywny za naruszenie obowiązków w zakresie zgłaszania ryzyka cybernetycznego i zarządzania nim.
- NIS2 nakłada bezpośrednie obowiązki na organy zarządzające w zakresie wdrażania i nadzorowania zgodności ich organizacji z przepisami - potencjalnie skutkując grzywnami i tymczasowym zakazem sprawowania funkcji zarządczych, w tym na poziomie C-suite.

Ponadto wprowadza bardziej precyzyjne przepisy dotyczące procesu zgłaszania incydentów, treści raportów i terminów (w ciągu 24 godzin od wykrycia incydentu). Na poziomie europejskim wniosek wzmacnia cyberbezpieczeństwo kluczowych technologii informacyjno-komunikacyjnych. Państwa członkowskie, we współpracy z Komisją i Agencją Unii Europejskiej ds. Cyberbezpieczeństwa ENISA, będą musiały przeprowadzać skoordynowane oceny ryzyka krytycznych łańcuchów dostaw.

Kogo dotyczy dyrektywa?

Podczas gdy na mocy starej dyrektywy NIS państwa członkowskie były odpowiedzialne za określenie, które podmioty spełniają kryteria kwalifikujące je jako operatorów usług kluczowych, nowa dyrektywa NIS2 wprowadza zasadę ograniczenia wielkości. Oznacza to, że **wszystkie średnie i duże podmioty działające w sektorach lub świadczące usługi objęte dyrektywą będą objęte jej zakresem**.

Poniżej znajdziesz klasyfikację według zasady wielkości limitu:

Kluczowe podmioty (Essential Entities - EE) Próg wielkości: różni się w zależności od sektora, ale generalnie 250 pracowników, roczny obrót w wysokości 50 mln EUR lub bilans w wysokości 43 mln EUR	**Podmioty ważne (Important Entities - IE)** Próg wielkości: różni się w zależności od sektora, ale zazwyczaj wynosi 50 pracowników, roczny obrót 10 mln EUR lub bilans 10 mln EUR
Energia	Usługi pocztowe
Transport	Gospodarka odpadami
Finanse	Chemikalia
Administracja publiczna	Badania
Zdrowie	Żywność
Przestrzeń	Produkcja
Zaopatrzenie w wodę (pitną i ściekową)	Dostawcy cyfrowi (np. sieci społecznościowe, wyszukiwarki, rynki internetowe)
Infrastruktura cyfrowa (np. dostawcy usług przetwarzania w chmurze i zarządzania ICT)	

NIS2 obejmuje również organy administracji publicznej na szczeblu centralnym i regionalnym, ale nie obejmuje parlamentów i banków centralnych.

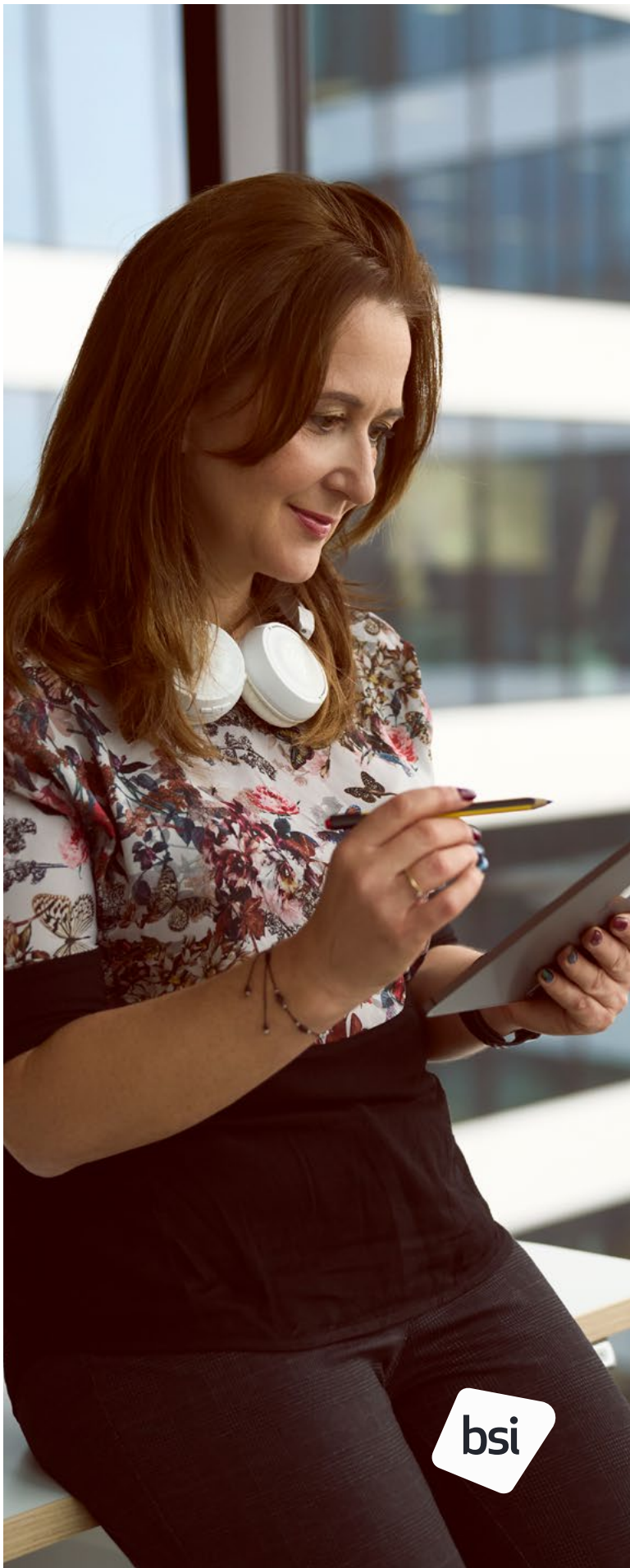
Kiedy dyrektywa będzie egzekwowana?

Wszystkie państwa członkowskie UE muszą włączyć te nowe obowiązki do swoich przepisów krajowych przed wrześniem 2024 roku. Po ostatecznym zatwierdzeniu, podmioty objęte zakresem dyrektywy będą miały 21-miesięczny okres na dostosowanie się do dyrektywy po jej wejściu w życie. Poniższa lista przedstawia harmonogram rozwoju NIS:

- **6 lipca 2016 r.:** Przyjęcie NIS 9 maja 2018 r.: Termin transpozycji NIS do prawa krajowego przez państwa członkowskie
- **7 lipca 2020 r.:** Komisja Europejska rozpoczyna konsultacje w sprawie reformy NIS
- **16 grudnia 2020 r.:** Komisja Europejska publikuje wniosek w sprawie NIS2
- **22 listopada 2021 r.:** Parlament Europejski przyjmuje stanowisko negocjacyjne
- **3 grudnia 2021 r.:** Rada Europejska przyjmuje stanowisko negocjacyjne
- **13 stycznia 2022 r.:** Pierwsza runda negocjacji trójstronnych
- **16 lutego 2022 r.:** Druga runda negocjacji trójstronnych
- **13 maja 2022 r.:** Osiągnięto porozumienie polityczne
- **10 listopada 2022 r.:** Parlament Europejski głosuje za przyjęciem NIS2
- **28 listopada 2022 r.:** NIS2 zatwierdzony przez Radę UE
- **27 grudnia 2022 r.:** dyrektywa NI2 zostaje opublikowana w Dzienniku Urzędowym UE i i wchodzi w życie 20 dni później, 16 stycznia 2023 r.
- **17 października 2024 r.:** Termin transpozycji NIS2 do prawa krajowego przez państwa członkowskie

Jak możemy pomóc Twojej firmie zachować zgodność z NIS2?

W BSI mamy duży zespół wysoce doświadczonych, wiodących w branży ekspertów, którzy pomogą zapewnić, że Ty i Twoja firma spełnicie wszystkie wymogi bezpieczeństwa, których potrzebujecie, aby wyprzedzić dyrektywę NIS2. Z naszą pomocą organizacje mogą uniknąć potencjalnych kar finansowych i wzbudzić dalsze zaufanie wśród klientów. Od wstępnej identyfikacji OES po samoocenę, ocenę ryzyka i postępowanie z ryzykiem, nasze doświadczenie we współpracy z organizacjami z różnych sektorów może pomóc Ci na drodze do osiągnięcia zgodności z dyrektywą NIS2.



BSI oferuje obecnie następujące usługi związane z wymogami NIS2:

- Strategia/zarządzanie cyberbezpieczeństwem
- Oceny stanu/dojrzałości cyberbezpieczeństwa w odniesieniu do standardowych ram branżowych
- Rozwój bezpieczeństwa informacji/strategii cybernetycznej/prezentacje dla zarządu
- Analiza luk i wsparcie wdrożenia (ISO 27001, SOC 2, NIST CSF/800-53)
- Świadomość i szkolenia w zakresie bezpieczeństwa informacji Ciągłość działania (ISO 22301)

Krisenmanagement und Maßnahmen bei Sicherheitsvorfällen

- Ciągłość działania (ISO 22301)
  - Analiza wpływu na biznes / (BIA) / rozwój polityki / planowanie ciągłości działania
- Wsparcie, wdrażanie i okresowe testowanie odzyskiwania danych po awarii
- Testy penetracyjne oparte na zagrożeniach (TLPT)
- Wywiad z otwartych źródeł (OSINT)
- Ocena bezpieczeństwa fizycznego Symulacja ataku (zespół czerwony/niebieski/fioletowy)
- Planowanie i wdrażanie reagowania na incydenty (ISO27035)
- Modelowanie zagrożeń/oceny zagrożeń
- Ocena bieżących możliwości planowania i raportowania reakcji na incydenty
- Testowanie reakcji na incydenty/szkolenie personelu

Zarządzanie ryzykiem i raportowanie

- Opracowanie i wdrożenie ram zarządzania ryzykiem IT (ISO 27005)
  - Zarządzanie ryzykiem stron trzecich (ISO 27036-2)
  - Bieżąca ocena stanu zarządzania cyklem życia podmiotów zewnętrznych
  - Opracowanie kompleksowych ram zarządzania dostawcami
  - Wdrożenie ram zarządzania ryzykiem stron trzecich wraz z bieżącym wsparciem zarządzania ryzykiem
- BSI współpracuje z partnerami technologicznymi, którzy dysponują narzędziami ułatwiającymi zarządzanie całym cyklem życia dostawcy
  - Analiza zagrożeń/Certyfikacja zespołu reagowania kryzysowego (CERT)
  - Oceń obecną pozycję i określ przyszły stan
  - Zbuduj ramy raportowania

Dlaczego ISO 27001 i ISO 22301 są kluczowe dla zgodności z NIS2?

Przepisy NIS zalecają, aby firmy w swoich wysiłkach na rzecz zapewnienia zgodności traktowały priorytetowo „zgodność z międzynarodowymi standardami". Ponadto wytyczne techniczne Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) dostosowują każdy cel bezpieczeństwa do standardów najlepszych praktyk, takich jak ISO 27001.

Spośród wszystkich usług, które BSI może zapewnić Twojej firmie w związku z NIS2, dwie normy wydają się być kluczowe: ISO 27001 i ISO 22301.

- Wdrożenie Systemu Zarządzania Informacją (ISMS) zgodnego z ISO 27001 umożliwia organizacjom zminimalizowanie ryzyka i narażenia na zagrożenia bezpieczeństwa. Wiąże się to z określeniem niezbędnych zasad, zastosowaniem odpowiednich technologii i zapewnieniem szkoleń dla personelu w celu zapobiegania błędom. Wymagając corocznej oceny ryzyka, ISO 27001 umożliwia organizacjom proaktywne reagowanie na zmieniający się krajobraz ryzyka.
- ISO 27001 nie tylko ułatwia spełnienie wymagań NIS2, ale także umożliwia organizacjom uzyskanie niezależnie audytowanej certyfikacji. Certyfikat ten służy jako namacalny dowód dla dostawców, interesariuszy i organów regulacyjnych, pokazując przyjęcie "odpowiednich i proporcjonalnych" środków technicznych i organizacyjnych oraz zapewniając przewagę konkurencyjną na rynku.
- Organizacjom poszukującym bardziej zaawansowanego podejścia zaleca się dodanie normy ISO 22301 w zakresie zarządzania ciągłością działania. Norma ISO 22301 pomaga we wdrażaniu, utrzymywaniu i ciągłym doskonaleniu praktyk w zakresie ciągłości działania. Podczas gdy ISO 27001 obejmuje aspekty zarządzania ciągłością działania (BCM), ISO 22301 zapewnia zdefiniowany proces wdrażania BCM. Certyfikacja zgodności z ISO 22301 dodatkowo wzmacnia zgodność z NIS2.

Synergia między ISO 27001 i ISO 22301 pozwala organizacjom na opracowanie zintegrowanego systemu zarządzania obejmującego zarówno ISMS, jak i BCMS. To holistyczne podejście nie tylko pomaga w zapewnieniu zgodności, ale także sprzyja rozwojowi solidnej odporności cybernetycznej.

Dlaczego BSI?

W BSI nasze światowej klasy możliwości wzbudzają zaufanie klientów w zakresie cyberbezpieczeństwa i higieny. Oferujemy dogłębną wiedzę specjalistyczną w zakresie cyberbezpieczeństwa, zarządzania ryzykiem i odporności informacji, z globalną perspektywą międzysektorową. Nasze zrozumienie obejmuje kwestie wpływające na sektor publiczny, pojawiające się zagrożenia i praktyczne doświadczenie branżowe w zarządzaniu ryzykiem cybernetycznym i odpornością.

Co możesz zrobić już teraz?

- Sprawdź, czy Twoja organizacja jest objęta dyrektywą
- Poinformuj zarząd/radę nadzorczą o zbliżających się regulacjach
- Skontaktuj się z nami, aby uzyskać wsparcie w zakresie zgodności z NIS2
  certyfikacja@bsigroup.com