EUROPEJSKA DYREKTYWA

NETWORK AND INFORMATION SYSTEMS (NIS2)

Czy jesteś na nią gotowy?

Arkanet

Bezpieczeństwo to my

Dyrektywa NIS2 – co to właściwie jest?

To dyrektywa Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 14 grudnia 2022 r., w sprawie środków na rzecz wysokiego, wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej. NIS2 uchyla dyrektywę UR 2016/1148 zwaną NIS. Dyrektywa weszła w życie 16 stycznia 2023 roku i musi zostać wprowadzona w państwach członkowskich do 21 miesięcy od tej daty, czyli maksymalnie do 18 października 2024 r.

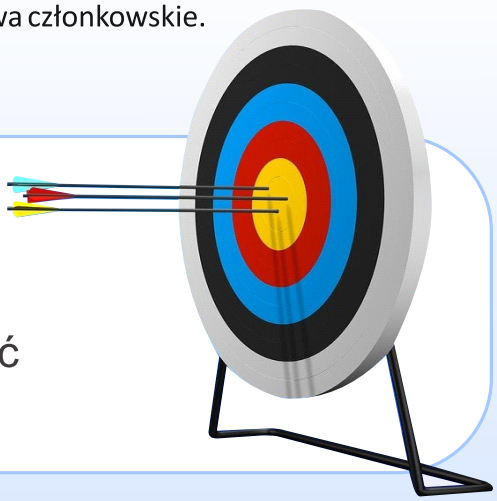
Według zapisów dyrektywy NIS2 od momentu wejścia w życie NIS zostały poczynione znaczne postępy w podnoszeniu poziomu cyberbezpieczeństwa UE, jednak jej przegląd ujawnił tkwiące w niej braki. Bez ich uzupełnienia nie można zaradzić obecnym i pojawiającym się wyzwaniom w zakresie cyberodporności. Państwa członkowskie wdrażały pierwszą dyrektywę w bardzo rozbieżny od siebie sposób, co mogło znacząco wpływać na poziom cyberbezpieczeństwa w przypadku współpracy transgranicznej.

Dyrektywa określa:

- obowiązki państw członkowskich dotyczące przyjęcia krajowych strategii cyberbezpieczeństwa oraz powołania właściwych organów i zespołów zarządzania, reagowania itp.,
- środki zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązki w zakresie zgłaszania incydentów,
- zasady i obowiązki w zakresie wymiany informacji o cyberbezpieczeństwie,
- obowiązki w zakresie nadzorowania i egzekwowania przepisów przez państwa członkowskie.

CEL DYREKTYWY NIS2

Osiągnięcie wspólnego, wysokiego poziomu cyberbezpieczeństwa w całej Unii, aby poprawić funkcjonowanie rynku wewnętrznego.



Jaki jest zakres podmiotowy dyrektywy?

NIS2 ma zastosowanie do podmiotów mających charakter krytyczny, a także podmiotów świadczących usługi rejestracji nazw domen – w obu przypadkach niezależnie od ich wielkości.

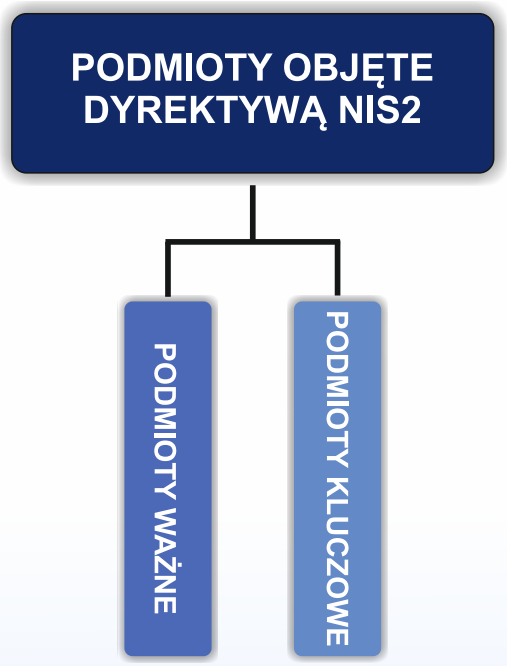
Dyrektywa ma zastosowanie także do podmiotów publicznych lub prywatnych (szczegółowy opis znajduje się w załączniku I oraz II), które kwalifikują się jako średnie przedsiębiorstwa (zatrudniają od 50 do 250 osób oraz ich obroty roczne lub suma bilansowa mieszczą się w przedziale 10-50 mln euro) lub przekraczają pułapy dla średnich przedsiębiorstw oraz świadczą usługi albo prowadzą działalność w Unii Europejskiej.

Wytyczne tego dokumentu stosuje się także do podmiotów administracji publicznej:
„-na poziomie rządu centralnego, zdefiniowanym przez państwo członkowskie zgodnie z prawem krajowym, lub
- na poziomie regionalnym zdefiniowanym przez państwo członkowskie zgodnie z prawem krajowym, który zgodnie z oceną opartą na analizie ryzyka świadczy usługi, których zakłócenie mogłoby mieć znaczący wpływ na krytyczną działalność społeczną lub gospodarczą."

NIS2 nie obowiązuje podmiotów administracji publicznej, które prowadzą działalność w dziedzinach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, w tym zapobiegania jego naruszeniom. Państwa członkowskie mogą również zwolnić podmioty, które prowadzą działania w obszarach wyżej wymienionych lub świadczą usługi wyłącznie na rzecz wyżej wymienionych podmiotów administracji publicznej.

Arkanet
Bezpieczeństwo to my

Powyższe zapisy nie mają zastosowania gdy podmiot działa jako dostawca usług zaufania (usługi zaufania to usługi elektroniczne, które obejmują m.in. wydawanie kwalifikowanych podpisów elektronicznych, pieczęci elektronicznych i elektronicznych znaczników czasu, a także odpowiednich dla nich certyfikatów).



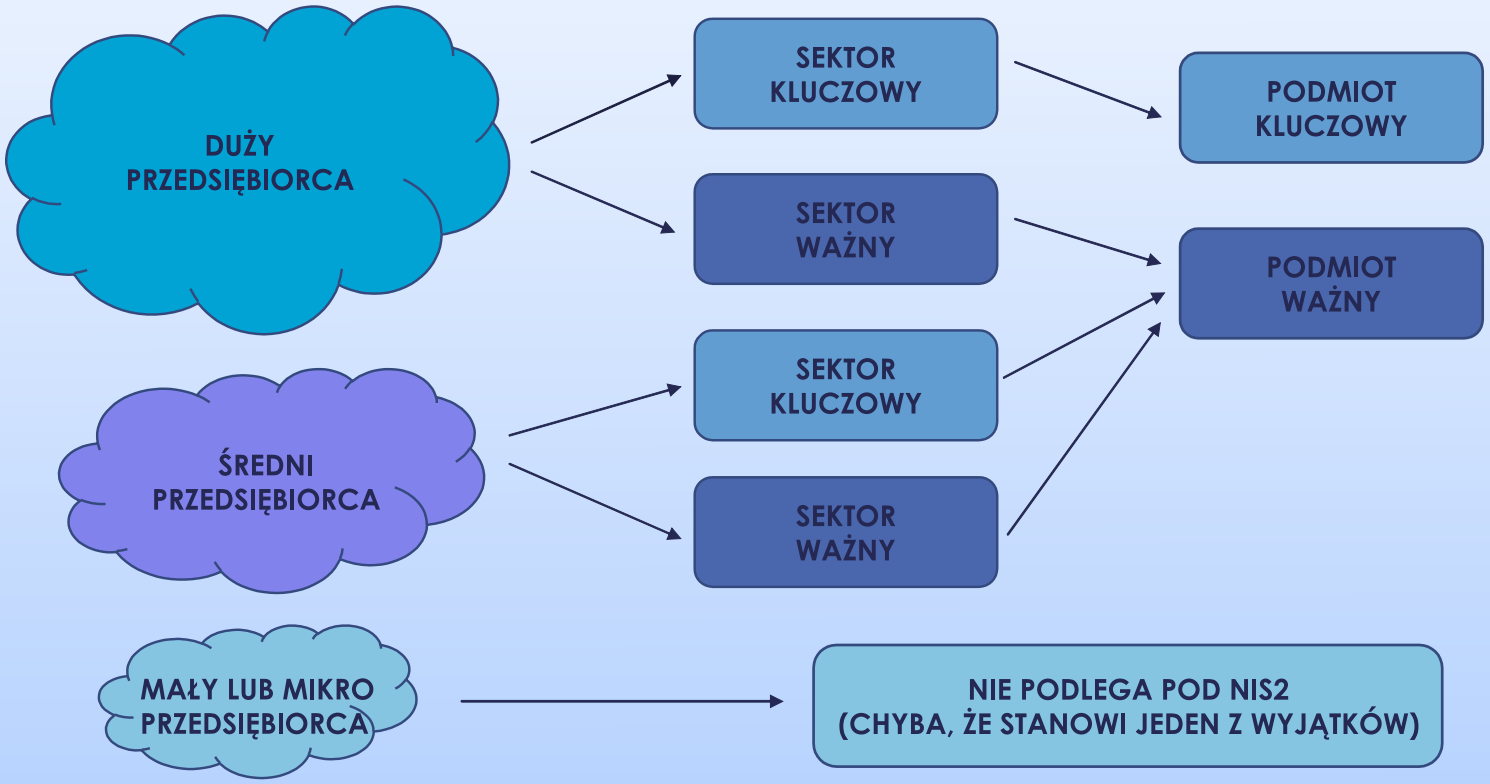
Podmioty kluczowe i ważne

Definicję podmiotów kluczowych i ważnych szczegółowo objaśniają załączniki I oraz II dyrektywy. Do 17 kwietnia 2025 państwa członkowskie mają ustanowić wykaz tych podmiotów oraz osobno podmiotów świadczących usługi rejestracji nazw domen. Państwa członkowskie minimum co 2 lata muszą dokonać przeglądu i aktualizacji tego wykazu.

Do określenia kategorii podmiotu państwa członkowskie będą wymagać przedłożenia informacji:

- nazwa,
- adres,
- aktualne dane kontaktowe,
- adresy poczty elektronicznej,
- zakresy adresów IP oraz numerów telefonów.

W stosownych przypadkach mogą wymagać sektora i podsektora podmiotu zgodnie z załącznikiem I lub II oraz wykazu państw członkowskich, w których świadczy usługi objęte zakresem stosowania dyrektywy.



Arkanet
Bezpieczeństwo to my

Skoordynowane ramy w zakresie cyberbezpieczeństwa

„Polityka cyberhigieny stanowi podstawę pozwalającą chronić infrastrukturę sieci i systemów informatycznych, bezpieczeństwo sprzętu, oprogramowania i aplikacji internetowych oraz dane przedsiębiorstw lub użytkowników końcowych wykorzystywane przez podmioty. Polityka cyberhigieny obejmująca wspólny podstawowy zestaw praktyk – w tym aktualizacje oprogramowania i sprzętu, zmianę haseł, zarządzanie nowymi instalacjami, ograniczanie kont dostępu na poziomie administratora oraz tworzenie kopii zapasowych danych – umożliwia utworzenie proaktywnych ram gotowości oraz zapewnienie ogólnego bezpieczeństwa i ochrony w razie incydentów lub cyberzagrożeń. ENISA powinna monitorować i analizować politykę państw członkowskich dotyczącą cyberhigieny."

„W ostatnich latach Unia doświadcza gwałtownego wzrostu liczby cyberataków z użyciem oprogramowania typu >>ransomware<<, w których złośliwe oprogramowanie szyfruje dane i systemy oraz domaga się okupu za ich odblokowanie. Coraz większa częstotliwość i dotkliwość cyberataków z użyciem oprogramowania typu >>ransomware<< może wynikać z szeregu czynników, takich jak różne wzorce ataków, przestępcze modele biznesowe typu >>oprogramowanie wymuszające okup jako usługa<< i kryptowaluty, żądania okupu oraz wzrost liczby ataków w łańcuchu dostaw. W ramach krajowych strategii cyberbezpieczeństwa państwa członkowskie powinny opracować politykę odnoszącą się do wzrostu liczby cyberataków z wykorzystaniem oprogramowania typu >>ransomware<<."

Krajowa strategia bezpieczeństwa

„Każde państwo członkowskie przyjmuje krajową strategię cyberbezpieczeństwa, która przewiduje cele strategiczne, zasoby kluczowe do osiągnięcia tych celów i odpowiednie środki z zakresu polityk publicznych i regulacji, z myślą o osiągnięciu i utrzymaniu wysokiego poziomu cyberbezpieczeństwa."

Państwo członkowskie przekazuje Komisji Wspólnot Europejskich krajową strategię cyberbezpieczeństwa do 3 miesięcy od jej przyjęcia i regularnie, nie rzadziej niż co 5 lat, przeprowadzają jej ocenę. W razie potrzeby musi zaktualizować tę strategię – w czym może pomóc ENISA (na prośbę danego państwa).

Właściwe organy, zarządzanie kryzysowe i reagowanie na incydenty

Zgodnie z artykułem 8 dyrektywy, każde państwo wyznacza przynajmniej jeden organ odpowiedzialny za cyberbezpieczeństwo i zadania nadzorcze. Ponadto ustanawia jeden pojedynczy punkt kontaktowy, który zapewnia transgraniczną współpracę z innymi państwami członkowskimi, a w specjalnych sytuacjach z komisją i ENISA.

Artykuł 9 stanowi , że każde państwo członkowskie wyznacza przynajmniej jeden organ odpowiedzialny za zarządzanie incydentami i kryzysowe na dużą skalę. Musi on mieć odpowiednie zasoby do wykonywania swoich obowiązków oraz mieć zapewnioną spójność z ogólnymi krajowymi ramami zarządzania kryzysowego.

Państwa członkowskie muszą wyznaczyć przynajmniej jeden Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT), który odpowiedzialny jest za obsługę incydentów w sektorach, podsektorach i podmiotach zgodnie z załącznikami I i II. W Polsce funkcjonuje taki zespół – jest prowadzony przez szefa Agencji Bezpieczeństwa Wewnętrznego. Więcej informacji na jego temat można uzyskać tutaj -> https://csirt.gov.pl/

Zarządzanie ryzykiem

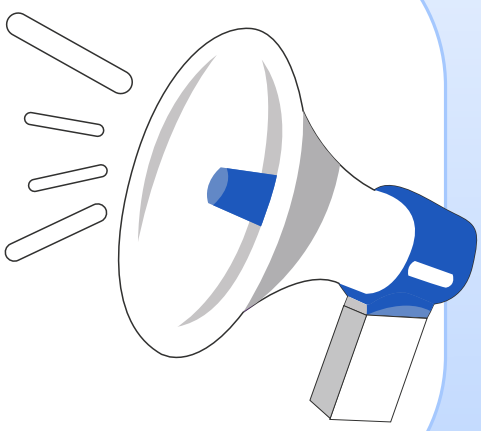
Państwa członkowskie zapewniają, aby podmioty kluczowe i ważne wprowadziły odpowiednie środki zarządzania ryzykiem dla bezpieczeństwa sieci i systemów IT danej organizacji, w celu zapobiegania oraz minimalizowania wpływu incydentów na odbiorców ich usług.

Środki te muszą obejmować co najmniej następujące elementy: politykę analizy ryzyka i bezpieczeństwa systemów IT, obsługę incydentu, ciągłość działania, bezpieczeństwo łańcucha dostaw, bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów IT, procedury oceniające skuteczność środków zarządzania ryzykiem, praktyki cyberhigieny i szkolenia, procedury stosowania kryptografii i szyfrowania, bezpieczeństwo zasobów ludzkich, a w stosownych przypadkach stosowanie uwierzytelniania wieloskładnikowego (MFA) lub ciągłego oraz zabezpieczanie korespondencji.

Zgłaszanie incydentów

Podmioty kluczowe i ważne mają zgłaszać właściwemu CSIRT lub właściwemu innemu organowi poważny incydent, który staje się takowym jeżeli:

- spowodował lub może spowodować dotkliwe zakłócenia usług lub straty finansowe;
- wpłynął lub jest w stanie wpłynąć na osoby fizyczne lub prawne powodując jej szkody (majątkowe i niemajątkowe).



Zgłoszenie musi nastąpić w terminie 24 godzin od wystąpienia incydentu – wczesne ostrzeżenie oraz 72 godzin – zgłoszenie incydentu z aktualizacją informacji. Do miesiąca od zgłoszenia musi zostać wysłane sprawozdanie końcowe, w którym znaleźć muszą się następujące elementy: szczegółowy opis incydentu, rodzaj zagrożenia lub jego przyczyna, zastosowane środki bezpieczeństwa, transgraniczne skutki incydentu (jeśli dotyczy).

KARY

Kary pieniężne w dyrektywie NIS2 to temat bardzo głośny – kwoty robią wrażenie. Zanim jednak o tym, zgodnie z artykułem 32 dyrektywy „państwa członkowskie zapewniają, by środki nadzoru lub egzekwowania przepisów nakładane na podmioty kluczowe w odniesieniu do obowiązków określonych w niniejszej dyrektywie były skuteczne, proporcjonalne i odstraszające, stosownie do okoliczności każdego indywidualnego przypadku."

Państwa członkowskie zapewniają, że wykonując uprawnienia nadzorcze odpowiednie organy mogą objąć je m.in. kontrolami, audytami doraźnymi, skanami bezpieczeństwa czy wnioskami o udzielenie dostępu do danych. Ponadto powołane instytuacje mają być uprawnione do wydawania ostrzeżeń i wiążących poleceń dotyczących działań niezgodnych z dyrektywą NIS2. Jeśli te środki nie przyniosą rezultatu mogą nałożyć lub zwrócić się do odpowiednich organów lub sądów o nałożenie kary pieniężnej, a ich wartość to:

- dla podmiotów kluczowych maksymalna wysokość co najmniej 10 000 000 EUR lub 2% rocznego światowego obrotu w poprzednim roku obrotowym przedsiębiorstwa,
- dla podmiotów ważnych maksymalna wysokość co najmniej 7 000 000 EUR lub 1,4% rocznego światowego obrotu w poprzednim roku obrotowym przedsiębiorstwa.

Przepisy końcowe – najważniejsze informacje

- Do dnia 17 października 2027 r., a następnie co 36 miesięcy Komisja Eurpejska przeprowadza przegląd funkcjonowania niniejszej dyrektywy i składa Parlamentowi Europejskiemu sprawozdanie na ten temat.

- Do dnia 17 października 2024 r. państwa członkowskie przyjmują i publikują przepisy niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie powiadamiają one o tym Komisję. Państwa członkowskie stosują te przepisy od dnia 18 października 2024 r.

- Dyrektywa (UE) 2016/1148 (NIS1) traci moc ze skutkiem od dnia 18 października 2024 roku.

- Niniejsza dyrektywa skierowana jest do państw członkowskich UE.

Wszystkie cytaty pochodzą z Dyrektywy NIS2 dostępnej pod adresem https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

Arkanet
Bezpieczeństwo to my