

Krystian Mączka<sup>1</sup>  
Akademia WSB  
ORCID 0000-0001-6341-8189

## Dyrektywa NIS2 jako wytyczna do wdrożenia systemu zarządzania bezpieczeństwem informacji w organizacji

The NIS2 Directive as a guideline for implementing an information security management system in an organization

### Wprowadzenie

W dobie niemalże pełnej cyfryzacji i postępującej zależności jednostki oraz całych społeczeństw od technologii informatycznych zapewnienie bezpieczeństwa danych przechowywanych w systemach IT staje się jednym z kluczowych wyzwań zarówno dla organizacji publicznych, jak i prywatnych. Rozwój cyfrowych usług, Internetu rzeczy (IoT), a także rosnąca liczba zagrożeń związanych z cyberatakami sprawiają, że zarządzanie ryzykiem cyfrowym staje się absolutnym priorytetem. W obliczu tych wyzwań Unia Europejska podjęła kroki w celu ujednoczenia wymagań w zakresie cyberbezpieczeństwa państw członkowskich, czego efektem jest dyrektywa NIS2 (ang. *Network and Information Security Directive 2*), która zastąpiła wcześniejszą dyrektywę NIS (Dyrektywy UE, 2022, 2016).

Dyrektywa NIS2 wyznacza ujednoczone standardy ochrony kluczowych zasobów i infrastruktur, które mają na celu podniesienie odporności Unii Eu-

<sup>1</sup> Krystian Mączka: dr inż., Akademia WSB, kmaczka@wsb.edu.pl

ropejskiej na zagrożenia związane z cyberatakami oraz incydenty związane z ciągłością działania, a także wzmocnienie bezpieczeństwa sieci, systemów informatycznych i łańcucha dostaw w zakresie systemów i usług. Narzuca państwom członkowskim obowiązek wdrożenia określonych przepisów oraz nałożenia wyższych, ale przede wszystkim, ujednoliconych standardów bezpieczeństwa na organizacje krytyczne dla gospodarki i społeczeństwa. Wskazać tutaj należy dostawców usług cyfrowych, sektor energetyczny, wodociągowy, finansowy, a także instytucje publiczne oraz jednostki badawcze. Celem NIS2 jest nie tylko zwiększenie odporności poszczególnych organizacji, ale również poprawa koordynacji działań w całej Unii Europejskiej, co ma kluczowe znaczenie dla przeciwdziałania cyberzagrożeniom, które najczęściej wykraczają poza granice jednego kraju, a ich ściganie w ramach kompetencji organów ścigania działających samodzielnie w zakresie wewnętrznym danego kraju jest bardzo ograniczone (Wrzosek, 2021).

Polska jako członek Unii Europejskiej zobowiązana jest do implementacji postanowień dyrektywy NIS2 poprzez stworzenie prawnego instrumentu na poziomie krajowym. Naturalnym stała się więc nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) (Ministerstwo Cyfryzacji, 2024). Wprowadzenie NIS2 wiąże się z nowymi obowiązkami dla organizacji, które muszą dostosować swoje struktury, procesy oraz rozwiązania technologiczne do nowych standardów. Zrozumienie dyrektywy oraz noweli polskiej ustawy KSC i ich głównych założeń staje się więc kluczowe dla instytucji działających na polskim rynku, aby skutecznie chronić swoje zasoby i minimalizować ryzyko strat związanych z potencjalnymi incydentami cybernetycznymi.

Artykuł ten ma na celu przedstawienie najważniejszych aspektów dyrektywy NIS2 i idącej za nią nowelizacji ustawy o KSC oraz ich wpływu na bezpieczeństwo danych w organizacjach. W kolejnych sekcjach zostaną omówione kluczowe wymagania dyrektywy, szczegóły nowelizacji ustawy o KSC oraz wyzwania i możliwości, jakie niesie za sobą implementacja nowych regulacji. W szczególności artykuł ten podejmie próbę analizy, w jaki sposób dyrektywa NIS2 może stanowić drogowskaz dla organizacji, które chcą efektywnie podnosić poziom swojego bezpieczeństwa oraz dostosować się do rosnących wymagań w zakresie ochrony danych.

## Omówienie głównych wytycznych dyrektywy NIS2 i zakresu jej stosowania

Dyrektywa NIS2 jest rozwinięciem i aktualizacją dyrektywy NIS, przyjętej w 2016 roku, która miała na celu ustanowienie pierwszego wspólnotowego, ramowego podejścia do bezpieczeństwa sieci i informacji. Zapisy dyrektywy NIS były jednak zbyt ogólne i rozmyte (Polćák, 2022), dlatego, w obliczu dynamicznego rozwoju technologii i nowych cyberzagrożeń oraz znacznego postępu cyfryzacji podmiotów publicznych i prywatnych, Unia Europejska postanowiła zaostrzyć i rozszerzyć regulacje w tym obszarze. Dyrektywa NIS2, przyjęta w 2022 roku, odzwierciedliła te potrzeby, ukazując główny cel, jakim było wzmocnienie „cyberodporności” oraz poprawę zdolności do przeciwdziałania incydentom związanym z cyberbezpieczeństwem na poziomie organizacji, krajowym i wspólnotowym.

Dyrektywa NIS2 obejmuje szeroki zakres sektorów i organizacji, których działalność jest kluczowa dla funkcjonowania gospodarki, infrastruktury krytycznej i usług społecznych. Jej postanowienia dotyczą między innymi sektora energetycznego, transportowego, finansowego, zdrowotnego, wodociągowego, dostawców usług cyfrowych, ale także sektor badań naukowych i organizacje badawcze. Co istotne, dyrektywa rozszerza zakres podmiotów objętych obowiązkami bezpieczeństwa o małe i średnie przedsiębiorstwa, które spełniają określone kryteria znaczenia w danym sektorze. Oznacza to, że do stosowania NIS2 zobowiązane są nie tylko duże korporacje, ale także mniejsze jednostki, które mogą mieć znaczący wpływ na funkcjonowanie łańcucha dostaw lub dostępności usług kluczowych dla bezpieczeństwa obywateli i gospodarki, lub te, które realizują projekty naukowo-badawcze w partnerstwie z organizacjami badawczymi. Podstawowym kryterium podlegania regulacjom dyrektywy NIS2 jest więc znaczenie organizacji dla funkcjonowania kluczowych sektorów gospodarki, a nie tylko jej wielkość czy obszar działania. Dyrektywa wprowadza również nowe obowiązki dla dostawców usług cyfrowych, takich jak platformy handlu internetowego, wyszukiwarki oraz dostawcy chmur obliczeniowych, podkreślając tym samym kluczową rolę sektora IT w zapewnieniu bezpieczeństwa danych i usług (Rogalski, 2024).

Dyrektywa NIS2 nakłada na organizacje obowiązki w zakresie oceny ryzyka, wdrożenia odpowiednich środków ochrony oraz regularnego monitorowania stanu bezpieczeństwa. Podmiot objęty dyrektywą musi udowodnić, że dysponuje zasobami technologicznymi oraz organizacyjnymi umożliwiającymi szybką reakcję na zagrożenia i incydenty. W praktyce oznacza to konieczność wdrożenia środków kontroli dostępu, szyfrowania danych, regularnego monitorowania sieci oraz stosowania systemów detekcji i ochrony przed atakami. W odróżnieniu od poprzedniej dyrektywy, NIS2 wprowadza bardziej szczegółowe wytyczne, które wymagają między innymi, aby organizacje posiadały spójną politykę zarządzania ryzykiem oraz plan reagowania na incydenty (Van't Schip, 2024).

Różnicą względem poprzedniego rozporządzenia jest wymóg zgłaszania incydentów bezpieczeństwa na poziomie krajowym, ale również na poziomie międzynarodowym, w przypadku, gdy incydent ma potencjalne skutki transgraniczne. Podmioty podlegające pod dyrektywę NIS2 są zobowiązane do raportowania incydentów o istotnym wpływie na bezpieczeństwo do tak zwanych „krajowych punktów kontaktowych” w możliwie najkrótszym czasie (Chałubińska-Jentkiewicz, Nowikowska, 2024).

Dyrektywa NIS2 wprowadza także mechanizm kar i sankcji za nieprzestrzeganie wymagań dotyczących cyberbezpieczeństwa, które mogą obejmować zarówno kary finansowe, jak i administracyjne, a w niektórych przypadkach mogą skutkować ograniczeniem dostępu do rynku.

Konsekwencje wynikające z konieczności wdrożenia dyrektywy NIS2 będą miały wpływ na funkcjonowanie wielu sektorów, tworząc nową rzeczywistość w obszarze ochrony danych i wzmacniając bezpieczeństwo cyfrowe zarówno na poziomie organizacyjnym, krajowym i europejskim.

## Nowelizacja polskiej ustawy o KSC

W Polsce dyrektywa NIS2 będzie implementowana poprzez nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), co oznacza, że polskie organizacje będą musiały dostosować swoje procesy do nowych wytycznych, a sama nowelizacja ma za zadanie dostosować polskie przepisy do

unijnej dyrektywy oraz poprawić ogólny poziom zabezpieczeń w kraju. Wdrażanie NIS2 dla polskich organizacji z pewnością stanowić będzie wyzwanie, ale będzie również szansą na unowocześnienie infrastruktury cyberbezpieczeństwa i podniesienie świadomości w zakresie zarządzania ryzykiem w organizacjach o różnej wielkości i charakterze.

Projekt ustawy, nazywany roboczo „KSC 2.0”, został opublikowany 23 kwietnia 2024 roku i poddany konsultacjom publicznym. W październiku 2024 opublikowana została kolejna wersja projektu, po uwzględnieniu prawie 1500 zgłoszonych poprawek (Ministerstwo Cyfryzacji, 2024, grudzień, 20). Ministerstwo Cyfryzacji ogłosiło, że nowelizacja ustawy o KSC została przekazana do dalszego procedowania przez odpowiednie komitety Rady Ministrów, a po zakończeniu prac na tym etapie, projekt trafi pod obrady samej Rady Ministrów. Równolegle propozycja zmian w ustawie zostanie skierowana do Komisji Wspólnej Rządu i Samorządu Terytorialnego w celu uzyskania opinii, a przedłożenie nowelizacji do Sejmu nastąpi jeszcze w bieżącym roku (Ministerstwo Cyfryzacji, 2024, sekcja „Kluczowe zmiany”).

Do kluczowych założeń projektu przedmiotowej ustawy zaliczyć można kilka obszarów. Głównym celem KSC 2.0 jest dostosowanie krajowych regulacji do dyrektywy NIS2, która z założenia wymaga od państw członkowskich UE ujednoczenia standardów ochrony kluczowych sektorów gospodarki. KSC 2.0 wdraża te regulacje, co umożliwi Polsce pełne włączenie się w jednolity system cyberbezpieczeństwa w UE. Projekt ustawy obejmuje także nowe grupy podmiotów, które będą musiały przestrzegać zaawansowanych wymogów bezpieczeństwa. Zgodnie z założeniami rozszerzony katalog podmiotów obejmuje dostawców usług chmurowych, zarządzanych usług cyberbezpieczeństwa, a także kluczowe sektory infrastruktury cyfrowej, takie jak dostawcy usług DNS i rejestry nazw domen. Regulacje te dotyczą również firm działających pośrednio w łańcuchach dostaw infrastruktury krytycznej, co ma na celu wzmocnienie zabezpieczeń na każdym etapie usług i produktów kluczowych dla bezpieczeństwa państwa. Ważnym aspektem projektu ustawy KSC 2.0 jest wprowadzenie obowiązku regularnych audytów cyberbezpieczeństwa dla organizacji kluczowych i ważnych. W szczególności, po nadaniu statusu podmiotu kluczowego, organizacja ma 24 miesiące na przeprowadze-

nie pierwszego audytu, a jego ważność wynosić będzie trzy lata – w pierwszej wersji projektu wynosić miała dwa lata (Ministerstwo Cyfryzacji, 2024). Wydłużenie terminu daje firmom więcej czasu na wdrożenie odpowiednich środków bezpieczeństwa, jednakże podmioty kluczowe muszą zapewniać ich skuteczność i zgodność z regulacjami na bieżąco.

W projekcie ustawy KSC 2.0 zaproponowane zostały wysokie kary finansowe za niespełnianie wymogów bezpieczeństwa, mające na celu egzekwowanie przepisów i zmobilizowanie organizacji do poważnego traktowania zagadnień cyberbezpieczeństwa. Przewidziano kary administracyjne sięgające do 10 mln EUR lub 2% rocznych przychodów w przypadku podmiotów kluczowych, oraz 7 mln EUR lub 1,4% łącznego obrotu rocznego dla podmiotów ważnych. Wiele dyskusji wywołały również zapisy dotyczące konieczności wycofania komponentów pochodzących od dostawców uznanych za dostawców wysokiego ryzyka, zwłaszcza w infrastrukturze sieci komórkowych 5G. Organizacje mają siedem lat na usunięcie takiego typu sprzętu oraz technologii, co ma na celu minimalizację zagrożeń dla bezpieczeństwa narodowego.

Implementacja ustawy o KSC 2.0 będzie wymagała dużych nakładów finansowych i organizacyjnych od przedsiębiorstw, które będą musiały dostosować swoje struktury i procesy do nowych wymogów. Dla firm prywatnych, zwłaszcza tych działających w sektorze kluczowym lub ważnym, nowelizacja oznacza konieczność wdrożenia zaawansowanych zabezpieczeń i procedur zgodności. Z drugiej strony, dla sektora publicznego KSC 2.0 stwarza większą odpowiedzialność za ochronę infrastruktury krytycznej oraz lepszą integrację z europejskim systemem cyberbezpieczeństwa, co ma sprzyjać szybkiemu reagowaniu na zagrożenia w skali międzynarodowej.

W zgłaszanych do projektu ustawy poprawkach często pojawiał się problem klasyfikacji danej organizacji jako podmiotu kluczowego lub ważnego. Wątpliwości w tym zakresie wydają się być kluczowe, bo od tej definicji zależy, czy dany podmiot będzie podlegał wytycznym ustawy. Najnowsza wersja projektu omawianej ustawy lepiej precyzuje kryteria, na podstawie których organizacje są klasyfikowane jako podmioty kluczowe lub ważne. W szczególności wprowadzono rozróżnienie na duże przedsiębiorstwa w sektorach kluczowych (takich jak energetyka, zdrowie, transport) i średnie przedsiębiorstwa

działające w sektorach ważnych (np. usługi cyfrowe czy przemysł chemiczny). Dostosowanie tych definicji ułatwia organizacjom ocenę, czy i jakie obowiązki cyberbezpieczeństwa ich dotyczą, zgodnie z nowymi regulacjami unijnymi.

Warto podkreślić także, że nowela obejmuje i narzuca wysokie obowiązki na tak zwanych dostawców usług zarządzanych w zakresie cyberbezpieczeństwa oraz usług chmurowych, szczególnie w zakresie przejrzystości danych podmiotu świadczącego takie usługi, jak i konieczności raportowania do właściwych organów w przypadku wystąpienia incydentu. Nowe przepisy nakładają na te podmioty obowiązek dostosowania środków ochrony do wytycznych Komisji Europejskiej, co ma na celu harmonizację działań zabezpieczających na poziomie UE.

Dostosowanie polskiej ustawy o KSC do wymagań NIS2 stanowi znaczący krok w kierunku unifikacji podejścia do cyberbezpieczeństwa na poziomie europejskim, umożliwiając skuteczniejsze zarządzanie ryzykiem oraz reagowanie na incydenty zagrażające infrastrukturze krytycznej w Polsce i całej UE.

## **Analiza głównych założeń związanych z podnoszeniem poziomu bezpieczeństwa w organizacji w oparciu o NIS2**

Dyrektywa NIS2 (a w ślad za nią nowelizacja ustawy o KSC) kładzie nacisk na wzmocnienie odporności organizacji na cyberzagrożenia poprzez wdrożenie wymogów dotyczących zarządzania ryzykiem, obowiązków raportowania incydentów, a także ustanowienie spójnych procedur zarządzania kryzysowego i zwiększenia zdolności do reakcji na zagrożenia. Poniżej analizie poddano kluczowe założenia NIS2 w kontekście podnoszenia poziomu bezpieczeństwa organizacji, które zostaną omówione w ramach czterech głównych obszarów.

### Zarządzanie ryzykiem i obowiązki związane z cyberbezpieczeństwem

Dyrektywa nakłada na organizacje obowiązek wdrożenia kompleksowego systemu zarządzania ryzykiem w zakresie cyberzagrożeń, które polegać powinno na systematycznym identyfikowaniu zagrożeń, ocenie potencjalnych skutków z nim związanych oraz wdrożeniu środków minimalizujących takie

ryzyko. Organizacje muszą opracować polityki bezpieczeństwa, które uwzględniają specyfikę ich działalności oraz zagrożenia charakterystyczne dla swojego sektora.

Dyrektywa narzuca obowiązek regularnej oceny ryzyka oraz identyfikacji kluczowych zasobów, które wymagają szczególnej ochrony. Na tej podstawie ustalane powinny być odpowiednie środki zapobiegawcze oraz priorytety w zakresie cyberbezpieczeństwa (Clausmeier, 2023).

Dyrektywa nie pomija również aspektów technicznych, a organizacje zarządzające kluczowymi infrastrukturami, takimi jak energia, transport, służba zdrowia czy infrastruktura cyfrowa, są zobowiązane do wdrożenia zaawansowanych zabezpieczeń technicznych, takich jak systemy UTM/firewall, IDS/IPS oraz technologie szyfrowania danych.

Ważnym elementem zarządzania ryzykiem jest także edukacja i podniesienie świadomości pracowników w zakresie cyberbezpieczeństwa. Pracownicy powinni być przeszkoleni, aby rozpoznawać potencjalne zagrożenia i stosować dobre praktyki bezpieczeństwa. Ważnym jest, aby szkolenia pracownicze były udokumentowane (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555).

#### Obowiązki w zakresie zgłaszania incydentów

Jednym z kluczowych założeń NIS2 jest wprowadzenie bardziej rygorystycznych zasad zgłaszania incydentów cyberzagrożeń. Zgodnie z dyrektywą organizacje zobowiązane są do szybkiego informowania krajowych organów nadzorczych o incydentach, które mogą mieć istotny wpływ na bezpieczeństwo. Celem tych działań jest zapewnienie sprawnego przepływu informacji, co z kolei umożliwi podjęcie odpowiednich działań zapobiegawczych oraz koordynację działań na poziomie międzynarodowym. Projekt ustawy o KSC szczegółowo definiuje obowiązki raportowania do odpowiednich Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (tzw. CSIRT) w zależności od klasyfikacji zgłaszającego podmiotu (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555).

W toku zgłaszania incydentów organizacje muszą dokonywać szybkiej oceny wpływu incydentu w odniesieniu do potencjalnej jego skali i potencjal-

nych skutków. Incydenty powinny podlegać klasyfikacji i być raportowane zgodnie z wytycznymi określonymi przez NIS2 (do organów krajowych, te zaś do międzynarodowych) w określonych przez przepisy ramach czasowych. Organizacja zobowiązana jest do sporządzenia raportu opisującego przyczyny incydentu, podjęte środki zaradcze oraz skutki dla swojej działalności operacyjnej. Celem tak dokładnego raportowania ma być wyciąganie wniosków i analiza trendów, które mogą pomóc w przyszłym zapobieganiu podobnym cyberzagrożeniom.

### Wymagania dotyczące zarządzania kryzysowego i odporności organizacyjnej

Dyrektywa nakłada na organizacje obowiązek przygotowania planów zarządzania kryzysowego, które umożliwią skuteczną reakcję na incydenty oraz szybkie przywrócenie ciągłości działania po wystąpieniu zakłóceń w ciągłości działania. Wprowadzenie spójnych i kompleksowych procedur kryzysowych ma na celu zwiększenie odporności organizacji, co przy atakach komputerowych realizowanych na dużą skalę jest kluczowe.

Do kluczowych wyzwań, w zakresie zarządzania kryzysowego w kontekście cyberzagrożeń, jakie narzuca dyrektywa, należy także opracowanie planów ciągłości działania, które zawierać muszą procedury postępowania w przypadku wystąpienia zakłóceń operacyjnych. Plany takie zawierać powinny określenie krytycznych zasobów, priorytety odtworzenia ich działania, jak również minimalne standardy dostępności usług (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555).

Pamiętać należy, że równie ważnym jest regularne testowanie przygotowanych planów i procedur, co również wskazuje NIS2. Symulacje ataków i przeprowadzanie scenariuszy testowych reagowania na incydenty są jednym z bardziej skutecznych metod szkolenia i audytu i pozwalają na identyfikację ewentualnych luk oraz usprawnienie procesów reakcji (MyCompany Polska, 2024).

Na koniec wspomnieć należy także ważną rolę komunikacji kryzysowej. Istotne jest skuteczne informowanie kluczowych interesariuszy – zarówno wewnętrznych, jak i zewnętrznych – o podjętych działaniach oraz aktualnym stanie zagrożenia. Organizacje muszą być przygotowane do komunikacji z

pracownikami, partnerami biznesowymi, klientami, a także organami nadzorczymi, aby minimalizować chaos informacyjny oraz wpływ incydentu na reputację.

### Budowanie kultury bezpieczeństwa i współpracy wewnątrzorganizacyjnej

Niezależnie od poziomu zaawansowania systemu informatycznego, zawsze wpływ na jego bezpieczeństwo ma i będzie miał człowiek, a zdecydowana większość incydentów cyberbezpieczeństwa spowodowana jest błędem ludzkim (Campean, 2019). Wzrost poziomu bezpieczeństwa wymaga nie tylko rozwiązań technologicznych, ale także zaangażowania pracowników na poziomie całej organizacji. Dyrektywa NIS2 kładzie nacisk na tworzenie swojej kultury bezpieczeństwa, która obejmuje nie tylko kadrę zarządzającą, ale także pracowników na każdym poziomie. Budowanie kultury bezpieczeństwa wymaga zaangażowania wszystkich pracowników i wyznaczania standardów postępowania, które powinny stać się częścią codziennej pracy. Bezpieczeństwo w organizacji nie powinno być traktowane jako element dodatkowy, ale jako integralna część procesów i podejmowanych decyzji. Wdrażanie zasad bezpieczeństwa na poziomie operacyjnym pozwala na zmniejszenie ryzyka wynikającego z codziennych działań. Organizacje powinny wyznaczać osoby odpowiedzialne za cyberbezpieczeństwo na poziomie zarządu, aby zagwarantować, że decyzje strategiczne uwzględniają ryzyka związane z cyberzagrożeniami. NIS2 wymaga, aby kadra zarządzająca była świadoma zagrożeń i regularnie szkolona oraz aby wspierała działania mające na celu ich minimalizację (Ministerstwo Cyfryzacji, 2024). Bezpieczeństwo cyfrowe wymaga skutecznej współpracy między działami takimi jak: IT, działy bezpieczeństwa, działy zarządzania i analizy ryzyka, działy prawne oraz HR. Dzięki wymianie informacji i wspólnym działaniom organizacja może lepiej przeciwdziałać zagrożeniom, a także szybciej i sprawniej reagować na incydenty.

## Podsumowanie

Dyrektywa NIS2 wprowadza szerokie i kompleksowe podejście do cyberbezpieczeństwa, które wymaga wdrożenia nowych standardów, procedur oraz środków technicznych. Analiza jej założeń wskazuje, że dla organizacji

oznacza to nie tylko konieczność implementacji technologicznych narzędzi ochrony, ale także rozwój i zaangażowanie pracowników oraz zarządu w budowanie kultury bezpieczeństwa. Dzięki podejściu zakładającemu wdrożenie zarządzania ryzykiem, systemów raportowania incydentów oraz przygotowania do reagowania na sytuacje kryzysowe, dyrektywa NIS2 stanowi wyznacznik dla organizacji, które chcą podnosić swój poziom bezpieczeństwa i budować odporność na cyberzagrożenia.

Dyrektywa ma przyczynić się do harmonizacji i uporządkowania działań w zakresie zarządzania ryzykiem cyberbezpieczeństwa na poziomie instytucji i organizacji. Przepisy wprowadzone przez NIS2 stawiają ambitne cele w zakresie podniesienia poziomu zabezpieczeń infrastruktury krytycznej, ochrony danych oraz budowania świadomości cyberzagrożeń, a ich wdrożenie może stać się wartościowym elementem zarządzania dla organizacji, które dążą do uporządkowania swoich praktyk bezpieczeństwa.

Jednym z kluczowych aspektów NIS2 jest holistyczne podejście do bezpieczeństwa cyfrowego, które wymaga uwzględnienia wszystkich obszarów działalności organizacji w procesach zarządzania ryzykiem. Dyrektywa wskazuje na potrzebę integracji systemów bezpieczeństwa w różnych sektorach gospodarki i administracji publicznej, co pozwala na ograniczenie potencjalnych luk i słabych punktów, które mogłyby być wykorzystywane przez cyberprzestępców. Organizacje, które podejmą wyzwanie dostosowania się do wymagań NIS2, zyskają nie tylko wyższy poziom zabezpieczeń, ale także lepszą koordynację działań i możliwość szybszego reagowania na zagrożenia w cyberprzestrzeni.

Kolejną korzyścią wynikającą z wdrożenia NIS2 jest systematyczna analiza i audyt zabezpieczeń, które stanowią fundament budowania trwałej odporności na zagrożenia cybernetyczne. Dzięki obowiązkowym audytom oraz raportowaniu incydentów organizacje zyskują narzędzie do monitorowania swoich systemów oraz możliwość natychmiastowego reagowania na pojawiające się zagrożenia. Wprowadzenie regularnych audytów w ramach NIS2 pozwala na szybsze identyfikowanie i naprawianie potencjalnych słabości, co jest szczególnie istotne w dynamicznie zmieniającym się środowisku cyfrowym.

Dyrektywa NIS2 wprowadza także wymogi dotyczące budowania kompetencji i świadomości w zakresie cyberbezpieczeństwa, co jest kluczowym elementem skutecznej strategii ochrony przed zagrożeniami cyfrowymi. W praktyce oznacza to, że organizacje będą musiały zadbać o regularne szkolenia pracowników, co pozwala na budowanie kultury bezpieczeństwa cyfrowego na poziomie każdego pracownika. Wyposażenie kadry w wiedzę i umiejętności umożliwiające rozpoznawanie zagrożeń oraz stosowanie odpowiednich procedur postępowania w sytuacjach kryzysowych znacząco zmniejsza ryzyko popełnienia błędów i zwiększa szanse na skuteczne przeciwdziałanie cyberatakam.

Jednocześnie wdrożenie dyrektywy NIS2 przyniesie ze sobą szereg wyzwań, zwłaszcza dla organizacji z sektorów kluczowych i ważnych, które dotąd nie miały obowiązku stosowania zaawansowanych zabezpieczeń. Wdrożenie wymagań NIS2 będzie wymagało inwestycji w zasoby techniczne oraz kadrowe, a także zmian w strukturze organizacyjnej oraz strategii zarządzania bezpieczeństwem. Wdrożenie tych wymogów może być wyzwaniem, ale również stanowi szansę na podniesienie konkurencyjności poprzez wyższy poziom zabezpieczeń, co będzie miało pozytywny wpływ na postrzeganie organizacji przez klientów i partnerów biznesowych.

Podsumowując, dyrektywa NIS2 wyznacza kompleksowe podejście do uporządkowanego zarządzania bezpieczeństwem i stanowić będzie w najbliższych latach fundament do budowania świadomości przedsiębiorstw w zakresie cyberzagrożeń, co jest szczególnie istotne w czasach, gdy zagrożenia stają się coraz bardziej zaawansowane i złożone.

**Streszczenie:** W obliczu znaczącego wzrostu wszelkich incydentów związanych z szeroko pojętym cyberbezpieczeństwem dyrektywa NIS2 wprowadza w Unii Europejskiej jednolite zasady ochrony systemów teleinformatycznych, narzucając nowe obowiązki firmom i instytucjom z sektorów kluczowych i ważnych. W artykule analizie poddano, na ile dyrektywa NIS2 wraz z krajową ustawą wykonawczą może stać się dla wielu organizacji nie tylko wyzwaniem, ale także rzeczywistym drogowskazem do wdrożenia lub zmodernizowania już działającego systemu zarządzania bezpieczeństwem informacji (SZBI). Omówione zostały kluczowe założenia NIS2 oraz ich potencjalny wpływ na zwiększenie poziomu bezpieczeństwa i zarządzanie ryzykiem, a także wyzwania, które towarzyszą wdrożeniu. W artykule poruszono także zagadnienia związane z implementacją nowelizacji polskiej ustawy o Krajowym Systemie Cyberbezpieczeństwa.

**Abstract:** In the face of a significant increase in incidents related to cybersecurity in its broadest sense, the NIS2 Directive introduces uniform rules for protecting information and communication systems across the European Union, imposing new obligations on companies and institutions from critical and important sectors. This article examines the extent to which the NIS2 Directive, along with its national implementing act, can become not only a challenge but also a practical guide for many organizations to implement or modernize their existing Information Security Management System (ISMS). Key provisions of NIS2 and their potential impact on enhancing security levels and risk management are discussed, as well as the challenges associated with its implementation. The article also addresses issues related to the adoption of amendments to the Polish Act on the National Cybersecurity System.

**Słowa kluczowe:** cyberbezpieczeństwo, Dyrektywa NIS2, zarządzanie ryzykiem, ochrona infrastruktury krytycznej

**Keywords:** cybersecurity, NIS2 Directive, risk management, critical infrastructure protection

## Bibliografia

- Campean, S. (2019). The human factor at the center of a cyber security culture. *International Journal of Information Security and Cybercrime (IJISC)*, 8(1), 51–58.
- Chałubińska-Jentkiewicz, K., Nowikowska, M. (2024). Podmioty zaangażowane w politykę zapewnienia bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS 2 (cz. 2). *Cybersecurity and Law*, 11.
- Clausmeier, D. (2023). Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). *International Cybersecurity Law Review*, 4(1), 79–90.
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).
- Ministerstwo Cyfryzacji. (2024). Kluczowe zmiany dla ochrony polskiej infrastruktury przed cyberatakami.
- Ministerstwo Cyfryzacji. (2024). Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw.
- MyCompany Polska. (2024). Dyrektywa NIS2 – co to jest i jak ją wdrożyć w firmie?
- NASK. (2024). Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa: Najważniejsze zmiany dla podmiotów.
- Polćák, R. (2022). Cybersecurity certification and compliance in financial services. In: *Data Governance in AI, FinTech and LegalTech* (p. 213–237). Cheltenham: Edward Elgar Publishing.
- Rogalski, M. (2024). Bezpieczeństwo sieci i usług łączności elektronicznej w prawie Unii Europejskiej oraz w prawie polskim. Uczelnia Łazarskiego.
- Van 't Schip, M. (2024). The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things. *European Journal of Law Technology*, 15(1).
- Wrzosek, M. (2021). Dyrektywa w sprawie odporności podmiotów krytycznych i Dyrektywa NIS 2–nowe wyzwania dla operatorów w zakresie cyberbezpieczeństwa. *Nowa Energia*, 5/6.