
DOI: 10.4467/29567610PIB.25.041.23026

mgr Marcin Chodyka

Akademia Bialska im. Jana Pawła II

ORCID: 0009-0004-6585-5541

BEZPIECZEŃSTWO CYFROWE MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW A DYREKTYWA NIS2

DIGITAL SECURITY OF SMALL AND MEDIUM-SIZED ENTERPRISES AND THE NIS2 DIRECTIVE

Streszczenie

Celem niniejszego artykułu jest analiza wpływu dyrektywy NIS2 na bezpieczeństwo cyfrowe małych i średnich przedsiębiorstw, ze szczególnym uwzględnieniem nowych obowiązków w zakresie zarządzania ryzykiem, odpowiedzialności najwyższej kadry kierowniczej oraz bezpieczeństwa łańcucha dostaw. Artykuł osadza problematykę w kontekście rosnącej podatności MŚP na cyberataki oraz ich roli jako ogniw łańcuchów dostaw podmiotów większych; wskazuje, że NIS2 rozszerza zakres regulacji poza klasycznie rozumianą infrastrukturę krytyczną i czyni cyberbezpieczeństwo elementem ładu korporacyjnego również w firmach średniej wielkości. W głównej części opracowania omówiono katalog minimalnych środków zarządzania cyberbezpieczeństwem przewidzianych w art. 21 NIS2, charakter i skalę odpowiedzialności zarządów (w tym mechanizmy sankcyjne) oraz pośredni wpływ wymogów dotyczących bezpieczeństwa dostawców na najmniejsze podmioty, które formalnie pozostają poza zakresem dyrektywy. W celu przeprowadzenia badań sformułowano problem badawczy: w jaki sposób rozwiązania przyjęte w NIS2 kształtują poziom bezpieczeństwa cyfrowego sektora MŚP oraz jakie konsekwencje praktyczne dla małych i średnich firm wynikają z nowych obowiązków regulacyjnych? Problem badawczy koncentruje się na identyfikacji zakresu bezpośrednich i pośrednich obowiązków nakładanych na MŚP, ocenie ich wpływu na system zarządzania ryzykiem i funkcjonowanie łańcucha dostaw oraz wskazaniu kluczowych barier wdrożeniowych po stronie przedsiębiorstw. Odpowiednio do postawionego problemu badawczego autor sformułował hipotezę badawczą, zgodnie z którą NIS2 – poprzez wprowadzenie ujednoliconych minimalnych wymogów w obszarze cyberbezpieczeństwa oraz przypisanie formalnej odpowiedzialności zarządom – przyczyni się do wzrostu odporności cyfrowej MŚP, pod warunkiem zapewnienia tym podmiotom adekwatnego wsparcia instytucjonalnego i finansowego; w przeciwnym razie nowe wymogi

mogą okazać się dla najmniejszych firm nadmiernym obciążeniem, grożącym ich wykluczeniem z łańcuchów dostaw. W ramach badania przeprowadzono szczegółową analizę przepisów dyrektywy NIS2 i powiązanych aktów prawnych, raportów ENISA oraz literatury przedmiotu, uzupełnioną o studia przypadków głośnych incydentów cyberbezpieczeństwa oraz analizę rekomendacji praktycznych dla sektora MŚP. Wyniki pozwoliły sformułować zestaw zaleceń dla małych i średnich przedsiębiorstw, obejmujących m.in. podniesienie rangi cyberbezpieczeństwa na poziomie zarządu, przeprowadzenie analizy luk względem wymogów NIS2, wdrożenie podstawowych mechanizmów cyberhigieny, rozwój kompetencji pracowników oraz wykorzystanie zewnętrznego wsparcia eksperckiego, co w perspektywie długoterminowej może uczynić z MŚP bardziej odporne i wiarygodne ogniwa europejskiego ekosystemu cyfrowego.

Słowa kluczowe: dyrektywa NIS2, cyberbezpieczeństwo, małe i średnie przedsiębiorstwa (MŚP), obowiązki prawne, zarządzanie ryzykiem, łańcuch dostaw, odpowiedzialność zarządu

Summary

The aim of this article is to analyse the impact of the NIS2 Directive on the digital security of small and medium-sized enterprises (SMEs), with particular emphasis on the new obligations concerning risk management, the responsibility of top management and supply chain security. The article situates this issue in the context of SMEs' increasing vulnerability to cyberattacks and their role as links in the supply chains of larger organisations; it argues that NIS2 extends the scope of regulation beyond traditionally understood critical infrastructure and turns cybersecurity into an element of corporate governance also in medium-sized firms. The main part of the paper discusses the catalogue of minimum cyber risk management measures laid down in Article 21 NIS2, the nature and extent of boards' liability (including sanctioning mechanisms), and the indirect impact of supplier-security requirements on the smallest entities that formally remain outside the scope of the directive. To address the research objectives, the following research question was formulated: how do the solutions introduced by NIS2 shape the level of digital security in the SME sector, and what practical implications do the new regulatory obligations have for small and medium-sized firms? The research problem focuses on identifying the scope of direct and indirect obligations imposed on SMEs, assessing their impact on risk management systems and supply-chain functioning, and indicating the key implementation barriers faced by enterprises. In line with the adopted research problem, the author formulated the research hypothesis that NIS2 – by introducing harmonised minimum requirements in the field of cybersecurity and by assigning formal responsibility to company boards – will contribute to an increase in SMEs' digital resilience, provided that these entities receive adequate institutional and financial support; otherwise, the new requirements may prove an excessive burden for the smallest firms, threatening their exclusion from supply chains. The study is based on a detailed

analysis of the provisions of the NIS2 Directive and related legal acts, ENISA reports and the relevant literature, complemented by case studies of high-profile cybersecurity incidents and an examination of practical recommendations for the SME sector. The findings made it possible to develop a set of recommendations for small and medium-sized enterprises, including, inter alia, elevating cybersecurity to board level, conducting gap analyses against NIS2 requirements, implementing basic cyber-hygiene mechanisms, developing employee competences and making use of external expert support, which in the long term may turn SMEs into more resilient and trustworthy links in the European digital ecosystem.

Keywords: NIS2 directive, cybersecurity, small and medium enterprises (SMEs), legal obligations, risk management, supply chain, board accountability

Wstęp

Cyfryzacja gospodarki sprawia, że bezpieczeństwo systemów teleinformatycznych urasta do rangi kluczowego zagadnienia dla organizacji ze wszystkich sektorów – nie tylko tych tradycyjnie uznawanych za infrastrukturę krytyczną. Małe i średnie przedsiębiorstwa (MŚP), stanowiące 99% firm w Unii Europejskiej, padają coraz częściej ofiarą cyberataków ze względu na relatywnie niższy poziom zabezpieczeń i świadomości zagrożeń¹. Według badań Komisji Europejskiej jedynie około 27% małych firm i 51% średnich posiadało sformalizowaną politykę cyberbezpieczeństwa, podczas gdy w dużych organizacjach odsetek ten wynosił 72%. Taka luka w dojrzałości czyni MŚP łatwym celem dla cyberprzestępców. Co więcej, małe firmy bywają kluczowymi ogniwami łańcuchów dostaw podmiotów większych – atak na pozornie niewielkiego dostawcę może posłużyć jako „wejście” do naruszenia bezpieczeństwa większej organizacji. Głośne incydenty ostatnich lat (atak ransomware WannaCry w 2017 r., atak typu supply chain na SolarWinds w 2020 r. itp.) pokazały, że zagrożenia cybernetyczne mogą dotknąć każdą firmę, niezależnie od jej wielkości.

W odpowiedzi na rosnące ryzyko cyfrowe, organy Unii Europejskiej podjęły działania w kierunku zaostrzenia i ujednoczenia wymogów w zakresie cyberbezpieczeństwa. Ich konsekwencją jest nowa dyrektywa NIS2 – kompleksowa regulacja przyjęta pod koniec 2022 r., która zastąpiła pierwszą dyrektywę NIS z 2016 r., znacząco rozszerzając jej zakres i wprowadzając szereg nowych obowiązków. NIS2 podnosi poprzeczkę wymagań, czyniąc cyberbezpieczeństwo kwestią ładu korporacyjnego: od teraz najwyższe

1 E. Kaiser, *The new NIS II Directive and its impact on small and medium enterprises (SMEs): initial considerations*, "MediaLaws", 1/2023, <https://www.medialaws.eu/rivista/the-new-nis-ii-directive-and-its-impact-on-small-and-medium-enterprises-smes-initial-considerations/> (dostęp: 24.10.2025).

kierownictwo przedsiębiorstw ma ustawowy obowiązek zaangażowania się w ten obszar. Zarządy MŚP muszą zatem zyskać świadomość nowych obowiązków i zagrożeń, tym bardziej że w razie niezgodności grożą im dotkliwe kary finansowe (do 10 mln euro lub 2% światowego obrotu dla podmiotu) oraz potencjalne sankcje indywidualne. Poniżej przeanalizowano kluczowe zmiany, wprowadzone przez NIS2, ze szczególnym uwzględnieniem nowych obowiązków i odpowiedzialności nałożonych na przedsiębiorstwa MŚP, a następnie przedstawiono rekomendacje, mające ułatwić tym podmiotom dostosowanie się do wymogów dyrektywy.

Nowe obowiązki i odpowiedzialność w świetle NIS2

NIS wprowadza jakościowo nowy sposób definiowania podmiotów objętych przepisami, opierając go na kryterium wielkości przedsiębiorstwa (tzw. zasadzie *size-cap*)². W przeciwieństwie do NIS1, która pozostawiała państwom członkowskim dużą swobodę w wyznaczaniu operatorów usług kluczowych³, NIS2 automatycznie obejmuje wszystkie średnie i duże przedsiębiorstwa, działające w sektorach wymienionych w załącznikach I lub II dyrektywy⁴. Oznacza to znaczne poszerzenie kręgu regulowanych organizacji – nawet firmy nie wpisujące się w tradycyjne definicje infrastruktury krytycznej (np. średniej wielkości producent żywności) stają się z mocy prawa podmiotami ważnymi, o ile spełniają kryterium >250 pracowników lub >€50 mln obrotu i działają w sektorze wskazanym w dyrektywie. Mikro oraz małe przedsiębiorstwa (<50 pracowników, ≤€10 mln obrotu) zostały co do zasady wyłączone z bezpośredniego zakresu NIS2, aby uniknąć nieproporcjonalnych obciążeń (art. 2 ust. 2) – jednak istnieje szereg wyjątków, pozwalających objąć reżimem także niektóre mniejsze podmioty, jeśli ich działalność ma krytyczne znaczenie dla gospodarki lub bezpieczeństwa (np. jedyni dostawcy danej usługi, kwalifikowani dostawcy usług zaufania, operatorzy DNS itp.). Takie podejście ustawodawcy sprawia, że większość średnich firm w sektorach kluczowych i ważnych musi spełniać nowe wymogi, zaś mniejsze MŚP, choć generalnie nieobjęte NIS2, i tak odczują pośrednie skutki regulacji poprzez presję wymagań ze strony większych kontrahentów⁵.

2 Dyrektywa (UE) 2022/2555 Parlamentu Europejskiego i Rady z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dyrektywa NIS2), Dz. Urz. UE L 333 z 27.12.2022.

3 Dyrektywa (UE) 2016/1148 Parlamentu Europejskiego i Rady z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. Urz. UE L 194 z 19.07.2016.

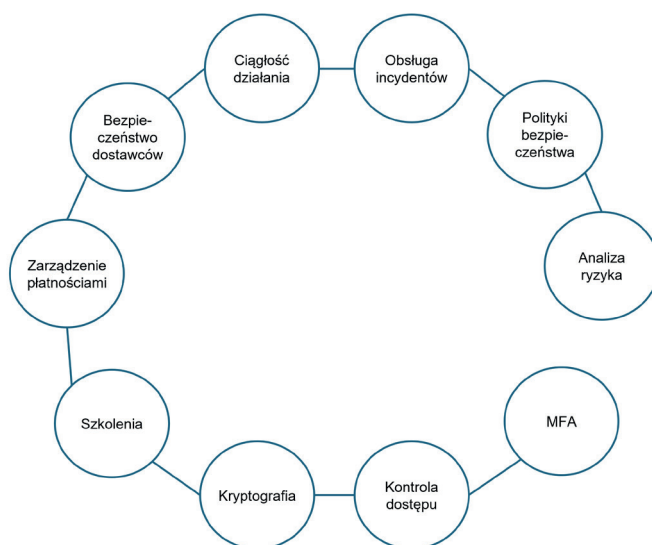
4 Parlament Europejski i Rada UE, *Wspólny wniosek dotyczący oceny skutków regulacji – Proposal for Directive on measures for high common level of cybersecurity across the Union*, 2022.

5 J. Philpot, *DIGITAL SME launches guide to position SMEs as trusted NIS2 suppliers*. European DIGITAL SME Alliance, 2025.

Jednym z filarów NIS2 jest ustanowienie jednolitych minimalnych wymagań w zakresie zarządzania cyberbezpieczeństwem (art. 21 NIS2). Dyrektywa precyzuje katalog dziesięciu obszarów, w których podmioty objęte przepisami muszą wdrożyć odpowiednie polityki, procedury i środki techniczno-organizacyjne⁶. Obszary te zostały przedstawione na Rysunku 1. Stanowią one de facto podstawowy system zarządzania bezpieczeństwem informacji, zbliżony zakresem do norm typu ISO 27001. Do obowiązkowych elementów należą m.in.:

- a) Analiza ryzyka i polityka bezpieczeństwa – regularne przeprowadzanie ocen ryzyka oraz utrzymywanie adekwatnej polityki ochrony informacji.
- b) Reagowanie na incydenty – ustanowienie procedur obsługi incydentów (monitoring, wykrywanie, zgłaszanie właściwym organom, reagowanie).
- c) Ciągłość działania i zarządzanie kryzysowe – posiadanie planów ciągłości działania, *disaster recovery* i zarządzania kryzysowego, w tym regularne kopie zapasowe i procedury odtwarzania usług.
- d) Bezpieczeństwo łańcucha dostaw – identyfikacja i minimalizacja ryzyk związanych z dostawcami towarów i usług ICT; włączenie wymogów bezpieczeństwa do procesów zakupowych i umów z dostawcami.
- e) Bezpieczny rozwój i podatności – zapewnienie bezpieczeństwa na etapie nabywania, wytwarzania i utrzymania systemów (polityki bezpiecznego programowania, zarządzanie podatnościami, bieżące aktualizacje i łatki).
- f) Testy i audyty bezpieczeństwa – wdrożenie procedur regularnego testowania i oceny skuteczności środków bezpieczeństwa (np. audyty, testy penetracyjne, przeglądy zgodności).
- g) Cyberhigiena i szkolenia – promowanie kultury bezpieczeństwa wśród pracowników, obowiązkowe szkolenia z cyberbezpieczeństwa, zalecenia dot. haseł, zasad dostępu itp.
- h) Kryptografia – stosowanie odpowiednich polityk szyfrowania i ochrony kryptograficznej danych wrażliwych.
- i) Bezpieczeństwo personalne – weryfikacja personelu na stanowiskach krytycznych, kontrola dostępu wg zasady najmniejszych uprawnień, procedury *offboardingu* pracowników.
- j) Uwierzytelnianie wieloskładnikowe – wdrożenie mechanizmów MFA tam, gdzie to możliwe (zwłaszcza przy dostępie do systemów istotnych) oraz zabezpieczenie zdalnych kanałów komunikacji.

6 K. Mączka, *Dyrektywa NIS2 jako wytyczna do wdrożenia systemu zarządzania bezpieczeństwem informacji w organizacji*, *Ochrona ludności i dziedzictwa kulturowego*, 2024, 5/2024, s. 113.



Rysunek 1. Diagram systemu zarządzania bezpieczeństwem informacji

Źródło: Opracowanie własne na podstawie Dyrektywy NIS2.

Powyższe wymagania oznaczają, że przedsiębiorstwa muszą przyjąć bardziej systemowe podejście do bezpieczeństwa informacji. W praktyce wiele średnich firm będzie musiało zaktualizować lub rozszerzyć swoje wewnętrzne polityki i procedury, aby pokryć wszystkie ww. obszary. Dla organizacji, które dotąd nie wypracowały pełnego Systemu Zarządzania Bezpieczeństwem Informacji (ISMS), implementacja NIS2 będzie dużym wyzwaniem organizacyjnym. Szacunki z oceny skutków dyrektywy wskazywały, że przeciętne przedsiębiorstwo średniej wielkości, objęte nowymi regulacjami, może musieć zwiększyć swoje wydatki na cyberbezpieczeństwo nawet o ok. 22% w skali kilku lat, aby sprostać kosztom wdrożenia wymaganych środków. Równocześnie najnowsze badania pokazują, że 100% ankietowanych MŚP planuje zwiększyć inwestycje w bezpieczeństwo celem spełnienia NIS2, lecz aż 34% z nich przyznaje, że nie będzie w stanie pozyskać na ten cel dodatkowego budżetu⁷. Dane te obrazują, jak poważnym obciążeniem mogą okazać się nowe obowiązki dla firm sektora MŚP, operujących często na niskich marżach. Z drugiej strony, inwestycje w cyberbezpieczeństwo mogą przynieść MŚP długofalowe korzyści – wzrost zaufania klientów, utrzymanie kontraktów z wymagającymi partnerami czy uniknięcie kosztownych incydentów. Co istotne, dyrektywa przewiduje możliwość uznania korzystania z certyfikowanych produktów i usług za domniemanie zgodności z częścią wymogów (art. 21 ust. 5 NIS2) – dla firm już wdrożonych w standardy typu ISO/IEC 27001 może to ułatwić spełnienie nowych wymagań.

7 ENISA, NIS Investments 2024. Cybersecurity Policy Assessment, 2024.

Domniemanie to ma być w praktyce powiązane z europejskimi schematami certyfikacji cyberbezpieczeństwa, rozwijanymi na podstawie rozporządzenia (UE) 2019/881 (Cybersecurity Act)⁸.

Analizując odpowiedzialność zarządów i kadry kierowniczej, należy zaznaczyć, że NIS2 nie porzeka na określeniu „co” należy zrobić, ale również „kto” ma za to odpowiadać. Jedną z najistotniejszych zmian względem poprzedniego stanu prawnego jest *expressis verbis* przypisanie najwyższemu kierownictwu organizacji odpowiedzialności za zgodność z wymogami cyberbezpieczeństwa⁹. Zgodnie z art. 20 NIS2 organ zarządzający każdego podmiotu kluczowego lub ważnego musi zatwierdzać politykę zarządzania ryzykiem cyberbezpieczeństwa oraz sprawować nadzór nad jej wdrożeniem. Ustawodawca unijny podkreślił, że bezpieczeństwo informacji nie może być traktowane wyłącznie jako problem techniczny pozostawiony działom IT – problem ten powinien stać się elementem ładu korporacyjnego, za który odpowiada zarząd. Co ważne, dyrektywa otwiera drogę do pociągnięcia członków organu zarządzającego do osobistej odpowiedzialności w razie rażącego zaniedbania obowiązków przez firmę. Innymi słowy, jeśli przedsiębiorstwo notorycznie nie wdraża wymaganych środków ochrony lub nie zgłasza poważnych incydentów, to sankcje mogą dotknąć nie tylko sam podmiot, lecz także jego kierownictwo. Ponadto artykuł 20 ust. 4 NIS2 wprost wymaga, by członkowie organu zarządzającego regularnie uczestniczyli w szkoleniach z zakresu cyberbezpieczeństwa, zdobywając wiedzę i umiejętności niezbędne do wypełniania nowych obowiązków. Ten wymóg instytucjonalizuje podejście, zgodnie z którym bezpieczeństwo staje się wspólną odpowiedzialnością całej organizacji – od szeregowych pracowników po zarząd – a kadra menedżerska musi świecić przykładem w przestrzeganiu zasad cyberhigieny. Już teraz na rynku pojawiają się dedykowane szkolenia dla członków zarządów z zakresu NIS2 i zarządzania cyberryzykiem, co odzwierciedla rosnące zapotrzebowanie na wiedzę w tej grupie.

Przeniesienie ciężaru odpowiedzialności na zarządy, znajduje odzwierciedlenie w systemie sankcji administracyjnych określonych w NIS2. Państwa członkowskie są zobowiązane przewidzieć kary finansowe za naruszenie wymogów, sięgające maksymalnie 10 mln euro lub 2% rocznego obrotu dla podmiotów kluczowych oraz 7 mln euro lub 1,4% obrotu dla podmiotów ważnych. Kwoty te – porównywalne z sankcjami pod RODO¹⁰ – mają działać prewencyjnie

8 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (Cybersecurity Act), Dz. Urz. UE L 151 z 7.06.2019.

9 R. Hayes, S. Walsh, L. Moore, *NIS2: A Game-Changer for Senior Management and Boards*, William Fry, 2025.

10 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (Cybersecurity Act), Dz. Urz. UE L 151 z 7.06.2019.

i skłonić kierownictwo do poważnego traktowania compliance. Struktura zaangażowanych podmiotów publicznych została szczegółowo omówiona w literaturze przedmiotu, z uwzględnieniem kompetencji organów krajowych i europejskich¹¹. Dla wielu MŚP kary rządu milionów euro przewyższają ich roczne zyski, co tym bardziej mobilizuje do unikania zaniedbań. Oprócz kar dla przedsiębiorstw, implementacje krajowe NIS2 (np. projekt nowelizacji ustawy o KSC w Polsce) przewidują również kary dla osób pełniących funkcje kierownicze – w polskim projekcie proponuje się podniesienie maksymalnej grzywny z 200% do 600% miesięcznego wynagrodzenia menedżera¹². Inne państwa rozważają nawet odpowiedzialność karną – np. w Irlandii projekt ustawy implementującej NIS2 stanowi, że członek zarządu świadomie dopuszczający do naruszenia podlega przestępstwu i może zostać ukarany grzywną lub czasowym zakazem pełnienia funkcji kierowniczych. Tego rodzaju przepisy wskazują jednoznacznie, że cyberbezpieczeństwo stało się obowiązkiem o charakterze fiducyjnym – zbliżonym do odpowiedzialności zarządów za zgodność z prawem finansowym czy ochroną danych osobowych.

W praktyce przedsiębiorstwa powinny podjąć szereg działań dostosowawczych, aby sprostać nowym realiom¹³. Rekomenduje się m.in. dokonanie wewnętrznej oceny luk (gap assessment) względem wymogów NIS2 oraz formalne przypisanie nadzoru nad cyberbezpieczeństwem konkretnemu członkowi kierownictwa (np. wyznaczenie w zarządzie osoby odpowiedzialnej za IT/cyberbezpieczeństwo lub powołanie funkcji Chief Information Security Officer raportującej do zarządu). Podobną rolę przypisuje się organom zarządzającym także w sektorze finansowym – por. podejście przyjęte w rozporządzeniu DORA¹⁴. Dobre praktyki obejmują wprowadzenie stałych punktów dotyczących bezpieczeństwa do agendy posiedzeń zarządu, regularne raportowanie zarządowi o stanie zabezpieczeń i ryzykach, okresowe audyty zewnętrzne prezentowane kierownictwu, a także ćwiczenia typu table-top dla menedżerów, symulujące reakcję na poważny incydent. Wszystkie te kroki służą temu, by bezpieczeństwo informacji przestało funkcjonować w organizacjach MŚP jedynie jako domena działu IT, a stało się integralnym elementem zarządzania na najwyższym szczeblu. NIS2 wprost czyni cyberbezpieczeństwo kwestią governance – od decyzji inwestycyjnych po kulturę organizacyjną. Dla wielu małych firm oznacza to istotną zmianę kulturową: w niejednym mikro czy ma-

11 K. Chałubińska-Jentkiewicz, M. Nowikowska, *Podmioty zaangażowane w politykę zapewnienia bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS2 (cz. 2)*, „Cybersecurity and Law” 2024, nr 11, s. 7.

12 M. Stachoń, E. Zalewska-Czajczyńska, P. Słowiński, *Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa – najważniejsze zmiany dla podmiotów*. Cyberpolicy NASK – Analizy, 2024.

13 ENISA, *Cybersecurity for SMEs – Challenges and Recommendations*. European Union Agency for Cybersecurity, raport 2021.

14 D. Clausmeier, *Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)*, „International Cybersecurity Law Review” 2023, 4(1), s. 79–90.

łym przedsiębiorstwie decyzje w obszarze IT podejmował dotąd sam właściciel lub informatyk, często ad hoc, podczas gdy teraz wymagane będą formalne struktury i procedury, a zarząd będzie rozliczany z ich skuteczności. Choć stanowi to obciążenie, może przynieść pozytywny efekt – większą świadomość zagrożeń na szczycie firmy zazwyczaj przekłada się na lepszą alokację zasobów i poważniejsze traktowanie kwestii bezpieczeństwa. W dłuższej perspektywie zaangażowanie zarządów powinno ułatwić MŚP budowanie odporności cyfrowej, m.in. poprzez uzyskanie wsparcia dla inwestycji w zabezpieczenia, zatrudnienie specjalistów czy przeprowadzanie testów bezpieczeństwa, które zyskują priorytet dzięki aprobachie najwyższego kierownictwa.

Bezpieczeństwo łańcucha dostaw a pośredni wpływ NIS2 na MŚP

Współczesne łańcuchy dostaw sprawiają, że organizacje są silnie współzależne – atak na jeden element (dostawcę lub podwykonawcę) może przynieść skutki lawinowe¹⁵. Ustawodawca unijny, wyciągając wnioski z głośnych incydentów (jak wspomniany atak na SolarWinds, który umożliwił intruzom przeniknięcie do setek organizacji), położył w dyrektywie NIS2 duży nacisk na bezpieczeństwo łańcucha dostaw. Zgodnie z art. 21 ust. 2 lit. d) jednym z obowiązkowych elementów zarządzania ryzykiem uczyniono bezpieczeństwo dostawców i usługodawców ICT, co oznacza konieczność oceny ryzyka związanego z dostawcami oraz podejmowania adekwatnych działań ochronnych. Przedsiębiorstwa podlegające NIS2 muszą analizować podatności i poziom zabezpieczeń kluczowych kontrahentów – np. praktyki w zakresie bezpiecznego rozwoju oprogramowania, polityki zarządzania podatnościami, standardy ochrony danych. W praktyce wdrożenie tego wymogu może oznaczać konieczność wprowadzenia kryteriów bezpieczeństwa do procedur zakupowych (secure procurement), żądania od dostawców określonych certyfikatów lub wyników audytów, okresowej oceny najważniejszych dostawców, a nawet dywersyfikacji łańcucha dostaw celem unikania uzależnienia od jednego źródła dostaw.

Na poziomie systemowym NIS2 przewiduje mechanizmy wspomagające zarządzanie ryzykiem łańcucha dostaw. Grupa Współpracy NIS2 (złożona z przedstawicieli państw członkowskich, ENISA i Komisji) może inicjować ogólnounijną, skoordynowaną ocenę ryzyk dostaw w wybranych sektorach (art. 22). Ponadto kraje członkowskie zobowiązano do tworzenia wykazów dostawców wysokiego ryzyka – w Polsce projekt nowelizacji ustawy o KSC przewiduje formalny mechanizm oznaczania dostawców sprzętu lub oprogramowania jako „wysokiego ryzyka”, co umożliwi ograniczenie ich używania przez podmioty kluczowe i ważne. Tego typu regulacje (zbieżne z unijnymi zaleceniami po analizie ryzyka 5G) mają eliminować z ekosystemu technologie

15 J. Ostrowska, S. Skalski, *How will NIS2 affect the supply chain security approach?* EY Insights, 2023.

uznawane za podatne lub zależne od wrogich państw. W efekcie również MŚP będą musiały zwracać większą uwagę na bezpieczeństwo produktów i usług, z których korzystają – wybór dostawcy oznaczonego jako niebezpieczny może skutkować utratą kontraktów lub wykluczeniem z łańcucha dostaw¹⁶.

NIS2 wprowadza zatem perspektywę całościowego zabezpieczenia łańcucha wartości. Duże organizacje, dążąc do własnej zgodności z art. 21, będą kontraktowo przenosić część wymagań na swoich partnerów biznesowych. Już teraz obserwuje się rosnącą presję kontraktową – większe firmy wymagają od dostawców spełnienia minimalnych standardów cyberbezpieczeństwa (np. posiadania polityk bezpieczeństwa, szyfrowania danych, wdrożenia MFA, zgłaszania incydentów). Można mówić o efekcie domina, w ramach którego wymogi prawne i dobre praktyki „rozlewają się” w dół łańcucha dostaw na mniejsze podmioty. Dane empiryczne potwierdzają tę tendencję: według raportu ENISA średnie i małe przedsiębiorstwa, pomimo ograniczonych zasobów, przeznaczają już obecnie proporcjonalnie większą część swoich budżetów na cyberbezpieczeństwo niż firmy duże. Wynika to z rosnącej świadomości, że inwestycje w bezpieczeństwo są warunkiem utrzymania się w łańcuchach dostaw – coraz częściej postrzega się je nie jako koszt, lecz jako inwestycję w stabilność i konkurencyjność firmy. Niemniej jednak, aby mniejsze podmioty mogły sprostać nowym oczekiwaniom, potrzebne jest wsparcie instytucjonalne. Ekspertki wskazują na konieczność stworzenia zachęt w postaci np. instrumentów finansowych (dotacje, ulgi podatkowe) i inicjatyw edukacyjnych dla MŚP. Tego rodzaju działania pomogą utrzymać relatywnie wysoki poziom inwestycji w bezpieczeństwo bez nadmiernego obciążania bieżących budżetów małych firm.

Nacisk NIS2 na bezpieczeństwo dostawców oznacza zatem, że nawet przedsiębiorstwa formalnie nieobjęte dyrektywą nie mogą pozostawać bierne wobec nowych regulacji. Brak dostosowania się do podwyższonych standardów może skutkować konsekwencjami biznesowymi – utratą kontrahentów, wykluczeniem z przetargów czy pogorszeniem reputacji na rynku. Państwa członkowskie oraz agencje unijne (jak ENISA) są świadome tych wyzwań i zapowiadają działania wspierające MŚP – m.in. publikację wytycznych dotyczących minimalnych wymagań dla mniejszych dostawców, programy dotacyjne na poprawę zabezpieczeń czy rozwój platform wymiany informacji o zagrożeniach przeznaczonych także dla sektora MŚP. Takie kroki mają zapewnić, że podniesienie poziomu cyberbezpieczeństwa w dużych podmiotach pociągnie za sobą również wzrost odporności ich mniejszych partnerów, nie prowadząc zarazem do nadmiernych barier ekonomicznych dla najmniejszych firm.

16 J. Ostrowska, S. Skalski, *How will NIS2 affect the supply chain security approach?* EY Insights, 2023.

Rekomendacje dla MŚP

Małe i średnie przedsiębiorstwa stają obecnie przed koniecznością sprostania zaostrzonym wymogom dyrektywy NIS2, co stanowi wyzwanie ze względu na ich ograniczone zasoby oraz dotychczas niższy poziom dojrzałości w obszarze cyberbezpieczeństwa. Analiza wcześniejszych rozdziałów wykazała, że brak dostosowania się MŚP do nowych standardów może skutkować poważnymi konsekwencjami – od dotkliwych kar finansowych po utratę kontrahentów – a jednocześnie ujawniła potrzebę systemowego wsparcia tych podmiotów w procesie transformacji. Dlatego poniżej przedstawiono rekomendacje dla sektora MŚP, wynikające z zidentyfikowanych wyzwań i luk, których celem jest ułatwienie małym firmom skutecznego wdrożenia wymogów NIS2. Zalecenia te mają nie tylko zapewnić zgodność z regulacjami, ale także wzmocnić odporność cyfrową MŚP – tak, aby korzyści z podniesienia poziomu bezpieczeństwa przeważały nad kosztami i trudnościami wdrożenia nowych środków. Realizacja poniższych wskazówek pozwoli małym i średnim firmom stać się bardziej świadomymi oraz wiarygodnymi uczestnikami ekosystemu cyfrowego, zamiast pozostawać jego najsłabszym ogniwem.

1. **Priorytet dla bezpieczeństwa na poziomie zarządu:** Zaleca się, aby cyberbezpieczeństwo stało się kwestią strategiczną nadzorowaną bezpośrednio przez najwyższą kadre kierowniczą. MŚP powinny formalnie wyznaczyć w swoich strukturach osobę odpowiedzialną za obszar bezpieczeństwa (np. członka zarządu pełniącego rolę CISO) oraz regularnie włączać przegląd stanu zabezpieczeń i ryzyk cybernetycznych do agendy posiedzeń zarządu. Budowanie kultury bezpieczeństwa od góry – poprzez osobisty przykład kierownictwa przestrzegającego ustanowionych polityk – w połączeniu z podnoszeniem kompetencji zarządu (wymóg art. 20 NIS2) przełoży się na lepszą alokację zasobów na ochronę i sprawniejsze reagowanie na incydenty.
2. **Analiza luk i plan wdrożenia wymogów:** Należy przeprowadzić dogłębną analizę luk w obecnym systemie zabezpieczeń przedsiębiorstwa w odniesieniu do wymagań NIS2. Taka ocena pozwoli zidentyfikować najsłabsze obszary (np. brak formalnej polityki bezpieczeństwa, nieprzeprowadzanie ocen ryzyka, brak planów ciągłości działania) i na tej podstawie opracować realistyczny plan dostosowania – wyznaczający priorytety oraz rozkładający wdrożenie poszczególnych środków w czasie. Proces ten warto oprzeć na uznanych standardach zarządzania bezpieczeństwem (jak ISO/IEC 27001 czy odpowiadające mu normy krajowe), co zapewni metodyczne podejście i ułatwi ewentualną certyfikację zgodności w przyszłości.
3. **Wdrożenie podstawowych mechanizmów cyberhigieny:** Priorytetem powinno być zaimplementowanie fundamentalnych środków ochronnych,

które znacząco utrudnią działania cyberprzestępców. Do kluczowych praktyk należą m.in. regularne aktualizacje i instalowanie poprawek bezpieczeństwa, wykonywanie częstych kopii zapasowych istotnych danych, stosowanie oprogramowania ochronnego (antywirusowego, firewall), restrykcyjna kontrola dostępu zgodnie z zasadą najmniejszych uprawnień (silne hasła, uwierzytelnianie wieloskładnikowe – MFA, segmentacja sieci) oraz szyfrowanie wrażliwych informacji. Spełnienie tych podstawowych wymogów – spójnych z art. 21 NIS2 – podniesie bazowy poziom ochrony organizacji i zredukuje ryzyko sukcesu ataku. Ponadto MŚP powinny ustanowić jasne procedury zgłaszania incydentów oraz reagowania na nie, aby w sytuacji kryzysowej działać szybko, skutecznie i zgodnie z obowiązkiem prawnym.

4. Szkolenia i budowanie świadomości: Czynnikiem ludzki pozostaje krytycznym elementem bezpieczeństwa, dlatego niezbędne jest systematyczne podnoszenie kompetencji pracowników. Zaleca się regularne szkolenia z zakresu cyberbezpieczeństwa dla całej załogi – zarówno nowo zatrudnionych, jak i doświadczonych pracowników – obejmujące m.in. rozpoznawanie ataków socjotechnicznych (takich jak phishing czy malware) oraz stosowanie firmowych polityk bezpieczeństwa (np. właściwe zarządzanie hasłami, zasady korzystania z zasobów IT i zgłaszanie incydentów). Szczególny nacisk należy położyć na doskonalenie wiedzy kadry zarządzającej (zgodnie z wymogami art. 20 NIS2), tak aby decydenci lepiej rozumieli naturę zagrożeń cyfrowych oraz własne obowiązki w zakresie nadzoru nad bezpieczeństwem. Warto przy tym korzystać z dostępnych materiałów edukacyjnych oferowanych przez wyspecjalizowane instytucje (np. poradniki ENISA czy alerty CSIRT), co ułatwi wdrażanie aktualnych najlepszych praktyk. Świadomy i przeszkolony personel staje się pierwszą linią obrony organizacji – nawet najlepsze procedury nie zadziałają, jeśli pracownicy nie będą ich znać i przestrzegać.
5. Wykorzystanie wsparcia zewnętrznego i współpraca: W przypadku braku dostatecznych wewnętrznych zasobów IT zaleca się korzystanie ze wsparcia zewnętrznych specjalistów. Usługi typu Managed Security Service Provider (MSSP), takie jak całodobowe monitorowanie bezpieczeństwa, zarządzanie systemami ochronnymi czy dostęp do eksperta bezpieczeństwa (CISO-as-a-Service), mogą okazać się dla MŚP bardziej opłacalne niż budowa takich kompetencji od podstaw. Równoległe małe firmy powinny aktywnie uczestniczyć w inicjatywach wymiany informacji o zagrożeniach – na przykład dołączając do sektorowych centrów typu ISAC lub przynajmniej śledząc ostrzeżenia publikowane przez krajowe

CSIRT (CERT Polska, CSIRT NASK) i ENISA. Takie zaangażowanie pozwala szybciej reagować na pojawiające się cyberzagrożenia, czerpać z doświadczeń innych podmiotów, a niekiedy uprzedzić atak poprzez wcześniejsze wdrożenie stosownych zabezpieczeń¹⁷. Ponadto należy monitorować dostępne programy wsparcia finansowego (fundusze unijne, granty rządowe) ukierunkowane na poprawę bezpieczeństwa – pozyskane dofinansowanie może znacząco złagodzić ciężar inwestycji koniecznych do spełnienia nowych wymogów.

6. Proaktywna współpraca z kontrahentami: Nacisk NIS2 na bezpieczeństwo łańcucha dostaw oznacza, że nawet firmy formalnie wyłączone spod tej regulacji odczuwają pośrednią presję ze strony większych partnerów biznesowych. MŚP powinny zatem proaktywnie współdziałać ze swoimi kluczowymi kontrahentami, aby poznać i – o ile to możliwe – uprzedzająco spełnić ich oczekiwania w zakresie zabezpieczeń. W praktyce warto z wyprzedzeniem dostosować wewnętrzne środki ochronne do standardów wymaganych przez większych odbiorców (np. wdrożyć dodatkowe polityki bezpieczeństwa, uzyskać certyfikat zgodności taki jak ISO/IEC 27001 czy przygotować procedury raportowania incydentów na żądanie klienta). Takie podejście pozwoli utrzymać zaufanie oraz relacje biznesowe, a jednocześnie zbuduje wizerunek wiarygodnego partnera – w warunkach zaostrzonych regulacji cyberbezpieczeństwa może to stanowić istotną przewagę konkurencyjną.

Wdrożenie powyższych rekomendacji jest pilne. Badania wskazują, że dla 90% europejskich MŚP tygodniowy paraliż działalności w wyniku poważnego cyberataku oznacza poważne perturbacje, a dla 57% mógłby skończyć się nawet bankructwem. Mimo to znaczna część małych firm nadal nie podejmuje wystarczających działań ochronnych, czy to z braku świadomości, czy ograniczeń finansowych. Dyrektywa NIS2 stanowi wyraźny impuls do działania – przy wsparciu regulatorów oraz większych partnerów biznesowych, sektor MŚP musi niezwłocznie podnieść swój bazowy poziom cyberbezpieczeństwa, aby dalsza cyfrowa transformacja tych przedsiębiorstw opierała się na solidnych fundamentach zaufania i odporności.

Podsumowanie

Dyrektywa NIS2 wprowadza nową jakość w europejskim ekosystemie cyberbezpieczeństwa. Rozszerza ona zakres regulacji poza tradycyjnie rozumianą infrastrukturę krytyczną, obejmując z mocy prawa wszystkie średnie i duże

¹⁷ M. Stachoń, E. Zalewska-Czajczyńska, P. Słowiński, *Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa – najważniejsze zmiany dla podmiotów*. Cyberpolicy NASK – Analizy, 2024.

przedsiębiorstwa z sektorów kluczowych i ważnych, a także – w uzasadnionych przypadkach – wybrane mniejsze podmioty o krytycznym znaczeniu. Następuje zatarcie prostej dotąd granicy między „podmiotem krytycznym” a „zwykłym przedsiębiorstwem” – o objęciu obowiązkami decyduje rola w łańcuchu gospodarczym i skala działalności, co w krajach takich jak Polska oznacza objęcie wymogami cyberbezpieczeństwa wielu nowych sektorów oraz części administracji publicznej. Jednocześnie NIS2 ujednocila i podnosi poprzeczkę wymagań: dyrektywa enumeratywnie wylicza minimalny zestaw środków technicznych i organizacyjnych (analiza ryzyka, ciągłość działania, bezpieczeństwo łańcucha dostaw, zarządzanie podatnościami, szyfrowanie, MFA itd.), co stanowi jakościowy krok naprzód względem ogólnych zasad NIS1. Precyzyjny katalog obowiązków przekłada się jednak na istotne wyzwania wdrożeniowe, zwłaszcza dla średnich przedsiębiorstw, które dotąd nie musiały realizować wielu z tych praktyk. Harmonizacja wymogów powinna ograniczyć zjawisko „najsłabszego ogniwa” regulacyjnego w UE i w horyzoncie kilku lat podnieść bazowy poziom cyberodporności w populacji firm średniej wielkości.

Najbardziej doniosłą zmianą NIS2 jest przeniesienie akcentu na ład korporacyjny i odpowiedzialność zarządu. Organy zarządzające zyskują obowiązki zatwierdzania polityk, nadzoru nad ryzykiem, odbywania szkoleń, a w określonych sytuacjach ponoszenia osobistych konsekwencji za rażące zaniedbania. Wymusza to utworzenie stałych kanałów raportowania między funkcją bezpieczeństwa a kierownictwem oraz realokację zasobów na zabezpieczenia. Można oczekiwać pozytywnego efektu systemowego w postaci bardziej strategicznego, proaktywnego podejścia do zarządzania cyberbezpieczeństwem i lepszej integracji celów ochrony z celami biznesowymi. Jednocześnie istnieje ryzyko „papierowego” wdrażania wymogów przez część MŚP – tzn. tworzenia polityk jedynie dla pozoru zgodności. Przeciwdziałać temu powinien efektywny nadzór publiczny i egzekwowanie sankcji: dopiero realne kontrole i kary, zbudują rynkową percepcję powagi nowych obowiązków. Dyrektywa wzmacnia także mechanizmy raportowania incydentów i współpracy – nowe, krótkie terminy zgłaszania incydentów (24h na wstępną notyfikację, 72h na raport szczegółowy, 1 miesiąc na raport końcowy) wymuszają sprawne informowanie o zagrożeniach, a rozbudowa europejskich sieci współpracy (CSIRT Network, EU-CyCLONe) sprzyja skoordynowanemu reagowaniu na incydenty transgraniczne.

Implementacja NIS2 przebiega jednak z zróżnicowaną dynamiką w poszczególnych krajach. Formalny termin wdrożenia upłynął 17 października 2024 r., tymczasem jedynie 4 państwa UE zdążyły przyjąć stosowne regulacje do tej daty – Komisja Europejska wszczęła postępowania przeciw pozostałym 23 krajom. Do połowy 2025 r. liczba państw z pełną transpozycją wzrosła do 9, a następnie (III kw. 2025) do kilkunastu, lecz nadal widoczna jest dywer-

gencja podejść krajowych. Różnice dotyczą m.in. zakresu sektorów objętych dodatkowymi obowiązkami, wysokości kar, procedur rejestracji podmiotów czy terminów osiągnięcia zgodności, co stwarza ryzyko fragmentacji rynku i wyzwania dla firm działających transgranicznie. Wiele jurysdykcji przewidziało okresy przejściowe i stopniowe wejście wymogów w życie, aby dać sektorowi czas na dostosowanie. W Polsce prace legislacyjne nad wdrożeniem NIS2 wciąż trwają (stan na IV kw. 2025), a organy rządowe zapowiadają umożliwienie rynkowi *vacatio legis* na przygotowanie się do nowych obowiązków¹⁸. Jednym z praktycznych sposobów zapełnienia luki kompetencyjnej w MŚP może być popularyzacja usług zarządzanych i outsourcingu funkcji bezpieczeństwa (MSSP).

Reasumując, NIS2 to ambitny krok w kierunku wzmocnienia bezpieczeństwa cyfrowego europejskiej gospodarki na wszystkich poziomach. Dla małych i średnich organizacji niesie on zarówno obciążenia – w postaci znaczącego wzrostu kosztów zgodności i konieczności wdrożenia nowych mechanizmów kontroli ryzyka – jak i szanse: na podniesienie dojrzałości cyberbezpieczeństwa, poprawę odporności operacyjnej oraz lepsze osadzenie bezpieczeństwa w procesach zarządczych. W perspektywie długofalowej można spodziewać się efektu kulturowego, podobnego do tego, jaki w obszarze ochrony danych wywołało RODO, pod warunkiem zapewnienia odpowiedniego wsparcia regulacyjnego (jasne wytyczne interpretacyjne, punkty kontaktowe), organizacyjnego (koordynacja między instytucjami, sieci współpracy) oraz finansowego (programy dotacyjne, ulgi i szkolenia). W takim ekosystemie dyrektywa NIS2 ma szansę stać się realnym katalizatorem pozytywnej zmiany – uczynić z europejskich MŚP nie „najsłabsze ogniwo” cyfrowego świata, lecz świadomych i wiarygodnych uczestników wspólnego systemu bezpieczeństwa.

18 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560 z późn. zm.; projekt nowelizacji implementującej NIS2 – stan legislacyjny sierpień 2025, RCL.

Bibliografia

1. Chałubińska-Jentkiewicz K., Nowikowska M., *Podmioty zaangażowane w politykę zapewnienia bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS2 (cz. 2)*, „Cybersecurity and Law” 2024, nr 11, s. 7.
2. Clausmeier D., *Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)*, „International Cybersecurity Law Review” 2023, 4(1), s. 79–90.
3. Hayes R., Walsh S., Moore L., *NIS2: A Game-Changer for Senior Management and Boards*, William Fry, 2025.
4. Mączka K., *Dyrektywa NIS2 jako wytyczna do wdrożenia systemu zarządzania bezpieczeństwem informacji w organizacji*, „Ochrona ludności i dziedzictwa kulturowego” 2024, 5/2024, s. 113.
5. Ostrowska J., Skalski S., *How will NIS2 affect the supply chain security approach?*, „EY Insights” 2023.
6. Philpot J., *DIGITAL SME launches guide to position SMEs as trusted NIS2 suppliers*, European DIGITAL SME Alliance, 2025.
7. Stachoń M., Zalewska-Czajczyńska E., Słowiński P., *Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa – najważniejsze zmiany dla podmiotów*, „Cyberpolicy NASK – Analizy” 2024.

Akty Prawne

1. Dyrektywa (UE) 2016/1148 Parlamentu Europejskiego i Rady z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. Urz. UE L 194 z 19.07.2016.
2. Dyrektywa (UE) 2022/2555 Parlamentu Europejskiego i Rady z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dyrektywa NIS2), Dz. Urz. UE L 333 z 27.12.2022.
3. Parlament Europejski i Rada UE, Wspólny wniosek dotyczący oceny skutków regulacji – Proposal for Directive on measures for high common level of cybersecurity across the Union, 2022.
4. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (Cybersecurity Act), Dz. Urz. UE L 151 z 7.06.2019.
5. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560 z późn. zm.; projekt nowelizacji implementującej NIS2 – stan legislacyjny sierpień 2025, RCL.

Raporty i dokumenty instytucjonalne

1. ENISA, *Cybersecurity for SMEs – Challenges and Recommendations*, European Union Agency for Cybersecurity, raport 2021.
2. ENISA, *NIS Investments 2024. Cybersecurity Policy Assessment*, 2024.

Netografia

1. Kaiser E., *The new NIS II Directive and its impact on small and medium enterprises (SMEs): initial considerations*, „MediaLaws” 2023, 1/2023, <https://www.medialaws.eu/rivista/the-new-nis-ii-directive-and-its-impact-on-small-and-medium-enterprises-smes-initial-considerations/> (dostęp: 24.10.2025).