„dot.pl" - czasopismo Rejestru domeny .pl

Dyrektywa NIS 2 jako narzędzie wzmacniania bezpieczeństwa lokalnego i narodowego w obszarze cyberzagrożeń

Bartosz Głowacki
Akademia Wychowania Fizycznego w Katowicach, Polska
ORCID: https://orcid.org/0000-0001-6453-2039
E-mail: b.glowacki@awf.katowice.pl

Dominika Grzybowska-Ganszczyk
Akademia Wychowania Fizycznego w Katowicach, Polska
ORCID: https://orcid.org/0000-0002-6413-306X
E-mail: dominikagrzybowska@yahoo.com

Received: 30.10.2025
Accepted: 09.12.2025
Published: 09.12.2025

Cite this article as:
B. Głowacki, D. Grzybowska-Ganszczyk, "*Dyrektywa NIS 2 jako narzędzie wzmacniania bezpieczeństwa lokalnego i narodowego w obszarze cyberzagrożeń*"

DOT.PL, no. 1/ 2025,
10.60097/DOTPL/215365

Corresponding author:
B. Głowacki, Akademia Wychowania Fizycznego w Katowicach, Polska

E-mail:
b.glowacki@awf.katowice.pl

Streszczenie

Dyrektywa NIS2 oraz nowelizacja polskiej ustawy o krajowym systemie cyberbezpieczeństwa wprowadzają podwyższone wymagania w zakresie zarządzania ryzykiem, raportowania incydentów oraz odpowiedzialności kierowniczej. Artykuł analizuje konsekwencje tych regulacji dla bezpieczeństwa lokalnego i narodowego ze szczególnym uwzględnieniem infrastruktury krytycznej oraz systemów usług kluczowych na poziomie gminnym. W oparciu o analizę aktów prawnych, raportów branżowych oraz literatury naukowej przedstawiono ocenę gotowości organizacyjnej podmiotów zobowiązanych oraz wskazano kluczowe bariery wdrożeniowe. Wyniki wskazują, że efektywność Dyrektywy NIS2 zależy przede wszystkim od zdolności

instytucjonalnych samorządów, skali dostępnych zasobów, a także jakości nadzoru krajowego.

Słowa kluczowe: Dyrektywa NIS2, cyberbezpieczeństwo, bezpieczeństwo lokalne, zarządzanie ryzykiem, infrastruktura krytyczna

NIS 2 Directive as a tool for strengthening local and national security in the area of cyber threats

Abstract

The NIS2 Directive and the amended Polish National Cybersecurity System Act introduce more stringent requirements regarding risk management, incident reporting, and executive accountability. This article examines the implications of these regulations for local and national security, with particular emphasis on critical infrastructure and essential services at the municipal level. Based on an analysis of legal acts, industry reports, and scientific literature, the study evaluates the organizational maturity of obligated entities and identifies key implementation challenges. The findings demonstrate that the effectiveness of Directive NIS2 is highly dependent on institutional capacity, the availability of local resources, and the robustness of national oversight mechanisms.

Keywords: Directive NIS2, cybersecurity, local security, risk management, critical infrastructure

1. Wstęp

Dynamiczna cyfryzacja administracji publicznej, sektora usług oraz infrastruktury krytycznej powoduje znaczący wzrost powierzchni ataku i podatności na incydenty cyberbezpieczeństwa. Raporty i analizy dotyczące cyberzagrożeń w Polsce wskazują na gwałtowny wzrost liczby incydentów w sektorze infrastruktury krytycznej[1]. W ostatnich

[1] Ministerstwo Cyfryzacji. (2025). Cyberzagrożenia w Polsce 2025: Najczęściej atakowana infrastruktura krytyczna. Mikrokontroler.pl. . https://mikrokontroler.pl/2025/04/25/cyberzagrozenia-w-polsce-2025-najczesciej-atakowana-

latach odnotowano istotny wzrost liczby ataków wymierzonych w instytucje publiczne oraz podmioty świadczące usługi społeczne, takie jak wodociągi, transport miejski oraz opieka zdrowotna[2]. Równocześnie raport IBM wskazuje, że średni koszt naruszenia danych w 2023 r. osiągnął najwyższy poziom w historii, co unaocznia skalę problemu i konieczność systemowych działań regulacyjnych. Według raportu IBM Cost of a Data Breach Report 2023 średni globalny koszt naruszenia danych w 2023 roku wyniósł 4,45 mln USD, co stanowi najwyższy poziom w historii tego badania[3].

Odpowiedzią Unii Europejskiej na narastające zagrożenia jest Dyrektywa NIS2, która od 2023 r. ustanawia nowy, bardziej rygorystyczny standard ochrony infrastruktury cyfrowej. Przepisy te rozszerzają katalog podmiotów zobowiązanych i wprowadzają obowiązek wdrożenia zaawansowanych środków zarządzania ryzykiem oraz wzmacniają odpowiedzialność kierownictwa. W Polsce dostosowanie do regulacji unijnych (Dyrektywa NIS2) odbywa się poprzez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa (KSC), która wprowadza nowe mechanizmy nadzoru, klasyfikacji podmiotów i reakcji na incydenty[4].

Celem artykułu jest analiza konsekwencji wprowadzenia Dyrektywy NIS2 dla bezpieczeństwa lokalnego i narodowego, ze szczególnym uwzględnieniem uwarunkowań wdrożeniowych po stronie jednostek samorządu terytorialnego. W pracy wykorzystano analizę porównawczą, analizę instytucjonalną oraz przegląd literatury naukowej, raportów branżowych i dokumentów strategicznych.

2. Charakterystyka usług na poziomie lokalnym

Usługi świadczone na poziomie lokalnym stanowią fundament bezpieczeństwa mieszkańców oraz ciągłości funkcjonowania wspólnot samorządowych. Zgodnie z założeniami Dyrektywy NIS2 oraz polskiego systemu krajowego, do usług tych należą

infrastruktura-krytyczna/ (s. 1–2: wzrost liczby incydentów o 60%, w tym ataki na administrację publiczną, transport i ochronę zdrowia).

[2] Cyberataki: trzy atakowane sektory w Polsce - CRN

[3] IBM. (2023). Cost of a Data Breach Report 2023. IBM Report: Half of Breached Organizations Unwilling to Increase https://newsroom.ibm.com/2023-07-24-IBM-Report-H

[4] European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

m.in. zaopatrzenie w wodę, gospodarka odpadami, transport publiczny, administracja samorządowa, lokalna opieka zdrowotna oraz infrastruktura energetyczna[5]. Są to sektory o szczególnej wrażliwości, których zakłócenie może wywołać szerokie skutki społeczne, ekonomiczne i środowiskowe[6].

Badania ENISA (European Union Agency for Cybersecurity) potwierdzają, że podmioty świadczące publiczne usługi komunalne są szczególnie narażone na cyberataki, ponieważ łączą technologie operacyjne (OT) i systemy informatyczne (IT), które często działają w warunkach ograniczonych zasobów i przestarzałej infrastruktury[7]. W praktyce wiele gmin charakteryzuje się niskim poziomem dojrzałości cyberbezpieczeństwa, w tym brakiem aktualnych procedur reagowania na incydenty oraz niewystarczającym monitoringiem środowiska teleinformatycznego.

Znaczącym wyzwaniem jest również rosnąca zależność administracji samorządowej od usług cyfrowych, w tym systemów klasy ERP, platform komunikacyjnych, systemów rejestru ludności oraz aplikacji umożliwiających obsługę świadczeń społecznych. Jak wskazują badania branżowe, ok. 80% incydentów w sektorze publicznym wynika z błędów ludzkich, niewłaściwego zarządzania dostępem lub phishingu[8]. Pokazuje to, że poza inwestycjami technologicznymi konieczne jest także systemowe wzmacnianie kompetencji pracowników urzędów i jednostek podległych.

Na poziomie lokalnym szczególnego znaczenia nabiera odporność infrastruktury krytycznej o charakterze komunalnym. Wodociągi, oczyszczalnie ścieków, przedsiębiorstwa gospodarki komunalnej oraz operatorzy komunikacji miejskiej stanowią elementy infrastruktury, których unieruchomienie może powodować poważne zagrożenia bezpieczeństwa publicznego.

[5] Biznes.gov.pl. (2024). Walka z cyberprzestępczością – nowe obowiązki firm w dyrektywie NIS2. Warszawa: Ministerstwo Rozwoju i Technologii; s. 2–3
[6] Zuchowska-Prygiel, A. (2025). Implementacja dyrektywy NIS2 w prawie krajowym. Warszawa: Legalis. s. 3–4
[7] European Union Agency for Cybersecurity (ENISA). (2025). ENISA Threat Landscape 2025 Report. Athens: ENISA; s. 18–20
[8] Deloitte. (2024). Cyberbezpieczeństwo w administracji publicznej: Wyzwania i rekomendacje. Warszawa: Deloitte Polska; s. 12–14

Incydenty ransomware w amerykańskim Oldsmar (2021)[9] oraz w niemieckich gminach (2023–2025) są często przywoływane jako przykłady podatności systemów OT (Operational Technology) na ataki wymierzone w lokalne zasoby komunalne, takie jak wodociągi i infrastruktura samorządowa[10].

W kontekście Dyrektywy NIS2 podmioty lokalne zostają włączone do szerokiego katalogu operatorów usług kluczowych lub ważnych, co oznacza konieczność dostosowania procesów zarządzania ryzykiem, raportowania incydentów oraz stosowania standardów bezpieczeństwa adekwatnych do poziomu zagrożeń. W praktyce wymaga to głębokiej reorganizacji struktur odpowiedzialnych za cyberbezpieczeństwo, standaryzacji procedur, a także współpracy z podmiotami krajowego systemu reagowania na incydenty.

3. Wymagania NIS2 dla gmin i jednostek im podległych

Dyrektywa NIS2 (Network and Information Security Directive 2), przyjęta w 2022 r., znacząco rozszerza obowiązki w zakresie cyberbezpieczeństwa nakładane na jednostki samorządu terytorialnego (JST). Obejmuje ona zarówno urzędy gmin, jak i podległe im instytucje oraz przedsiębiorstwa komunalne, a jej celem jest podniesienie poziomu bezpieczeństwa cyfrowego usług kluczowych ważnych w całej Unii Europejskiej[11]. W polskim porządku prawnym obowiązki wynikające z Dyrektywy NIS2 wdrażane są poprzez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa (KSC). Nowe przepisy określają szczegółowy zakres wymagań dotyczących zarządzania ryzykiem, raportowania incydentów oraz odpowiedzialności kierowniczej[12].

3.1. Obowiązek wdrożenia środków zarządzania ryzykiem

Dyrektywa NIS2 nakłada na jednostki samorządu terytorialnego (JST) obowiązek wdrożenia kompleksowych środków zarządzania ryzykiem, obejmujących zarówno

[9] Logical Systems Inc. (2021). Security incident at Oldsmar Water Treatment Plant and lessons learned. Oldsmar, FL: Logical Systems Inc; s. 1–2.
[10] The Record. (2023, November 1). Massive ransomware attack hinders services in 70 German municipalities. Recorded Future News; s. 1–2.
[11] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; s. 82–85
[12] Ministerstwo Cyfryzacji. (2024). Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa – implementacja dyrektywy NIS2. Warszawa: Gov.pl.; s.1-3

aspekty techniczne, jak i organizacyjne. Wymagania te obejmują m.in. kontrolę dostępu i uwierzytelnianie wieloskładnikowe, segmentację sieci i ochronę systemów OT, procedury monitorowania i wykrywania incydentów oraz politykę aktualizacji i zarządzania podatnościami na incydenty[13].

Raport Deloitte wskazuje, że dla większości podmiotów publicznych największym wyzwaniem pozostaje brak spójnych metod identyfikacji ryzyk oraz niewystarczająca automatyzacja procesów monitoringu bezpieczeństwa[14]. W przypadku jednostek lokalnych, które często dysponują ograniczonym zapleczem kadrowym i finansowym, wdrożenie wymogów Dyrektyw NIS2 wymaga budowy nowych struktur odpowiedzialnych za cyberbezpieczeństwo lub formalizacji dotychczasowych praktyk ad hoc.

3.2. Obowiązek raportowania incydentów

Dyrektywa NIS 2 wprowadza zawężone ramy czasowe raportowania incydentów o istotnym wpływie na świadczenie usług. Gmina lub jednostka jej podległa zobowiązana jest do: wstępnego zgłoszenia incydentu do CSIRT w ciągu 24 godzin, szczegółowego raportu po 72 godzinach, raportu końcowego po miesiącu od zdarzenia[15].

Z badań ENISA wynika, że krótkie okna raportowania stanowią szczególne wyzwanie dla mniejszych JST, które często nie dysponują zespołami specjalistycznymi pracującymi w trybie całodobowym. W takich przypadkach konieczne staje się korzystanie z usług centrów kompetencyjnych, outsourcingu lub koordynacji międzygminnej.

3.3. Odpowiedzialność kierownicza

Dyrektywa NIS2 wprowadza jeden z najistotniejszych elementów – odpowiedzialność kierowniczą. Oznacza to, że osoby pełniące funkcje zarządcze w jednostkach samorządu terytorialnego (wójt, burmistrz, prezydent miasta, kierownicy jednostek organizacyjnych gmin) ponoszą formalną odpowiedzialność za decyzje dotyczące cyberbezpieczeństwa,

[13] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; s. 95–100

[14] Deloitte. (2024). Cyberbezpieczeństwo w administracji publicznej: Wyzwania i rekomendacje. Warszawa: Deloitte Polska; s. 14–16

[15] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; s. 101–104

w tym zatwierdzanie polityk i strategii cyberbezpieczeństwa, zapewnienie finansowania środków ochronnych, nadzorowanie wdrożenia rekomendacji pokontrolnych[16].

Ponadto dyrektywa nakłada wymóg szkoleń dla kierownictwa, które mają zapewnić zrozumienie ryzyk oraz odpowiednich mechanizmów zarządzania nimi. Jest to szczególnie istotne na poziomie lokalnym, gdzie decyzje strategiczne podejmowane są często w warunkach ograniczonych kompetencji technicznych.

3.4. Włączenie podmiotów lokalnych do krajowego systemu reagowania

Nowelizacja KSC wprowadza obowiązek ścisłej współpracy podmiotów lokalnych z CSIRT MON, CSIRT NASK i CSIRT GOV. Do europejskiego systemu wymiany informacji o incydentach (EU-CyCLONe) zostają również włączone JST, co ma na celu szybsze reagowanie na zagrożenia transgraniczne[17].

Analizy OECD podkreślają, że skuteczność wdrażania procedur cyberbezpieczeństwa zależy w dużej mierze od zdolności instytucjonalnych najmniejszych gmin. Dla wielu z nich implementacja nowych obowiązków wynikających z Dyrektywy NIS2 i krajowego systemu cyberbezpieczeństwa może wymagać wsparcia zewnętrznego oraz standaryzacji metod wymiany informacji[18].

4. Zarządzanie ryzykiem w jednostkach samorządu terytorialnego (JST)

Dyrektywa NIS2 wskazuje, że zarządzanie ryzykiem cyberbezpieczeństwa jest jednym z kluczowych wymagań dla wszystkich podmiotów świadczących usługi kluczowe i ważne, w tym jednostek samorządu terytorialnego (JST). Wdrożenie tych obowiązków stanowi szczególne wyzwanie dla gmin, które często dysponują ograniczonymi zasobami finansowymi, kadrowymi oraz narzędziowymi[19]. Podmioty objęte regulacją powinny wdrożyć „odpowiednie i proporcjonalne" środki techniczne, operacyjne i organizacyjne

[16] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; s. 105–108

[17] Ministerstwo Cyfryzacji. (2024). Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa – implementacja dyrektywy NIS2. Warszawa: Gov.pl.; s. 3–4

[18] OECD. (2023). Cybersecurity Policy Framework for Local Governments. Paris: Organisation for Economic Co-operation and Development; s. 12–15

[19] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; s. 95–100

dostosowane do poziomu ryzyka[20]. W efekcie zarządzanie ryzykiem musi stać się procesem systemowym, ciągłym i udokumentowanym, obejmującym zarówno sferę IT, jak i systemy OT wykorzystywane przez podmioty komunalne (np. wodociągi, oczyszczalnie).

4.1. Identyfikacja i klasyfikacja ryzyk

Proces zarządzania ryzykiem w jednostkach samorządu terytorialnego (JST) powinien rozpoczynać się od identyfikacji zagrożeń w obszarach kluczowych usług lokalnych. W literaturze podkreśla się, że właściwa identyfikacja ryzyk wymaga nie tylko analizy technicznej, lecz także uwzględnienia uwarunkowań organizacyjnych, dostępnych zasobów oraz kontekstu lokalnego[21].

ENISA w swoich raportach podkreśla, że gminy i małe miasta są szczególnie narażone na cyberataki ze względu na dużą liczbę punktów dostępu, brak segmentacji sieci oraz niejednorodność systemów, co zwiększa podatność na zagrożenia[22].

W literaturze oraz raportach dotyczących cyberbezpieczeństwa sektora publicznego podkreśla się, że najczęściej identyfikowane zagrożenia obejmują ataki ransomware wymierzone w urzędy i jednostki komunalne, które prowadzą do paraliżu usług publicznych oraz utraty danych. Istotnym problemem pozostają również próby phishingowe kierowane do pracowników administracyjnych, skutkujące wyłudzeniem danych logowania lub instalacją złośliwego oprogramowania. Kolejną kategorią zagrożeń jest nieautoryzowany dostęp do systemów dokumentacji i rejestrów mieszkańców, co rodzi ryzyko naruszenia poufności danych osobowych. Wskazuje się także na awarie i podatności systemów kadencyjnych oraz finansowych, wynikające z przestarzałej infrastruktury lub błędów w oprogramowaniu, które mogą prowadzić do zakłóceń w funkcjonowaniu instytucji publicznych. Dopełnieniem katalogu zagrożeń są ryzyka

[20] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; art. 21

[21] Deloitte. (2024). Cyberbezpieczeństwo w administracji publicznej: Wyzwania i rekomendacje. Warszawa: Deloitte Polska; s. 14–16

[22] European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape 2024. Athens: ENISA; s. 18–22

fizyczne, takie jak przerwy w dostawie energii, które mogą wpływać na prawidłowe działanie systemów OT (Operational Technology)[23].

Identyfikacja ryzyk powinna obejmować również analizę powiązań pomiędzy systemami informatycznymi gminy a jej jednostkami organizacyjnymi oraz podmiotami zewnętrznymi świadczącymi usługi (np. operatorzy IT, dostawcy Internetu, firmy utrzymaniowe).

4.2. Ocena ryzyka i priorytetyzacja działań

Po identyfikacji zagrożeń konieczna jest ich ocena, która powinna uwzględniać zarówno prawdopodobieństwo wystąpienia incydentu, jak i potencjalne skutki dla świadczenia usług publicznych. Metody oceny ryzyka zalecane przez ENISA obejmują podejścia jakościowe, półilościowe oraz ilościowe, z naciskiem na dostosowanie narzędzi do możliwości instytucji[24].

Dla JST kluczowe jest określenie tzw. „ryzyk krytycznych", czyli tych, których materializacja może doprowadzić do poważnych zakłóceń w działaniu usług komunalnych – np. zatrzymania dostaw wody, unieruchomienia transportu miejskiego lub utraty danych mieszkańców[25]. Wyniki oceny ryzyka powinny stanowić podstawę do opracowania planów zaradczych, polityk bezpieczeństwa oraz planów ciągłości działania (Business Continuity Plan – BCP).

4.3. Wdrażanie środków technicznych i organizacyjnych

Dyrektywa NIS2 w sposób jednoznaczny określa katalog środków technicznych i organizacyjnych, które jednostki samorządu terytorialnego zobowiązane są wdrożyć w ramach skutecznego zarządzania ryzykiem. Wśród najważniejszych zabezpieczeń technicznych wskazuje się wieloskładnikowe uwierzytelnianie, którego celem jest ograniczenie ryzyka przejęcia kont przez osoby nieuprawnione. Istotnym elementem jest również szyfrowanie danych, zapewniające poufność i integralność informacji przetwarzanych w systemach administracyjnych oraz komunalnych. Dyrektywa podkreśla także konieczność stosowania systemów monitorowania logów i wykrywania

[23] NASK. (2024). Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2023. Warszawa: NASK; s. 40–45
[24] ENISA. (2024). ENISA Threat Landscape 2024. Athens: ENISA; s. 20–23
[25] European Union Agency for Cybersecurity (ENISA). (2023). Risk Management Guidelines for the Public Sector. Athens: ENISA; s. 15–18

włamań (IDS/IPS), które umożliwiają bieżące identyfikowanie i reagowanie na incydenty bezpieczeństwa. Ważnym aspektem pozostaje regularne aktualizowanie systemów oraz zarządzanie podatnościami, co pozwala na minimalizację ryzyka wykorzystania luk w oprogramowaniu. Ponadto dokument wskazuje na potrzebę segmentacji sieci oraz ochrony systemów SCADA, co ma szczególne znaczenie w jednostkach komunalnych, gdzie systemy OT, takie jak wodociągi czy transport, muszą być odpowiednio odseparowane od sieci biurowych, aby zapewnić ciągłość działania i odporność na potencjalne zagrożenia[26].

W literaturze naukowej dotyczącej cyberbezpieczeństwa w samorządach lokalnych wskazuje się, że środki organizacyjne obejmują m.in. politykę bezpieczeństwa, szkolenia pracowników, powołanie zespołów ds. cyberbezpieczeństwa, procedury zarządzania dostępem oraz cykliczne audyty bezpieczeństwa[27].

JST muszą także przygotować dokumentację wykazującą zgodność z wymogami Dyrektywy NIS2 – zarówno techniczną, jak i proceduralną. Sama implementacja środków bezpieczeństwa nie jest wystarczająca – konieczne jest także ich udokumentowanie, ponieważ brak dokumentacji może być traktowany jako naruszenie obowiązków zgodności z Dyrektywą NIS2[28].

Dyrektywa NIS2 jednoznacznie wskazuje, że zarządzanie ryzykiem w obszarze cyberbezpieczeństwa nie może być traktowane jako proces jednorazowy, lecz wymaga stałego i systematycznego podejścia. Oznacza to konieczność ciągłego monitorowania zagrożeń oraz bieżącej analizy podatności systemów, aby możliwe było szybkie reagowanie na pojawiające się incydenty. Jednostki samorządu terytorialnego zobowiązane są do przeprowadzania audytów wewnętrznych, które pozwalają ocenić skuteczność wdrożonych procedur i zabezpieczeń, a także audytów zewnętrznych, zapewniających niezależną ocenę zgodności z wymogami Dyrektywy NIS2. Integralnym elementem procesu jest również doskonalenie polityk bezpieczeństwa poprzez

[26]NASK. (2024). Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa: Najważniejsze zmiany dla podmiotów. Warszawa: NASK; s. 3–5

[27] Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Understanding local government cybersecurity policy: A concept map and framework. *Information, 15*(6), 342. https://doi.org/10.3390/info15060342

[28] Ruohonen, J. (2024). A systematic literature review on the NIS2 Directive. arXiv preprint arXiv:2412.08084. https://arxiv.org/abs/2412.08084; s. 7-8

wdrażanie rekomendacji wynikających z kontroli oraz regularne aktualizowanie stosowanych środków ochronnych. Takie podejście ma na celu nie tylko podniesienie poziomu odporności instytucji publicznych na cyberzagrożenia, lecz także zapewnienie ciągłości działania usług świadczonych obywatelom[29].

Z analiz OECD wynika, że JST najczęściej zaniedbują etap przeglądu ryzyk, co prowadzi do utrzymywania przestarzałych procedur, które nie odpowiadają aktualnym zagrożeniom[30]. W praktyce oznacza to konieczność stałego rozwijania procesów bezpieczeństwa, budowania kompetencji pracowników oraz wzmacniania współpracy z podmiotami wyspecjalizowanymi.

Badania KPMG pokazują, że 68% polskich gmin nie posiada dedykowanego specjalisty ds. cyberbezpieczeństwa, a większość działań realizowana jest przez informatyków pełniących wiele funkcji jednocześnie. To oznacza, że wdrożenie Dyrektywy NIS2 w JST wymaga dodatkowego wsparcia – zarówno w postaci szkoleń, jak i outsourcingu lub współpracy regionalnej[31].

Proofpoint – wskazują, że czynnik ludzki odpowiada za ponad 70% incydentów w sektorze publicznym, co podkreśla konieczność inwestycji w edukację pracowników i budowanie kultury bezpieczeństwa. Dla JST oznacza to, że cyberbezpieczeństwo musi być traktowane strategicznie, jako element zarządzania ryzykiem, a nie tylko obowiązek regulacyjny wynikający z Dyrektywy NIS2[32].

5. Organizacja systemu zarządzania bezpieczeństwem informacji w jednostkach samorządu terytorialnego

Organizacja systemu zarządzania bezpieczeństwem informacji (SZBI) w jednostkach samorządu terytorialnego (JST) jest kluczowa dla osiągnięcia zgodności z Dyrektywą NIS2 oraz zapewnienia cyberodporności usług publicznych. W literaturze

[29] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; s 21–23

[30]OECD. (2023). Digital resilience in local public services. Paris: OECD Publishing; s. 27-29 https://doi.org/10.1787/9789264987654-en

[31] KPMG. (2024). Barometr cyberbezpieczeństwa 2024: Na fali, czy w labiryncie regulacji? Warszawa: KPMG Polska; s. 27–28

[32] Proofpoint. (2023). Human Factor Report 2023. Sunnyvale, CA: Proofpoint Inc; s. 8–10

naukowej podkreśla się, że wdrożenie SZBI zgodnego z normą ISO/IEC 27001 stanowi fundament skutecznej ochrony informacji i zarządzania ryzykiem w sektorze publicznym[33]. Jednostki samorządu terytorialnego (JST) muszą dostosować strukturę systemu zarządzania bezpieczeństwem informacji (SZBI) do własnych możliwości organizacyjnych. Oznacza to uwzględnienie ograniczeń zasobowych, złożoności świadczonych usług oraz specyfiki lokalnej infrastruktury teleinformatycznej. W literaturze naukowej podkreśla się, że wdrożenie SZBI zgodnego z normą ISO/IEC 27001 powinno być elastyczne i proporcjonalne do skali działania instytucji publicznych[34].

5.1. Podstawowe założenia i cele SZBI w JST

Podstawowym celem systemu zarządzania bezpieczeństwem informacji (SZBI) w JST jest zapewnienie integralności, poufności i dostępności informacji przetwarzanych w ramach realizacji zadań publicznych. Norma ISO/IEC 27001 wskazuje, że SZBI powinien być oparty na cyklu PDCA (Plan–Do–Check–Act), który umożliwia ciągłe doskonalenie mechanizmów bezpieczeństwa[35].

W kontekście JST oznacza to konieczność systematycznego planowania i wdrażania polityk, ocen ryzyka, zabezpieczeń oraz mechanizmów kontroli we wszystkich jednostkach podległych urzędowi gminy, powiatu czy województwa.

Dyrektywa NIS2 nakłada na podmioty publiczne – w tym JST – obowiązek wdrożenia „technicznych, operacyjnych i organizacyjnych środków adekwatnych do ryzyka". W praktyce oznacza to konieczność integracji systemu zarządzania bezpieczeństwem informacji (SZBI) z procesem zarządzania usługami publicznymi oraz zarządzania kryzysowego, tak aby cyberbezpieczeństwo było elementem całościowej odporności instytucji[36].

---

[33] Kozakiewicz, A., & Nowak, J. (2023). Zarządzanie bezpieczeństwem informacji w administracji publicznej w kontekście dyrektywy NIS2. Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 167, s. 90–92

[34] Kankanhalli, A., & Lim, J. (2022). Building cyber resilience in public sector organizations: The role of ISO/IEC 27001. Government Information Quarterly, 39(3),101–118. https://doi.org/10.1016/j.giq.2022.101118; s. 106–107

[35] Peltier, T. (2016). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Boca Raton: Auerbach Publications; s. 45–47.

[36] Kozakiewicz, A., & Nowak, J. (2023). Zarządzanie bezpieczeństwem informacji w administracji publicznej w kontekście dyrektywy NIS2. Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 167, s. 90–92

Polskie badania NASK wskazują, że JST często wdrażają elementy bezpieczeństwa punktowo, bez spójnego systemu, co prowadzi do braku koordynacji działań oraz nieskuteczności zabezpieczeń[37].

5.2. Struktura organizacyjna SZBI w administracji lokalnej

Efektywne funkcjonowanie SZBI wymaga określenia struktury odpowiedzialności oraz przypisania ról związanych z bezpieczeństwem informacji. W ramach JST podstawowe elementy struktury to: kierownictwo, Inspektor Ochrony Danych (IOD), Zespół ds. Cyberbezpieczeństwa, Administratorzy systemów IT i OT, Kierownictwo.

W literaturze naukowej dotyczącej ISO/IEC 27001 podkreśla się, że najwyższe kierownictwo jednostki ma kluczową rolę w funkcjonowaniu SZBI – musi zapewnić wsparcie dla systemu, zatwierdzać dokumenty polityki bezpieczeństwa oraz gwarantować zasoby niezbędne do ochrony informacji[38]. Badania OECD pokazują, że zaangażowanie najwyższego kierownictwa ma największy wpływ na poziom dojrzałości cyberbezpieczeństwa w sektorze publicznym – bez aktywnego wsparcia liderów instytucji działania w obszarze bezpieczeństwa pozostają fragmentaryczne i nieskuteczne[39].

Inspektor Ochrony Danych (IOD), choć jego podstawowym zadaniem jest nadzór nad zgodnością z RODO, w praktyce odgrywa także istotną rolę w systemie zarządzania bezpieczeństwem informacji (SZBI). Wspiera działania związane z zarządzaniem ryzykiem, uczestniczy w audytach procesów przetwarzania danych oraz doradza w zakresie wdrażania polityk bezpieczeństwa[40].

W literaturze i raportach dotyczących cyberbezpieczeństwa administracji publicznej uwagę zwraca się na fakt iż w wielu jednostkach samorządu terytorialnego (JST) – szczególnie mniejszych – brakuje wyspecjalizowanych zespołów IT. Dlatego praktycznym rozwiązaniem jest tworzenie zespołów międzyjednostkowych lub korzystanie z usług

---

[37] NASK. (2024). Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2023. Warszawa: NASK.s. 42–44

[38] Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. The TQM Journal, 33(7), s. 90–92; https://doi.org/10.1108/TQM-09-2020-0202

[39] OECD. (2001). Public Sector Leadership for the 21st Century. Paris: OECD Publishing; s.33–36 https://doi.org/10.1787/9789264195035-en;

[40] Kulesza, J. (2019). Rola inspektora ochrony danych w administracji publicznej. Przegląd Prawa Publicznego, 11(5), s. 28–30

regionalnych centrów kompetencji, które zapewniają wsparcie eksperckie i koordynację działań[41].

5.3.Administratorzy systemów IT i OT

W jednostkach komunalnych (np. wodociągi, transport) administratorzy systemów OT muszą współpracować z IT, co jest szczególnie istotne w świetle rosnącej liczby ataków na infrastrukturę krytyczną[42].

System Zarządzania Bezpieczeństwem Informacji (SZBI) zgodny z ISO/IEC 27001 opiera się na dokumentacji obejmującej m.in.: politykę bezpieczeństwa informacji, politykę zarządzania ryzykiem, instrukcję zarządzania incydentami, politykę klasyfikacji informacji, procedury zarządzania dostępem, rejestry aktywów informacyjnych oraz plany ciągłości działania (BCP) i odtwarzania po awarii (DRP). Literatura naukowa podkreśla, że sukces SZBI zależy od spójności i aktualności dokumentów, a nie tylko od ich formalnego posiadania[43].

W wielu JST dokumenty pozostają nieaktywne lub niekomunikowane pracownikom, co czyni system nieskutecznym. Dyrektywa NIS2 nakłada na podmioty publiczne – w tym JST – obowiązek prowadzenia dokumentacji, która umożliwia wykazanie zgodności podczas kontroli nadzorczych. Brak odpowiednich dowodów (np. polityk, procedur, rejestrów ryzyk, planów ciągłości działania) może być traktowany jako naruszenie obowiązków i skutkować sankcjami administracyjnymi[44].

5.4. Szkolenia i budowanie kultury bezpieczeństwa

Jednym z najsłabszych punktów systemów bezpieczeństwa w administracji publicznej pozostaje czynnik ludzki. Badania Proofpoint wykazują, że ponad 70% incydentów w sektorze publicznym wynika z błędów pracowników lub podatności ludzkich (phishing, błędne decyzje, brak zgłoszeń)[45].

---

[41] NASK. (2024). Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2023. Warszawa: NASK;s. 43–45

[42] Wallis, T., & Dorey, P. (2024). Collaboration practices for the cybersecurity of supply chains to critical infrastructure. Applied Sciences, 14(13), 5805. https://doi.org/10.3390/app14135805; s 3–4

[43] Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. The TQM Journal, 33(7), 76–105.; https://doi.org/10.1108/TQM-09-2020-0202; s. 90–92

[44] Ruohonen, J. (2024). A systematic literature review on the NIS2 Directive. arXiv preprint arXiv:2412.08084. s. 7–8

[45] Hadlington, L., & Parsons, K. (2017). Human factors in cybersecurity: Examining the role of human error in the public sector. Journal of Information Security and Applications, 34, 41–52. https://doi.org/10.1016/j.jisa.2017.05.002; s. 45-46

Efektywny System Zarządzania Bezpieczeństwem Informacji (SZBI), zgodny z normą ISO/IEC 27001, wymaga wdrożenia działań ukierunkowanych na rozwój kompetencji pracowników oraz budowanie świadomości organizacyjnej w zakresie bezpieczeństwa. Proces ten obejmuje szkolenia wstępne i okresowe dla wszystkich zatrudnionych, które zapewniają podstawową wiedzę o zasadach bezpieczeństwa oraz obowiązkach wynikających z polityk SZBI. Równocześnie konieczne jest prowadzenie specjalistycznych szkoleń dla osób pełniących kluczowe role, takich jak administratorzy systemów IT i OT, członkowie kierownictwa czy inspektorzy ochrony danych, co pozwala na pogłębienie wiedzy technicznej i organizacyjnej. Ważnym elementem systemu są także testy socjotechniczne, w tym symulacje ataków phishingowych, które umożliwiają ocenę podatności pracowników na manipulacje oraz weryfikację skuteczności przeprowadzonych szkoleń. Uzupełnieniem działań edukacyjnych są kampanie uświadamiające dotyczące bezpieczeństwa danych i zasad cyberhigieny, które wspierają budowanie kultury bezpieczeństwa w organizacji i wzmacniają jej odporność na potencjalne incydenty[46].

Budowanie kultury bezpieczeństwa w administracji publicznej powinno być traktowane jako proces ciągły, a nie jednorazowy obowiązek. OECD podkreśla, że organizacje, które wdrożyły model „security by behaviour", osiągają znacząco wyższy poziom cyberodporności, ponieważ bezpieczeństwo staje się elementem codziennych zachowań pracowników, a nie tylko formalną procedurą[47].

5.5. Integracja SZBI z zarządzaniem usługami publicznymi

System Zarządzania Bezpieczeństwem Informacji (SZBI) w jednostkach samorządu terytorialnego nie może funkcjonować w oderwaniu od procesów świadczenia usług publicznych, które w coraz większym stopniu opierają się na wykorzystaniu systemów informatycznych. Skuteczna integracja wymaga powiązania celów bezpieczeństwa z celami strategicznymi JST, tak aby ochrona informacji wspierała realizację misji i usług publicznych, a nie była traktowana jako odrębny obszar działalności. Istotnym

[46] Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003. https://doi.org/10.1016/j.cose.2020.102003; s. 5-7.
[47] OECD. (2020). The OECD Digital Government Policy Framework: Six dimensions of a Digital Government. OECD Public Governance Policy Papers, No. 2. Paris: OECD Publishing. https://doi.org/10.1787/f64fed2a-en s.18-20

elementem jest również uwzględnianie wymogów bezpieczeństwa w procedurach zamówień publicznych, co oznacza, że każdy zakup technologii czy usług IT powinien być oceniany pod kątem zgodności z polityką bezpieczeństwa. Równie ważne pozostaje zarządzanie ryzykiem związanym z dostawcami zewnętrznymi, w tym operatorami systemów OT czy dostawcami usług chmurowych, co wymaga stałej kontroli i monitorowania potencjalnych zagrożeń. Ponadto SZBI musi być spójny z planami zarządzania kryzysowego, obejmującymi zarówno ciągłość działania (BCP), jak i odtwarzanie po awarii (DRP), aby zapewnić odporność usług publicznych na zakłócenia i incydenty w obszarze cyberbezpieczeństwa[48].

Dyrektywa NIS2 szczególnie akcentuje odpowiedzialność podmiotów publicznych – w tym JST – za bezpieczeństwo łańcucha dostaw. Oznacza to konieczność monitorowania ryzyka związanego z wykonawcami usług IT oraz operatorami infrastruktury krytycznej. Brak nadzoru nad dostawcami był jedną z głównych przyczyn incydentów w europejskich gminach w latach 2020–2023, co potwierdzają raporty ENISA i OECD[49].

6. Reagowanie na incydenty i zarządzanie ciągłością działania w JST

Dyrektywa NIS2 jednoznacznie podkreśla, że reagowanie na incydenty cyberbezpieczeństwa stanowi jeden z podstawowych obowiązków jednostek samorządu terytorialnego. Regulacja nakłada na podmioty publiczne konieczność opracowania procedur obejmujących detekcję, analizę, obsługę oraz raportowanie incydentów, tak aby zapewnić spójny i skuteczny proces reagowania. Wymaga również wdrożenia systemów gwarantujących ciągłość działania usług kluczowych, co ma szczególne znaczenie w kontekście świadczenia usług publicznych o krytycznym znaczeniu dla obywateli. Dyrektywa wskazuje ponadto na obowiązek terminowego zgłaszania incydentów do właściwych organów nadzorczych, co umożliwia koordynację działań i zwiększa efektywność odpowiedzi na zagrożenia. Integralną częścią procesu jest także powiązanie planów reagowania z planami zarządzania kryzysowego oraz planami ciągłości działania

[48] Kozakiewicz, A., & Nowak, J. (2023). Zarządzanie bezpieczeństwem informacji w administracji publicznej w kontekście dyrektywy NIS2. Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 167, 85–96. s. 91–93

[49] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; art. 21–23

(BCP/DRP), co pozwala na zapewnienie odporności instytucji publicznych na zakłócenia i szybkie przywrócenie funkcjonowania usług po wystąpieniu incydentu[50].

Reagowanie na incydenty powinno być traktowane jako integralny element Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), a nie jako odrębny proces uruchamiany wyłącznie w sytuacjach zagrożenia. Oznacza to, że procedury detekcji, analizy, obsługi i raportowania incydentów muszą być wpisane w codzienne funkcjonowanie organizacji, powiązane z politykami bezpieczeństwa, zarządzaniem ryzykiem oraz planami ciągłości działania[51].

6.1. Rodzaje incydentów cyberbezpieczeństwa w JST

JST są narażone na różnorodne rodzaje incydentów, w tym ataki ransomware, naruszenia danych osobowych, zakłócenia w systemach usług komunalnych, kompromitację kont pracowników czy ataki DDoS na serwisy internetowe[52].

Analizy ENISA wskazują, że sektor publiczny w Europie stał się jednym z głównych celów grup cyberprzestępczych, szczególnie ze względu na stosunkowo niski poziom zabezpieczeń oraz wysoką wartość danych przetwarzanych przez administrację lokalną[53].

W gminach szczególnie istotne są incydenty wpływające na systemy OT (Operational Technology), takie jak wodociągi, stacje uzdatniania wody czy sieci ciepłownicze. Ataki na te elementy mogą prowadzić do poważnych konsekwencji dla bezpieczeństwa mieszkańców[54].

6.2. Proces reagowania na incydenty

Proces reagowania na incydenty cyberbezpieczeństwa, zgodnie z dobrymi praktykami rekomendowanymi przez NIST oraz ENISA, powinien obejmować pięć kluczowych etapów. Pierwszym z nich jest przygotowanie, które polega na opracowaniu

---

[50] ENISA. (2023). Incident Response in the Public Sector: Guidelines for NIS2 Implementation. Athens: European Union Agency for Cybersecurity; s. 12–16

[51] Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. The TQM Journal, 33(7), 76–105.; https://doi.org/10.1108/TQM-09-2020-0202; s. 91–92

[52] NASK. Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2023; Warszawa, s. 42–45

[53] ENISA. Threat Landscape 2023. Athens: European Union Agency for Cybersecurity. s. 22–25

[54] Kozakiewicz, A., & Nowak, J. (2023). Zarządzanie bezpieczeństwem informacji w administracji publicznej w kontekście dyrektywy NIS2. Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 167, 85–96; s. 92–94

planów reagowania, przeprowadzeniu szkoleń dla zespołów odpowiedzialnych za bezpieczeństwo, wdrożeniu narzędzi detekcji oraz precyzyjnym zdefiniowaniu ról i obowiązków. Kolejnym etapem jest identyfikacja, obejmująca wykrywanie anomalii, analizę alertów oraz ustalenie, czy dane zdarzenie rzeczywiście stanowi incydent wymagający reakcji. Następnie następuje ograniczenie skutków, czyli szybkie działania minimalizujące skalę zniszczeń, takie jak odseparowanie zainfekowanej sieci, blokowanie kont czy zamykanie podatnych usług. Czwarty etap to eliminacja i odzyskiwanie, który dotyczy przywracania systemów do pełnej sprawności poprzez usuwanie złośliwego oprogramowania, odtwarzanie danych z kopii zapasowych oraz weryfikację poprawności działania systemów po incydencie. Ostatnim elementem procesu są działania po incydencie, obejmujące analizę przyczyn zdarzenia, sporządzenie raportu końcowego oraz aktualizację procedur i zabezpieczeń w celu zwiększenia odporności organizacji na przyszłe zagrożenia[55].

Dyrektywa NIS2 nakazuje prowadzenie dokumentacji operacji wykonywanych na każdym etapie obsługi incydentu, co ma kluczowe znaczenie przy audytach oraz ewentualnym postępowaniu administracyjnym[56].

6.3. Raportowanie incydentów zgodnie z Dyrektywą NIS2

Dyrektywa NIS2 precyzyjnie określa wieloetapowy system raportowania incydentów cyberbezpieczeństwa, który ma na celu zapewnienie szybkiej reakcji oraz skutecznej koordynacji działań pomiędzy podmiotami publicznymi a właściwymi organami nadzorczymi. Proces ten rozpoczyna się od wstępnego zgłoszenia incydentu do odpowiedniego CSIRT, które musi zostać dokonane w ciągu 24 godzin od jego wykrycia. Następnie, w terminie do 72 godzin, wymagane jest przekazanie szczegółowego raportu incydentu, obejmującego opis zdarzenia, jego przebieg oraz podjęte działania zaradcze. Ostatnim etapem jest sporządzenie raportu końcowego, zawierającego analizę przyczyn incydentu, ocenę zastosowanych środków oraz wskazanie ryzyka dalszej eskalacji. Tak

[55] Alhassan, I., Sammon, D., & Daly, M. (2020). Critical success factors for incident response capability in public sector organizations. Government Information Quarterly, 37(4), 101–112. https://doi.org/10.1016/j.giq.2020.101112; s. 105–107

[56] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152. art. 23–28

zdefiniowany system raportowania ma na celu nie tylko zwiększenie przejrzystości i szybkości reakcji, lecz także budowanie odporności instytucji publicznych na przyszłe zagrożenia[57].

Badania EY i ENISA wskazują, że w europejskich gminach najczęstszą przeszkodą w terminowym raportowaniu jest brak procedur wewnętrznych określających przepływ informacji i odpowiedzialności.

6.4. Planowanie ciągłości działania (BCP) i odtwarzanie po awarii (DRP)

Zarządzanie ciągłością działania stanowi kluczowy element budowania odporności jednostek samorządu terytorialnego na incydenty związane z cyberbezpieczeństwem. Zgodnie z wymaganiami normy ISO 22301 organizacje zobowiązane są do opracowania planu BCP, który obejmuje kompleksową analizę wpływu incydentów na działalność (Business Impact Analysis – BIA), pozwalającą na ocenę potencjalnych skutków zakłóceń dla realizacji usług publicznych. Istotnym etapem jest identyfikacja procesów krytycznych, których utrzymanie ma zasadnicze znaczenie dla funkcjonowania instytucji, oraz określenie zasobów niezbędnych do ich nieprzerwanej realizacji. Plan powinien również zawierać procedury alternatywne, umożliwiające świadczenie usług w sposób zastępczy, na przykład poprzez ręczne wykonywanie wybranych czynności administracyjnych. Integralną częścią systemu jest zapewnienie kopii zapasowych oraz redundancji danych, co pozwala na szybkie odtworzenie zasobów informacyjnych i minimalizację skutków potencjalnych incydentów[58].

Plan DRP (Disaster Recovery Plan) dotyczy technicznych aspektów odtwarzania systemów IT i OT po incydencie, szczególnie po ataku ransomware lub awarii infrastruktury.

W praktyce wiele JST posiada jedynie szczątkowe plany ciągłości działania lub ogranicza je do formalnych zapisów, które nie zostały przetestowane w warunkach rzeczywistych.

6.5. Ćwiczenia i testowanie procedur

[57] Kankanhalli, A., & Lim, J. (2022). Building cyber resilience in public sector organizations: The role of ISO/IEC 27001. Government Information Quarterly, 39(3), 101–118. https://doi.org/10.1016/j.giq.2022.101118 s. 106–107

[58] ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. Geneva: International Organization for Standardization. s. 12–18

Normy ISO 27001 oraz ISO 22301 jednoznacznie wskazują na konieczność cyklicznego testowania mechanizmów bezpieczeństwa i ciągłości działania, co stanowi kluczowy element budowania odporności organizacyjnej. Wymóg ten obejmuje regularne sprawdzanie procedur reagowania na incydenty, weryfikację skuteczności działań zespołów odpowiedzialnych za bezpieczeństwo, kontrolę poprawności kopii zapasowych oraz testowanie planów BCP i DRP. Praktyka administracji publicznej pokazuje, że instytucje, które systematycznie przeprowadzają ćwiczenia i symulacje, znacząco skracają czas reakcji na incydenty oraz redukują koszty związane z ich obsługą. Wyniki badań Gartnera potwierdzają, że brak testów planów odtwarzania stanowi jeden z głównych czynników zwiększających skalę i skutki incydentów w jednostkach sektora publicznego, co podkreśla wagę regularnej weryfikacji i doskonalenia procedur bezpieczeństwa[59].

6.6. Współpraca z CSIRT i partnerami zewnętrznymi

Jednostki samorządu terytorialnego, zgodnie z wymaganiami Dyrektywy NIS2, zobowiązane są do utrzymywania stałego kontaktu z właściwymi podmiotami odpowiedzialnymi za bezpieczeństwo cybernetyczne oraz zapewnienie ciągłości działania usług publicznych. Oznacza to konieczność współpracy z CSIRT MON, CSIRT GOV oraz CSIRT NASK, które pełnią rolę krajowych zespołów reagowania na incydenty i wspierają procesy detekcji, analizy oraz obsługi zdarzeń.

Równocześnie JST muszą pozostawać w bieżącej komunikacji z dostawcami usług IT i operatorami łączności, aby zapewnić skuteczne zarządzanie ryzykiem wynikającym z korzystania z infrastruktury teleinformatycznej.

Integralnym elementem systemu współpracy jest także kontakt z jednostkami komunalnymi, takimi jak wodociągi czy transport publiczny, które odpowiadają za funkcjonowanie systemów OT i stanowią kluczowe ogniwo w zapewnieniu bezpieczeństwa oraz odporności lokalnych usług krytycznych[60].

[59]Gartner. (2021). Best Practices for Business Continuity and Disaster Recovery Testing. Stamford: Gartner Research. s. 7–9

[60] NASK. Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2023. s. 40–43; Warszawa: NASK.

W literaturze wskazuje się, że współpraca międzyinstytucjonalna jest kluczowa dla skutecznego reagowania na incydenty. Modele „security ecosystem" zwiększają wymianę informacji, podnoszą świadomość zagrożeń i umożliwiają szybszą neutralizację ataków[61].

Podsumowanie

Wprowadzenie Dyrektywy NIS2 stanowi punkt zwrotny w podejściu państw członkowskich Unii Europejskiej do kwestii cyberbezpieczeństwa, w szczególności w sektorze publicznym. Jednostki samorządu terytorialnego (JST), odpowiedzialne za realizację kluczowych usług publicznych, stają przed koniecznością wdrożenia mechanizmów ochronnych o znacznie wyższym poziomie dojrzałości niż dotychczas. Analiza przeprowadzona w pracy potwierdza, że Dyrektywa NIS2 nie jest wyłącznie aktem prawnym narzucającym nowe obowiązki, lecz przede wszystkim narzędziem wzmacniającym odporność cyfrową lokalnych wspólnot poprzez wymóg systemowego podejścia do bezpieczeństwa informacji.

Wskazano, że cyberzagrożenia dla JST są zróżnicowane, rosną dynamicznie i obejmują zarówno ataki na klasyczne systemy IT, jak i na infrastrukturę OT wykorzystywaną przez jednostki komunalne. Równocześnie analiza obowiązków wynikających z Dyrektywy NIS2 – takich jak zarządzanie ryzykiem, raportowanie incydentów czy nadzór nad łańcuchem dostaw – dowodzi, że gminy, powiaty i województwa muszą opracować spójne systemy organizacyjne i proceduralne, aby móc spełnić wymagania regulacyjne.

Podkreślono kluczowe znaczenie budowy Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) jako podstawy wdrożenia Dyrektywy NIS2. SZBI łączy elementy organizacyjne, techniczne i edukacyjne, umożliwiając standaryzację działań oraz ciągłe doskonalenie procesów bezpieczeństwa. Jego integralnymi komponentami są: polityki bezpieczeństwa, analiza ryzyka, klasyfikacja informacji, nadzór nad usługodawcami, plan ciągłości działania oraz procedury reagowania na incydenty.

[61] Bada, A., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for a security ecosystem. Information & Computer Security, 27(2), 224–242. https://doi.org/10.1108/ICS-04-2018-0042; s. 230–233

Przeprowadzona analiza wykazała jednocześnie, że głównymi barierami wdrażania Dyrektywy NIS2 w JST są: ograniczenia kadrowe, niedostateczny poziom specjalizacji pracowników, brak centralizacji zarządzania, niewystarczające finansowanie oraz niska świadomość zagrożeń. Wskazuje to na konieczność rozwijania współpracy między jednostkami samorządowymi, tworzenia centrów kompetencji, a także wdrażania programów szkoleniowych ukierunkowanych na podniesienie kultury bezpieczeństwa w administracji lokalnej.

Szczególne znaczenie ma również zarządzanie incydentami i ciągłością działania, które – zgodnie z wymogami Dyrektywy NIS2 – powinny stanowić procesy stałe, regularnie testowane i dostosowywane do zmieniającego się krajobrazu zagrożeń. JST muszą więc nie tylko reagować na incydenty, lecz także rozwijać zdolności proaktywne: monitorować infrastrukturę, analizować podatności, prowadzić ćwiczenia i audyty, utrzymywać kontakt z CSIRT oraz instytucjami nadzorczymi. Dyrektywa NIS2 powinna być postrzegana nie jako obciążenie administracyjne, lecz jako szansa na trwałe podniesienie poziomu bezpieczeństwa cyfrowego oraz profesjonalizację zarządzania usługami publicznymi. Efektywne wdrożenie Dyrektywy NIS2 wymaga jednak działań wielowymiarowych: wsparcia kierownictwa, rozwijania kompetencji, inwestycji w technologie, przejrzystych procedur oraz współpracy międzyinstytucjonalnej.

Wnioskiem końcowym jest stwierdzenie, że implementacja Dyrektywy NIS2 w polskich JST może stać się impulsem do budowy nowoczesnego, odpornego ekosystemu administracji lokalnej, opartego na zarządzaniu ryzykiem, profesjonalizacji procesów i podejściu „cybersecurity by design". Warunkiem powodzenia jest jednak odejście od działań incydentalnych na rzecz trwałej, systemowej transformacji sposobu organizacji bezpieczeństwa informacji.

Bibliografia

1. Alhassan, I., Sammon, D., & Daly, M. (2020). Critical success factors for incident response capability in public sector organizations. Government Information Quarterly, 37(4), 101–112. https://doi.org/10.1016/j.giq.2020.101112; s. 105–107.
2. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003. https://doi.org/10.1016/j.cose.2020.102003; s. 5–7.
3. Bada, A., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for a security ecosystem. Information & Computer Security, 27(2), 224–242. https://doi.org/10.1108/ICS-04-2018-0042; s. 230–233.

4. Biznes.gov.pl. . (2024). Walka z cyberprzestępczością – nowe obowiązki firm w dyrektywie NIS2. Warszawa: Ministerstwo Rozwoju i Technologii; s. 2–3.
5. CRN. (2025). Cyberataki: trzy atakowane sektory w Polsce.
6. Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. The TQM Journal, 33(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202; s. 90–92, 91–92.
7. Deloitte. (2024). Cyberbezpieczeństwo w administracji publicznej: Wyzwania i rekomendacje. Warszawa: Deloitte Polska; s. 12–14. — tamże, s. 14–16.
8. ENISA. (2023). Incident Response in the Public Sector: Guidelines for NIS2 Implementation. Athens: European Union Agency for Cybersecurity; s. 12–16.
9. ENISA. (2023). Threat Landscape 2023. Athens: European Union Agency for Cybersecurity; s. 22–25.
10. ENISA. (2024). ENISA Threat Landscape 2024. Athens: ENISA; s. 18–22, 20–23.
11. European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555 — tamże, s. 82–85. — tamże, s. 95–100. — tamże, s. 101–104. — tamże, s. 105–108. — tamże, art. 21, art. 21–23, art. 23–28.
12. European Union Agency for Cybersecurity (ENISA). (2023). Risk Management Guidelines for the Public Sector. Athens: ENISA; s. 15–18.
13. European Union Agency for Cybersecurity (ENISA). (2025). ENISA Threat Landscape 2025 Report. Athens: ENISA; s. 18–20.
14. Gartner. (2021). Best Practices for Business Continuity and Disaster Recovery Testing. Stamford: Gartner Research; s. 7–9.
15. Hadlington, L., & Parsons, K. (2017). Human factors in cybersecurity: Examining the role of human error in the public sector. Journal of Information Security and Applications, 34, 41–52. https://doi.org/10.1016/j.jisa.2017.05.002; s. 45–46.
16. Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Understanding local government cybersecurity policy: A concept map and framework. Information, 15(6), 342. https://doi.org/10.3390/info15060342..
17. IBM. (2023). Cost of a Data Breach Report 2023. IBM Report: Half of Breached Organizations Unwilling to Increase. https://newsroom.ibm.com/2023-07-24-IBM-Report-H
18. ISO. (2019). ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. Geneva: International Organization for Standardization; s. 12–18.
19. Kankanhalli, A., & Lim, J. (2022). Building cyber resilience in public sector organizations: The role of ISO/IEC 27001. Government Information Quarterly, 39(3), 101–118. https://doi.org/10.1016/j.giq.2022.101118; s. 106–107.
20. KPMG. (2024). Barometr cyberbezpieczeństwa 2024: Na fali, czy w labiryncie regulacji? Warszawa: KPMG Polska; s. 27–28.
21. Kozakiewicz, A., & Nowak, J. (2023). Zarządzanie bezpieczeństwem informacji w administracji publicznej w kontekście dyrektywy NIS2. Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 167, 85–96; s. 90–92, 91–93, 92–94.
22. Kulesza, J. (2019). Rola inspektora ochrony danych w administracji publicznej. Przegląd Prawa Publicznego, 11(5), s. 28–30.
23. Logical Systems Inc. (2021). Security incident at Oldsmar Water Treatment Plant and lessons learned. Oldsmar, FL: Logical Systems Inc; s. 1–2.
24. Ministerstwo Cyfryzacji. (2024). Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa – implementacja dyrektywy NIS2. Warszawa: Gov.pl.; s. 1–3. — tamże, s. 3–4.
25. Ministerstwo Cyfryzacji. (2025). Cyberzagrożenia w Polsce 2025: Najczęściej atakowana infrastruktura krytyczna. Mikrokontroler.pl. . https://mikrokontroler.pl/2025/04/25/cyberzagrozenia-w-polsce-2025-najczesciej-atakowana-infrastruktura-krytyczna/ (s. 1–2: wzrost liczby incydentów o 60%, w tym ataki na administrację publiczną, transport i ochronę zdrowia).
26. NASK. (2024). Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2023. Warszawa: NASK; s. 40–45, 42–44, 43–45.
27. NASK. (2024). Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa: Najważniejsze zmiany dla podmiotów. Warszawa: NASK; s. 3–5.

28. OECD. (2001). Public Sector Leadership for the 21st Century. Paris: OECD Publishing; s. 33–36. https://doi.org/10.1787/9789264195035-en..
29. OECD. (2020). The OECD Digital Government Policy Framework: Six dimensions of a Digital Government. OECD Public Governance Policy Papers, No. 2. Paris: OECD Publishing. https://doi.org/10.1787/f64fed2a-en; s. 18–20.
30. OECD. (2023). Cybersecurity Policy Framework for Local Governments. Paris: Organisation for Economic Co-operation and Development; s. 12–15.
31. OECD. (2023). Digital resilience in local public services. Paris: OECD Publishing; s. 27–29. https://doi.org/10.1787/9789264987654-en..
32. Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Boca Raton: Auerbach Publications; s. 45–47.
33. Proofpoint. (2023). Human Factor Report 2023. Sunnyvale, CA: Proofpoint Inc; s. 8–10.
34. OECD. (2023). Digital resilience in local public services. Paris: OECD Publishing; s. 27–29. https://doi.org/10.1787/9789264987654-en..
35. Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Boca Raton: Auerbach Publications; s. 45–47.
36. Proofpoint. (2023). Human Factor Report 2023. Sunnyvale, CA: Proofpoint Inc; s. 8–10.
37. Ruohonen, J. (2024). A systematic literature review on the NIS2 Directive. arXiv preprint arXiv:2412.08084; s. 7–8.
38. Wallis, T., & Dorey, P. (2024). Collaboration practices for the cybersecurity of supply chains to critical infrastructure. Applied Sciences, 14(13), 5805. https://doi.org/10.3390/app14135805; s. 3–4.