Dr hab. MBA, Kamil Mroczka
Uniwersytet Warszawski
e-mail: ks.mroczka@uw.edu.pl
ORCID: 0000-0003-3809-3479

Dr Michał Szczegielniak
Uniwersytet Warszawski
e-mail: m.szczegielniak@uw.edu.pl
ORCID: 0000-0003-2001-8622

Jakub Brzozowski
Uniwersytet Stefana Kardynała Wyszyńskiego
e-mail: jakubjmbrzozowski@gmail.com
ORCID: 0009-0002-8722-6303

KLUCZOWE PROBLEMY I WYZWANIA W ZAKRESIE BUDOWANIA ODPORNOŚCI CYFROWEJ I CYBERBEZPIECZEŃSTWA JEDNOSTEK SAMORZĄDU TERYTORIALNEGO W POLSCE – ANALIZA EMPIRYCZNA W ŚWIETLE WYNIKÓW KONTROLI[1]

Abstrakt

Zasadniczym celem artykułu jest analiza – na podstawie danych empirycznych zawartych w ustaleniach m.in. Najwyższej Izby Kontroli – poziomu cyberbezpieczeństwa i odporności cyfrowej jednostek samorządu terytorialnego w Polsce. Kwestie cyberbezpieczeństwa w ostatnich latach stały się obszarem intensywnych prac legislacyjnych zarówno na poziomie unijnym, jak i krajowym. Od 2018 r. uchwalono szereg przepisów, których celem jest zwiększanie poziomu cyberbezpieczeństwa w ujęciu państwa i jego instytucji. Legislacja obejmuje również inne segmenty kluczowe z perspektywy bezpieczeństwa takie jak rynek finansowy, czy podmioty tworzące infrastrukturę krytyczną.

Słowa kluczowe: Cyberbezpieczeństwo, odporność cyfrowa, samorząd terytorialny.

Wprowadzenie

We współczesnym świecie zarówno osoby fizyczne, jak i podmioty publiczne oraz prywatne coraz intensywniej wykorzystują technologie ICT. W przypadku administracji publicznej technologie te usprawniają funkcjonowanie urzędu, a także poprawiają wymianę informacji pomiędzy podmiotami publicznymi oraz komunikację na linii klient-urząd[2]. Jednakże, zdaniem Naukowej i Akademickiej Sieć Komputerowej (NASK) *wraz ze wzrostem popularności usług cyfrowych i pojawianiem się nowych technologii*

[1] Na potrzeby procesu konceptualizacji terminów badawczych wykorzystano wcześniejsze prace autorów.
[2] M. Szczegielniak, *Dostęp do informacji w administracji publicznej a rozwój partycypacji obywatelskiej w Polsce*, Warszawa 2025, s. 125.

rośnie także cyberprzestępczość, co jest wyraźnie widoczne w statystykach zespołów zajmujących się reagowaniem na incydenty bezpieczeństwa komputerowego. Dodatkowo sytuacja międzynarodowa sprawia, że systematycznie rośnie liczba ataków na instytucje publiczne. W takich okolicznościach ważne jest – jak nigdy przedtem – zadbanie o cyberbezpieczeństwo podmiotów świadczących usługi publiczne i przetwarzających dane obywateli[3]. W ocenie Katarzyny Chałubińska-Jentkiewicz oraz Agnieszki Brzostek *współcześnie cyberprzestrzeń (...) i jej ochrona stały się (...) elementem systemu ochrony bezpieczeństwa państwa i obronności*[4]. W konsekwencji ochrona systemów teleinformatycznych stanowi dziś nieodzowny elementem sprawnego funkcjonowania administracji publicznej, w tym również administracji samorządowej.

Hipotezą badawczą artykułu jest twierdzenie, że jednostki samorządu terytorialnego nie zapewniają odpowiedniego poziomu odporności cyfrowej i cyberbezpieczeństwa z uwagi na brak odpowiednich kompetencji i zasobów oraz niską świadomość ryzyk związanych z funkcjonowaniem cyberprzestrzeni i zagrożeń z tego wynikających, a także brakiem indywidualnej odpowiedzialności decydentów samorządowych za cyberbezpieczeństwo. W celu weryfikacji założonej hipotezy sformułowano następujące pytania badawcze: jak definiowane jest cyberbezpieczeństwo? Czym różni się cyberbezpieczeństwo od cyberodporności? Jakie są zadania administracji samorządowej w zakresie cyberbezpieczeństwa? Jak są one realizowane w świetle ustaleń kontroli NIK oraz badań empirycznych? Jakie są przyczyny nieprawidłowości? Jakie wyzwania wiążą się budowaniem odporności cyfrowej administracji samorządowej? Jakie zmiany organizacyjne i prawne należy wprowadzić, aby osiągnąć zakładane cele?

Na potrzeby prowadzonych rozważań zastosowano zarówno metody teoretyczne, jak i empiryczne. W ujęciu teoretycznym wykorzystano m.in. metodę dogmatyczno-prawną oraz analizę systemową, a w wymiarze empirycznym: analizę dokumentów źródłowych, danych ilościowych i jakościowych oraz obserwację uczestniczącą wynikającą z doświadczeń zawodowych autorów.

Konceptualizacja kluczowych terminów badawczych: cyberbezpieczeństwo, odporność cyfrowa i krajowy system cyberbezpieczeństwa

Cyberbezpieczeństwo

Pojęcie cyberbezpieczeństwa jest różnie definiowane przez teoretyków i praktyków. W słowniku Narodowych Standardów Cyberbezpieczeństwa termin ten definiowany jest jako „zapobieganie naruszeniom, ochrona i odtwarzanie systemów komputerowych, systemów łączności elektronicznej, usług łączności elektronicznej, łączności przewodowej i łączności elektronicznej, w tym informacji w nich zawartych, w celu zapewnienia ich dostępności,

[3] NASK, *Cyberbezpieczny samorząd. Poradnik*, Warszawa 2023, s. 16.
[4] K. Chałubińska-Jentkiewicz, A. Brzostek, *Wstęp*, [w:] Tychże (red.), *Modele rozwiązań prawnych w systemie cyberbezpieczeństwa RP. Rekomendacje*, Warszawa 2021, s. 5.

integralności, uwierzytelniania, poufności i niezaprzeczalności”[5]. Słownik Merriam Webster Dictionary określa cyberbezpieczeństwo jako „środki podjęte w celu ochrony komputera lub systemu komputerowego (na przykład w Internecie) przed nieautoryzowanym dostępem lub atakiem”[6]. Na podstawie przywołanych definicji możemy przyjąć, że cyberbezpieczeństwo obejmuje ochronę i gwarancję zabezpieczenia systemów komputerowych przed nieautoryzowanymi przypadkami ataków naruszeń, oszustw, czyli działań nielegalnych, ingerujących w integralność systemów informatycznych.

W doktrynie pojęcie cyberbezpieczeństwa analizowane jest z różnych perspektyw. Warto przytoczyć definicję zaproponowaną przez Roberta Siudaka, który interpretuje cyberbezpieczeństwo jako proces, który ma za zadanie „doprowadzenie do stanu, w którym możliwe niebezpieczeństwa nie przekraczają akceptowalnego poziomu ryzyka dla poszczególnych podmiotów bezpieczeństwa”[7]. Z kolei Cezary Banasiński podkreśla trudność interpretacyjną i nieostrość pojęcia cyberbezpieczeństwa (bezpieczeństwa w cyberprzestrzeni), co podkreśla jego złożoność i wieloaspektowy, niejednoznaczny charakter[8].

Trzecią kategorię definicji stanowią definicje legalne, zdefiniowane w przepisach prawa. W polskim systemie prawnym istnieje definicja cyberbezpieczeństwa wywodząca się z art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Przepis ten stanowi, że cyberbezpieczeństwo to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”[9]. W przywołanej definicji ustawodawca wymienia naruszenia konkretnych atrybutów, które wymagają szczególnej ochrony: poufność, integralność, dostępność i autentyczność.

Filip Radoniewicz wyjaśnia, że w kontekście ochrony systemów informacyjnych, poufnością określa się dostęp do danych tylko przez osoby do tego uprawnione[10]. Integralność z kolei oznacza dokładność i kompletność danych i informacji wraz z utrzymaniem ich w takim stanie[11]. Dostępność jest tym atrybutem, który związany jest z możliwością korzystania z informacji przez uprawnione osoby, ilekroć zajdzie taka potrzeba[12]. Na koniec autentyczność, jako atrybut pochodzący z katalogu innych atrybutów ujętych w normie PN-EN ISO/IEC 27001, definiowany jest w Rozporządzeniu Rady Ministrów z dnia 22 maja 2024 r. w sprawie Krajowych Ram

---

[5] *Narodowe Standardy Cyberbezpieczeństwa, Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa (wersja 1.0.), definicja pojęcia cyberbezpieczeństwo (cybersecurity),* [online], https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber, 21 IV 2025.
[6] *Merriam-Webster Dictionary,* [online] *https://www.merriam-webster.com/dictionary/cybersecurity, 21 IV 2025., tłumaczenie własne.*
[7] R. Siudak, *Cyberbezpieczeństwo w Polsce. Od dyskursów do polityk publicznych*, Kraków 2022, s. 280-281.
[8] C. Banasiński, *Pojęcie cyberbezpieczeństwa* [w:] *Cyberbezpieczeństwo. Zarys wykładu* red. C. Banasiński, Warszawa 2023, s. 31-37.
[9] *Ustawa o krajowym systemie cyberbezpieczeństwa*, Dz. U. 2018 poz. 1560, art. 2 pkt 4.
[10] F. Radoniewicz, *Objaśnienie pojęć* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, s. 31.
[11] *Tamże*.
[12] *Tamże*.

Interoperacyjności jako „właściwość polegającą na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie, jak deklarowane”[13].

Należy podkreślić, że krajowy ustawodawca konstruując definicję w przywołanej powyżej ustawie uwzględnił definicję wdrożoną w dyrektywie NIS[14]. Regulacja ta nie zawiera wprost pojęcia „cyberbezpieczeństwo”, lecz w art. 4 definiuje pojęcie „bezpieczeństwa sieci i systemów informatycznych” określając je jako „odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne”[15]. Już pobieżna analiza wskazuje, że definicja z dyrektywy NIS oraz ustawy z lipca 2018 r. są bardzo zbliżone.

Odporność cyfrowa

Termin „odporność cyfrowa” (lub „cyfrowa odporność”) jest terminem stosunkowo nowym zarówno w ujęciu krajowej doktryny, jak i systemu prawnego. Należy wobec tego odwołać się do źródeł zagranicznych. National Institute of Standards and Technology definiuje pojęcie odporności cyfrowej (*cyber resiliency*) jako „zdolność do przewidywania, wytrzymywania, odzyskiwania i dostosowywania się do niekorzystnych warunków, napięć, ataków lub naruszeń systemów, które wykorzystują lub są obsługiwane przez zasoby cybernetyczne”[16]. W doktrynie wskazuje się, że „odporność cyfrowa odnosi się do zdolności do nieprzerwanego osiągania zamierzonego celu pomimo niekorzystnych zdarzeń w cyberprzestrzeni”[17]. Podkreśla się przy tym, że zdolność do nieprzerwanego osiągania zamierzonego celu polega na zapewnieniu efektów i ciągłego funkcjonowania, pomimo występującego kryzysu lub naruszeniu bezpieczeństwa z jednoczesną zdolnością do przywrócenia regularnych mechanizmów i usprawnienia ich w celu prewencji[18].

W innej definicji odporność cyfrową definiowana jest jako „zdolność podmiotu do przeciwstawienia się incydentom, reagowaniu na nie i odzyskaniu sprawności po ich wystąpieniu w celu zapewnienia ciągłości operacyjnej podmiotu”[19]. W tym ujęciu podkreśla się, że odporność cyfrowa

---

[13] *Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności , minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*, Dz. U. z 2024 r. poz. 773, §2, pkt 2.

[14] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/ 1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*, Dz. U. UE L. z 2016 r. Nr 194.

[15] *Tamże,* art. 4, pkt 2.

[16] *NIST Glossary*, [online] https://csrc.nist.gov/glossary/term/cyber_resiliency, 18 IV 2025., tłumaczenie własne.

[17] F. Björck, M. Henkel, J. Stirna, J. Zdravkovic, *Cyber Resilience – Fundamentals for a Definition,* “New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing” 2015, vol. 353, s. 311-312, tłumaczenie własne.

[18] *Tamże*.

[19] K. Hausken, *Cyber resilience in firms, organizations and societies*, “Internet of Things” 2020, vol. 11, tłumaczenie własne.

obejmuje zarówno działania prewencyjne, ukierunkowane na zapewnienie silnych mechanizmów ochrony przed incydentami, jak i skuteczne zarządzanie kryzysowe w przypadku ich wystąpienia. Obejmuje to procedury reagowania na incydenty oraz procesy odbudowy i przywracania sprawności systemów po zaistniałym zagrożeniu.

Pojęcie odporności cyfrowej nie funkcjonuje na chwilę obecną w polskim porządku prawnym. Należy jednak odnotować, że jest ono wykorzystywane w prawie unijnym np. w rozporządzeniu DORA. Preambuła tego aktu prawnego kilkakrotnie odwołuje się do pojęcia „odporności cyfrowej", stosując ją naprzemiennie z określeniem bardziej szczegółowym, umocowanym w artykule 3 punkcie 1, czyli „operacyjnej odporności cyfrowej". Motywy zawarte w preambule odnoszące się do „odporności cyfrowej" nadają jej waloru ogólnego standardu, koniecznego do zapewnienia w sektorze finansowym. Definicja legalna zawarta w przytoczonym powyżej przepisie stanowi, że „operacyjna odporność cyfrowa" to „zdolność podmiotu finansowego do budowania, gwarantowania i weryfikowania swojej operacyjnej integralności i niezawodności przez zapewnianie, bezpośrednio albo pośrednio – korzystając z usług zewnętrznych dostawców usług ICT – pełnego zakresu możliwości w obszarze ICT niezbędnych do zapewnienia bezpieczeństwa sieci i systemów informatycznych, z których korzysta podmiot finansowy i które wspierają ciągłe świadczenie usług finansowych oraz ich jakość, w tym w trakcie zakłóceń"[20].

Choć przytoczona definicja została sformułowana na potrzeby sektora finansowego, zawiera elementy charakterystyczne również dla szerszego ujęcia tego pojęcia. Ustawodawca podkreśla, że operacyjna odporność cyfrowa jest to pewien proces – „zdolność do (...) budowania, gwarantowania i weryfikowania swojej operacyjnej integralności i niezawodności", a więc ustanowienia stałego, trwałego systemu zabezpieczeń. Ma on funkcjonować nieprzerwanie w warunkach standardowych, a jednocześnie gwarantować odpowiedni poziom jakości także w sytuacjach zakłóceń czy incydentów operacyjnych.

Krajowy system cyberbezpieczeństwa

Pojęcie krajowego systemu cyberbezpieczeństwa powstało dzięki polskiemu ustawodawcy, który dokonał transpozycji przepisów dyrektywy NIS do krajowego systemu prawnego. W wyniku tego działania uchwalono przywoływaną już ustawę z lipca 2018 r. Regulacja ta definiuje sposób działania krajowego systemy cyberbezpieczeństwa, zadania poszczególnych podmiotów tworzących ten system oraz reguluje system sankcji za nieprzestrzeganie przepisów.

W art. 3 ustawy zdefiniowano cel wprowadzenia rozwiązań systemowych. Przepis ten stanowi, że: „krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych

[20] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011*, art. 3 pkt. 1.

służących do świadczenia tych usług oraz zapewnienie obsługi incydentów”[21]. W przypadku zapewnienia cyberbezpieczeństwa na poziomie krajowym, ustawodawca miał przede wszystkim na celu ochronę wspominanych już atrybutów bezpieczeństwa informacji, według normy PN-EN ISO 27001, czyli poufność, integralność, dostępność oraz autentyczność[22]. Natomiast w przypadku obsługi incydentu, ustawodawca zakłada podjęcie czynności umożliwiających wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, a także podejmowanie działań naprawczych i ograniczenie skutków jego wystąpienia[23].

Jakub Dysarz zauważa, że polski ustawodawca zdecydował się rozszerzyć zakres regulacji o elementy bezpieczeństwa narodowego, na przykład w postaci współpracy CSIRT, elementy instytucjonalne, w postaci utworzenia Pełnomocnika Rządu ds. Cyberbezpieczeństwa, czy w końcu rozszerzył katalog sektorów gospodarki, którego obejmuje, w przeciwieństwie do minimalnego katalogu wyznaczonych sektorów z dyrektywy NIS[24]. Autor ten dodaje, że wszelkie dodatkowe regulacje wprowadzone przez polskiego ustawodawcę tworzy polski model systemu cyberbezpieczeństwa, który charakteryzuje się między innymi wskazaniem szczegółowych obowiązków operatora usług kluczowych, sposób wyboru operatorów w postaci decyzji administracyjnej, czy też rozdzielenie odpowiedzialności organów właściwych ds. cyberbezpieczeństwa według sektorów gospodarki i administracji rządowej[25].

Krajowy system cyberbezpieczeństwa zgodnie ze swoimi założeniami dedykowany jest konkretnym podmiotom wyznaczonym w katalogu zamkniętym określonym w artykule 4 ustawy. Tym samym obejmuje on m.in.. operatorów usług kluczowych, dostawców usług cyfrowych, CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa, czy też jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[26], w których skład w chodzą m.in. organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały, czy też jednostki samorządu terytorialnego oraz ich związki[27] i inne. Każdy z wymienionych podmiotów oraz inne, które nie zostały wymienione z nazwy zostały podzielone w ustawie na konkretne kategorie podmiotów ustawy. Wobec tego w ustawie mamy podział obowiązków i zadań dedykowanych oddzielnie dla różnych kategorii podmiotów, czyli kolejno: obowiązki operatorów usług kluczowych (rozdział 3), dostawców usług cyfrowych (rozdział 4), podmiotów publicznych (rozdział 5), zespołów CSIRT MON, CSIRT NASK, CSIRT GOV (rozdział 6), organów właściwych do spraw cyberbezpieczeństwa (rozdział 8), ministra właściwego do spraw informatyzacji

[21] *Ustawa o krajowym systemie cyberbezpieczeństwa*, Dz. U. 2018 poz. 1560, art. 3.
[22] J. Dysarz, *Art. 3 Cel krajowego systemu cyberbezpieczeństwa* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. A. Besiekierska, Warszawa 2019, s. 17.
[23] F. Radoniewicz, *Art. 3 Cel wdrożenia krajowego systemu cyberbezpieczeństwa* [w:] *Ustawa…*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, s. 52.
[24] J. Dysarz, *Implementacja dyrektywy NIS* [w:] *Ustawa…*, red. A. Besiekierska, s. 5.
[25] *Tamże*.
[26] *Ustawa o krajowym systemie cyberbezpieczeństwa*, art. 4 pkt. 1-7.
[27] *Ustawa o finansach publicznych*, Dz. U. 2009 Nr 157 poz. 1240, art. 9, pkt 1-2.

(rozdział 9), Ministra Obrony Narodowej (rozdział 10), oraz Pełnomocnika oraz Kolegium (rozdział 12)[28].

Tak zarysowany podział zadań tworzy podmiotowe ujęcie krajowego systemu cyberbezpieczeństwa. Implementuje bezpośrednio zapisy z dyrektywy NIS, która wprowadziła zasadę harmonizacji minimalnej[29], a którą polski ustawodawca rozszerzył o dodatkowe elementy, wprowadzając bardziej kompleksowy system. W tym miejscu należy również podkreślić, że z uwagi na uchwaloną przez unijnego ustawodawcę dyrektywę NIS2, która zastąpiła wspominaną dyrektywę NIS, polski ustawodawca zobligowany jest do transpozycji przepisów nowej dyrektywy do polskiego systemu prawnego. Na chwilę obecną prace nad transpozycją trwają w dalszym ciągu, pomimo przekroczenia terminu na implementację, który minął 17 października 2024 r., co skutkuje wszczętym postępowaniem przez Komisję Europejską przeciwko Polsce[30].

Zadania jednostek samorządu terytorialnego w krajowym systemie cyberbezpieczeństwa

Głównym aktem prawnym nakładającym na jednostki samorządu terytorialnego obowiązek utrzymania odpowiedniego poziomu bezpieczeństwa w sferze cyfrowej jest ustawa z lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[31]. Filip Radoniewicz podkreśla, że obejmuje ona m. in. gminy, powiaty, województwa, związki jednostek samorządu terytorialnego, związki metropolitalne oraz samorządowe zakłady budżetowe[32]. Obowiązki podmiotów publicznych realizujących zadania publiczne zostały określone w rozdziale piątym ustawy, przede wszystkim w art. 21-23.

W art. 21 ustawa nakłada obowiązek wyznaczenia osoby odpowiedzialnej za utrzymanie kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa. Ustawodawca nie precyzuje dokładnie jakie kompetencje musi posiadać taka osoba, ani nie precyzuje szczegółów jakie musi spełniać taka jednostka kontaktowa, jak również nie jest powiedziane, że wyznaczona musi być osobą fizyczną, jednakże, z praktycznego punktu widzenia, jednostki takie wyznaczają właśnie osoby fizyczne o właściwych kompetencjach[33]. Do zadań takiej osoby należy obowiązek kontaktu z właściwym CSIRT, w formie założenia „punktu kontaktowego", w terminie 14 dni od dnia wyznaczenia takiej osoby, przedstawiając konkretne dane wymienione w artykule 22 ust. 1 pkt 5 ustawy[34]. Warto zaznaczyć, że dla

[28] *Ustawa o krajowym systemie cyberbezpieczeństwa*.
[29] C. Banasiński, W. Nowak, *Dyrektywa NIS* [w:] *Cyberbezpieczeństwo, zarys...,* red. C. Banasiński, s. 180.
[30] CyberDefence24, *Dwa postępowania KE przeciwko Polsce. Chodzi o dyrektywę NIS2*, 28 XI 2024, [online] https://cyberdefence24.pl/polityka-i-prawo/dwa-postepowania-ke-przeciwko-polsce-chodzi-o-dyrektywe-nis2, data wejścia: 21 IV 2025.
[31] *Ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa* (t.j. Dz. U. z 2024 r. poz. 1077, 1222).
[32] F. Radoniewicz, *Zakres podmiotowy* [w:], W. Kitler, Tenże, J. Taczkowska-Olszewska, *Ustawa o krajowym...,* s. 58-59.
[33] W. Dziomdziora, *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Warszawa 2021, s. 31.
[34] *Ustawa o krajowym systemie cyberbezpieczeństwa*, Dz. U. 2018 poz. 1560, art. 22, ust. 1, pkt 5.

jednostek samorządu terytorialnego wyznacza się tylko jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jej jednostki organizacyjne[35]. Informację o wyznaczeniu osoby kontaktowej dla jednostki samorządu terytorialnego przekazuje się do CSRIT NASK, który jest właściwy w przypadku jednostek samorządu terytorialnego, z wyjątkiem przypadku wynikającego z art. 27 ustawy, czyli w zakresie incydentów związanych ze zdarzeniami o charakterze terrorystycznym, na adres ksc@cert.pl, przedstawiając niezbędne dane wynikające z ustawy[36].

Zgodnie z art. 22 ustawy jednostki samorządu terytorialnego „są zobowiązane do zapewnienia zarządzania incydentami w podmiocie publicznym"[37]. Zdaniem Kamila Czaplickiego jest to „czynność wewnętrzna podmiotu publicznego"[38]. Jednostki samorządu terytorialnego są zobowiązane do dokonywania zgłoszeń incydentów, obsługi incydentów, wraz z incydentami krytycznymi, zestawiania właściwych danych o incydentach dla odpowiedniego CSRIT, czy też dzielenia się wiedzę dotyczącą incydentów dla właściwych jednostek, w celu zrozumienia cyberzagrożeń[39]. Należy także zaznaczyć, że zarządzanie incydentami nie ogranicza się jedynie do wymiany informacji, ale zakłada również podejmowanie działań mających na celu przywrócenie pełnej sprawności systemu informacyjnego do realizacji zadania publicznego, co następuje po usunięciu przyczyn zakłócających jego prawidłowe działanie[40].

W doktrynie podkreśla się, że jednostki samorządu terytorialnego powinny również „umieć zaimplementować procedury i narzędzia chroniące podmiot publiczny w przyszłości przed zaistnieniem analogicznego incydentu" oraz dokumentować wszystkie incydenty, które miały miejsce w przeszłości[41]. Ponadto, jak zauważył Krzysztof Wąsowski, „na wypełnienie obowiązku przekazania podstawowych danych osoby odpowiedzialnej jest aż 14 dni od dnia [jej – przyp. autorów] wyznaczenia (...). Przy dzisiejszym postępie technologicznym i konieczności szybkiego (w zasadzie natychmiastowego) reagowania na incydenty aż tak szeroka przestrzeń czasowa wydaje się zbyt szeroka"[42].

Zgłoszenie incydentów dokonuje się zgodnie z wytycznymi przedstawionymi w art. 23 ustawy. Obowiązek obejmuje przekazanie następujących informacji: danych podmiotu zgłaszającego, danych osoby składającej zgłoszenie, danych osoby uprawnionej do składania wyjaśnień,

---

[35] *Tamże*, art. 21, ust. 3.
[36] W. Dziomdziora, *Cyberbezpieczeństwo...*, s. 35.
[37] A. Besiekierska [w:] Tejże (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, s. 107.
[38] K. Czaplicki, *Obowiązki w zakresie zgłaszania i obsługi incydentu w podmiocie publicznym* [w:] G. Szpor, A. Gryszczyńska, Tenże (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019, s. 199.
[39] *Ustawa o krajowym...,* art. 22 ust. 1.
[40] Por. K. Czaplicki, *Obowiązki w zakresie zgłaszania...*, s. 199.
[41] *Tamże.*
[42] K. Wąsowski, *Zakres obowiązków podmiotu publicznego* [w:], W. Kitler, Tenże, J. Taczkowska-Olszewska, *Ustawa o krajowych systemie cyberbezpieczeństwa. Komentarz*, s. 187-188.

opisu wpływu incydentu na realizowane zadanie publiczne oraz informacje o przyczynie i źródle incydentu, a także podjętych działaniach zapobiegawczych i naprawczych[43]. Nie jest to katalog zamknięty bowiem jednostka samorządu terytorialnego powinna przekazać do właściwego CSIRT inne istotne informacje, które mają znaczenie dla sprawy[44], przykładowo Krzysztof Wąsowski uważa, że „opis incydentu winien zawierać opis zadania publicznego, który powinien być powiązany, ze wskazaniem podstaw prawnych realizacji takiego zadnia[45]. Dodatkowo ustawodawca wprowadził także obowiązek bieżącego, permanentnego uzupełniania informacji w zgłoszeniu"[46].

W art. 24 zdefiniowano zasady przekazywania informacji przez jednostkę samorządu terytorialnego do właściwego CSIRT. Cytowany już Kamil Czaplicki podkreśla, że „w przeciwieństwie do obowiązków wskazanych w art. 22 i 23, uprawnienie z art. 24 nie dotyczy zaistniałego w podmiocie publicznym incydentu a wczesnego ostrzegania właściwych CSIRT o możliwych zagrożeniach w przyszłości[47]. Sama procedura przekazania informacji nie została w zasadzie sformalizowana"[48], wiadomo tylko że powinny one zostać przekazane w postaci elektronicznej[49] jeżeli jest to możliwe. Co prawda „do informacji nie mają zastosowania przepisy dotyczące terminów"[50], jednakże zważywszy na cel przedmiotowego przepisu powinny one zostać przekazane bez zbędnej zwłoki, „aby umożliwić CSIRT odpowiednią reakcję"[51]. Warto również podkreślić, że zgodnie z art. 25 wobec podmiotu publicznego może zostać również wydana decyzja o uznaniu tego podmiotu za operatora usługi kluczowej co nakłada na niego dodatkowe obowiązki określone w art. 8-16 ustawy[52].

Podmioty wykonujące zadania publiczne są również zobowiązane do korzystania z systemów teleinformatycznych spełniających minimalne wymagania oraz zapewniających interoperacyjność, zgodnie z zasadami określonymi w Krajowych Ramach Interoperacyjności[53]. Oznacza to, że wykorzystywane przez jednostki samorządu terytorialnego systemy teleinformatyczne oraz prowadzone przez nie publiczne rejestry danych muszą spełnić odpowiednie wymagania techniczne określone w Rozporządzeniu Rady Ministrów w sprawie Krajowych Ram Interoperacyjności[54]. Nakłada ono m. in.

---

[43] *Ustawa o krajowym…* , art. 25.
[44] *Tamże,* art. 25 ust. 1 pkt 8.
[45] K. Wąsowski, *Zgłoszenie incydentu w podmiocie publicznym* [w:], W. Kitler, Tenże, J. Taczkowska-Olszewska, *Ustawa o krajowych systemie cyberbezpieczeństwa. Komentarz*, s. 189.
[46] *Tamże.*
[47] K. Czaplicki, dz. cyt., s. 214.
[48] K. Wąsowski, *Obowiązek przekazywania informacji* [w:], W. Kitler, Tenże, J. Taczkowska-Olszewska, *Ustawa o krajowych systemie cyberbezpieczeństwa. Komentarz,* s. 191.
[49] *Ustawa o krajowym…,* art. 24.
[50] K. Czaplicki, dz. cyt., s. 214.
[51] *Tamże.*
[52] NASK, *Cyberbezpieczny samorząd. Poradnik,* s. 19.
[53] *Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* (t.j. Dz. U. z 2024 r. poz. 1557, 1717), art. 13. ust. 1.
[54] *Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności , minimalnych wymagań dla rejestrów publicznych i wymiany informacji w*

obowiązek zapewnienia odpowiednich standardów dotyczących bezpieczeństwa, dostępności oraz integralności danych, a także stosowania uzgodnionych standardów komunikacji, które pozwalają na współpracę z systemami innych instytucji publicznych.

Należy również pamiętać, że specyfika działania jednostek samorządu terytorialnego sprawia, że należy je uznać za administratora danych w rozumieniu RODO[55]. Nakłada to na nie obowiązek przeprowadzenia analizy ryzyka i wdrażania środków technicznych i organizacyjnych, które owo ryzyko minimalizują[56]. Oznacza to, że jednostki te muszą nieustannie chronić systemy teleinformatyczne przed zagrożeniami, zapewniać integralność, poufność i dostępność danych, a także wdrażać procedury zarządzania incydentami, mechanizmy kontroli dostępu oraz regularne szkolenia dla pracowników w zakresie bezpiecznego przetwarzania informacji zawierających dane osobowe.

Stan cyberbezpieczeństwa w samorządzie terytorialnym w wynikach kontroli NIK oraz badaniach empirycznych

W kwietniu 2025 r. prezes NIK opublikował informację o wynikach kontroli „Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego”[57]. Celem kontroli było zweryfikowanie, czy wybrane w próbce kontrolnej jednostki samorządu terytorialnego „prawidłowo, rzetelnie i skutecznie realizowały zadania związane z zapewnieniem bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych”. Próba kontrolna obejmowała 24 jednostki – 17 gmin, 7 powiatów. Kontrolę realizowano od stycznia 2023 r. do września 2024 r.[58].

Od strony metodycznej kontrolerzy sformułowali trzy pytania definiujące cele szczegółowe kontroli: (1) Czy podjęto prawidłowe, rzetelne i skuteczne działania dla zapewnienia organizacji bezpieczeństwa informacji oraz dla zapewnienia ciągłości działania systemów informatycznych, tj. czy przeprowadzono odpowiednie analizy oraz czy opracowano i przyjęto do stosowania odpowiednie procedury, polityki, instrukcje oraz określono i zapewniono niezbędne zasoby osobowe i techniczne? (2) Czy prawidłowo, rzetelnie i skutecznie wdrożono przyjęte rozwiązania organizacyjne i techniczne, tj. czy są one faktycznie stosowane i egzekwowane? (3) Czy są cyklicznie podejmowane prawidłowe działania mające na celu zapobieganie

postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773).

[55] NASK, *Cyberbezpieczny samorząd. Poradnik,* s. 17.

[56] *Rozporządzenie Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (Dz. U. UE z 2016 r. L 119/1), art. 24 i 25.

[57] *Informacja o wynikach kontroli „Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego”,* Nr ewidencyjny: P/24/004, Najwyższa Izba Kontroli, Warszawa, luty 2025 r.

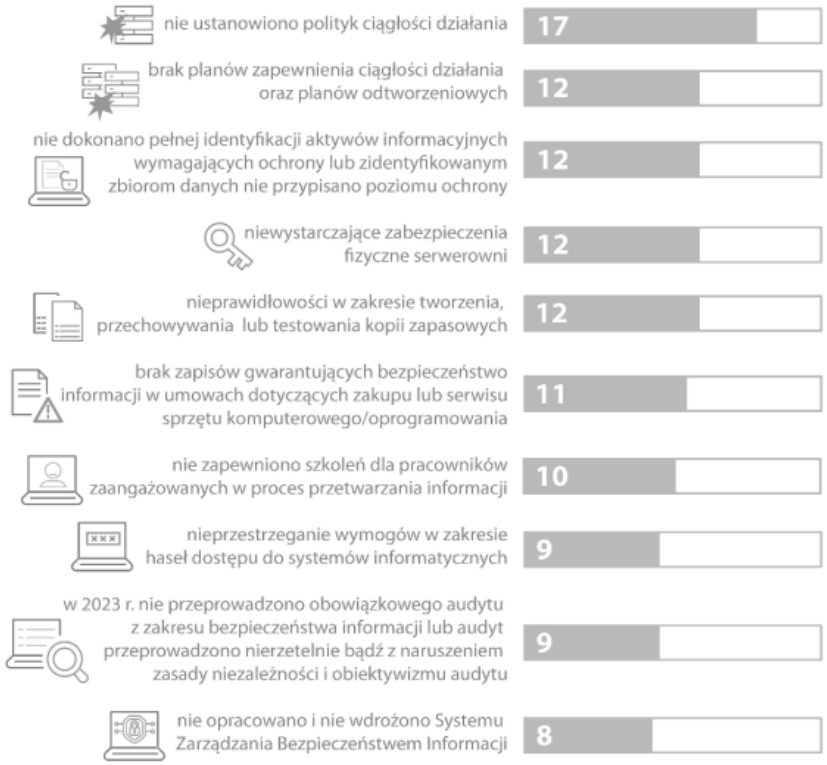
[58] *Cyberbezpieczeństwo w samorządach kuleje,* Najwyższa Izba Kontroli 2025, 17 IV, [online] https://www.nik.gov.pl/aktualnosci/cyberbezpieczenstwo-w-samorzadach-2025.html, 20 IV 2025.

incydentom bezpieczeństwa informacji (szkolenia, analiza incydentów, audyty, analiza ryzyka)?

Generalny wniosek płynący z ustaleń kontroli mówi, że „zadania w zakresie zapewnienia bezpieczeństwa informacji nie były skutecznie, rzetelnie i prawidłowo wykonywane w większości skontrolowanych urzędów jednostek samorządu terytorialnego". Na podstawie powyższego Izba negatywnie oceniła przygotowanie do zapewnienia ciągłości działania systemów informatycznych w 71% kontrolowanych urzędów. Istotne nieprawidłowości stwierdzono w 23 z 24 badanych jednostek, a w przypadku dwóch sformułowano negatywną ocenę ogólną[59].

Katalog najczęściej występujących nieprawidłowości w kontrolowanych podmiotach prezentuje poniższa grafika.

Grafika 1. Najczęściej stwierdzane nieprawidłowości w 24 kontrolowanych podmiotach



Źródło: *Informacja o wynikach kontroli „Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego",* Nr ewidencyjny: P/24/004, Najwyższa Izba Kontroli, Warszawa, luty 2025 r., s. 12.

Z powyższych informacji wynika, że w ponad 70% badanych jednostek nie ustanowiono polityk ciągłości działania, kluczowych dokumentów z perspektywy zarządzania ryzykiem w przypadku wystąpienia sytuacji kryzysowej. Brak polityk ciągłości działania należy analizować łącznie z kolejną stwierdzoną nieprawidłowością polegającą na braku planów zapewnienia ciągłości działania oraz planów odtworzeniowych.

[59] *Informacja o wynikach kontroli „Zapewnienie bezpieczeństwa informacji…,* s. 8.

Nieprawidłowość taką stwierdzono w połowie badanych jednostek. Warto w tym miejscu przywołać wyjaśnienia składane przez wybrane jednostki poddane kontroli. Przykładowo Starostwo Powiatowe w Sochaczewie wskazało, że plany zapewnienia ciągłości i plany odtworzeniowe nie zostały sporządzone w formie pisemnej. Nie przeprowadzono również testów. Stwierdzono, że „taki stan rzeczy jest wynikiem posiadania sprzętu jaki można do takiej symulacji wykorzystać, brak urządzeń zapasowych o parametrach takich samych jak posiadane lub lepszych". W dalszej części wyjaśnień podkreślono, że „akceptowalny czas przywrócenia ciągłości działania systemów informatycznych nie został określony w sposób dokładny z powodu braku możliwości przetestowania takiej sytuacji, z uwagi na brak sprzętu zapasowego. W przybliżeniu takie działanie zajęłoby ok. 24 h w momencie posiadania identycznego lub lepszego sprzętu jaki jest obecnie na wyposażeniu Urzędu"[60].

W połowie badanych jednostek samorządu terytorialnego nie dokonano pełnej identyfikacji aktywów informacyjnych wymagających ochrony lub zidentyfikowanym zbiorom danych nie przypisano odpowiedniego poziomu ochrony. Jak ustalili kontrolerzy NIK, w procesie identyfikacji „pomijano na ogół informacje wymagające ochrony – inne niż dane osobowe, takie jak powierzone przez kontrahentów tajemnice przedsiębiorstwa, zasady bezpieczeństwa fizycznego i informatycznego w jednostce, informacje finansowe z deklaracji podatkowych itp."[61]. Wicestarosta Ostrołęcki wyjaśniając przyczyny nieprawidłowości stwierdził, że wynikały one z braków kadrowych i finansowych na zadania związane z zapewnieniem bezpieczeństwa informacji.

Z raportu NIK wynika również, że wdrażane w kontrolowanych podmiotach rozwiązania w zakresie bezpieczeństwa informacji nie zawsze były właściwie stosowane i egzekwowane. Część ustaleń kontrolerów w tym zakresie jest szokująca. W 20 kontrolowanych jednostkach (83%) stwierdzono nieprawidłowości w zakresie: zabezpieczenia serwerowni, sporządzania kopii zapasowych, braku w umowach na zakup usług IT lub serwis sprzętu/oprogramowania odpowiednich zapisów w zakresie bezpieczeństwa informacji, co stanowiło naruszenie obowiązków wynikających z przepisów rozporządzenia KRI. Kontrola stwierdziła również, że ok. 5% pracowników objętych badaniem wykonujących zadania w systemach informatycznych miało możliwość zainstalowania na użytkowanych komputerach dowolnego oprogramowania. W jednym z urzędów wszyscy badani użytkownicy systemów informatycznych niebędący pracownikami służb informatycznych posiadali uprawnienia administratora systemu na używanych przez nich komputerach, w związku z czym mogli samodzielnie instalować dowolne oprogramowanie[62].

NIK zbadał również proces blokowania lub odbierania dostępu do systemów informatycznych na próbie 240 osób, które zakończyły zatrudnienie w kontrolowanych urzędach. W wyniku badania stwierdzono, że 52 byłym pracownikom (tj. 22 %) 15 urzędów konta nie zostały zablokowane i pozostawały wciąż aktywne. W tym kontekście należy również przywołać następujące ustalenie NIK. Jak stwierdzono w kontroli, jedynie w trzech

[60] *Tamże,* s. 22.
[61] *Tamże,* s. 14.
[62] *Tamże,* s. 23-24.

urzędach wprowadzono rozwiązania techniczne umożliwiające monitorowanie oprogramowania wykorzystywanego na telefonach służbowych/tabletach. Kontrolerzy słusznie podkreślili, że oprogramowanie instalowane na urządzeniach mobilnych (telefony służbowe/tablety) nie powinno pozostawać poza nadzorem. Każda organizacja powinna wdrożyć rozwiązania techniczne do monitorowania oprogramowania na tych urządzeniach.

W ostatnich latach legislator unijny oraz krajowy podejmował działania mające na celu porządkowanie relacji z zewnętrznymi dostawcami usług ICT. Przykładem takiej regulacji dedykowanej dla rynku finansowego jest rozporządzenie DORA, które obowiązuje od 17 stycznia 2025 r.[63]. Z tymi inicjatywami mocno kontrastują ustalenia NIK w kontekście rzeczywistości funkcjonowania administracji samorządowej. Jak stwierdzono w wystąpieniu pokontrolnym, w 11 urzędach (46%) w umowach na zakup usług informatycznych, zakup lub serwis sprzętu komputerowego/oprogramowania stwierdzono brak zapisów gwarantujących zabezpieczenie poufności informacji uzyskanych przez wykonawców w związku z realizacją tych umów. Na 101 zbadanych umów, w 30 z nich nie zawarto takich zapisów. Działanie to istotnie obniża poziom bezpieczeństwa jednostek samorządowych. Zabezpieczenie interesów jednostki samorządowej na poziomie umowy na zakup usług informatycznych lub oprogramowania jest fundamentem budowania cyfrowej odporności zarówno w ujęciu jednostkowym, jak i systemowym.

NIK w trakcie kontroli stwierdziła również istotne nieprawidłowości w zakresie tworzenia, przechowywania lub testowania kopii zapasowych. W połowie kontrolowanych urzędów stwierdzono nieprawidłowości polegające na niespełnieniu wymogów stypizowanych w §19 ust. 2 pkt 12 lit. b rozporządzenia KRI. Polegały one m.in. na:

- niewłaściwym przechowywaniu kopii zapasowych danych z systemów informatycznych, tj. w sposób, który nie minimalizuje ryzyka utraty informacji i stwarza zagrożenie, że w przypadku zdarzeń losowych, np. pożaru lub zalania, urząd może utracić zarówno dane źródłowe, jak i ich kopie zapasowe. W siedmiu urzędach (29%) stwierdzono, że sporządzane kopie zapasowe przechowywane były w serwerowniach, a więc w miejscach wytwarzania danych lub w innym miejscu do którego dostęp miały osoby nieupoważnione. Kopie zapasowe powinny być przechowywane w innej lokalizacji, w odległości pozwalającej uniknąć uszkodzeń spowodowanych katastrofą, która dotknęła ośrodek podstawowy;
- niesporządzaniu kopii zapasowych lub tworzeniu ich niezgodnie z przyjętymi procedurami – w trzech urzędach; oraz
- braku testowania kopii zapasowych w sześciu urzędach[64].

Istotne – zdaniem autorów – są również nieprawidłowości stwierdzone przez NIK w wymiarze szkoleń i podnoszenia kwalifikacji pracowników. W 10 urzędach (42 %) nie zapewniono szkoleń dla pracowników zaangażowanych w

[63] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011*, Dz. U. UE. L. z 2022 r. Nr 333, str. 1 z późn. zm.

[64] *Informacja o wynikach kontroli „Zapewnienie bezpieczeństwa informacji…,* s. 11.

proces przetwarzania informacji, co było niezgodne z § 19 ust. 2 pkt 6 obowiązującego rozporządzenia KRI.

Po kontroli Izba sformułowała kilka wniosków. Pierwszy skierowany do Ministra Cyfryzacji dotyczył konieczności wspierania przez administrację rządową jednostek samorządu terytorialnego w zakresie wdrażania rozwiązań organizacyjnych i technicznych dotyczących bezpieczeństwa informacji oraz zapewnienia ciągłości działania urzędów. W odpowiedzi na wniosek Prezesa NIK, Minister Cyfryzacji wskazał, że „konsekwentnie buduje i rozwija krajowy system cyberbezpieczeństwa, aby zapewnić ochronę cyberprzestrzeni RP na właściwym poziomie", a „zapewnienie cyberbezpieczeństwa jest jednym z głównych priorytetów ministra cyfryzacji"[65].

Do wójtów, burmistrzów, prezydentów miast i starostów zaadresowano łącznie 12 wniosków. Dotyczyły one:

1) opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z § 19 ust. 1 w związku z ust. 3 obowiązującego rozporządzenia KRI;
2) zapewnienia dokonywania okresowego przeglądu i aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z § 19 ust. 2 pkt 1 obowiązującego rozporządzenia KRI;
3) ustanowienia polityk ciągłości działania oraz opracowanie i wdrożenie planów zapewnienia ciągłości działania urzędów, planów odtworzeniowych oraz zapewnienie ich okresowego testowania;
4) zapewnienia pracownikom zaangażowanym w proces przetwarzania informacji odpowiednich szkoleń w tym zakresie, zgodnie z § 19 ust. 2 pkt 6 obowiązującego rozporządzenia KRI;
5) prowadzenia okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, zgodnie z § 19 ust. 2 pkt 3 obowiązującego rozporządzenia KRI;
6) wdrożenia rozwiązań zapewniających odpowiednie zabezpieczenie pomieszczeń serwerowni, zgodnie z § 19 ust. 2 pkt 9 obowiązującego rozporządzenia KRI;
7) regularnego testowania kopii zapasowych oraz przechowywanie ich poza miejscem wytworzenia;
8) zapewnienia prowadzenia przynajmniej raz w roku okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji, zgodnie z § 19 ust. 2 pkt 14 obowiązującego rozporządzenia KRI;
9) przyznawania i odbierania pracownikom urzędów uprawnień w systemach informatycznych adekwatnie do realizowanych zadań, zgodnie z § 19 ust. 2 pkt 4 obowiązującego rozporządzenia KRI;
10) egzekwowania wdrożonych rozwiązań organizacyjnych i technicznych w zakresie bezpieczeństwa informacji;
11) zawierania w umowach o świadczenie usług informatycznych postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji, zgodnie z § 19 ust. 2 pkt 10 obowiązującego rozporządzenia KRI;
12) objęcia nadzorem oprogramowania instalowanego na urządzeniach mobilnych (komórkowe telefony służbowe/tablety).

[65] Pismo Ministra Cyfryzacji do Prezesa Najwyższej Izby Kontroli, syng.: BM.WN.0810.8.2025, Warszawa, 12 marca 2025 r.

Wnioski NIK należy ocenić jako w pełni uzasadnione i niezbędne do zwiększenia poziomu odporności cyfrowej administracji samorządowej. Autorzy mają jednak wątpliwość, czy jednostki samorządu terytorialnego dysponują odpowiednimi zasobami aby je właściwie zaadresować. W tym kontekście należy przywołać wcześniejsze ustalenia NIK. W latach 2014[66], 2016[67] i 2017[68] Izba przeprowadziła łącznie trzy kontrole dotyczące zarządzania bezpieczeństwem informacji w urzędach administracji publicznej[69]. W wyniku kontroli z 2017 r. NIK negatywnie oceniła wykonywanie przez blisko 70% skontrolowanych urzędów jednostek samorządu terytorialnego zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji w okresie objętym kontrolą. Kontrolerzy stwierdzili wprost, że brak jest systemowego podejścia do zapewnienia bezpieczeństwa informacji w jednostkach samorządu terytorialnego. W wyniku kontroli sformułowano szereg wniosków. Istotna ich część – jak wynika z najnowszych ustaleń – nie została właściwie zaadresowana przez decydentów samorządowych. W tym wymiarze trudno zakładać, że w przyszłości stan ten ulegnie znaczącej poprawie.

Ustalenia Najwyższej Izby Kontroli z 2024 r., wynikające z kontroli przeprowadzonej w gminach województwa zachodniopomorskiego[70], ujawniają poważne uchybienia, które jednoznacznie podważają skuteczność i adekwatność mechanizmów zarządzania oraz nadzoru w jednostkach samorządu terytorialnego w zakresie cyberbezpieczeństwa[71]. W wystąpieniu pokontrolnym jednoznacznie wskazano, że „wieloletnie zaniedbania dotyczące cyberbezpieczeństwa, nieświadomość i brak skutecznych procedur reagowania na zagrożenia, a także wykorzystywanie oprogramowania, które miało krytyczne luki – to główne nieprawidłowości wykryte w urzędach gmin w województwie zachodniopomorskim. W konsekwencji samorządy te nie były w stanie zapewnić skutecznej ochrony przed potencjalnymi atakami cyberprzestępców”[72].

We wszystkich objętych kontrolą jednostkach stwierdzono poważne nieprawidłowości w zakresie zapewnienia bezpieczeństwa systemów teleinformatycznych. Wyniki kontroli ujawniły wieloletnie zaniedbania

---

[66] *Informacja o wynikach kontroli NIK „Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu”,* Nr ewidencyjny: 205/2014/P/14/004/KAP, Najwyższa Izba Kontroli, Warszawa, 2 lutego 2015 r.

[67] *Informacja o wynikach kontroli NIK „System rejestrów państwowych – bezpieczeństwo, funkcjonowanie i użyteczność”,* Nr ewidencyjny: 208/2016/P/16/006/KAP, Najwyższa Izba Kontroli, Warszawa, 27 lutego 2017 r.

[68] *Informacja o wynikach kontroli NIK „Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego”,* Nr ewidencyjny: 187/2018/P/18/006/KAP, Najwyższa Izba Kontroli, Warszawa, 18 lutego 2019 r.

[69] A. Chodakowska, S. Kańduła, J. Przybylska, *Jak polskie gminy radzą sobie z cyberbezpieczeństwem,* „Kontrola Państwowa” 2022, nr 1, s. 135.

[70] *Informacja o wynikach kontroli „Zapewnienie bezpieczeństwa teleinformatycznego przez jednostki samorządu terytorialnego województwa zachodniopomorskiego*”, Nr ewidencyjny: I/23/001/LSZ, Najwyższa Izba Kontroli, Warszawa, 3 kwietnia 2024 r.

[71] *Zachodniopomorskie gminy nieprzygotowane na cyberzagrożenia,* Najwyższa Izba Kontroli, 2024, 3 IV, [online] https://www.nik.gov.pl/aktualnosci/zachodniopomorskie-gminy-cyberzagrozenia.html 21 IV 2025.

[72] *Tamże.*

odnoszące się do obszaru cyberbezpieczeństwa, stanu infrastruktury IT, poziomu kompetencji cyfrowych pracowników oraz brak systematycznych szkoleń. Dodatkowo odnotowano wykorzystywanie przestarzałego bądź nieprawidłowo skonfigurowanego oprogramowania. W rezultacie jednostki samorządu terytorialnego pozostawały w wysokim stopniu narażone na zagrożenia o charakterze cybernetycznym i nie dysponowały odpowiednimi mechanizmami obronnymi. Pomimo opracowania dokumentacji w zakresie cyberbezpieczeństwa, w tym Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w żadnym z analizowanych przypadków nie spełniała ona w pełni wymogów określonych w obowiązujących przepisach prawa[73].

Blisko połowa skontrolowanych urzędów nie opracowała procedur umożliwiających odtworzenie utraconych zasobów w przypadku incydentu o charakterze cybernetycznym. W jednym z przypadków, mimo formalnego istnienia procedury, nie przeprowadzono żadnych testów weryfikujących jej skuteczność. Choć większość jednostek tworzyła kopie zapasowe danych, działania te nie były objęte systematyczną weryfikacją pod względem ich kompletności ani rzeczywistej możliwości przywrócenia informacji. W jednej z jednostek ujawniono poważny błąd konfiguracyjny, który skutkowałby automatycznym zawirusowaniem kopii zapasowej w przypadku infekcji głównego serwera. W innym urzędzie, pomimo posiadania dedykowanego oprogramowania zabezpieczającego, nieprawidłowa konfiguracja uniemożliwiała skuteczną ochronę systemu[74].

Dodatkowo w żadnym z badanych urzędów nie funkcjonowało formalnie zinwentaryzowane środowisko informatyczne, co znacząco utrudniało zarządzanie infrastrukturą IT. W połowie przypadków wykorzystywano nieaktualne oprogramowanie, zawierające luki umożliwiające zdalne przejęcie kontroli nad systemami informatycznymi przez osoby nieuprawnione. Kontrola Najwyższej Izby Kontroli wykazała również, że niektóre urzędy korzystały z usług chmurowych bez uprzedniego określenia zasad korzystania z tych rozwiązań oraz bez wdrożenia mechanizmów nadzoru i kontroli nad przetwarzaniem danych w środowisku chmurowym[75].

Z przeprowadzonej kontroli wynika, iż nie we wszystkich jednostkach samorządu terytorialnego zapewniono serwerom wymaganą ochronę fizyczną. W jednym z przypadków ujawniono, że serwer został umieszczony w otwartej szafie znajdującej się w przejściowym pomieszczeniu biurowym, wykorzystywanym przez pracownika urzędu (*vide* grafika 21). Takie usytuowanie infrastruktury kluczowej dla funkcjonowania systemów informatycznych nie tylko nie spełnia podstawowych standardów bezpieczeństwa fizycznego, lecz także naraża zasoby cyfrowe na potencjalny dostęp osób nieuprawnionych oraz ryzyko przypadkowego uszkodzenia.

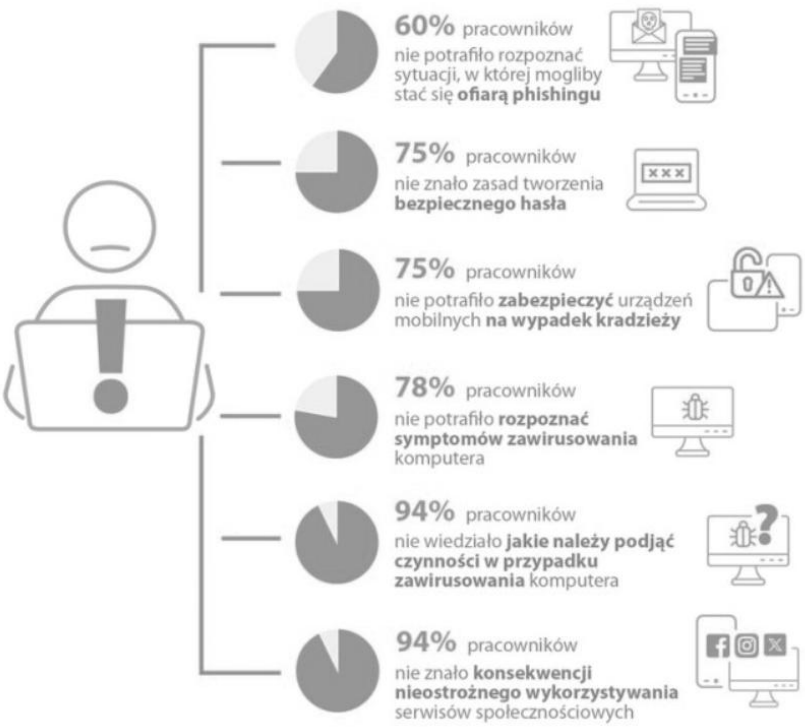
Grafika 2. Zabezpieczenie fizyczne serwerowni w jednym z urzędów samorządowych województwa zachodniopomorskiego

[73] *Tamże.*
[74] *Tamże.*
[75] *Tamże.*

Źródło: *Zachodniopomorskie gminy nieprzygotowane na cyberzagrożenia,* Najwyższa Izba Kontroli, 2024, 3 IV, [online] https://www.nik.gov.pl/aktualnosci/zachodniopomorskie-gminy-cyberzagrozenia.html 21 IV 2025.

Dodatkowo ustalono, iż w żadnej z objętych kontrolą jednostek samorządu terytorialnego nie przeprowadzono szkoleń z zakresu cyberbezpieczeństwa, adekwatnych do pełnionych przez pracowników funkcji oraz poziomu zagrożeń. Wyniki przeprowadzonego testu wiedzy jednoznacznie potwierdziły niedostateczny poziom kompetencji cyfrowych wśród personelu, co znacząco zwiększa ryzyko błędów ludzkich stanowiących potencjalny wektor ataku (*vide* grafika 3).

Grafika 3. Wyniki testu wiedzy pracowników samorządowych z zakresu cyberbezpieczeństwa



Źródło: *Zachodniopomorskie gminy nieprzygotowane na cyberzagrożenia,* Najwyższa Izba Kontroli, 2024, 3 IV, [online] https://www.nik.gov.pl/aktualnosci/zachodniopomorskie-gminy-cyberzagrozenia.html 21 IV 2025.

Zdaniem NIK, stwierdzone w trakcie kontroli istotne nieprawidłowości mogły skutkować przede wszystkim:

1) trwałą utratą danych (w tym danych osobowych obywateli) lub ich udostępnianiem osobom nieuprawnionym;
2) ujawnieniem poufnych informacji lub uprawnień do innych systemów (np. bankowych);
3) wgraniem przez cyberprzestępców oprogramowania, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych, w celu wyłudzenia środków finansowych (tzw. ransomware);
4) zakłóceniami w świadczeniu usług publicznych dla obywateli;
5) wykorzystaniem luk istniejących w systemach, w tym włączeniem komputerów do sieci typu „botnet", która może być wykorzystywana do działań przestępczych sterowanych z zewnątrz;
6) brakiem możliwości wychwytywania incydentów, a także brakiem reakcji w przypadku ich wystąpienia (np. nielegalne lub podatne na atak oprogramowanie).

Cyberbezpieczeństwo w świetle wyników badań empirycznych

O tym, że administracja samorządowa nie radzi sobie z zadaniami z zakresu cyberbezpieczeństwa wiadomo od dawna. W 2015 r. zespół badawczy pod kierownictwem Przemysława Jatkiewicza przeprowadził szeroko zakrojone badania, których celem było stwierdzenie, czy jednostki samorządowe spełniają przepisy KRI lub podjęły prace nad wdrożeniem odpowiednich

mechanizmów. Badana populacja była imponująca i objęła 2 918 podmiotów: urzędy marszałkowskie, starostwa i urzędy gmin[76]. Z przeprowadzonego badania wynika, że jednostki samorządu terytorialnego „w większości nie podjęły adekwatnych starań odnośnie wdrożenia systemu zarządzania bezpieczeństwem informacji. Nie projektują, nie wdrażają oraz nie eksploatują systemów teleinformatycznych z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk”[77].

Kolejne wartościowe badania przeprowadzono w 2020 r. Objęto nim wszystkie gminy w Polsce, a odpowiedzi otrzymano łącznie od 1 787 gmin (72,1%)[78]. Z badania tego wynika, że system zarządzania bezpieczeństwem informacji wdrożyło 76,9% gmin, jednak w 82,2% jednostek system nie miał akredytacji zgodności z normą PN-ISO/IEC 27001:2017-063030. Systemu zarządzania bezpieczeństwem informacji nie wdrożono w 23,1% badanych jednostek. Główne powody takiego stanu to: brak wystarczających środków finansowych (37,5%) oraz elektronicznego obiegu dokumentów (24,9%). Do podjęcia stosownych działań decydentów samorządowych przekonałoby przede wszystkim przekazanie na ten cel dodatkowych środków przez organy administracji rządowej (52,3%) lub wprowadzenie elektronicznego obiegu dokumentów (19,6%). Nie wchodząc w szczegółową analizę warto w tym miejscu przywołać jeszcze jeden wniosek płynący z badania. W opinii respondentów cyberprzestępczość stanowi średnie (34,9%) lub duże (31,4%) zagrożenie dla urzędu[79].

Ustalenia badaczy oraz kontrolerów NIK powinny – zdaniem autorów – doprowadzić do systemowych zmian w zakresie cyberbezpieczeństwa jednostek administracji samorządowej. Dotychczasowe działania państwa w tym zakresie są niewystarczające. Od kilku lat państwo polskie doświadcza działań hybrydowych.

Dlaczego samorządy lokalne są atrakcyjnym celem ataków hakerskich?

Eksperci do spraw cyberbezpieczeństwa podkreślają, że władze lokalne „wypełniają niszę, którą cyberprzestępcy uwielbiają atakować – mają ograniczone zasoby, muszą dzielić swoją uwagę na wiele działów i przechowywać dane publiczne. To sprawia, że organizacje samorządowe są głównym celem ataku”[80]. Rzeczywistość potwierdza powyższe twierdzenie nie tylko w odniesieniu do polskiej administracji samorządowej. Kilka lat temu firma Barracuda Networks przeprowadziła badanie, w którym przeanalizowano 71 globalnych incydentów związanych z oprogramowaniem ransomware. Uzyskane wyniki wskazują, że samorządy lokalne są bardziej

[76] P. Jatkiewicz, *Wdrożenie wybranych wymagań dotyczących systemów informatycznych oraz Krajowych Ram Interoperacyjności w jednostkach samorządu terytorialnego Raport z badań,* Warszawa 2016.
[77] *Tamże*, s. 47.
[78] A. Chodakowska, S. Kańduła, J. Przybylska, *Jak polskie gminy…,* s. 137.
[79] *Tamże,* s. 139.
[80] *Why Local Governments Are Being Targeted by Cyber Attacks. And What You Can Do About It, Harris Local Governments,* “Harris Local Government” 2021, 10 II, [online] https://www.harrislocalgov.com/why-local-government-are-being-attacked/, 20 IV 2025.

narażone na ataki *ransomware* niż jakikolwiek inne typy organizacji. Okazało się, że 44% globalnych ataków ransomware, które miały miejsce w analizowanym okresie dotyczyło administracji lokalnej[81].

Przenosząc rozważania na grunt krajowy należy podkreślić, że polskie samorządy „są atrakcyjnym celem dla cyberprzestępców oraz grup hakerskich powiązanych ze służbami obcych państw"[82]. Współcześnie jednostki samorządu terytorialnego można uznać za szczególnie wrażliwy element krajowego systemu cyberbezpieczeństwa. Przyjmując szerszą definicję administracji samorządowej, obejmującą również instytucje takie jak żłobki, przedszkola, a także przedsiębiorstwa świadczące usługi komunalne (np. wodociągi i ciepłownie), należy stwierdzić, iż państwo funkcjonuje w warunkach znacznego ryzyka, porównywalnego do uczestnictwa w walce bez podstawowych mechanizmów ochrony.

Na potrzeby prowadzonego wywodu przeprowadzono również eksperyment z wykorzystaniem dostępnych narzędzi sztucznej inteligencji. W tym celu zapytano Chat GPT o to, dlaczego samorząd terytorialny w Polsce jest atrakcyjnym celem ataków hakerskich? Zdaniem Chat`a GPT samorząd terytorialny w Polsce jest atrakcyjnym celem ataków hakerskich z kilku istotnych powodów:

1) duża ilość danych osobowych. Urzędy samorządowe przetwarzają ogromne ilości danych wrażliwych, m.in.:
   a) dane osobowe mieszkańców (PESEL, adresy, dane rodzinne),
   b) dane podatkowe,
   c) dane dotyczące pomocy społecznej,
   d) dane medyczne (np. w jednostkach ochrony zdrowia podległych gminom);

   Zdaniem AI, dla cyberprzestępców to skarb – można je wykorzystać do kradzieży tożsamości, szantażu, czy też sprzedaży w darknecie;
2) ograniczone zasoby na cyberbezpieczeństwo. Wiele jednostek samorządowych:
   a) nie ma wykwalifikowanych specjalistów IT na etacie;
   b) korzysta z przestarzałego oprogramowania;
   c) ma ograniczone budżety na zabezpieczenia;
3) potencjalne zyski z ataków ransomware. Hakerzy często stosują ransomware – szyfrują dane i żądają okupu. Samorządy, które nie mogą pozwolić sobie na przestoje w działaniu (np. przedszkola, szkoły, MOPS-y, urzędy), mogą być bardziej skłonne zapłacić okup, by szybko odzyskać dostęp do danych;
4) brak świadomości zagrożeń wśród pracowników. Często ataki zaczynają się od *phishingu* – pracownik kliknie w złośliwy link lub otworzy podejrzany załącznik. Samorządy nie zawsze prowadzą szkolenia z cyberbezpieczeństwa, więc ludzki błąd to częsty wektor ataku;

[81] J. Coker, *Local Government Organizations Most Frequently Targeted by Ransomware,* „Infosecurity Magazine" 2020, 20 VIII, [online] https://www.infosecurity-magazine.com/news/local-government-targeted/, 20 IV 2025.
[82] Sz. Palczewski, *Ataki hakerskie na polskie samorządy. W co inwestować?,* „CyberDefence24" 2025, 2 IV, [online] https://cyberdefence24.pl/cyberbezpieczenstwo/ataki-hakerskie-na-polskie-samorzady-w-co-inwestowac, 20 IV 2025.

5) część większego łańcucha ataków. Samorządy współpracują z innymi instytucjami (np. ministerstwami, urzędami skarbowymi, placówkami zdrowia). Przejęcie kontroli nad jedną z jednostek może być „furtką" do ataku na inne instytucje publiczne.

Analiza wybranych ataków na jednostki samorządu terytorialnego w Polsce – *case studies*

W ostatnich latach polskie samorządy były przedmiotem ataków cyberprzestępców. Ich liczba rośne rokrocznie. Analiza wszystkich ataków wykracza poza przyjęte założenia badawcze. Zdecydowano się na przywołanie kilku cyberataków na jednostki samorządu terytorialnego w Polsce.

W dniu 5 grudnia 2022 r. o godz. 19:36 Monika Gontarczyk opublikowała w Biuletynie Informacji Publicznej Samorządu Województwa Mazowieckiego komunikat o incydencie cyberbezpieczeństwa w infrastrukturze Węzła Regionalnego[83]. W ramach węzła funkcjonują systemy informatyczne wykorzystywane przez partnerów projektów, realizowanych przez urząd. Wedle komunikatu, incydent stwierdzono 5 grudnia 2022 r. Polegał on „na ataku złośliwego oprogramowania szyfrującego pliki (ransomware). Zgodnie z posiadanymi informacjami istnieje duże prawdopodobieństwo, że dane przetwarzane w systemach objętych incydentem są w posiadaniu osób trzecich. Trwają działania mające na celu ustalenie pozostałych okoliczności zdarzenia"[84]. Wedle komunikatu incydent nie miał wpływu na funkcjonowanie urzędu, mógł jednak mieć wpływ na inne jednostki samorządu terytorialnego, które korzystają z systemów informatycznych, dostarczanych w ramach projektów[85].

Urząd o cyberataku poinformował odpowiednie instytucje, w tym zespół CSIRT NASK oraz złożył zawiadomienie o możliwości popełnienia przestępstwa. Podjęto również działania mające na celu przywrócenie normalnego funkcjonowania urzędu[86]. Wedle dostępnych informacji w wyniku ataku nie doszło do pozyskania danych osobowych klientów Urzędów, jednak cyberatak miał wpływ na nieterminowe załatwienie spraw przez UMWM, chwilowy brak dostępności niektórych usług oferowanych oraz chwilowe utrudnienie w kontakcie z pracownikami. Urząd zadeklarował, że realizuje

---

[83] *Komunikaty. Incydent cyberbezpieczeństwa,* „Biuletyn Informacji Publicznej Samorządu Województwa Mazowieckiego" 2022, 5 XII, [online] https://mazovia.pl/pl/bip/komunikaty/incydent-cyberbezpieczenstwa-1.html, 20 IV 2025.

[84] *Tamże.*

[85] *Cyberatak na urząd marszałkowski. Złośliwe oprogramowanie mogło zainfekować elektroniczne kontakty z radomskim magistratem,* „www.MojRadom.pl" 2022, 8 XII, [online] https://www.mojradom.pl/cyberatak-na-urzad-marszalkowski-zlosliwe-oprogramowanie-moglo-zainfekowac-elektroniczne-kontakty-z-radomskim-magistratem/, 20 IV 2025.

[86] Zob. także: M. Sajdak, *Ransomware zaatakował Urząd Marszałkowski Województwa Mazowieckiego: zaszyfrowane dane systemu Elektronicznego Zarządzania Dokumentami (EZD) oraz innych systemów,* „Sekurak" 2022, 6 XII, [online] https://sekurak.pl/ransomware-zaatakowal-urzad-marszalkowski-wojewodztwa-mazowieckiego-zaszyfrowane-dane-systemu-elektronicznego-zarzadzania-dokumentami-ezd-oraz-innych-systemow/, 20 IV 2025, *Zhakowano Urząd Marszałkowski Województwa Mazowieckiego,* „CyberDefence24" 2022, 6 XII, [online] https://cyberdefence24.pl/cyberbezpieczenstwo/zhakowano-urzad-marszalkowski-wojewodztwa-mazowieckiego, 20 IV 2025.

działania mające na celu odzyskanie danych z istniejących kopii zapasowych. Zadeklarowano również, że podjęte zostaną niezbędne działania, aby podobna sytuacja nie miała miejsca w przyszłości.

Warto w tym miejscu po raz kolejny odwołać się do ustaleń NIK. W 2015 r. Izba prowadziła kontrolę w Urzędzie Marszałkowskim Województwa Mazowieckiego w zakresie świadczenia usług publicznych w formie elektronicznej. W wystąpieniu pokontrolnym stwierdzono jednoznacznie, że „nie zapewniono regularnego tworzenia kopii zapasowych zbiorów baz danych Elektronicznego Systemu Obiegu Dokumentów (dalej ESOD) oraz nie zapewniono właściwego przechowywania utworzonych kopii zapasowych baz danych oraz plików ESOD”[87]. Atak z 2022 r. poddaje w wątpliwość, czy zalecenia NIK sprzed kilku lat zostały właściwie zaadresowane.

Usuwanie skutków ataku zajęło Urzędowi kilkanaście dni[88]. Przedstawiciele UMWM wskazali, że ataku dokonała grupa Play Ransomware[89]. Co ciekawe, ta sama grupa hakerska przeprowadziła kilka dni później atak na infrastrukturę belgijskiego miasta Antwerpia[90]. W jego efekcie hakerzy uzyskali dostęp do ponad 500gb danych[91].

Drugi przykład wybrany do analizy dotyczy otwockiego magistratu. Do ataku hakerów doszło w nocy z piątku na sobotę 16 października 2021 r. Biuro prasowe w odpowiedzi na otrzymane pytania wskazało, że w wyniku ataku „zaszyfrowane zostały dane znajdujące się na urzędowych serwerach. Był to atak typu ransomware. Nie wiadomo jeszcze co było źródłem ataku. Trwają czynności wyjaśniające w tym kierunku. Sprawą zajmują się organy ścigania i dla dobra śledztwa na tym etapie postępowania nie udzielamy więcej informacji”[92]. We wcześniejszym komunikacie opublikowanym na stronie internetowej Urzędu incydent określono jako „nowatorski typ ataku, któremu dotychczas poddały się największe światowe instytucje”.

W przypadku otwockiego magistratu, cyberprzestępcy zaatakowali serwery urzędu przy użyciu *ransomware* dzięki złośliwemu oprogramowaniu LockBit 2.0. Spowodowało ono zaszyfrowanie danych przechowywanych przez

---

87 *Wystąpienie pokontrolne P/15/003 – Świadczenie usług publicznych w formie elektronicznej na przykładzie wybranych jednostek samorządu terytorialnego,* Nr ewidencyjny: KAP.410.004.02.2015, Najwyższa Izba Kontroli, Warszawa 2015, s. 3.

88 Sz. Palczewski, *Cyberatak na mazowiecki urząd. Wciąż są problemy z infrastrukturą*, „CyberDefence24” 2022, 16 XII, [online] https://cyberdefence24.pl/cyberbezpieczenstwo/cyberatak-na-mazowiecki-urzad-wciaz-sa-problemy-z-infrastruktura, 20 IV 2025.

89 *Szturm na „Wrota Mazowsza”. Atak ransomware na Urząd Marszałkowski Województwa Mazowieckiego! [Aktualizacja],* „itWiz.pl” 2022, 5 XII, [online] https://www.itweek.pl/atak-ransomware-na-umwm/, 20 IV 2025.

90 L. Abrams, *Play ransomware claims attack on Belgium city of Antwerp,* “BLEEPINGCOMPUTER” 2022, 12 XII, [online] https://www.bleepingcomputer.com/news/security/play-ransomware-claims-attack-on-belgium-city-of-antwerp/, 20 IV 2025.

91 M. Sajdak, *Grupa ransomware Play grozi ujawnieniem danych belgijskiego miasta Antwerpia. To najpewniej ta sama grupa, która zaatakowała Urząd Marszałkowski Mazowsze,* „Sekurak” 2022, 13 XII, [online] https://sekurak.pl/grupa-ransomware-play-grozi-ujawnieniem-danych-belgijskiego-miasta-antwerpia-to-najpewniej-ta-sama-grupa-ktora-zaatakowala-urzad-marszalkowski-mazowsze/, 20 IV 2025.

92 M. Mastalerz, *Urząd miejski w Otwocku padł ofiarą cyberataku,* „Serwis Samorządowy PAP” 2021, 22 X, [online] https://samorzad.pap.pl/kategoria/e-urzad/urzad-miejski-w-otwocku-padl-ofiara-cyberataku, 20 IV 2025.

urząd oraz umożliwiło przestępcom ich przejęcie[93]. Dane, w których posiadanie mogli wejść przestępcy to m.in.: imię, nazwisko, adres zamieszkania, numer PESEL, numer NIP, seria i numer dowodu osobistego lub paszportu, data i miejsce urodzenia, numer telefonu, wykonywany zawód, wysokość wynagrodzenia, wizerunek, stan cywilny, obywatelstwo, stan zdrowia, wykształcenie, karalność, adres e-mail, numer konta bankowego. Ponadto, atak ten związany był ze znacznym utrudnieniem w ramach obsługi mieszkańców w sprawach w zakresie kart metropolitarnych, kart dużej rodziny, kart rodziny 3+, opłat za gospodarowanie odpadami czy spraw podatkowych[94].

Z doniesień medialnych publikowanych po ataku cyberprzestępców można wnioskować, że poziom cyberbezpieczeństwa w otwockim magistracie był na bardzo niskim poziomie. Serwis wyborcza.pl, powołując się na ustalenia ekspertów wykonujących audyt po ataku, wskazywał, że „sieć urzędu miasta stoi otworem dla wszystkich w obrębie siedziby. Każdy obcy wpinający się do dowolnego gniazda w urzędzie miasta uzyska do niej nieautoryzowany dostęp. W serwerowni jest tak wiele śmieci, że w każdej chwili mogło dojść do pożaru. Dział informatyki tak dalece nie panował nad swoimi obowiązkami, że właściwie działał na szkodę urzędu"[95]. W dalszej części raportu zawarto jeszcze bardziej druzgocące wnioski. Eksperci wskazali, że znaleźli „50 wysoce niebezpiecznych luk pozwalających na przejęcie kontroli nad dziurawymi systemami i wstrzyknięcie złośliwego oprogramowania, które da możliwość przejęcia całej sieci. Najstarsze znalezione luki bezpieczeństwa zostały odkryte i opisane w 1999 r."[96].

Ostatni przykład skutecznego cyberataku dotyczy Starostwa Powiatowego w Oświęcimiu. Autorzy zdecydowali się na jego analizę, z uwagi na podejrzenie zrealizowania żądania zapłacenia okupu. Analizę należy jednak rozpocząć od przywołania podstawowych informacji dotyczących ataku.

W październiku 2020 r. geodeci działający na terenie powiatu oświęcimskiego otrzymali wiadomość następującej treści: „serwer bazami danych Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej w Oświęcimiu został 13. października zablokowany przez hakerów. (…) W związku z tym nie ma możliwości zgłaszania prac, udostępniania materiałów, przyjmowania prac geodezyjnych do zasobu, a także składania projektów do uzgodnień na naradach koordynacyjnych"[97]. Paweł Maziarz podejrzewał, że urząd nie dysponował odpowiednimi kopiami zapasowymi (lub pojawił się problem z ich właściwym odtworzeniem), co w efekcie doprowadziło do „paraliżu funkcjonowania jednostki – utracono możliwość zgłaszania prac, udostępniania materiałów, przyjmowania prac geodezyjnych do zasobu, a

[93] *Cyberatak na Urząd Miasta Otwocka – jak można go było uniknąć?,* „iOtwock" 2021, 7 XII, [online] https://iotwock.info/artykul/cyberatak-na-urzad-miasta/1250396 20 IV 2025.
[94] M. Mastalerz, *Urząd miejski w Otwocku…*
[95] M. Wojtczuk, *Gigantyczny wyciek danych w Otwocku. Hakerzy wykradli PESEL-e i numery dowodów wszystkich mieszkańców,* „wyborcza.pl" 2022, 19 VII, [online] https://warszawa.wyborcza.pl/warszawa/7,54420,28700276,gigantyczny-wyciek-danych-w-otwocku-hakerzy-wykradli-pesele.html, 20 IV 2025.
[96] *Tamże.*
[97] *Ataki na systemy geodezyjne w Polsce – kolejne gminy/miasta zgłaszają poważne problemy,* „Sekurak" 2022, 20 X, [online] https://sekurak.pl/ataki-na-systemy-geodezyjne-w-polsce-kolejne-gminy-miasta-zglaszaja-powazne-problemy/, 20 IV 2025.

także składania projektów do uzgodnień na naradach koordynacyjnych”[98]. Z dużym prawdopodobieństwem hakerzy zażądali okupu za odszyfrowanie danych. W pierwszym etapie żądania tego nie spełniono. Urząd zdecydował się na inne rozwiązanie. W listopadzie 2020 r. ogłoszono postępowanie przetargowe „Odzyskanie zaszyfrowanych baz danych systemu geodezyjno-kartograficznego Starostwa Powiatowego w Oświęcimiu”[99].

Przedmiotem zamówienia było odzyskanie zaszyfrowanych baz danych systemu geodezyjno- kartograficznego Starostwa Powiatowego w Oświęcimiu. Odzyskanie miało polegać na „całkowitym odszyfrowaniu danych oraz konwersji danych do bazy wynikowej, która będzie mogła zostać skutecznie zaimportowana do systemu geodezyjnego”. Poinformowano również, że „baza danych składa się z plików dbf, które zawierają zarówno dane geodezyjne z ewidencji gruntów i budynków oraz skany map, rastry oraz pliki dołączane za pomocą systemów informatycznych przez m.in. geodetów. Łącza pojemność bazy danych to ok 2 TB”[100].

W postępowaniu przetargowym wyłoniono wykonawcę, który zaproponował wykonanie usługi za kwotę 620 000 zł. Eksperci wskazywali, że w praktyce były dwie możliwości – albo zewnętrzna firma po prostu zdecydowała się zapłacić okup cyberprzestępcom za odszyfrowanie plików albo opracowano dekryptor[101]. Jak pisze Sekurak „gdyby miał miejsce scenariusz pierwszy, to wszyscy w zasadzie są zadowoleni – urząd: odzyskał dane, przestępca – zarobił, firma zewnętrzna zarobiła. No dobra – podatnik stracił. Tzn. stracił trochę pieniędzy na okup/odszyfrowanie danych, jednak nie stracił dostępu do dość kluczowych danych – więc zapewne i tutaj zyskał…”[102].

Temat przetargu wzbudził emocje zarówno z powodu konieczności dokonani zmian w planie finansowym, jak i podejrzeń o opłacenie ze środków publicznych okupu dla przestępców. Politycy publicznie formułowali wątpliwości co do postępowania oświęcimskich decydentów w kontekście prawdopodobnego opłacenia okupu ze środków publicznych[103].

Syntetyzując analizę wybranych cyberataków na jednostki samorządu terytorialnego w Polsce należy podkreślić, że motywacje przestępców są różne. Ataki mogą być realizowane na zlecenie państw (np. działania grup ATP) lub motywacja może być czysto finansowa – żądanie okupu. W części przypadków decydenci publiczni decydują się na spełnienie żądań i opłacenie okupu[104].

---

[98] P. Maziarz, *Hakerzy zaszyfrowali bazy w Oświęcimiu – urzędnicy... obcięli środki na drogi,* „Benchmark.pl” 2021, 25 II, [online] https://www.benchmark.pl/aktualnosci/hakerzy-zaszyfrowali-bazy-w-oswieciumiu-kontrowersyjna-decyzja.html 20 V 2025.

[99] *Przetarg w urzędzie na odszyfrowanie danych po ransomware? Zapłata w PLN nie BTC ;-) Bohater? System geodezyjno-kartograficzny w Oświęcimiu,* „Sekurak” 2021, 21 II, [online] https://sekurak.pl/przetarg-w-urzedzie-na-odszyfrowanie-danych-po-ransomware-zaplata-w-pln-nie-btc-bohater-system-geodezyjno-kartograficzny-w-oswiecimiu/ 20 IV 2025.

[100] *Tamże.*

[101] P. Maziarz, *Hakerzy zaszyfrowali bazy…*

[102] *Przetarg w urzędzie na odszyfrowanie…*

[103] M. Pawłowska, *Oświęcim. Działacze PiS pytają, czy Starostwo Powiatowe zapłaciło okup za odblokowanie danych po ataku hakerskim,* „Oświęcim Nasze Miasto” 2021, 11 III, [online] https://oswiecim.naszemiasto.pl/oswiecim-dzialacze-pis-pytaja-czy-starostwo-powiatowe/ar/c15-8174297 21 IV 2025.

[104] P. Malinowski, Mias*to na Florydzie zapłaci hakerom okup w bitcoinach,* „rp.pl” 2019, 20 VI, [online] https://cyfrowa.rp.pl/it/art16920091-miasto-na-florydzie-zaplaci-hakerom-okup-w-bitcoinach, 20 IV 2025.

Zdaniem Witolda Skomry „jak grupa żąda okupu, to jest to jeszcze w miarę bezpieczne, bo gorzej, jeżeli się ktoś włamał, pobrał dane i nie zażądał okupu, bo to znaczy, że miał inne cele ukryte. Natomiast tak całkiem nie możemy być spokojni, bo nie jest wykluczone, że ten kto żąda okupu tych danych już komuś nie sprzedał wcześniej. Nawet przewidujemy sytuację, w której ktoś żąda okupu tylko po to, żeby zamaskować rzeczywisty cel, bo o co innego mu chodziło”[105].

Autorzy nie podzielają poglądu Witolda Skomry ponieważ jest on wewnętrznie sprzeczny. Z jednej strony czytamy bowiem, że „jest w miarę bezpiecznie”, a z drugiej „całkiem nie możemy być spokojni”. Każdy cyberatak wpływa negatywnie na bezpieczeństwo zarówno danej organizacji, jak i jej klientów i innych interesariuszy.

Najważniejsze wyzwania w zakresie cyberbezpieczeństwa na poziomie samorządu

Przeprowadzona na potrzeby niniejszego artykułu analiza wyników kontroli NIK w zakresie odporności cyfrowej i cyberbezpieczeństwa jednostek samorządu terytorialnego połączona z doświadczeniami autorów oraz obserwacją trendów rynkowych pozwala na sformułowanie zestawu kluczowych wyzwań i niezbędnych działań. Aby uporządkować wywód zaproponowano podział wyzwań na te o charakterze systemowym (strategicznym) i operacyjnym. Zbiór wyzwań systemowych obejmuje te legislacyjne, organizacyjne, edukacyjne i finansowe. Z kolei zbiór operacyjny dotyczy kwestii kadrowych oraz świadomości decydentów samorządowych.

Wyniki kontroli NIK pokazują, że konieczne jest wdrożenie kompleksowych rozwiązań, które zapewnią odpowiedni poziom bezpieczeństwa systemom wykorzystywanym przez jednostki samorządu terytorialnego. W ramach działań na rzecz podniesienia poziomu bezpieczeństwa istotną rolę może odegrać wdrażanie mechanizmów znanych w sektorze prywatnym np. normy ISO/IEC 27001[106] promującej holistyczne podejście do kwestii bezpieczeństwa. Standard ten określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji (SZBI). Implementacja normy umożliwi jednostkom samorządowym systematyczne identyfikowanie ryzyk, stosowanie odpowiednich środków ochronnych oraz budowanie kultury bezpieczeństwa na wszystkich poziomach organizacji co sprzyja zwiększeniu odporności na zagrożenia cybernetyczne.

W 2023 r. NASK opracował poradnik skierowany do jednostek samorządu terytorialnego, w którym zwrócono uwagę na znaczenie wdrażania SZBI oraz konieczność systematycznego podnoszenia świadomości zagrożeń cyberbezpieczeństwa wśród pracowników[107]. Dokument zawiera również

[105] Wypowiedź Witolda Skomry doradcy w Rządowym Centrum Bezpieczeństwa, p.o. Szefa Wydziału Ochrony Infrastruktury Krytycznej na posiedzeniu Podkomisji stałej do spraw funkcjonowania zarządzania kryzysowego, Sejm Rzeczypospolitej Polskiej X kadencji, 27 XI 2024 r. [online] https://www.sejm.gov.pl/sejm10.nsf/biuletyn.xsp?skrnr=ASW02S-7, 20 IV 2025.
[106] Norma PN-EN ISO/IEC 27001:2023-08.
[107] NASK, *Cyberbezpieczny samorząd. Poradnik*.

przegląd wybranych rozwiązań organizacyjnych i technologicznych, w tym modelu Centrów Usług Wspólnych oraz wykorzystania technologii chmurowych, mających na celu skuteczną identyfikację oraz ograniczanie ryzyka związanego z incydentami bezpieczeństwa. Ponadto poradnik przedstawia procedury zgłaszania oraz obsługi incydentów, a także wskazuje możliwości uzyskania wsparcia finansowego i technicznego. Jednostki samorządu terytorialnego powinny wykorzystać zawarte w nim rekomendacje do budowy własnego systemu bezpieczeństwa informacji zgodnego z wymogami wynikającymi z ustawy o krajowym systemie cyberbezpieczeństwa oraz RODO.

Praktyka pokazuje również, że zwykle najsłabszym ogniwem w systemie bezpieczeństwa są ludzie[108]. Steve Woźniak podkreśla, że w obecnych czasach, kiedy tak dużo uwagi poświęca się bezpieczeństwu, wydaje ogromne kwoty na ochronę sieci komputerowych i danych, powinniśmy zdać sobie sprawę z tego, jak łatwo można oszukać ludzi „z wewnątrz" i obejść wszystkie możliwe zabezpieczenia technologiczne[109]. Faktem jest, że to właśnie w znacznej mierze, błędne działania, niestosowanie się do procedur, nieprzestrzeganie regulacji w zakresie cyberbezpieczeństwa, lekceważenie obowiązków wynikających z dokumentów, niedopatrzenia czy podatność na metody socjotechniki sprawiają, że największym zagrożeniem dla instytucji, w tym samorządu terytorialnego jest właśnie człowiek. Wnioski można wyciągnąć na przykładzie przytaczanych badań i raportów. Znaczny procent badanych pracowników z kontrolowanych przez NIK urzędów wykazało się generalną niewiedzą w zakresie podstawowej wiedzy dotyczącej cyberbezpieczeństwa swojej organizacji, takich jak: brak wiedzy w zakresie tworzenia bezpiecznych haseł, brak wiedzy w zakresie procedury w przypadku zawirusowania sprzętu komputerowego, czy brak wiedzy w zakresie nieostrożnego wykorzystywania serwisów społecznościowych. Wielokrotnie przytaczane przypadki ataków *phishingowych*, czyli wykorzystanie metod socjotechniki jest również dowodem na to, że błędy ludzkie powodują największe zagrożenie dla całej organizacji. Ostatecznie, to wciąż człowiek oraz prowadzona przez niego polityka bezpieczeństwa, odpowiedzialny jest za wdrożenie takich rozwiązań jak tworzenie kopii zapasowych danych, instalacja oprogramowania chroniącego, np. antywirusy czy dbanie o bezpieczeństwo haseł czy sieci. Wraz z błędami ludzkimi, powiązać można problematykę odpowiedniego zarządzania instytucji. Wielokrotnie podnosi się zarzuty wobec braku wykonywania odpowiednich audytów wewnętrznych lub zlecanie na podstawie *outsoucringu* audytów przez wyspecjalizowane firmy zewnętrzne oraz dedykowanych dla pracowników szkoleń z zakresu cyberbezpieczeństwa. NASK podkreśla, że zakres szkoleń z zakresów cyberbezpieczeństwa powinien być dostosowany do roli, jaką poszczególne osoby pełnią w organizacji i obejmować: wszystkich pracowników, kadrę kierowniczą oraz specjalistów zatrudnionych w IT[110]. Dopasowanie zakresu szkoleń do wszystkich trzech grup pozwoli uwrażliwić

[108] J. Skulska, W. Pławińska, *Człowiek jako najsłabsze ogniwo bezpieczeństwa informacyjnego*, „Nowoczesne Systemy Zarządzania" 1/2021 vol. 16, s. 98-119.
[109] S. Woźniak, *Słowo wstępne* [w:] K. Mitnick, W. Simon, *Sztuka podstępu*, Gliwice 2003, s. 7-8.
[110] NASK, *Cyberbezpieczny samorząd. Poradnik*, s. 24 i s. 119.

je na istniejące zagrożenia oraz uwidocznić rolę, które pełnią one w systemie bezpieczeństwa informacji.

Na podstawie przywołanych danych, informacji i przykładów należy zastanowić się nad właściwymi przyczynami takich incydentów bezpieczeństwa. Powodów, dlaczego i w jaki sposób dochodzi do ataków na jednostki samorządu terytorialnego może być wiele, jednakże warto pochylić się nad kilkoma najbardziej istotnymi podatnościami.

Pierwszą z istotnych podatności, z którą zmaga się samorząd terytorialny jest zarządzanie sprzętem komputerowym w organizacji. Organizacje, w tym administracja samorządowa, w pierwszej kolejności powinny zadbać o bezpieczny, jakościowy i wydajny sprzęt przeznaczony zarówno do właściwego użytkowania przez pracowników, jak i infrastrukturę krytyczną w organizacji, na przykład poprzez zadbanie o bezpieczne środowisko dla serwerów utrzymujących systemy informacyjne. Przytaczane wcześniej raporty wskazywały, że niektóre gminy nie zapewniały właściwego zabezpieczenia serwerowni, co mogło przełożyć się na zwiększenie ryzyka uszkodzenia, zniszczenia serwerów bądź wykorzystania niezabezpieczonych serwerów do nieautoryzowanych dostępów, bądź zainstalowania szkodliwego oprogramowania. W XXI wieku technologia *hardware'owa* funkcjonuje na bardzo zaawansowanym poziomie, co można również wykorzystać do działań przestępczych. W kontekście podatności zabezpieczenia sprzętów IT zwykłego pracownika czy serwera, na którym funkcjonuje system informacyjny organizacji, przykładowym zagrożeniem może być instalacja szkodliwego sprzętu zewnętrznego, jakim może być Rubber Ducky, czyli urządzenie służące do infekowania komputerów, które działa jak zdalna klawiatura[111] , czy chociażby urządzenie USB Killer, które jest w stanie trwale uszkodzić sprzęt poprzez zniszczenie podzespołów sprzętu komputerowego. Są to jedynie przykłady potencjalnych niebezpieczeństw, związanych z niezabezpieczaniem sprzętu komputerowego. Instytucje, w tym samorządy, z różnych powodów, często posiadają przestarzały sprzęt, istotny z punktu widzenia bezpieczeństwa infrastruktury informatycznej lub nie posiadają go w ogóle.

Innym istotnym czynnikiem, który wpływa na zwiększenie zagrożenia cyberbezpieczeństwa samorządu terytorialnego jest bezpieczeństwo oprogramowania komputerowego i systemów informacyjnych bądź teleinformatycznych. Tak samo jak w przypadku niebezpieczeństw związanych z hardware instytucji, tak i software tym bardziej zagrożony jest podatnością na ataki. Wielokrotnie hakerzy wykorzystywali luki w oprogramowaniu systemowym w celu przeprowadzenia cyberataku. Przytaczane wcześniej wyniki kontroli NIK z 2022 wykazały, że gminy wykorzystywały „nieaktualne bądź nieprawidłowo skonfigurowane oprogramowania"[112]. Ta sama kontrola wykazała, że istniejące luki w oprogramowaniu urzędów umożliwiały zdalne przejęcie kontroli nad systemem, zablokowaniem dostępu do systemu, bądź

[111] P. Konieczny, *Złośliwy kabel USB, który zmienia się w klawiaturę i infekuje Twój komputer,* „Niebezpiecznik.pl" [online] 21 II 2019, https://niebezpiecznik.pl/post/zlosliwy-kabel-usb-ktory-zmienia-sie-w-klawiature-i-infekuje-twoj-komputer/, 21 IV 2025.

[112] *Informacja o wynikach kontroli „Zapewnienie bezpieczeństwa teleinformatycznego przez jednostki samorządu terytorialnego województwa zachodniopomorskiego",* Nr ewidencyjny: I/23/001/LSZ, Najwyższa Izba Kontroli, Warszawa, 3 kwietnia 2024 r.

wgraniem złośliwego oprogramowania[113]. Warto również przytoczyć inne wyniki kontroli Najwyższej Izby Kontroli z roku 2023 dotyczące zarządzania oprogramowaniem komputerowym przez administrację publiczną. Wyniki kontroli określone zostały jako negatywne, gdzie można wyróżnić takie uchybienia jak instalację nieautoryzowanego oprogramowania, w tym instalacja oprogramowania bez wsparcia producenta czy instalację w nieaktualnej wersji oprogramowania[114]. Andrzej Chrząszcz podkreśla, że „aby system mógł poprawnie działać, niezbędna jest właściwa jego obsługa, zarządzanie i utrzymanie"[115]. Jak można zauważyć, również gwarancja bezpieczeństwa software'u jest niezwykle istotnym czynnikiem potrzebnym do zagwarantowania bezpieczeństwa informacyjnego w jednostkach samorządu terytorialnego.

Zakończenie

Przedstawiony w artykule stan cyberbezpieczeństwa i odporności cyfrowej samorządu terytorialnego w Polsce nie napawa optymizmem. Skala problemów stwierdzonych przez Najwyższą Izbę Kontroli jest porażająca i wymaga natychmiastowych działań ze strony decydentów rządowych. Należy bowiem pamiętać, że system cyberbezpieczeństwa jest tak odporny, jak jego najsłabsze ogniwo.

Zdaniem autorów zasadne jest zwiększenie poziomu centralizacji zadań związanych z cyberbezpieczeństwem na poziomie. Obecny stan jest bowiem nie do zaakceptowania w wymiarze bezpieczeństwa państwa i jego obywateli. Jednym z rozwiązań, które warto poddać głębszej analizie zakłada powołanie na poziomie centralnym dedykowanej agencji odpowiedzialnej za cyberbezpieczeństwo jednostek samorządu terytorialnego. Agencja taka powinna zostać wyposażona w odpowiednie kompetencje prawne i zasoby po to, aby przejmować od samorządów terytorialnych kolejne zadania związane z budowaniem odporności cyfrowej. Na poziomie państwa powinna powstać wspólna i spójna architektura systemów ICT wspierających świadczenie usług publicznych. Należy również rozważyć przyspieszenie działań mających na celu budowę wspólnej infrastruktury państwa. Tysiące, a może i dziesiątki tysięcy serwerowi funkcjonujących w administracji samorządowej powinno być stopniowo migrowane do profesjonalnych centrów usług. Centra takie można utworzyć w każdym województwie co powinno pozytywnie wpłynąć na strukturę wydatków publicznych.

Działaniem pożądanym i komplementarnym w tym kontekście jest również standaryzacja usług publicznych i rozwijanie wspólnych aplikacji i narzędzi wspierających ich świadczenie na rzecz obywateli i innych interesariuszy. Nie znajduje bowiem logicznego i ekonomicznego uzasadnienia tworzenie i wdrażanie tożsamych aplikacji wspierających realizację tych samych usług publicznych w różnych jednostkach samorządowych. Jeżeli na

---

[113] *Tamże.*

[114] *Informacja o wynikach kontroli „Zarządzanie oprogramowaniem komputerowym przez administrację publiczną", Nr ewidencyjny: 15/2023/P/22/082/LPO,* Najwyższa Izba Kontroli, Warszawa, 29 kwietnia 2024 r.

[115] A. Chrząszcz, *Bezpieczeństwo IT – siedem grzechów głównych,* „Zeszyty Naukowe WWSI" 7/2012, s. 47-65.

poziomie państwa możliwe było wdrożenie jednego rozwiązania IT do rozliczania podatku PIT, to można założyć, że w identyczny sposób można zaimplementować narzędzie do rozliczania podatku od nieruchomości.

Przykładów oczywiście jest istotnie więcej, jednak ich analiza wykracza poza przyjęte założenia. Celem autorów było zasygnalizowanie potencjalnych i pożądanych kierunków działania na poziomie państwa.

Trudno nie zgodzić się, z Katarzyną Badźmirowską-Masłowską, która uważa, że „zwiększenie odporności w dziedzinie bezpieczeństwa cybernetycznego w Unii Europejskiej spoczywa zarówno na: unijnych instytucjach (zwłaszcza Komisji Europejskiej) i organach) (ENISA), krajowych władzach publicznych różnych szczebli jak i na podmiotach prywatnych, które zobowiązane są do rozwijania zdolności i skutecznego w tej materii współdziałania”[116]. Na dzisiaj jednostki samorządu terytorialnego stanowią „miękkie podbrzusze” krajowego systemu cyberbezpieczeństwa. Jeżeli przyjmiemy szerszą perspektywę i do pojęcia „administracji samorządowej” włączymy również jednostki, takie jak: żłobki, przedszkola, zakłady wodociągowe i ciepłownicze to okaże się, że uczestniczymy jako państwo w walce bokserskiej bez trzymywania gardy. Rację ma Michał Kurek, który pisze, że „cyberataki są dziś zjawiskiem powszechnym. Łupem hakerów stają się najbardziej zaawansowane technologicznie firmy. Nie należy dziś pytać »czy?«, ale »kiedy?« nastąpi cyberatak w organizacji. Nie ma zabezpieczeń gwarantujących bezpieczeństwo, w związku z czym krytyczne stają się inwestycje w procesy monitorowania bezpieczeństwa i reakcji na cyberataki. Tylko dzięki nim możliwe jest skrócenie czasu, w jakim niewykryty haker bezkarnie działa w firmowej infrastrukturze. Czasu, który wynosi obecnie średnio ponad pół roku i mocno skorelowany jest z poziomem poniesionych strat”[117].

Zdaniem autorów niezbędne jest również wprowadzenie przepisów prawnych regulujących indywidualną odpowiedzialność decydentów samorządowych za zagadnienia związane z zapewnieniem odpowiedniego poziomu cyberodporności. Rozwiązania takie zostały zaimplementowane w rozporządzeniu DORA dotyczącym podmiotów finansowych, jednak zdaniem autorów nie ma przeciwwskazań, aby rozwiązania takie miały zastosowanie do podmiotów publicznych, nie tylko tych samorządowych. Przedstawiciele Ministerstwa Cyfryzacji dostrzegli tę słabość systemu i nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa zakłada sankcje indywidualne. Projekt zakłada, że „to kierownik danej jednostki będzie odpowiedzialny za to, aby przekierować odpowiednie środki na cyberbezpieczeństwo. Jeżeli tego nie robi, zostanie uznany za osobę, która nie wywiązała się ze swoich zadań”[118].

Bibliografia

[116] K. Badźmirowska-Masłowska, *Europejskie uwarunkowania cyberbezpieczeństwa RP. Wybrane aspekty strategiczne i prawne*, [w:] K. Chałubińska-Jentkiewicz, A. Brzostek (red.), *Modele rozwiązań prawnych w systemie cyberbezpieczeństwa RP. Rekomendacje*, s. 93.

[117] M. Sikorska, *5 najgroźniejszych ataków ransomware w Polsce. Czy Twoja firma na pewno jest bezpieczna?* Grandmetric, 4 IV 2023, [online] https://www.grandmetric.com/pl/5-najgrozniejszych-atakow-ransomware-w-polsce/, 19 IV 2025.

[118] *Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa i niektórych innych ustaw*, 24 IV 2024 [online] https://legislacja.rcl.gov.pl/projekt/12384504/katalog/13055195#13055195, 10 V 2025.

Literatura

Banasiński C. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2023.
Besiekierska A. (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.
Björck F., Henkel M., Stirna J., Zdravkovic J., *Cyber Resilience – Fundamentals for a Definition*, "New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing" 2015, vol. 353.
Chałubińska-Jentkiewicz K., Brzostek A. (red.) *Modele rozwiązań prawnych w systemie cyberbezpieczeństwa RP. Rekomendacje*, Warszawa 2021.
Chodakowska A., Kańduła S., Przybylska J., *Jak polskie gminy radzą sobie z cyberbezpieczeństwem*, „Kontrola Państwowa" 2022, nr 1.
Chrząszcz A., *Bezpieczeństwo IT – siedem grzechów głównych*, „Zeszyty Naukowe WWSI" 7/2012.
Dziomdziora W., *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Warszawa 2021.
Hausken K., *Cyber resilience in firms, organizations and societies*, "Internet of Things" 2020, vol. 11.
Jatkiewicz P., *Wdrożenie wybranych wymagań dotyczących systemów informatycznych oraz Krajowych Ram Interoperacyjności w jednostkach samorządu terytorialnego Raport z badań,* Warszawa 2016.
Kitler W., Taczkowska-Olszewska J., Radoniewicz F. (red.) *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.
Mitnick S., W. Simon, *Sztuka podstępu*, Gliwice 2003.
Siudak R., *Cyberbezpieczeństwo w Polsce. Od dyskursów do polityk publicznych*, Kraków 2022.
Skulska J. , Pławińska W., *Człowiek jako najsłabsze ogniwo bezpieczeństwa informacyjnego*, „Nowoczesne Systemy Zarządzania" 1/2021 vol. 16.
Szczegielniak M., *Dostęp do informacji w administracji publicznej a rozwój partycypacji obywatelskiej w Polsce,* Warszawa 2025.
Szpor G., Gryszczyńska A., Czaplicki K. (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. U. UE L. z 2016 r. Nr 194.
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE), 2016/1011, Dz. U. UE. L. z 2022 r. Nr 333.
Rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Dz. U. UE z 2016 r. L 119/1.

Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności , minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz. U. z 2024 r. poz. 773.
Ustawa o finansach publicznych, Dz. U. 2009 Nr 157 poz. 1240.
Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, t.j. Dz. U. z 2024 r. poz. 1557, 1717.
Ustawa o krajowym systemie cyberbezpieczeństwa, Dz. U. 2018 poz. 1560.

Inne dokumenty i źródła internetowe

Abrams L., *Play ransomware claims attack on Belgium city of Antwerp,* "BLEEPINGCOMPUTER" 2022, 12 XII, [online] https://www.bleepingcomputer.com/news/security/play-ransomware-claims-attack-on-belgium-city-of-antwerp/.
Ataki na systemy geodezyjne w Polsce – kolejne gminy/miasta zgłaszają poważne problemy, „Sekurak" 2022, 20 X, [online] https://sekurak.pl/ataki-na-systemy-geodezyjne-w-polsce-kolejne-gminy-miasta-zglaszaja-powazne-problemy/.
Cyberbezpieczeństwo w samorządach kuleje, Najwyższa Izba Kontroli 2025, 17 IV, [online] https://www.nik.gov.pl/aktualnosci/cyberbezpieczenstwo-w-samorzadach-2025.html.
Cyberatak na urząd marszałkowski. Złośliwe oprogramowanie mogło zainfekować elektroniczne kontakty z radomskim magistratem, „www.MojRadom.pl" 2022, 8 XII, [online] https://www.mojradom.pl/cyberatak-na-urzad-marszalkowski-zlosliwe-oprogramowanie-moglo-zainfekowac-elektroniczne-kontakty-z-radomskim-magistratem/.
Cyberatak na Urząd Miasta Otwocka – jak można go było uniknąć?, „iOtwock" 2021, 7 XII, [online] https://iotwock.info/artykul/cyberatak-na-urzad-miasta/1250396.
Coker J., *Local Government Organizations Most Frequently Targeted by Ransomware,* „Infosecurity Magazine" 2020, 20 VIII, [online] https://www.infosecurity-magazine.com/news/local-government-targeted/.
Dwa postępowania KE przeciwko Polsce. Chodzi o dyrektywę NIS2, „CyberDefence24", 28 XI 2024, [online] https://cyberdefence24.pl/polityka-i-prawo/dwa-postepowania-ke-przeciwko-polsce-chodzi-o-dyrektywe-nis2.
Informacja o wynikach kontroli NIK „System rejestrów państwowych – bezpieczeństwo, funkcjonowanie i użyteczność", Nr ewidencyjny: 208/2016/P/16/006/KAP, Najwyższa Izba Kontroli, Warszawa, 27 lutego 2017 r.
Informacja o wynikach kontroli NIK „Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu", Nr ewidencyjny: 205/2014/P/14/004/KAP, Najwyższa Izba Kontroli, Warszawa, 2 lutego 2015 r.
Informacja o wynikach kontroli NIK „Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu

terytorialnego”, Nr ewidencyjny: P/24/004, Najwyższa Izba Kontroli, Warszawa, luty 2025 r.
Informacja o wynikach kontroli NIK „Zapewnienie bezpieczeństwa teleinformatycznego przez jednostki samorządu terytorialnego województwa zachodniopomorskiego”, Nr ewidencyjny: I/23/001/LSZ, Najwyższa Izba Kontroli, Warszawa, 3 kwietnia 2024 r.
Informacja o wynikach kontroli NIK „Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego”, Nr ewidencyjny: 187/2018/P/18/006/KAP, Najwyższa Izba Kontroli, Warszawa, 18 lutego 2019 r.
Informacja o wynikach kontroli „Zarządzanie oprogramowaniem komputerowym przez administrację publiczną”, Nr ewidencyjny: 15/2023/P/22/082/LPO, Najwyższa Izba Kontroli, Warszawa, 29 kwietnia 2024 r.
Komunikaty. Incydent cyberbezpieczeństwa, „Biuletyn Informacji Publicznej Samorządu Województwa Mazowieckiego” 2022, 5 XII, [online] https://mazovia.pl/pl/bip/komunikaty/incydent-cyberbezpieczenstwa-1.html.
Konieczny P., *Złośliwy kabel USB, który zmienia się w klawiaturę i infekuje Twój komputer*, „Niebezpiecznik.pl” [online] 21 II 2019, https://niebezpiecznik.pl/post/zlosliwy-kabel-usb-ktory-zmienia-sie-w-klawiature-i-infekuje-twoj-komputer/.
Malinowski P., Mias*to na Florydzie zapłaci hakerom okup w bitcoinach,* „rp.pl” 2019, 20 VI, [online] https://cyfrowa.rp.pl/it/art16920091-miasto-na-florydzie-zaplaci-hakerom-okup-w-bitcoinach.
Mastalerz M., *Urząd miejski w Otwocku padł ofiarą cyberataku,* „Serwis Samorządowy PAP” 2021, 22 X, [online] https://samorzad.pap.pl/kategoria/e-urzad/urzad-miejski-w-otwocku-padl-ofiara-cyberataku.
Maziarz P., *Hakerzy zaszyfrowali bazy w Oświęcimiu – urzędnicy... obcięli środki na drogi,* „Benchmark.pl” 2021, 25 II, [online] https://www.benchmark.pl/aktualnosci/hakerzy-zaszyfrowali-bazy-w-oswieciumiu-kontrowersyjna-decyzja.html.
Merriam-Webster Dictionary, [online] https://www.merriam-webster.com/dictionary/cybersecurity.
NASK, *Cyberbezpieczny samorząd. Poradnik*, Warszawa 2023.
Narodowe Standardy Cyberbezpieczeństwa, Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa (wersja 1.0.), definicja pojęcia cyberbezpieczeństwo (cybersecurity), [online], https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber.
NIST Glossary, [online] https://csrc.nist.gov/glossary/term/cyber_resiliency.
Norma PN-EN ISO/IEC 27001:2023-08.
Palczewski Sz., *Ataki hakerskie na polskie samorządy. W co inwestować?,* „CyberDefence24” 2025, 2 IV, [online] https://cyberdefence24.pl/cyberbezpieczenstwo/ataki-hakerskie-na-polskie-samorzady-w-co-inwestowac.
Palczewski Sz., *Cyberatak na mazowiecki urząd. Wciąż są problemy z infrastrukturą,* „CyberDefence24” 2022, 16 XII, [online]

https://cyberdefence24.pl/cyberbezpieczenstwo/cyberatak-na-mazowiecki-urzad-wciaz-sa-problemy-z-infrastruktura.
Pawłowska M., *Oświęcim. Działacze PiS pytają, czy Starostwo Powiatowe zapłaciło okup za odblokowanie danych po ataku hakerskim,* „Oświęcim Nasze Miasto" 2021, 11 III, [online] https://oswiecim.naszemiasto.pl/oswiecim-dzialacze-pis-pytaja-czy-starostwo-powiatowe/ar/c15-8174297.
Pismo Ministra Cyfryzacji do Prezesa Najwyższej Izby Kontroli, syng.: BM.WN.0810.8.2025, Warszawa, 12 marca 2025 r.
Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa i niektórych innych ustaw, 24 IV 2024 [online] https://legislacja.rcl.gov.pl/projekt/12384504/katalog/13055195#13055195.
Przetarg w urzędzie na odszyfrowanie danych po ransomware? Zapłata w PLN nie BTC ;-) Bohater? System geodezyjno-kartograficzny w Oświęcimiu, „Sekurak" 2021, 21 II, [online] https://sekurak.pl/przetarg-w-urzedzie-na-odszyfrowanie-danych-po-ransomware-zaplata-w-pln-nie-btc-bohater-system-geodezyjno-kartograficzny-w-oswiecimiu/.
Sajdak M., *Grupa ransomware Play grozi ujawnieniem danych belgijskiego miasta Antwerpia. To najpewniej ta sama grupa, która zaatakowała Urząd Marszałkowski Mazowsze,* „Sekurak" 2022, 13 XII, [online] https://sekurak.pl/grupa-ransomware-play-grozi-ujawnieniem-danych-belgijskiego-miasta-antwerpia-to-najpewniej-ta-sama-grupa-ktora-zaatakowala-urzad-marszalkowski-mazowsze/.
Sajdak M., *Ransomware zaatakował Urząd Marszałkowski Województwa Mazowieckiego: zaszyfrowane dane systemu Elektronicznego Zarządzania Dokumentami (EZD) oraz innych systemów,* „Sekurak" 2022, 6 XII, [online] https://sekurak.pl/ransomware-zaatakowal-urzad-marszalkowski-wojewodztwa-mazowieckiego-zaszyfrowane-dane-systemu-elektronicznego-zarzadzania-dokumentami-ezd-oraz-innych-systemow/.
Sikorska M., *5 najgroźniejszych ataków ransomware w Polsce. Czy Twoja firma na pewno jest bezpieczna?* „Grandmetric", 2023, 4 IV [online] https://www.grandmetric.com/pl/5-najgrozniejszych-atakow-ransomware-w-polsce/.
Słownik Języka Polskiego, [online] https://sjp.pl/odporny.
Szturm na „Wrota Mazowsza". Atak ransomware na Urząd Marszałkowski Województwa Mazowieckiego! [Aktualizacja], „itWiz.pl" 2022, 5 XII, [online] https://www.itweek.pl/atak-ransomware-na-umwm/.
Why Local Governments Are Being Targeted by Cyber Attacks. And What You Can Do About It, Harris Local Governments, "Harris Local Government" 2021, 10 II, [online] https://www.harrislocalgov.com/why-local-government-are-being-attacked/.
Wojtczuk M., *Gigantyczny wyciek danych w Otwocku. Hakerzy wykradli PESEL-e i numery dowodów wszystkich mieszkańców,* „wyborcza.pl" 2022, 19 VII, [online] https://warszawa.wyborcza.pl/warszawa/7,54420,28700276,gigantyczny-wyciek-danych-w-otwocku-hakerzy-wykradli-pesele.html.
Wypowiedź Witolda Skomry doradcy w Rządowym Centrum Bezpieczeństwa, p.o. Szefa Wydziału Ochrony Infrastruktury Krytycznej na posiedzeniu Podkomisji stałej do spraw funkcjonowania zarządzania kryzysowego, Sejm

Rzeczypospolitej Polskiej X kadencji, 27 XI 2024 r. [online] https://www.sejm.gov.pl/sejm10.nsf/biuletyn.xsp?skrnr=ASW02S-7.
Wystąpienie pokontrolne P/15/003 – Świadczenie usług publicznych w formie elektronicznej na przykładzie wybranych jednostek samorządu terytorialnego, Nr ewidencyjny: KAP.410.004.02.2015, Najwyższa Izba Kontroli, Warszawa 2015.
Zachodniopomorskie gminy nieprzygotowane na cyberzagrożenia, Najwyższa Izba Kontroli, 2024, 3 IV, [online] https://www.nik.gov.pl/aktualnosci/zachodniopomorskie-gminy-cyberzagrozenia.html.
Zhakowano Urząd Marszałkowski Województwa Mazowieckiego, „CyberDefence24" 2022, 6 XII, [online] https://cyberdefence24.pl/cyberbezpieczenstwo/zhakowano-urzad-marszalkowski-wojewodztwa-mazowieckiego.

KEY ISSUES AND CHALLENGES IN BUILDING DIGITAL RESILIENCE AND CYBERSECURITY IN LOCAL GOVERNMENT UNITS IN POLAND – AN EMPIRICAL ANALYSIS IN THE LIGHT OF AUDIT FINDINGS

Abstract

The main objective of this article is to analyse – based on empirical data included in the findings of, among others, the Supreme Audit Office (NIK) – the level of cybersecurity and digital resilience of local government units in Poland. In recent years, cybersecurity has become the subject of intensive legislative work at both the EU and national levels. Since 2018, a number of legal provisions have been adopted to enhance cybersecurity across the state and its institutions. The legislation also covers other areas crucial from a security perspective, such as the financial market and entities forming critical infrastructure.

Keywords: Cybersecurity, digital resilience, local government.