ARTUR GAJOWNICZEK
ORCID: 0000-0002-8770-7089
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Społecznych

Wybrane aspekty funkcjonowania Krajowego Systemu Cyberbezpieczeństwa w jednostkach samorządu terytorialnego na przykładzie województwa mazowieckiego

Problematyka cyberbezpieczeństwa w jednostkach samorządu terytorialnego (JST) nabiera szczególnego znaczenia w kontekście rozwoju e-administracji. Pojawia się wiele platform o zasięgu regionalnym (Wrota Mazowsza, Wrota Podlasia) oraz ogólnopolskim (elektroniczna Platforma Usług Administracji Publicznej – e-PUAP), które służą mieszkańcom i przedsiębiorcom do załatwiania spraw administracyjnych drogą elektroniczną. Kontakt JST z organami administracji rządowej (wojewodami) i centralnymi (Zakładem Ubezpieczeń Społecznych, Urzędem Skarbowym) oraz wszelkie rozliczenia finansowe również odbywają się drogą elektroniczną[1]. Zakres świadczenia usług przez JST w cyberprzestrzeni oraz przekazywania i przetwarzania informacji w systemach teleinformatycznych na przestrzeni ostatnich 15 lat znacznie się zwiększył. Podwaliny budowy e-administracji w Polsce stanowiły akty prawne uchwalane w latach 2001–2005[2].

[1] Zob. P. Nadybski, *Elektroniczna administracja w Polsce – ograniczenia i bariery*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy" 2013, nr 9, s. 31-33.

[2] Akty prawne uchwalane w latach 2001-2005: Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych; Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym; Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej; Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną; Ustawa z dnia 12 września 2002 r. o elektronicznych instrumentach

W literaturze przedmiotu wskazywane są dwa najważniejsze akty normatywne tworzące podstawy e-administracji Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, która nałożyła na władze publiczne obowiązek udostępniania informacji publicznych oraz Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[3].

Jednocześnie JST stały się potencjalnym podmiotem ataków i włamań do zasobów gromadzonych w przestrzeni cyfrowej. Spowodowało to konieczność identyfikowania zagrożeń występujących w cyberprzestrzeni i stosowania skutecznych narzędzi przeciwdziałania na wypadek prób przełamania zabezpieczeń. W literaturze przedmiotu podkreślane są dwa aspekty zagrożenia informatycznego, w którym celem jest technologia informatyczna lub jest ona narzędziem oraz formy zagrożenia związanego z Internetem: włamania, wirusy, ataki konwencjonalne[4]. Natomiast o skali zagrożeń, jakie wiążą się z rozwojem i wykorzystaniem Internetu, świadczą statystyki publikowane przez zespół CERT (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego). W 2016 r. CERT Polska działający w NASK – Państwowym Instytucie Badawczym – obsłużył 1926 incydentów, tj. o 32% więcej niż w 2015 r. Do najczęściej zgłaszanych należą następujące kategorie incydentów: oszustwa komputerowe (55,5%), obraźliwe i nielegalne treści (12,31%), złośliwe oprogramowanie (10,96%), próby włamań (5,66%), gromadzenie informacji (3,37%), włamania (2,8%), dostępność zasobów (2,34%), atak na bezpieczeństwo informacji (2,34%), inne (4,72%). Dla przykładu phishing (podszywanie się pod znane marki celem wyłudzenia wrażliwych danych) był zgłaszany do CERT Polska 722 584 razy, a otrzymanych zgłoszeń dotyczących unikalnych adresów IP, które są narażone na ataki oraz wyciek informacji, było 1,8 miliona[5].

płatniczych; Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

[3] R. Perdał, *Czynniki rozwoju elektronicznej administracji w samorządzie lokalnym w Polsce*, Poznań 2014, s. 46-48.

[4] Zob. S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki – organizacji – państwa*, Warszawa 2016, s. 207-209.

[5] *Krajobraz bezpieczeństwa polskiego Internetu 2016. Raport roczny z działalności CERT Polska*, NASK, https://www.cert.pl/PDF/Raport_CP_2016.pdf [dostęp marzec 2018].

W literaturze przedmiotu często podkreślana jest zależność między bezpieczeństwem informacji, w tym w systemach teleinformatycznych, a bezpieczeństwem w szerokim znaczeniu – dla administracji publicznej i JST[6]. Bardzo ważnym aspektem prowadzenia aktywności w cyberprzestrzeni jest postęp technologiczny zarówno w zakresie sprzętowym, jak i wykorzystywanego oprogramowania. Brak reakcji na zmiany technologiczne w sferze sprzętowej lub uaktualnienia oprogramowania może powodować znaczące skutki dla bezpieczeństwa systemów teleinformatycznych. Zmiany w podejściu do omawianego zagadnienia widać szczególnie wyraźnie w ewolucji samej definicji cyberbezpieczeństwa, która na przestrzeni ostatnich lat zmieniała się w aktach prawnych i teorii bezpieczeństwa. Podobnie zmianom ulegał zakres podmiotowy tego pojęcia, który dotyczył początkowo tylko sektora bankowego i biznesowego oraz administracji rządowej, a w kolejnych latach obejmował inne podmioty, w tym JST[7].

W 2013 r., powstał pierwszy w Polsce strategiczny dokument w zakresie cyberbezpieczeństwa: Polityka ochrony cyberprzestrzeni RP. Zostały w nim zdefiniowane między innymi pojęcia: „bezpieczeństwo cyberprzestrzeni – jako zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych, mający na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni" oraz „cyberprzestrzeń RP (CRP) – cyberprzestrzeń w obrębie terytorium państwa polskiego i poza jego terytorium, w miejscach gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)"[8]. Cel strategiczny został określony w dokumencie jako osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa. Polityka została przyjęta uchwałą Rady Ministrów 25 czerwca 2013 r. i obowiązywała tylko administrację rządową. W 2017 r. została ona zastąpiona przez Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 (Krajowe Ramy)[9]. W dokumencie określono cztery cele, które wskazywały na potrzeby wynikające z rozbudowy Krajowego Systemu

[6] Zob. R. Cichocki, P. Jatkiewicz, *Bezpieczeństwo informacji w jednostkach samorządu terytorialnego*, „Roczniki Kolegium Analiz Ekonomicznych SGH" 2013, z. 99.

[7] Zob. D. Liszak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016.

[8] Definicje z Polityki ochrony cyberprzestrzeni, uchwała RM nr 111/2013 z dnia 25 czerwca 2013 r.

[9] Dokument został przyjęty 9 maja 2017 r. uchwałą Rady Ministrów nr 52/2017. Polityka ochrony cyberprzestrzeni RP, https://cyberpolicy.nask.pl/polityka-ochrony-cyberprzestrzeni-rp/ [dostęp 27.03.2020].

Cyberbezpieczeństwa. Pierwszy dotyczył osiągnięcia zdolności do skoordynowanego działania w skali kraju, które pozwoli zapobiegać, wykrywać, zwalczać oraz minimalizować skutki incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa. Kolejny cel zakładał wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom. Trzeci cel związany był ze zwiększaniem potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni. Ostatni z celów wymienionych w Krajowych Ramach zmierzał do zbudowania silnej pozycji międzynarodowej Polski w obszarze cyberbezpieczeństwa[10]. W Krajowych Ramach pojawiła się następująca definicja cyberbezpieczeństwa: „odporność systemów teleinformatycznych, 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 przez te sieci i systemy informatyczne”[11]. Krajowe Ramy zostały również ustanowione tylko dla administracji rządowej: na pięć lat.

22 października 2019 r. Rada Ministrów przyjęła uchwałę w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (strategii cyberbezpieczeństwa)[12]. Dokument obowiązuje od 31 października 2019 r. i zastąpił Krajowe Ramy. Podstawa prawna przyjęcia strategii cyberbezpieczeństwa wynika z art. 68 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (ustawa o krajowym systemie)[13]. Głównym celem przyjęcia i wdrożenia strategii cyberbezpieczeństwa jest podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym, a także promowanie dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.

[10] Zob. M. Wrzosek, *Krajowe ramy polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, https://cyberpolicy.nask.pl/rb-dokumenty-krajowe-2-krajowe-ramy-polityki-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/ [dostęp 12.12.2019].

[11] Uchwała nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.

[12] Uchwała Nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M.P. z 2019 r., 1037).

[13] Ustawa z dnia 5 lipca 2018 r.o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560).

W obecnie obowiązującym stanie prawnym w art. 2 ustawy o krajowym systemie została zawarta definicja cyberbezpieczeństwa oznaczająca „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”[14]. W literaturze przedmiotu znajdujemy wiele definicji tego pojęcia, w ocenie autora najbardziej trafna jest szersza definicja zawierająca nie tylko sprawy ochrony skuteczności zabezpieczeń technicznych infrastruktury informacyjnej, ale również aspekt np. organizacyjny: „cyberbezpieczeństwo – proces, na który składają się działania podejmowane przy pomocy środków technicznych i nietechnicznych dla ochrony cyberprzestrzeni, w tym urządzeń, oprogramowania oraz informacji lub danych”[15].

Ustawa o krajowym systemie jest wdrożeniem do polskiego porządku prawnego Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. Dyrektywa NIS)[16]. Zobowiązuje ona państwa członkowskie do zagwarantowania minimalnego poziomu cyberbezpieczeństwa poprzez ustanowienie organów właściwych oraz pojedynczych punktów kontaktowych do spraw cyberbezpieczeństwa, powołanie zespołów reagowania na incydenty komputerowe (CSIRT) oraz przyjęcie krajowych strategii w zakresie cyberbezpieczeństwa[17].

Ustawa o krajowym systemie usankcjonowała trzy podmioty na poziomie krajowym, które zajmują się reagowaniem na incydenty komputerowe i zarządzanie nimi. Są to CSIRT GOV, CSIRT MON, CSIRT NASK[18]. Obsługą incydentów

[14] Ustawa z dnia 5 lipca 2018 r., o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560 ze zm.).

[15] *Vademecum bezpieczeństwa*, red. O. Wasiuta, R. Klepka, R. Kopeć, Kraków 2018, s. 223.

[16] Dz.Urz. UE L 194/1 z 2016 r.

[17] M. Sławińska, *Rok funkcjonowania ustawy o krajowym systemie cyberbezpieczeństwa – najważniejsze postanowienia i rozwiązania,* https://rcb.gov.pl/rok-funkcjonowania-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-najwazniejsze-postanowienia-i-rozwiazania/ [dostęp 27.04.2020].

[18] CSIRT GOV – prowadzony jest przez Agencję Bezpieczeństwa Wewnętrznego. Główne zadania CSIRT GOV to: rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych, z punktu widzenia ciągłości funkcjonowania państwa, systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej,

zgłaszanych przez JST jest CSIRT NASK prowadzony przez Naukową i Akademicką Sieć Komputerową. Zespoły CSIRT zapewniają spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym – są w europejskiej sieci CSIRT oraz przekazują do innych Państw i innych Punktów Kontaktowych informacje o incydentach. Zespołowi CERT Polska zostały powierzone obowiązki CSIRT NASK wynikające z ustawy o krajowym systemie. Podstawowe obowiązki wskazane w tej ustawie dla JST to wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa, szkolenie osób z cyberbezpieczeństwa w tym identyfikacji zagrożeń oraz zgłaszanie i obsługa incydentów będących zdarzeniami mającymi niekorzystny wpływ na cyberbezpieczeństwo[19]. Wagę tematu identyfikacji zagrożeń pokazuje przykład znaczącego incydentu, który miał miejsce w Holandii. Latem 2011 r. holenderski system zabezpieczeń informatycznych organu certyfikującego DigiNotar został poważnie naruszony, umożliwiając atakującym wygenerowanie fałszywych certyfikatów autentyczności. Przykład ilustruje naturę jednego z najpoważniejszych rodzajów utraty integralności urzędowego systemu certyfikacji[20].

a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej. CSIRT GOV zobowiązany jest do koordynacji incydentów zgłaszanych przez następujące podmioty: organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały; ZUS, KRUS, NFZ; Narodowy Bank Polski, Bank Gospodarstwa Krajowego. CSIRT MON – prowadzony przez Ministerstwo Obrony Narodowej. CSIRT MON zobowiązany jest do koordynacji incydentów zgłaszanych przez następujące podmioty: podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej; przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa jest Minister Obrony Narodowej. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT), https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt [dostęp 16.03.2020].

[19] CSIRT NASK, www.cert.gov.pl [dostęp 14.03.2020].

[20] Fałszywe certyfikaty, będące wynikiem naruszenia, zostały wykorzystane do podsłuchu komunikacji online setek tysięcy obywateli. Po naruszeniu wiele rządowych stron internetowych w Holandii było niedostępnych i uznanych za niebezpieczne. Rząd przejął zarządzanie operacyjne systemami DigiNotar, a sama firma wkrótce ogłosiła upadłość. Również utrata klucza prywatnego dowolnego rodzaju certyfikatu cyfrowego oznacza natychmiastowe unieważnienie danego certyfikatu. Szkodliwe ataki mogą wpływać na wszystkie rodzaje wyżej wymienionych usług zaufania

Zebrane dane ponad rok od wdrożenia ustawy o krajowym systemie (ustawa weszła w życie 28 sierpnia 2018 r.), dają możliwość podsumowania funkcjonowania systemu cyberbezpieczeństwa w Polsce przez podmioty do tego zobowiązane, w tym JST[21]. W literaturze przedmiotu zagadnienie funkcjonowania Krajowego Systemu Cyberbezpieczeństwa w JST jest nadal w niewielkim stopniu zbadane i opisane. Celem ogólnym badań prowadzonych przez autora od czerwca do sierpnia 2019 było bezpieczeństwo informacyjne, w tym ocena wdrożenia e-administracji i zapisów ustawy o krajowym systemie w jednostkach samorządowych na Mazowszu. Województwo mazowieckie zostało wybrane jako teren przeprowadzenia badań, ponieważ pod kątem poziomu innowacyjności jest jednym z najprężniej rozwijających się regionów w Polsce oraz umiarkowanym innowatorem wśród krajów Unii Europejskiej[22]. Jednocześnie system Elektronicznego Zarządzania Dokumentacją EZD wykorzystywało 59,6% ogółu urzędów w województwie mazowieckim, co spowodowało umieszczenie go na 7 pozycji w zestawieniu 16 województw[23]. Średnia stopa relatywnego ubóstwa w 2017 r.

i obejmować szereg usług, takich jak podpisy elektroniczne, znaczniki czasu i uwierzytelnianie witryn internetowych. Obecnie uwierzytelnianie strony internetowej, które pozwala użytkownikom zweryfikować autentyczność strony internetowej i powiązać osobę prawną ze stroną internetową, staje się dość powszechne. Źródło: *Implementation of article 15, of the draft regulation on electronic identification and trusted services for electronictransactions in the internal market*, s. 7-8 www.enisa.europa.eu, tłum. własne [dostęp 17.11.2019].

[21] Ustawa o krajowym systemie cyberbezpieczeństwa wprowadziła pojęcie systemu cyberbezpieczeństwa, który „ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych, służących do świadczenia tych usług oraz zapewnienie obsługi incydentów". Art. 2 pkt 4, Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560).

[22] Poziom innowacyjności – złożony wskaźnik opracowywany przez Komisję Europejską, na podstawie którego kraje UE sklasyfikowane są w czterech grupach w zależności od poziomu wskaźnika względem średniej unijnej: liderzy innowacji (powyżej 120% średniej unijnej), kraje doganiające (90-120%), umiarkowani innowatorzy (50-90%), słabi innowatorzy (poniżej 50%) Na podstawie *Atlasu statystycznego województwa mazowieckiego*, http://warszawa.stat.gov.pl/publikacje-i-foldery/inne-opracowania/atlas-statystyczny-wojewodztwa-mazowieckiego,28,1.html [dostęp 07.12.2018].

[23] *Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2013–2017*, https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/1/11/1/spoleczenstwo_informacyjne_w_polsce._wyniki_badan_statystycznych_z_lat_2013-2017.pdf [dostęp 15.12.2018].

mieszkańców województwa mazowieckiego wynosiła 10%[24], z czego dla Warszawy wynosiła ona 6%, dla podregionu warszawskiego zachodniego ok 10%, dla podregionu warszawskiego wschodniego – 14% i dla podregionów peryferyjnych aż 21-26% w stosunku do średniej stopy relatywnego ubóstwa w całym kraju – na poziomie 17,7%; województwo mazowieckie stanowi więc próbę reprezentatywną[25]. Reasumując, podobnie jak w całej Polsce, w województwie mazowieckim jest pełno dysproporcji i kontrastów, zarówno pod względem rozwoju gospodarczego poszczególnych gmin, jak i zaludnienia oraz ubóstwa. Właśnie te cechy decydują o tym, że jest to optymalny teren badawczy dla zakresu tematycznego dotyczącego sfery bezpieczeństwa w cyberprzestrzeni.

Badanie zostało przeprowadzone w formie elektronicznej, żeby zapewnić respondentom anonimowość udzielania odpowiedzi[26]. Na podstawie ustawy o dostępie do informacji publicznej został skierowany wniosek do samorządów z województwa mazowieckiego o udzielenie informacji publicznej[27]. Jednostki administracji publicznej mają ustawowy obowiązek udzielić odpowiedzi w ciągu 14 dni od otrzymania wniosku w określonej we wniosku formie.

Sondażem diagnostycznym objęto próbę reprezentatywną dla Polski, zawierającą wszystkie JST na Mazowszu. Wysłano ankietę za pomocą systemu e-PUAP do 37 powiatów (zwanych dalej powiatem ziemskim) i 5 miast na prawach powiatu (zwanych dalej powiatem miejskim), 35 gmin miejskich, 53 gmin miejsko-wiejskich i 226 gmin wiejskich. Odpowiedzi udzieliło 71% procent respondentów, z czego otrzymano z powiatów ziemskich 54% (20 sztuk ankiet) i z miast na prawach powiatu 60% (tj. 3 ankiety). Najwięcej wypełnionych ankiet otrzymano z gmin miejskich (aż 91%, czyli 32 ankiety). Na wysokim poziomie

[24] Coraz mniej mieszkańców Mazowsza żyje w ubóstwie, https://warszawa.stat.gov.pl/dla-mediow/informacje-prasowe/coraz-mniej-mieszkancow-mazowsza-zyje-w-ubostwie,151,1.html [dostęp 01.06.2019].

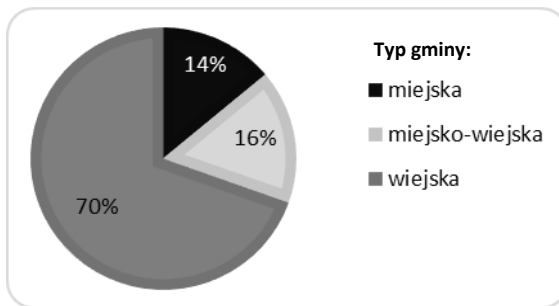
[25] Kancelaria Senatu, *Zróżnicowanie województwa mazowieckiego pod względem historycznym, demograficznym i warunków życia. Korekty do podziału terytorialnego kraju*, https://www.senat.gov.pl/gfx/senat/pl/senatekspertyzy/3842/plik/oe-256-internet.pdf [dostęp 02.01.2019].

[26] We wniosku o udzielenie informacji publicznej skierowanym do JST znajdował się link do adresu www portalu e-Badania, gdzie została przygotowana ankieta zawierająca pytania zamknięte i otwarte.

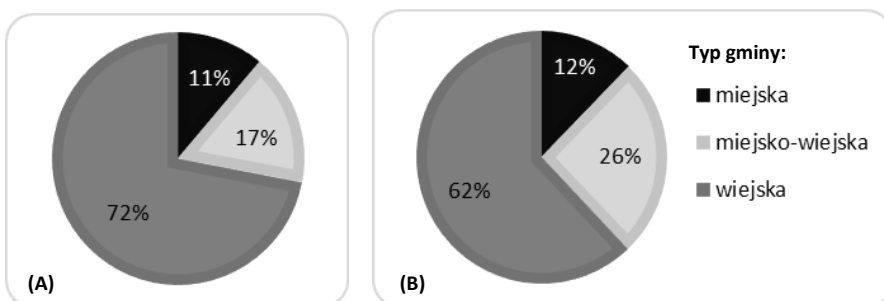
[27] Ustawa z dnia z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2018 r., poz. 1330).

prezentuje się odsetek respondentów z gmin miejsko-wiejskich (prawie 72%, tj. 38 ankiet) i gmin wiejskich (prawie 71%, czyli 160 ankiet). Część JST nie wypełniła ankiety, argumentując, że treść zadawanych pytań nie stanowi informacji publicznej.

Udział procentowy respondentów z poszczególnych gmin jest zbliżony do udziału procentowego gmin na Mazowszu, co oznacza, że zebrane dane są reprezentatywne dla całego województwa. Na rysunkach 1 i 2 zestawiono udział respondentów z poszczególnych typów gmin objętych badaniem z procentowym udziałem typów gmin na Mazowszu i w kraju.



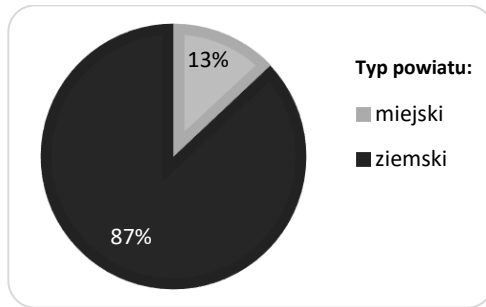
Rys. 1. Udział procentowy respondentów z poszczególnych typów gmin objętych badaniem
Źródło: opracowanie własne



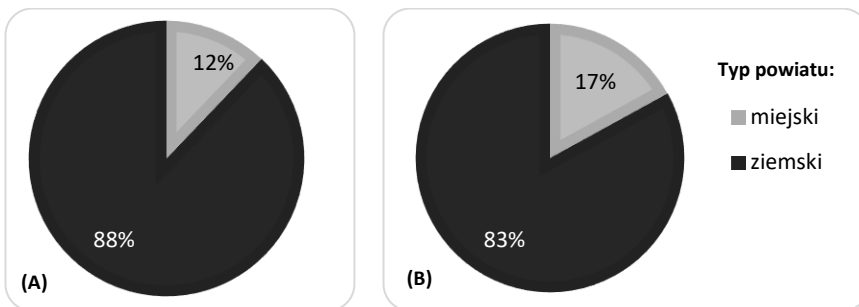
Rys. 2. Typy gmin na Mazowszu (A) i w Polsce (B) w ujęciu procentowym
Źródło: opracowanie własne

Podobne wnioski można wyciągnąć, obserwując dane na poziomie powiatu. Również w tym przypadku badana próba jest reprezentatywna dla całego województwa (różnica na poziomie 1%). Z kolei różnica 4 punktów procentowych dotyczy powiatów ziemskich i miejskich w skali Polski w porównaniu do próby

badawczej. Na rysunkach 3 i 4 przedstawiono porównanie rozkładu poszczególnych typów powiatów (ziemski i miejski) na Mazowszu i w Polsce z udziałem procentowym respondentów uczestniczących w badaniu sondażowym z poszczególnych powiatów.

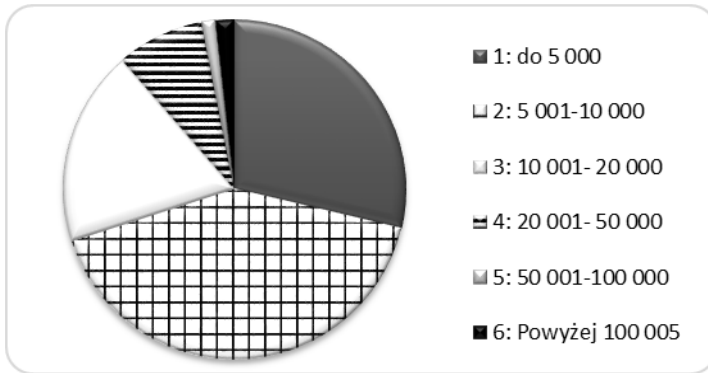


Rys. 3. Udział procentowy respondentów z poszczególnych typów powiatów objętych badaniem
Źródło: opracowanie własne



Rys. 4. Typy powiatów na Mazowszu (A) i w Polsce (B) w ujęciu procentowym
Źródło: opracowanie własne

Ankieta zasadniczo składała się z pytań zamkniętych, przy czym w niektórych przypadkach wybór określonej odpowiedzi wiązał się z możliwością jej uzupełnienia i rozwinięcia. Pierwsze trzy pytania dotyczyły identyfikacji rodzaju JST, jej cech i liczby mieszkańców (rysunek 5). Wśród badanych gmin dominują jednostki z relatywnie niedużą liczbą mieszkańców od 5 001 do 10 000 (41% ogółu) oraz do 5 000 (29% próby). W dziewiętnastu badanych jednostkach mieszka od 20 001 do 50 000 mieszkańców (8% całości). Najbardziej liczebne gminy, tj. takie, których liczba mieszkańców mieści się w zakresie od 50 001 do 100 000 (9% ogółu) i powyżej 100 000 (13% ogółu), stanowiły w badaniu najmniejszą grupę.



Rys.5. Liczba mieszkańców w gminach objętych badaniem [%]
Źródło: opracowanie własne

Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa jednym z podstawowych obowiązków JST jest zgłaszanie incydentów, czyli zdarzeń, które mają lub mogą mieć niekorzystny wpływ na odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[28]. Kolejnym obowiązkiem JST jest wyznaczenie w jednostce osoby do kontaktów z CSIRT-NASK oraz współpraca z CSIRT-NASK. Tego problemu dotyczyły w ankiecie następujące pytania:

- Czy w JST lub podległych jednostkach organizacyjnych w ostatnich 15 latach były próby przełamania zabezpieczeń sieci wewnętrznej w celu pozyskania danych (informacji) zlokalizowanych na serwerach JST?
- Czy w JST lub podległych jednostkach organizacyjnych w ostatnich 15 latach były przypadki włamań do sieci w celu kradzieży lub zablokowania danych (informacji) zlokalizowanych na serwerach JST?
- Czy JST poniosła straty finansowe związane z tymi włamaniami?
- Czy w JST i podległych jednostkach organizacyjnych wyznaczona jest osoba lub wyznaczone są osoby do kontaktu z CSIRT-NASK (Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzonym przez Naukową i Akademicką Sieć Komputerową)?
- Czy JST korzysta ze wsparcia CSIRT-NASK w zakresie bezpieczeństwa informacyjnego?

[28] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560 ze zm.).

Celem szczegółowym badań prowadzonych przez autora było ustalenie zakresu monitorowania przez JST prób przełamania zabezpieczeń lub włamań do sieci wewnętrznej (wyniki w tabelach od 1 do 6) oraz sprawdzenie realizacji współpracy z CSIRT-NASK (wyniki w tabelach od 7 do 11).

Tabela 1. Podsumowanie liczby odpowiedzi na pytanie ankiety własnej dotyczące wystąpienia prób przełamania zabezpieczeń sieci wewnętrznej w celu pozyskania danych (informacji) zlokalizowanych na serwerach JST w ciągu ostatnich 15 lat

Jednostka samorządu terytorialnego	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
gmina miejska	32	0	0	3	9,37	29	90,63
gmina wiejska	160	0	0	8	5,00	152	95,00
gmina miejsko-wiejska	38	0	0	2	5,26	36	94,74
powiat ziemski	20	0	0	1	5,00	19	95,00
powiat miejski	3	0	0	0	0	3	100,00
Liczba mieszkańców jednostki	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
do 5000	66	0	0	3	4,55	63	95,45
5001–10 000	95	0	0	3	3,16	92	96,84
10 001–20 000	43	0	0	4	9,30	39	90,70
20 001–50 000	25	0	0	4	16,00	21	84,00
50 001–100 000	13	0	0	0	0	13	100
powyżej 100 000	11	0	0	0	0	11	100

n – liczba obserwacji; *N* – liczba odpowiedzi Źródło: opracowanie własne

Tabela 2. Podsumowanie odpowiedzi na pytanie ankiety własnej dotyczące prób przełamania zabezpieczeń sieci wewnętrznej w celu pozyskania danych (informacji) zlokalizowanych na serwerach JST w ciągu ostatnich 15 lat

Jednostka samorządu terytorialnego	**Rodzaj zagrożeń, jakie wystąpiły**
gmina miejska	skanowanie portów, koń trojański
gmina wiejska	e-mail z niebezpiecznym załącznikiem (3), przelew środków na koncie gminy, włamanie na router główny, phishing, próba logowania z zewnątrz;
gmina miejsko-wiejska	e-mail z niebezpiecznym załącznikiem
powiat ziemski	--
powiat miejski	--

Źródło: opracowanie własne

Tabela 3. Podsumowanie liczby odpowiedzi na pytanie ankiety własnej dotyczące wystąpienia przełamania zabezpieczeń sieci wewnętrznej (włamań do sieci) w celu kradzieży lub zablokowania danych w ciągu ostatnich 15 lat

Jednostka samorządu terytorialnego	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
gmina miejska	32	0	0	3	9,37	29	90,63
gmina wiejska	160	1	0,62	6	3,75	153	95,63
gmina miejsko-wiejska	38	0	0	1	2,63	37	97,37
powiat ziemski	20	1	5,00	1	5,00	18	90,00
powiat miejski	3	0	0	0	0	3	100,00
Liczba mieszkańców jednostki	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
do 5000	66	0	0	2	3,03	64	96,97
5001–10 000	95	0	0	3	3,16	92	96,84
10 001–20 000	43	1	2,33	1	2,33	41	95,34
20 001–50 000	25	1	4	5	20,00	19	76,00
50 001–100 000	13	0	0	0	0	13	100,00
powyżej 100 000	11	0	0	0	0	11	100,00

n – liczba obserwacji; *N* – liczba odpowiedzi Źródło: opracowanie własne

Tabela 4. Podsumowanie odpowiedzi na pytanie ankiety własnej dotyczące wystąpienia przełamania zabezpieczeń sieci wewnętrznej (włamań do sieci) w celu kradzieży lub zablokowania danych w ciągu ostatnich 15 lat

Jednostka samorządu terytorialnego	**Rodzaj zagrożeń jakie wystąpiły** (liczba podobnych)
gmina miejska	wirus, wiadomość e-mail z BitLockerem
gmina wiejska	zaszyfrowanie plików, danych (4), logowanie na router główny, atak DDOS, wiadomość e-mail z niebezpiecznymi plikami
gmina miejsko-wiejska	wirus szyfrujący
powiat ziemski	zaszyfrowanie danych przez ransomware
powiat miejski	--

Źródło: opracowanie własne

Tabela 5. Podsumowanie liczby odpowiedzi na pytanie ankiety własnej dotyczące poniesionych strat finansowych związanych z włamaniami do sieci wewnętrznej w ciągu ostatnich 15 lat

Jednostka samorządu terytorialnego	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
gmina miejska	32	0	0	0	0	1	3,13
gmina wiejska	160	1	0,72	0	0	2	1,15
gmina miejsko-wiejska	38	1	2,63	0	0	0	0
powiat ziemski	20	1	5,00	0	0	0	0
powiat miejski	3	0	0	0	0	0	0
Liczba mieszkańców jednostki	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
do 5000	66	0	0	0	0	1	1,52
5001–10 000	95	1	1,06	0	0	1	1,05
10 001–20 000	43	1	2,33	0	0	0	0
20 001–50 000	25	1	4,00	0	0	0	0
50 001–100 000	13	0	0	0	0	0	0
powyżej 100 000	11	0	0	0	0	1	9,09

n – liczba obserwacji; *N* – liczba odpowiedzi Źródło: opracowanie własne

Tabela 6. Podsumowanie odpowiedzi badanych podmiotów na pytania dotyczące prób lub przełamania zabezpieczeń oraz poniesionych strat z powodu włamań w ciągu ostatnich 15 lat

Jednostka samorządu terytorialnego	**N**	**Brak odpowiedzi**	**Próby włamań**	**Dokonane włamania**	**Poniesione straty**
gmina miejska	32	0	3	3	0
gmina wiejska	160	0	8	6	0
gmina miejsko-wiejska	38	0	2	1	0
powiat ziemski	20	0	1	1	0
powiat miejski	3	0	0	0	0
Liczba mieszkańców jednostki	**N**	**Brak odpowiedzi**	**Próby włamań**	**Dokonane włamania**	**Poniesione straty**
do 5000	66	0	3	2	0
5001–10 000	95	0	3	3	0
10 001–20 000	43	0	4	1	0
20 001–50 000	25	0	4	5	0
50 001–100 000	13	0	0	0	0
powyżej 100 000	11	0	0	0	0

N – liczba odpowiedzi Źródło: opracowanie własne

Podsumowując wyniki badań związanych z monitorowaniem przez JST prób przełamania zabezpieczeń sieci wewnętrznej lub włamań do sieci wewnętrznej (wyniki w tabelach od 1 do 6) stwierdza się, że aż 9,37% badanych gmin miejskich, 5% gmin wiejskich i powiatów ziemskich oraz 5,26% gmin miejsko-wiejskich odnotowało próby przełamania zabezpieczeń sieci wewnętrznych swoich urzędów. Powiaty miejskie nie odnotowały takiego przypadku. Najwięcej zdarzeń miało miejsce w JST, gdzie liczba mieszkańców mieści się w przedziale między 20 001 a 50 000 mieszkańców – 16%. W JST w przedziałach między 50 001 a 100 000 mieszkańców i więcej nie odnotowano żadnej próby przełamania zabezpieczeń. Z kolei incydenty przełamania zabezpieczeń sieci wewnętrznych odnotowano w 9,37% gmin miejskich, 3,75% gmin wiejskich, 5% powiatów ziemskich oraz 2,63% gmin miejsko-wiejskich. Powiaty miejskie nie odnotowały takiego przypadku. Najwięcej zdarzeń (20%) miało miejsce w JST, gdzie liczba mieszkańców jest w przedziale między 20 001 a 50 000 mieszkańców. W JST w przedziałach między 50 001 a 100 000 mieszkańców i więcej nie odnotowano żadnej próby przełamania zabezpieczeń. Żaden z respondentów nie potwierdził poniesienia strat finansowych (było kilka odpowiedzi „brak rejestru"). Wyniki badań jakościowych prowadzonych przez autora (tabela 2 i 4) dotyczących rodzajów zdiagnozowanych zagrożeń (incydentów) mieści się w katalogu incydentów zaprezentowanych w Raporcie rocznym z działalności CERT Polska 2018 pod typami incydentów: obraźliwe i nielegalne treści, spam, dyskredytacja, obrażanie, niesklasyfikowane, złośliwe oprogramowanie, robak sieciowy, koń trojański, oszustwa komputerowe, dialer, próby włamań, próby nieuprawnionego logowania, podatne usługi, phishing, włamania, nieuprawniony dostęp, inne[29].

Porównując statystyki incydentów w Internecie odnotowywanych przez CERT z wynikami ankiety, można wysunąć hipotezę, że jest bardzo mało prawdopodobne, że JST, działając przez 15 lat w cyberprzestrzeni, nie zanotowały żadnych prób przełamania lub włamania do systemu zabezpieczeń sieci informatycznej. Wyniki badań wskazują, że systemy informatyczne JST w sposób niedostateczny są monitorowane i zabezpieczane. Jednocześnie włamanie do systemu JST zawsze będzie generowało straty finansowe (np. wymiana serwera, strony BIP lub

[29] Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2018 r., https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf [dostęp 07.01.2020].

audyt sprawdzający), a brak wykazania w ankiecie strat, oznaczać może, że zostały pokryte w inny, niepowiązany ze zdarzeniem, sposób. Przyczyną takiego działania samorządów może być fakt, że przyznając się do poniesionych strat finansowych, związanych z przełamaniem zabezpieczeń systemów informatycznych, mogłyby narazić się na zarzut niegospodarności majątkiem publicznym i narażeniem na straty majątkowe, które stanowią naruszenie dyscypliny finansów publicznych. Natomiast pracownicy komórek IT w JST mogliby narazić się na zarzut niedopełnienia obowiązków służbowych. Dlatego istnieje duże prawdopodobieństwo, że straty finansowe w JST z powodu przełamania systemów są dużo większe, ale ze względu na konsekwencje prawne są ukrywane.

Tabela 7. Podsumowanie liczby odpowiedzi na pytanie ankiety własnej dotyczące wyznaczenia osoby do kontaktu z CSIRT-NASK w obrębie jednostki

Jednostka samorządu terytorialnego	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
gmina miejska	32	0	0	8	25,00	24	75,00
gmina wiejska	160	1	0,62	34	21,25	125	78,13
gmina miejsko-wiejska	38	0	0	17	44,74	21	55,26
powiat ziemski	20	2	10,00	11	55,00	7	35,00
powiat miejski	3	0	0	0	0	3	100,00
Liczba mieszkańców jednostki	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
do 5000	66	1	1,51	8	12,12	57	86,36
5001–10 000	95	0	0	26	27,37	69	72,63
10 001–20 000	43	0	0	11	25,58	32	74,42
20 001–50 000	25	0	0	15	60,00	10	40,00
50 001–100 000	13	1	7,70	6	46,15	6	46,15
powyżej 100 000	11	1	9,09	4	36,36	6	54,55

n – liczba obserwacji; *N* – liczba odpowiedzi Źródło: opracowanie własne

Tabela 8. Podsumowanie odpowiedzi na pytanie ankiety własnej dotyczące wyznaczenia osoby do kontaktu z CSIRT-NASK w obrębie jednostki

Jednostka samorządu terytorialnego	**Podstawa do wyznaczenia osoby do kontaktu** (liczba podobnych)
gmina miejska	- zarządzenie 11/19 - zarządzenie 173.2019 - wyznaczenie - pracownik urzędu - pismo kierownika jednostki
gmina wiejska	- wyznaczony, wybór osób decyzyjnych, powołanie, zgłoszenie pracownika (6) - zarządzenie Wójta Gminy (5) - wyznaczony przez Wójta Gminy (3) - stanowisko do ochrony danych osobowych - firma zewnętrzna - Inspektor Bezpieczeństwa Informacji - elektroniczna - zatrudniony informatyk
gmina miejsko-wiejska	- zarządzenie burmistrza (5) - wyznaczenie pracownika (2) - zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa - w trakcie opracowywania
powiat ziemski	- zarządzenie starosty (4) - osoba wskazana - AS.212.25.2019
powiat miejski	--

Źródło: opracowanie własne

Tabela 9. Podsumowanie odpowiedzi na pytanie ankiety własnej dotyczące korzystania ze wsparcia CSIRT-NASK w zakresie bezpieczeństwa informacyjnego

Jednostka samorządu terytorialnego	**Rodzaj wykorzystania wsparcia**
gmina miejska	wykorzystanie wiedzy, wykorzystanie procedur, wykorzystanie instrukcji NASK
gmina wiejska	wykorzystanie wiedzy
gmina miejsko-wiejska	--
powiat ziemski	--
powiat miejski	--

Źródło: opracowanie własne

Tabela 10. Podsumowanie liczby odpowiedzi na pytanie ankiety własnej dotyczące korzystania ze wsparcia CSIRT-NASK w zakresie bezpieczeństwa informacyjnego

Jednostka samorządu terytorialnego	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
gmina miejska	32	0	0	4	12,5	28	87,5
gmina wiejska	160	0	0	3	1,88	157	98,12
gmina miejsko-wiejska	38	0	0	0	0	38	100,00
powiat ziemski	20	2	10	0	0	18	90,00
powiat miejski	3	0	0	0	0	3	100,00
Liczba mieszkańców jednostki	***N***	**Brak odpowiedzi**		**Tak**		**Nie**	
		n	%	*n*	%	*n*	%
do 5000	66	0	0	1	1,52	65	98,48
5001–10 000	95	0	0	2	2,11	93	97,89
10 001–20 000	43	0	0	2	4,65	41	95,35
20 001–50 000	25	0	0	1	4,00	24	96,00
50 001–100 000	13	1	7,69	0	0	12	92,31
powyżej 100 000	11	1	9,09	1	9,09	9	81,82

n – liczba obserwacji; *N* – liczba odpowiedzi Źródło: opracowanie własne

Uzyskane odpowiedzi przedstawicieli JST na temat ich współpracy z CSIRT-NASK poddano ocenie wartościującej (tabela 11). Pozytywnie oceniono odpowiedzi świadczące o prawidłowej współpracy. Negatywnie oceniono braki odpowiedzi i odpowiedzi świadczące o braku współpracy. Za nieprecyzyjne uznano odpowiedzi niepełne, świadczące o mankamentach tej współpracy. Najwięcej negatywnych odpowiedzi dotyczących nieprawidłowości w tym zakresie odnotowano w gminach wiejskich (aż 88,4%) i gminach miejskich (81,25%), a także w gminach z małą liczbą mieszkańców (93,2%). Pozytywną ocenę uzyskało najwięcej powiatów ziemskich (18,4%) oraz gmin ze średnią (16%) i dużą liczbą mieszkańców (24%).

Tabela 11. Podsumowanie liczbowe i procentowe odpowiedzi badanych podmiotów na grupę pytań dotyczących współpracy JST z CSIRT-NASK

Jednostka samorządu terytorialnego	***N***	**Negatywna**		**Pozytywna**		**Nieprecyzyjna**	
		n	%	*n*	%	*n*	%
gmina miejska	64	52	81,25	9	14,10	3	4,65
gmina wiejska	320	283	88,40	22	6,90	15	4,70
gmina miejsko-wiejska	76	59	77,63	9	11,84	8	10,53
powiat ziemski	38	27	71,10	7	18,40	4	10,5
powiat miejski	6	6	100	0	0	0	0
Liczba mieszkańców jednostki	***N***	**Negatywna**		**Pozytywna**		**Nieprecyzyjna**	
		n	%	*n*	%	*n*	%
do 5000	132	123	93,2	7	5,3	2	1,5
5001–10 000	190	162	85,3	16	8,4	12	6,3
10 001–20 000	86	73	84,9	8	9,3	5	5,8
20 001–50 000	50	34	68	8	16	8	16
50 001–100 000	25	19	76	6	24	0	0
powyżej 100 000	22	17	77,3	2	9,1	3	13,6

n – liczba obserwacji; *N* – liczba odpowiedzi Źródło: opracowanie własne

Podsumowując wyniki badań własnych, związanych ze współpracą z CSIRT-NASK, warto podkreślić, że 55% powiatów ziemskich, 44,74% gmin miejsko-wiejskich, 25% gmin miejskich oraz 21,25% gmin wyznaczyło osoby do kontaktu z CSIRT-NASK. Żaden powiat miejski nie wyznaczył osoby do kontaktu. Najczęściej osoby do kontaktu wyznaczały gminy, w których liczba mieszkańców mieści się w przedziale 5001–10000 mieszkańców, najrzadziej zaś te, w których mieszka do 5000 obywateli. Współpracę z CSIRT-NASK deklaruje jedynie 12,5% gmin miejskich i 1,88% gmin wiejskich. Gminy miejsko-wiejskie, powiaty miejskie i ziemskie nie korzystały ze wsparcia lub nie udzieliły odpowiedzi. Niepokojący jest fakt braku realizacji obowiązku wyznaczenia osoby do kontaktów oraz zakres współpracy JST z CSIRT-NASK. Szczególnie negatywnie wypadają powiaty miejskie (100% odpowiedzi negatywnych) oraz gminy wiejskie (88,4% odpowiedzi negatywnych).

Podsumowanie

W maju 2019 r. Najwyższa Izba Kontroli (NIK) opublikowała informację o wynikach kontroli: „Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego”[30]. W podsumowaniu NIK negatywnie ocenił wykonywanie przez blisko 70% skontrolowanych urzędów jednostek samorządu terytorialnego zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji w okresie objętym kontrolą. W 61% skontrolowanych urzędów brak było systemowego podejścia do zapewnienia bezpieczeństwa informacji. W 74% badanych urzędów brak było pełnej i aktualnej informacji o posiadanych zasobach informatycznych służących do przetwarzania danych, co w przypadku wystąpienia poważnej awarii lub innego zdarzenia losowego (zalanie, pożar, kradzież), może znacząco utrudnić szybkie odtworzenie infrastruktury i zapewnienie ciągłości świadczenia usług dla obywateli. W wielu skontrolowanych urzędach JST nie dostrzegano występujących zagrożeń. W 48% jednostek nie dokonywano analiz ryzyka, a w 70% nie przeprowadzono obowiązkowego corocznego audytu z zakresu bezpieczeństwa informacji. Brak cyklicznych analiz ryzyka i nieprowadzenie audytów bezpieczeństwa nie pozwalały na identyfikację istotnych ryzyk w zakresie bezpieczeństwa informacji. Kontrola wykazała, że w części urzędów JST zasady mające na celu zwiększenie bezpieczeństwa przetwarzania danych nie były przestrzegane. W ponad 80% skontrolowanych urzędów wystąpiły nieprawidłowości w zarządzaniu uprawnieniami użytkowników w systemach informatycznych. W zakresie uzyskiwania dostępu do systemów informatycznych, w ponad połowie kontrolowanych urzędów (57%) ustanowione zasady nie były przestrzegane (np. użytkownicy używali haseł do systemów informatycznych krótszych niż wymagane). W 56% jednostek wykorzystywano komputery z zainstalowanym systemem operacyjnym bez wsparcia producenta, a w 48% urzędów stwierdzono nieprawidłowości w zakresie tworzenia, przechowywania oraz weryfikacji kopii zapasowych danych. Kontrole NIK również w 2014 r. i 2016 r. ujawniły istotne nieprawidłowości w zakresie bezpieczeństwa systemów informatycznych i zgromadzonych w nich danych o obywatelach. Brak było systemowego podejścia

[30] Informacja o wynikach kontroli „Zarządzanie bezpieczeństwem informacji w Jednostkach Samorządu Terytorialnego”. Nr ewid. 187/2018/P/18/006/KAP, https://www.nik.gov.pl/plik/id,20027, vp,22647.pdf [dostęp 15.02.2020].

kierowników urzędów do zarządzania bezpieczeństwem informacji oraz właściwego zabezpieczenia danych będących w posiadaniu urzędów[31].

Wyniki przeprowadzonych kontroli NIK znajdują potwierdzenie w przeprowadzonych przez autora badaniach w JST na Mazowszu. Mniej niż 10% JST zidentyfikowało i wykazało próby przełamania systemów zabezpieczeń lub włamań do systemów teleinformatycznych urzędu. W 55% badanych powiatów ziemskich zostały wyznaczone osoby do kontaktów z CSIRT-NASK. Wśród gmin wiejskich odsetek ten wyniósł 21,25%. Efektem tego jest brak raportowania do CSIRT-NASK incydentów, co powoduje brak informacji wejściowych i niemożność zidentyfikowania skali zagrożeń przez zespół CERT Polska.

W ostatnich latach można zaobserwować stale rosnącą tendencję do załatwiania przez obywateli spraw w urzędach JST w formie elektronicznej. Zatem zapewnienie bezpieczeństwa przetwarzania informacji w systemach teleinformatycznych urzędów staje się jednym z najistotniejszych wyzwań stojących przed samorządami. Braki w systemach zabezpieczeń sieci wewnętrznej lub nieprzestrzeganie procedur bezpieczeństwa może doprowadzić do kradzieży informacji lub środków finansowych, utraty lub sfałszowania informacji będących w zasobach danej JST. W skrajnych przypadkach może to doprowadzić do paraliżu pracy urzędu i braku możliwości realizacji niektórych obowiązków ustawowych. Warto podkreślić, że każda kategoria JST – gmina, powiat, samorząd województwa – może mieć inną organizację wewnętrzną urzędu, ale realizuje taki sam zakres zadań ustawowych. Dlatego opracowanie jednolitych wytycznych w zakresie organizacji systemu cyberbezpieczeństwa na poziomie każdej z kategorii JST znacznie poprawiłoby spójność bezpieczeństwa systemów i zmobilizowałoby do ich wprowadzenia. Dodatkową wartość stanowiłyby praktyczne ćwiczenia w ramach gminnych i powiatowych zespołów zarządzania kryzysowego z zakresu identyfikacji ryzyk związanych z incydentami w sieciach teleinformatycznych urzędów JST oraz przeciwdziałania skutkom ich wystąpienia. Dużym ułatwieniem dla samorządów byłyby również szkolenia i propagowanie dobrych praktyk, czyli wzorców procedur cyberbezpieczeństwa. Najbardziej kompetentnym podmiotem w tym zakresie jest CSIRT-NASK (CERT Polska) wskazany w ustawie o krajowym systemie do współpracy z JST.

[31] Tamże, s. 7-10.

Bibliografia

Cichocki R., Jatkiewicz P., *Bezpieczeństwo informacji w jednostkach samorządu terytorialnego*, „Roczniki Kolegium Analiz Ekonomicznych SGH" 2013, z. 99.

Liszak-Felicka D., Szmit M., *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016.

Nadybski P., *Elektroniczna administracja w Polsce – ograniczenia i bariery*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy" 2013, nr 9.

Perdał R., *Czynniki rozwoju elektronicznej administracji w samorządzie lokalnym w Polsce*, Poznań 2014.

Sławińska M., *Rok funkcjonowania ustawy o krajowym systemie cyberbezpieczeństwa – najważniejsze postanowienia i rozwiązania*, https://rcb.gov.pl/rok-funkcjonowania-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-najwazniejsze-postanowienia-i-rozwiazania/.

Vademecum bezpieczeństwa, red. O. Wasiuta, R. Klepka, R. Kopeć, Kraków 2018.

Wojciechowska-Filipek S., Ciekanowski Z., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki – organizacji – państwa*, Warszawa 2016.

Wrzosek M., *Krajowe ramy polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, https://cyberpolicy.nask.pl/rb-dokumenty-krajowe-2-krajowe-ramy-polityki-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/.

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. Dyrektywa NIS) (Dz.Urz. UE L 194/1 z 2016 r.).

Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U. z 2020 r., poz. 288).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2018 r., poz. 1330).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2020 r., poz. 695).

Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. z 2015 r., poz. 1893).

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r., poz. 344).

Ustawa z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz.U. z 2012 r., poz. 1232).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2020 r., poz. 346).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560 ze zm.).

Uchwała Rady Ministrów nr 111/2013 z dnia 25 czerwca 2013 r. w sprawie Polityki Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej.

Uchwała Rady Ministrów nr 52/2017 z dnia 9 maja 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.

Uchwała Rady Ministrów Nr 125/2019 z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 (M.P. z 2019 r., 1037).

Źródła internetowe

www.cert.pl

www.lex.pl

www.cyberpolicy.nask.pl

www.enisa.europa.eu

www.warszawa.stat.gov.pl

www.stat.gov.pl

www.senat.gov.pl

www.nik.gov.pl

Selected aspects of the functioning of National Cybersecurity System in Local Government Units: A case of the Masovian Voivodeship

Summary: The scope of providing services in the field of e-administration by local governments in cyberspace and the transmission and processing of information in ICT systems has increased significantly over the last 15 years. At the same time, local governments have become a potential subject of attacks and hacks into resources collected in digital space. This resulted in the need to identify threats in cyberspace and to use effective countermeasures in the event of security breach attempts. Mazovian voivodeship has been selected as the area of the present research to study cybersecurity in the local government. In recent years, there has been a constantly growing tendency for citizens to handle matters in local government offices in electronic form. Therefore, ensuring the

security of information processing in the ICT systems of offices is becoming one of the most important challenges facing local governments.
Keywords: *cybersecurity, e-administration, National Cybersecurity System, local government, website threats, incident, computerization*