Państwo i społeczeństwo

Wyniki badań własnych

Jak polskie gminy radzą sobie z cyberbezpieczeństwem

Zapewnienie bezpieczeństwa teleinformatycznego (cyberbezpieczeństwa) należy do podmiotów publicznych, w tym także jednostek samorządu terytorialnego. Wynikające z tego problemy nie zostały jednak dotąd dobrze rozpoznane. Brakuje nowych danych na temat finansowych, organizacyjnych i kadrowych barier ograniczających tworzenie i implementację polityki z zakresu cyberbezpieczeństwa oraz informacji, czy rozwiązania prawne przyjęte w ostatnich latach na poziomie centralnym są przestrzegane. Autorki przeprowadziły badanie tych zagadnień, a artykuł zawiera jego najistotniejsze wyniki. Do kluczowych ustaleń należy brak świadomości zagrożeń związanych z coraz powszechniejszym funkcjonowaniem w cyberprzestrzeni oraz wynikających z tego nowych obowiązków samorządów, jak również niedostatek środków finansowych. W części urzędów gmin nie ma dokumentu polityki cyberbezpieczeństwa, ponieważ nie istnieje tam elektroniczny obieg dokumentów. To dowód, że polskie gminy są dopiero na drugim z czterech etapów ewolucji cyfrowej administracji i upłynie wiele czasu zanim cyberbezpieczeństwo będzie funkcją zarządzania.

 DOI: 10.53122/ISSN.0452-5027/2022.1.08

ANETA CHODAKOWSKA
SŁAWOMIRA KAŃDUŁA
JOANNA PRZYBYLSKA

Wstęp

W ostatnich latach obserwuje się upowszechnienie stosowania technologii informacyjno-komunikacyjnych (ICT) w działalności jednostek samorządu terytorialnego (JST) oraz przechodzenie podmiotów publicznych na standardy gospodarki 4.0. Zjawisko dostosowania JST do zmieniających się cyfrowo gospodarek jest na tyle masowe, że można mówić o transformacji cyfrowej samorządu terytorialnego[1].

Z tym zjawiskiem wiąże się jednak problem zapewnienia bezpieczeństwa teleinformatycznego (nazywanego też cyberbezpieczeństwem). Z roku na rok rośnie liczba zgłaszanych incydentów i ataków hakerskich na urzędy administracji publicznej, w tym samorządowej[2]. Na JST ciąży więc obowiązek zapewnienia bezpieczeństwa sieci i systemów teleinformatycznych. Konieczne jest wskazanie osób odpowiedzialnych za cyberbezpieczeństwo, opracowanie strategii i zabezpieczeń przed cyberatakami oraz regularna kontrola ich skuteczności[3]. Kwestie bezpieczeństwa i cyberbezpieczeństwa mają też podstawowe znaczenie w czasie sytuacji nadzwyczajnych, do których zalicza się pandemia COVID-19. Ponadto mimo konieczności wdrażania przez administrację publiczną strategii zapewniających cyberbezpieczeństwo, do tej pory przeprowadzono niewiele badań, które weryfikują przyjęte rozwiązania bądź analizują przykłady działalności cyberprzestępczej, ujawnione w jednostkach publicznych, zwłaszcza na poziomie samorządowym. Wykrycie tej luki doprowadziło do sformułowania celu prezentowanego tu badania, którym była diagnoza cyberbezpieczeństwa w urzędach gmin w Polsce.

Wybór zakresu podmiotowego był podyktowany kilkoma czynnikami. Po pierwsze, problematyka cyberbezpieczeństwa w samorządzie terytorialnym w Polsce nie została dotąd dobrze rozpoznana, a ostatnie kompleksowe (opublikowane) badania w tym zakresie przeprowadzono w 2015 roku. Po drugie, nie ma też nowych danych na temat finansowych, organizacyjnych i kadrowych barier ograniczających tworzenie i implementację polityki z zakresu cyberbezpieczeństwa. Wreszcie, do tej pory nie zweryfikowano,

---

1 A. Kaczyńska, S. Kańduła, J. Przybylska: *Transformacja cyfrowa z punktu widzenia samorządu terytorialnego – wybrane zagadnienia*, „Nierówności Społeczne a Wzrost Gospodarczy" nr 65(1)/2021.

2 K. Kubicka-Żach: *Urząd zaatakowany przez cyberprzestępców, wójtowi grozi kara*, <https://www.prawo.pl/samorzad/cyberatak-na-gminna-strone-internetowa-kto-odpowie-za,496647.html>, (dostęp 23.8.2021); *Małopolski Urząd Marszałkowski zaatakowany przez hakerów*, <https://samorzad.pap.pl/kategoria/aktualnosci/malopolski-urzad-marszalkowski-zaatakowany-przez-hakerow>, (dostęp 23.8.2021); B. Stech: *Atak hakerów na strony Urzędu Miasta w Kołobrzegu i serwisy informacyjne. Fake news o morderstwie księdza*, <https://koszalin.wyborcza.pl/koszalin/7,179397,27465486,atak-hakerow-na-strone-urzedu-miasta-w-kolobrzegu-zamiescili.html>, (dostęp 23.8.2021).

3 A. T. Chatfield, C.G. Reddick: *A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government*, „Government Information Quarterly" No 36(2)/2019; A. J. Dębicka: *Sprawne państwo*, Wolters Kluwer Polska, Warszawa 2008.

czy przyjęte w ostatnich latach na poziomie centralnym rozwiązania prawne, mające na celu zmniejszenie ryzyka wystąpienia cyberataków w samorządzie terytorialnym, są przestrzegane.

W artykule dokonano krótkiego przeglądu literatury oraz analizy aktów prawnych dotyczących cyberbezpieczeństwa w JST według stanu prawnego na 1 sierpnia 2021 r., przeprowadzono też badania ankietowe w urzędach wszystkich gmin. Miały one miejsce w okresie od 16 marca do 15 kwietnia 2020 r. Do zebrania danych wykorzystano kwestionariusz ankiety w wersji elektronicznej, wypełniany przez respondentów samodzielnie, po przesłaniu do nich prośby zawierającej adres dostępu do badania (C*omputer Assisted Web Interview* – CAWI). Zastosowano metodę pełną badania. Celem było zebranie informacji na temat: świadomości zagrożeń wśród kierownictwa i pracowników urzędów gmin, posiadanej przez nie polityki zarządzania bezpieczeństwem informacji, incydentów z tym związanych oraz o zarządzania cyberbezpieczeństwem.

Zadania JST w obszarze cyberbezpieczeństwa

W różnych aktach prawnych ustanowiono obowiązek odpowiedniego zarządzania bezpieczeństwem informacji przez JST. W celu zaspokajania zbiorowych potrzeb telekomunikacyjnych wspólnoty samorządowej, jednostka samorządu terytorialnego jest uprawniona do wykonywania następujących zadań[4]:

1) budowy lub eksploatacji (publicznej) infrastruktury telekomunikacyjnej i sieci telekomunikacyjnych oraz nabywania prawa do infrastruktury telekomunikacyjnej i sieci telekomunikacyjnych;
2) dostarczania sieci telekomunikacyjnych lub zapewniania dostępu do infrastruktury telekomunikacyjnej;
3) świadczenia, z wykorzystaniem posiadanej infrastruktury telekomunikacyjnej i sieci telekomunikacyjnych, usług na rzecz:
a) przedsiębiorców telekomunikacyjnych,
b) wybranych państwowych jednostek organizacyjnych i niektórych państwowych osób prawnych,
c) użytkowników końcowych (podmiotów korzystających z publicznie dostępnej usługi telekomunikacyjnej lub żądających świadczenia takiej usługi dla zaspokojenia własnych potrzeb).

Świadczenie przez JST usług, w tym za pomocą Internetu, wiąże się z koniecznością zapewnienia bezpieczeństwa danych w systemach informatycznych. Wykonywanie przez JST wielu zadań własnych i zleconych wiąże się bowiem z potrzebą przetwarzania danych osobowych jej mieszkańców. Jest nim każda czynność, która ich dotyczy, np. zbieranie, porządkowanie, utrwalanie, usuwanie[5]. Przetwarzanie odbywa

[4] Ustawa z 7.5.2010 o wspieraniu rozwoju usług i sieci telekomunikacyjnych (tekst jedn. Dz.U. z 2021 r. poz. 777, ze zm.).

[5] M. Magdziarczyk: *Wdrożenie i realizacja przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 przez jednostki samorządu terytorialnego – na przykładzie gminy*, „Samorząd Terytorialny" nr 4/2021, s. 73.

się według kilku reguł. Według jednej z nich – reguły integralności i poufności – dane osobowe powinny być przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem – za pomocą odpowiednich środków technicznych[6].

Szczególnie ważne w tym kontekście są programy z zakresu cyberbezpieczeństwa (polityka cyberbezpieczeństwa). W polskim prawie cyberbezpieczeństwo definiuje się jako odporność systemów informatycznych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub powiązanych usług oferowanych przez te systemy[7]. Opracowanie dokumentu (programu) polityki cyberbezpieczeństwa jest jednym z zadań własnych gmin w Polsce.

Jednostki samorządu terytorialnego należą do grupy podmiotów publicznych, na które nałożono określone obowiązki związane z ich rolą w krajowym systemie cyberbezpieczeństwa. Do zadań JST należy wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami tego systemu. Powinna to być osoba odpowiedzialna w urzędzie za bezpieczeństwo systemów teleinformatycznych oraz bezpieczeństwo informacji. Szczególnie w małych JST, ze względu na ograniczoną liczbę obowiązków, mogą to być ci sami pracownicy, którzy pełnią funkcję inspektora ochrony danych. Mogą oni utrzymywać kontakt z innymi podmiotami krajowego systemu cyberbezpieczeństwa jedynie w związku z systemami informatycznymi, którymi te jednostki posługują się przy wykonywaniu zadań publicznych[8].

Jednostki samorządu terytorialnego muszą również przygotować struktury i procedury umożliwiające odpowiednią reakcję na pojawienie się tzw. incydentu, czyli zdarzenia, które ma lub może mieć negatywny wpływ na cyberbezpieczeństwo. W ramach przyjętych rozwiązań konieczne jest:

- zapewnienie zarządzania incydentami, tj. zapewnienie obsługi incydentów, poszukiwanie powiązań między nimi, usuwanie przyczyn wystąpienia oraz wypracowanie wniosków;
- zgłoszenie incydentu właściwemu podmiotowi w ciągu 24 godzin od jego wykrycia;
- zapewnienie obsługi incydentu i incydentu krytycznego we współpracy z odpowiednim podmiotem przez podanie niezbędnych danych, w tym osobowych[9].

---

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych; Dz.U. UE L 119, tzw. RODO).

[7] Ustawa z 5.7.2018 o krajowym systemie cyberbezpieczeństwa (tekst jedn. Dz.U. z 2020 r. poz. 1369).

[8] ibid.

[9] ibid.; K. Świtała: *Obowiązki jednostek samorządu terytorialnego w krajowym systemie cyberbezpieczeństwa*. [w:] K. Czaplicki, A. Gryszczyńska, G. Szpor (red.): *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.

Jednostki samorządu terytorialnego mają również obowiązek zapewnienia podmiotom, na rzecz których wykonują zadania publiczne, dostępu do wiedzy umożliwiającej zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów ochrony przed nimi. Jednostki te muszą dodatkowo pamiętać, że ustawa o krajowym systemie cyberbezpieczeństwa obejmuje podmioty nadzorowane przez te jednostki lub w jakich mają udziały. Dotyczy to zwłaszcza tych przedsiębiorców, których można zaliczyć do kategorii operatorów usług kluczowych, a zatem z sektorów: energetyki, transportu, bankowości i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną oraz infrastruktury cyfrowej[10]. W JST mogą to być szpitale, przedsiębiorstwa wodociągowo-kanalizacyjne, operatorzy lotnisk. Na tych podmiotach spoczywa najwięcej obowiązków związanych z budową cyberbezpieczeństwa.

Samorządy jako podmioty wykonujące zadania publiczne są zobowiązane również do opracowania i ustanowienia, a następnie wdrożenia, eksploatacji i monitorowania systemu zarządzania bezpieczeństwem informacji, który ma zapewniać poufność, dostępność i integralność informacji, z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. W przepisach prawa określono szczegółowe działania, które muszą być podjęte w celu zapewnienia takiego systemu bezpieczeństwa. Jednym z najważniejszych elementów będących jego podstawą jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy[11]. Jednostki samorządu terytorialnego zostały zatem zobowiązane do dokonywania analizy ryzyka w odniesieniu do cyberbezpieczeństwa. Systematyczne jej przeprowadzanie ma charakter prewencyjny i z założenia powinno zmniejszać prawdopodobieństwo wystąpienia cyberzagrożeń.

Wyniki badań krajowych i kontroli NIK

Cyberbezpieczeństwo jest obecnie traktowane jako jedno z największych wyzwań społeczno-technicznych, z którymi muszą się mierzyć instytucje publiczne[12]. Konieczność zapewnienia go w działalności administracji publicznej, w tym w samorządzie terytorialnym, jest coraz mocniej artykułowana w literaturze, w dokumentach rządowych i raportach przygotowywanych przez niezależne instytucje[13].

[10] Patrz przyp. 7.

[11] Rozporządzenie Rady Ministrów z 12.4.2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jedn. Dz.U. z 2017 r. poz. 227).

[12] H. de Bruijn, M. Janssen: *Building Cybersecurity Awareness: The need for evidence-based framing strategies,* "Government Information Quarterly" No 34(1)/2017.

[13] J. Ruohonen: *An Acid Test for Europeanization: Public Cyber Security Procurement in the European Union*, "European Journal for Security Research" No 5(2)/2020; M. Salminen, K. Hossain: *Digitalisation and human security dimensions in cybersecurity: An appraisal for the European High North*, "Polar Record" No 54(2)/2018.

Mimo to, realna świadomość zagrożeń zarówno władz publicznych, jak i społeczeństwa jest ograniczona[14]. Potwierdza to również rzadkie przeprowadzanie badań nad cyberprzestępczością i cyberbezpieczeństwem na poziomie samorządu terytorialnego[15] – zarówno w Polsce, jak i w innych państwach Unii Europejskiej.

W 2015 roku odbyło się w Polsce badanie wśród 200 urzędników odpowiedzialnych za ICT w samorządzie terytorialnym[16]. Badani twierdzili, że urzędy są dobrze przygotowane do cyberataków, choć podstawowym narzędziem obrony jest antyspam. Według 62% pytanych największą barierą w podnoszeniu cyberbezpieczeństwa jest brak wystarczających funduszy, a według 17% – niska świadomość problemu na wyższych poziomach administracji. Jedynie blisko 13% ankietowanych dostrzegało problem braku centralnej strategii i standardów bezpieczeństwa informatycznego.

W latach 2012–2016 badania w 266 urzędach administracji publicznej przeprowadzili D. Lisiak-Felicka i M. Schmitt[17], którzy stwierdzili, że tylko w połowie urzędów wdrożono system zarządzania bezpieczeństwem informacji, a jedynie 14% z nich zdecydowało się na jego certyfikację. W 2015 roku przestrzeganie przez urzędy JST wymogów wynikających z przepisów prawa oceniał zespół P. Jatkiewicza. Było to najbardziej kompleksowe badanie, ponieważ uczestniczyło w nim aż 2917 urzędów JST różnych kategorii. Badacze stwierdzili, że ankietowane jednostki „w większości nie podjęły adekwatnych starań odnośnie do wdrożenia systemu zarządzania bezpieczeństwem informacji". Oznacza to, że nie zaplanowały, nie wdrożyły i nie wykorzystują „systemów teleinformatycznych z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk"[18].

W 2016 roku badanie stanu cyberbezpieczeństwa przeprowadzono wśród gmin województwa łódzkiego[19]. Wzięło w nim udział 44 JST (24,9% gmin tego regionu). Zebrano informacje o wdrożonych systemach zarządzania bezpieczeństwem

[14] H. de Bruijn, M. Janssen, op.cit.

[15] S. Kańduła, J. Przybylska: *Cybersecurity in local government: Essence, tasks and threats*, "Digital Transformation of the Financial Sector of Economy", <https://www.researchgate.net/publication/344172548_Cybersecurity_in_local_government_Essence_tasks_and_threats>, (dostęp 15.6.2021); KnowBe4: *The Economic Impact of Cyber Attacks on Municipalities*, <https://www.knowbe4.com/hubfs/Cyber-Attacks-on-Municipalities-White-Paper.pdf>, (dostęp 15.6.2021); M. Schallbruch, I. Skierka: *Cybersecurity in Germany*, Springer International Publishing, Nowy Jork 2018.

[16] *Jak to jest z cyberbezpieczeństwem w samorządach*?, <https://www.polskaszerokopasmowa.pl/technologie/artykuly/klucz,jak-to-jest-z-cyberbezpieczenstwem-w-samorzadach,akcja,pdf.html>, (dostęp 15.6.2021).

[17] D. Lisiak-Felicka, M. Schmit: *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, European Association for Security, Kraków 2016.

[18] P. Jatkiewicz: *Wdrożenie wybranych wymagań dotyczących systemów informatycznych oraz Krajowych Ram Interoperacyjności w jednostkach samorządu terytorialnego. Raport z badań*, Polskie Towarzystwo Informatyczne, Warszawa 2016, s. 47.

[19] D. Lisiak-Felicka, M. Pytko: *Cyberbezpieczeństwo urzędów gmin w województwie łódzkim*. „Przedsiębiorczość i Zarządzanie" nr 18(4)/2017.

informacji, incydentach oraz sposobach zarządzania cyberbezpieczeństwem w urzędach. Blisko 50% gmin stwierdziło, że cyberprzestępczość jest dla nich dużym i bardzo dużym zagrożeniem, choć jakiekolwiek incydenty wystąpiły tylko w 5 z nich (11,4%). Nie zawsze incydenty te były zgłaszane odpowiednim służbom. W powszechnym przekonaniu cyberzagrożenia są synonimem ataków hakerów. Jednak jeszcze większym problemem może być nieostrożność człowieka, wynikająca często z braku świadomości i odpowiedniej edukacji[20]. Potwierdzają to wyniki cytowanego badania: wskazano w nim, że na cyberataki najbardziej podatni są pracownicy, a następnie: dane osobowe, stacje robocze (komputery pracowników), systemy płatności, usługi online. Urzędy spotkały się przede wszystkim ze spamem, wprowadzaniem na zainfekowanej stronie złośliwego skryptu zawierającego odnośnik do witryny serwującej szkodliwe oprogramowanie (tzw. *drive-by-download*) oraz z phishingiem (oszustwem internetowym, w której przestępca podszywa się pod inną osobę lub instytucję). Podstawowymi narzędziami obrony były: zapora sieciowa (*firewall*), program antywirusowy, blokada i filtr spamu. System zarządzania bezpieczeństwem informacji stosowało 70,4% gmin, ale tylko w jednym urzędzie był on zgodny z normą Międzynarodowej Organizacji Normalizacyjnej (*International Organization for Standardization* – ISO). Bezpieczeństwem zarządzały przede wszystkim upoważnione osoby będące pracownikami JST. Autorzy badania nie komentują zgromadzonych danych, podkreślają jednak, że niewielka była skłonność gmin do dzielenia się swoimi doświadczeniami w tym obszarze[21].

W 2019 roku D. Lisiak-Felicka powtórzyła badania. Tym razem wzięły w nim udział 543 urzędy, z tego: 10 marszałkowskich, 64 starostw powiatowych oraz 469 urzędów gmin. Badanie pokazuje, że 25% ankietowanych nie ma systemu zarządzania bezpieczeństwem informacji, a tylko 23% urzędów posiadających taki system zdecydowało się na jego certyfikację. Za najbardziej podatny na ataki element urzędu uznano ludzi (pracowników). W 75% ankietowanych urzędów w ciągu 12 miesięcy poprzedzających badanie nie zarejestrowano żadnego incydentu. Zdaniem większości ankietowanych największe zagrożenie stanowi złośliwe oprogramowanie. Jednocześnie 60% respondentów ocenia, że w ich urzędzie bezpieczeństwo informacji jest wysokie i bardzo wysokie. Może dlatego w większości przypadków (61% odpowiedzi) roczne wydatki na ten cel nie przekraczały 10 tys. zł. Ankietowani wskazali też, że największym problemem są niedostateczne środki finansowe[22].

W latach 2014, 2016 i 2017 Najwyższa Izba Kontroli (NIK) przeprowadziła trzy kontrole odnoszące się do zarządzania

[20] C. Brumfield: *Why local governments are a hot target for cyberattacks*, <https://www.csoonline.com/article/3391589/why-local-governments-are-a-hot-target-for-cyberattacks.html>, (dostęp 14.5.2021).
[21] D. Lisiak-Felicka, M. Pytko, op.cit.
[22] D. Lisiak-Felicka: *Cyberbezpieczeństwo urzędów administracji samorządowej – wyniki badań*, „IT w administracji" nr 10(143)/2019.

bezpieczeństwem informacji w urzędach administracji publicznej. W 2014 roku sprawdzano wdrażanie wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności (KRI). Badanie odbyło się w Ministerstwie Administracji i Cyfryzacji oraz w 24 urzędach gmin miejskich, w tym miast na prawach powiatu, z sześciu województw. Kontrolerzy negatywnie ocenili działania kierownictwa JST (burmistrzów i prezydentów miast) związane z zarządzaniem bezpieczeństwem informacji w urzędach (§ 20 rozporządzenia w sprawie Krajowych Ram Interoperacyjności). Nieprawidłowości w tym obszarze stwierdzono w 87,5% skontrolowanych urzędów gmin. W piętnastu podmiotach (62,5% objętych kontrolą) nie opracowano i nie stosowano w praktyce dokumentu polityki bezpieczeństwa informacji. W czterech urzędach (17,4%) nie prowadzono odpowiednio inwentaryzacji zasobów informatycznych. W 9 (37,5%) kontrolowanych JST w okresie objętym kontrolą nie zapewniono audytu bezpieczeństwa informacji w systemach informatycznych. Trzeba jednak przyznać, że niemal we wszystkich urzędach samorządowych (91,7%) w okresie objętym kontrolą przeprowadzano okresowe analizy utraty integralności, poufności lub dostępności informacji. W większości, czyli w 17 (70,8%) zorganizowano dla pracowników szkolenia dotyczące bezpieczeństwa informacji[23].

Kontrola z 2016 roku dotyczyła systemu rejestrów państwowych. Przeprowadzono ją w Centralnym Ośrodku Informatyki oraz w 13 urzędach miast i gmin z czterech województw. Wykazała, że ich kierownicy na ogół nie przywiązywali dostatecznej wagi do zapewnienia bezpieczeństwa przetwarzania informacji. W szczególności, w 62% urzędów JST nie opracowano i nie wdrożono polityki bezpieczeństwa informacji, w 38% wystąpiły nieprawidłowości związane z blokowaniem lub odbieraniem dostępu do systemu byłym pracownikom, a w 23% nie przeprowadzano obowiązkowego corocznego audytu bezpieczeństwa informacji[24].

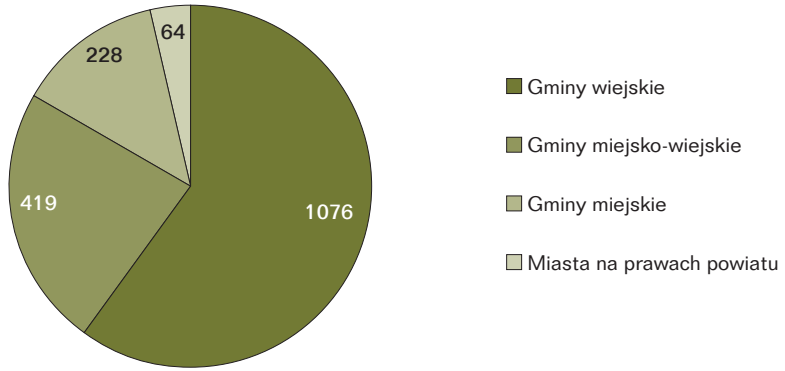
W 2017 roku przeprowadzono kontrolę zarządzania bezpieczeństwem informacji w 23 jednostkach samorządu terytorialnego, w tym w 14 gminach (miejskich i miejsko-wiejskich) z pięciu województw[25]. Wykazała ona, że większość (70%) skontrolowanych JST nie przestrzegało wymogów dotyczących bezpieczeństwa informacji, o których stanowi rozporządzenie o KRI. Kontrolerzy zwrócili uwagę, że pomimo upływu kilku lat od wcześniejszych kontroli nie nastąpiła poprawa. W dalszym ciągu brakowało systemowego podejścia kierowników urzędów do zarządzania bezpieczeństwem informacji (w 61%

[23] 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 ewid. 205/2014/P/14/004/KAP.

[24] Informacja o wynikach kontroli NIK: *System rejestrów państwowych – bezpieczeństwo, funkcjonowanie i użyteczność*, nr ewid. 208/2016/P/16/006/KAP.

[25] Informacja o wynikach kontroli NIK: *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego*, nr ewid. 187/2018/P/18/006/KAP.

Rysunek 1. **Statystyka gmin-respondentów według typu gmin**



Źródło: Opracowanie na podstawie badań własnych.

skontrolowanych JST) oraz właściwego zabezpieczenia danych będących w posiadaniu urzędów. Większość badanych jednostek (74%) nie miało pełnej i aktualnej wiedzy o posiadanych zasobach służących do przetwarzania danych. Kontrolerzy mieli zastrzeżenia do stanu świadomości potencjalnych zagrożeń. Blisko połowa skontrolowanych JST (48%) nie dokonywała analizy ryzyka, a w 70% nie przeprowadzono obowiązkowego corocznego audytu z zakresu bezpieczeństwa informacji[26].

Wyniki badań własnych

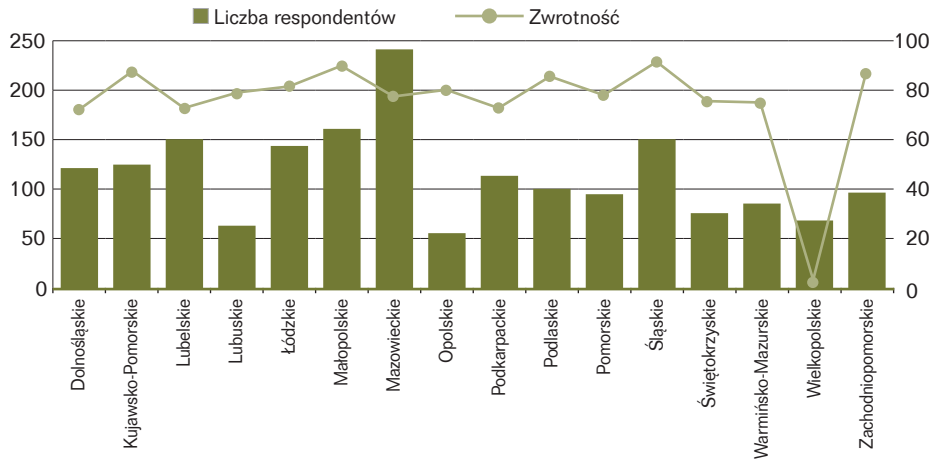
Badaniem ankietowym objęto urzędy wszystkich 2477 gmin w Polsce. Według stanu na dzień badania były to: 1532 gminy wiejskie, 643 miejsko-wiejskie oraz 302 miejskie, w tym 66 będących miastami na prawach powiatu. Ostatecznie otrzymano odpowiedzi łącznie od 1787 gmin (zwrotność ankiet wyniosła 72,1%), a liczbę i odsetek odpowiedzi według typu gminy prezentuje rys. 1[27].

W badaniu wzięły udział gminy wiejskie (60,2% respondentów), miejsko-wiejskie (23,4% respondentów), miejskie (12,8% respondentów) oraz miasta na prawach powiatu (3,6% respondentów), które wyodrębniono z grupy gmin miejskich. Zwrotność ankiet była najwyższa w przypadku miast na prawach powiatu (97,0%) i gmin miejskich (96,6%), a relatywnie niższa w gminach wiejskich (70,2%) oraz gminach miejsko-wiejskich (65,2%). Najwięcej odpowiedzi uzyskano z gmin z województwa mazowieckiego (13,5%), następnie małopolskiego (9,0%), lubuskiego (8,5%) i śląskiego (8,4%), a najmniej

[26] ibid.

[27] Anonimowość ankiety zapewniono przez wygenerowaniu jedynego linku do ankiety, dzięki czemu identyfikacja respondentów była niemożliwa. Przed duplikacją odpowiedzi zabezpieczono się analizując IP – nie było możliwości wypełnienia ankiety z tego samego adresu IP.

Rysunek 2. **Statystyka gmin-respondentów oraz zwrotność (w %) według województw**



Źródło: Opracowanie na podstawie badań własnych.

z województwa wielkopolskiego (rys. 2). Zwrotność ankiet w poszczególnych województwach była największa w przypadku województwa śląskiego (90,4%), a najmniejsza w przypadku województwa wielkopolskiego (2,7%).

Pod względem liczby mieszkańców przeważały odpowiedzi z gmin do 10 tys. mieszkańców (64,4%). Drugą co do znaczenia grupą były jednostki z liczbą mieszkańców w przedziale 10-20 tys. (20,9%). W badanej grupie przeważały gminy z dochodami bieżącymi poniżej 3 tys. zł na osobę (36,5%), a następnie z dochodami od 4 do 4,5 tys. zł (18,1%) na osobę[28].

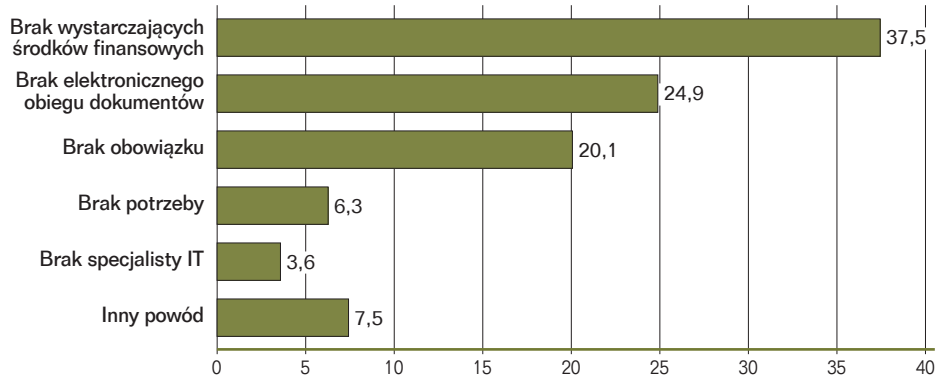
Jedynie 3,6% gmin uczestniczących w badaniu zostało uznanych za operatora usługi kluczowej. Do utrzymywania kontaktów z podmiotami krajowego systemu bezpieczeństwa w gminie zostali wyznaczeni głównie pracownicy zatrudnieni na stanowisku do spraw informatyki (40,6%) lub kierownik urzędu JST (40,6%)[29]. Wdrożenie systemu zarządzania bezpieczeństwem informacji potwierdziło 76,9% gmin, z czego w 82,2% jednostek system nie miał akredytacji zgodności z normą PN-ISO/IEC 27001:2017-0630[30]. Nie wdrożono systemu w 23,1% ankietowanych gmin. Powodem niewdrożenia

[28] Wskazane w artykule przepisy prawa obowiązują wszystkie gminy, bez względu na ich wielkość lub typ, odpowiedzi nie były więc analizowanego według wielkości ani typu gminy.

[29] W gminach innych niż wiejskie najprawdopodobniej wyznacza się inne osoby.

[30] Certyfikacja SZI podnosi świadomość pracowników jednostki, stanowi dowód dostosowania SZI do obowiązujących wymagań i przestrzegania międzynarodowych wytycznych dotyczących bezpieczeństwa informacji (co może być ważne dla obywateli, potencjalnych inwestorów i instytucji finansowych). Międzynarodowe wymagania dotyczące systemów zarządzania informacją ISO i Międzynarodowy Komitet Elektro-

Rysunek 3. **Przyczyny niewdrożenia w gminie systemu zarządzania bezpieczeństwem informacji (odsetek odpowiedzi, N=413)**



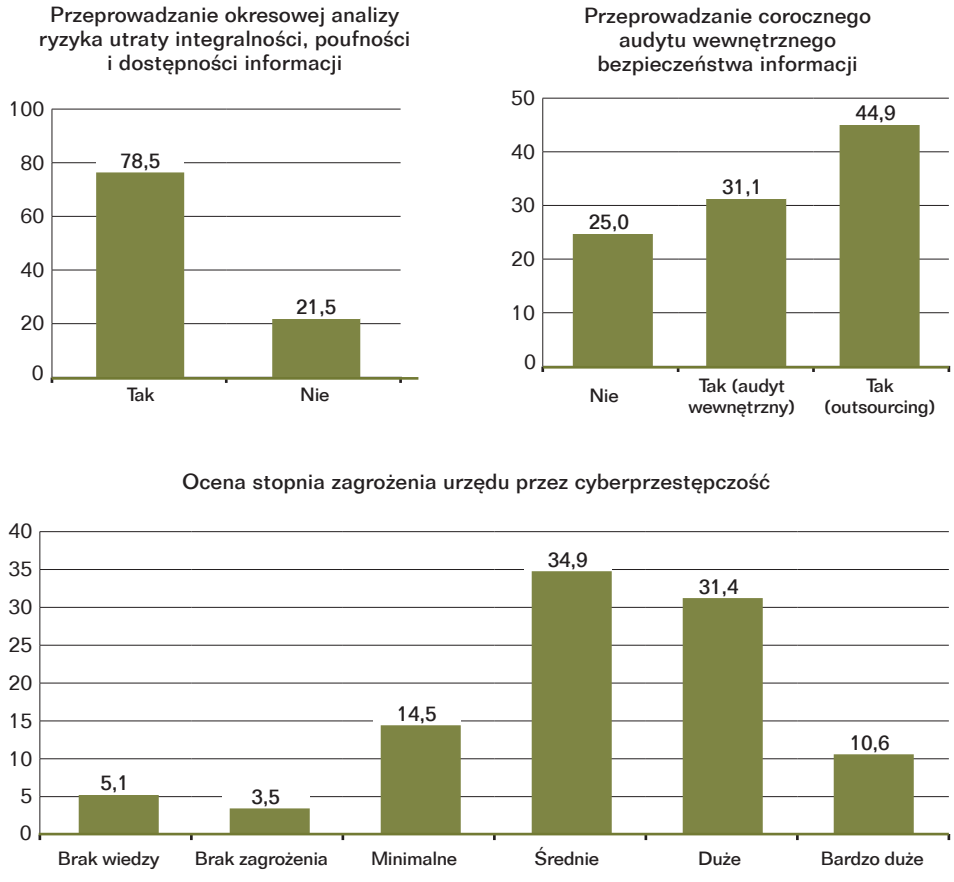
Źródło: Opracowanie na podstawie badań własnych.

go były głównie: brak wystarczających środków finansowych (37,5%) oraz elektronicznego obiegu dokumentów (24,9%) (rys. 3). Do podjęcia stosownych działań gminy przekonałoby przede wszytskim przekazanie na ten cel dodatkowych środków przez organy administracji rządowej (52,3%) lub wprowadzenie elektronicznego obiegu dokumentów (19,6%).

W opinii ankietowanych cyberprzestępczość stanowi średnie (34,9%) lub duże (31,4%) zagrożenie dla urzędu. W wypadku 78,5% urzędów była przeprowadzana okresowa analiza ryzyka utraty integralności, poufności i dostępności informacji. Te JST, które jej nie dokonywały tłumaczyły się głównie brakiem środków finansowych (35,6%) lub takiej potrzeby (24,7%). Aktualna i kompletna elektroniczna ewidencja sprzętu informatycznego była prowadzona w wypadku 81,0% urzędów. Coroczny audyt wewnętrzny bezpieczeństwa informacji przeprowadzano w urzędach przez usługodawcę zewnętrznego (w 44,9%) lub przez audytora wewnętrznego (w 30,1%). W 25,0% urzędów taki audyt nie miał miejsca (rys. 4). Powodem w większości sytuacji był również brak środków (59,3%). W latach 2017–2019 w 86,7% badanych JST nie wystąpiły incydenty

techniczny (IEC – *International Electrotechnical Commission*) zostały wydane w 2005 r. Norma PN-ISO/IEC 27001, wydana przez Polski Komitet Normalizacyjny, jest krajowym odpowiednikiem normy międzynarodowej. Przedstawia modelowy system zarządzania bezpieczeństwem informacji, a także określa wymagania do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia tego systemu. Jej założenia są uniwersalne, czyli może być stosowana przez dowolny podmiot publiczny i prywatny. Norma ta jest co jakiś czas aktualizowana (najważniejsze zmiany sygnalizuje się modyfikując jej nazwę/numer). W trakcie przeprowadzania badań ankietowych obowiązywała norma pod nazwą PN-ISO/IEC 27001:2017-06. Szerzej na temat normy piszą: J. Krawiec, G. Ożarek: *Certyfikacja w informatyce*, Polski Komitet Normalizacyjny, Warszawa 2014.

Rysunek 4. **Rozkład odpowiedzi na pytania dotyczące oceny bezpieczeństwa informacji w gminach (odsetek odpowiedzi)**

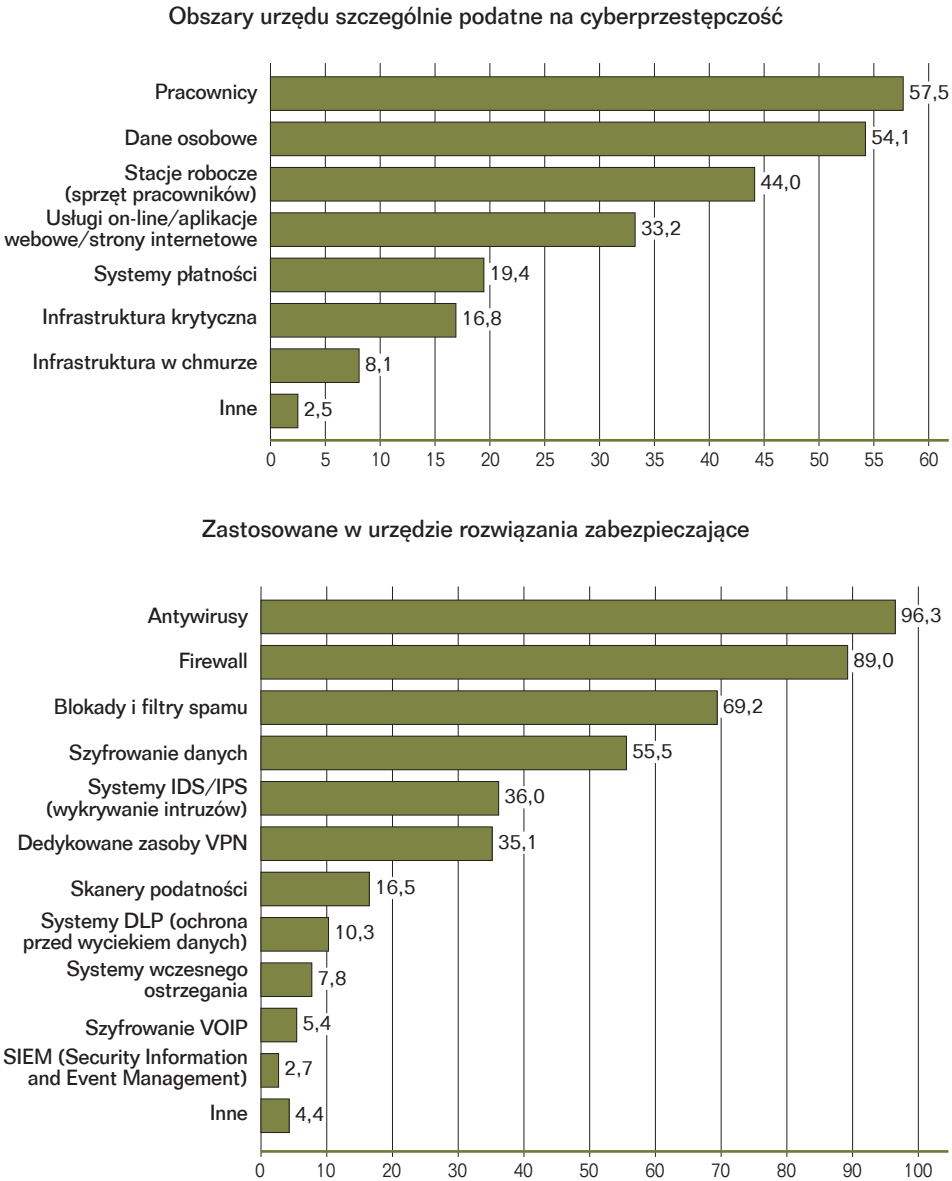


Źródło: Opracowanie na podstawie badań własnych.

związane z naruszeniem bezpieczeństwa informacji, a w pozostałych urzędach zaobserwowano do 5 takich incydentów (10,6%). Jeśli miały miejsce, aż w 44,4% urzędów nie dokonano zgłoszenia.

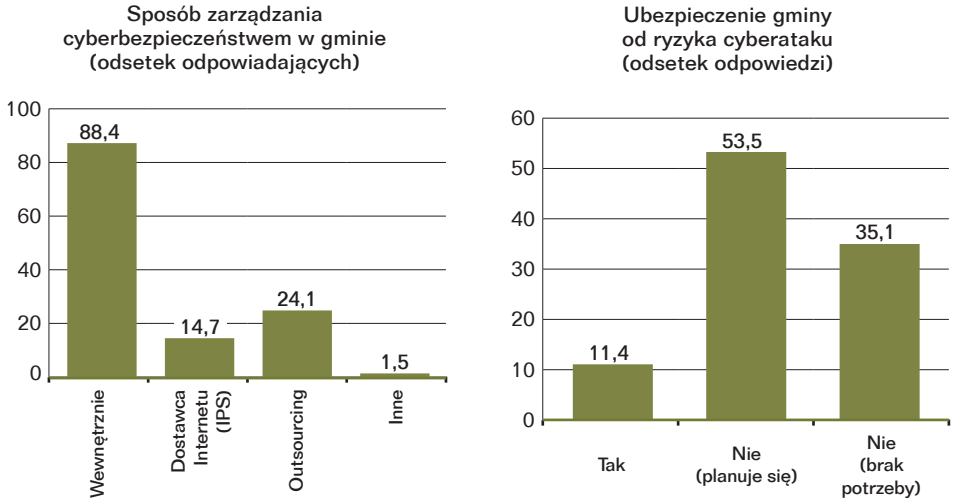
Najczęściej wymienianymi obszarami działalności urzędu podatnymi na cyberprzestępczość były: dane osobowe (54,1%), pracownicy (57,5%) i sprzęt pracowniczy (44%), a najmniej – infrastruktura w chmurze (8,1%). W badanej grupie najczęstszymi przykładami działalności cyberprzestępczej był spam (79,1%), a następnie phishing (26,5%) i złośliwe oprogramowanie (26,5%). W badanych jednostkach z narzędzi zabezpieczających używane były głównie antywirusy (96,3%), firewalle (89,0%) oraz blokady i filtry spamu (69,2%). W bardzo małej liczbie gmin stosowano oprogramowania

Rysunek 5. **Rozkład odpowiedzi na pytania dotyczące obszarów urzędu podatnych na cyberprzestępczość oraz zastosowanych rozwiązań zabezpieczających (odsetek odpowiadających)**



Źródło: Opracowanie na podstawie badań własnych.

Rysunek 6. **Rozkład odpowiedzi na pytania dotyczące zarządzania cyberbezpieczeństwem**



Źródło: Opracowanie na podstawie badań własnych.

typu *Security Information and Event Management* (SIEM) (2,7%), szyfrowanie typu *Voice over Internet Protocol* (VOIP) (5,4%) oraz systemy wczesnego ostrzegania (7,8%) (rys. 5, s. 141).

W badaniu podjęto też problematykę zarządzania cyberbezpieczeństwem w urzędach gmin (rys. 6). Zazwyczaj zajmowali się tym pracownicy (88,4%). W latach 2017–2019 w gminach zorganizowano szkolenia z zakresu cyberbezpieczeństwa. W 50,5% badanych jednostek wzięli w nich udział wszyscy pracownicy urzędu, a u 9% respondentów tylko kadra kierownicza. W 40,6% gmin nie przeprowadzono szkoleń. Wiązało się to również z niedostatkiem środków finansowych (54,3%) lub brakiem potrzeb (38,2%). Tylko 11,4% gmin było ubezpieczonych od ryzyka cyberataku, a 53,5% planowało rozszerzyć ubezpieczenie o to ryzyko.

Wnioski i rekomendacje

Z odpowiedzi respondentów uzyskanych w toku badania wynika, że w większości urzędów (76,9%) opracowano i wdrożono system (politykę) bezpieczeństwa informacji. Ponadto w większości gmin (75%) co roku przeprowadzano audyt wewnętrzny bezpieczeństwa informacji. Może to świadczyć o odpowiedniej organizacji systemu bezpieczeństwa informacji. Jednak część badanych jednostek nie podjęła wystarczających działań, aby zapobiec incydentom, np. nie przeprowadziła obowiązkowych audytów w tym zakresie. Tylko w połowie gmin uczestniczących w badaniu przeprowadzane są szkolenia urzędników z zakresu cyberbezpieczeństwa, w 9% przeszkolono tylko kadrę kierowniczą. Niespełna 12% badanych ubezpieczyło się od ryzyka cyberataku. Jest to o tyle zaskakujące, że jednocześnie dla około 66% JST cyberprzestępczość stanowi średnie

lub duże zagrożenie. Najbardziej podatne na ta zagrożenia są dane osobowe. W latach 2017–2019 w większości badanych gmin (86,7%) nie wystąpiły co prawda incydenty związane z naruszeniem bezpieczeństwa informacji, ale ich ryzyko jest coraz większe. Te JST, w których incydenty miały miejsce nie zawsze zgłaszały je odpowiednim organom.

Analiza uzyskanych odpowiedzi wskazuje, że przyczyną zaniedbań w tej sferze może być brak świadomości zagrożeń związanych z coraz powszechniejszym funkcjonowaniem w cyberprzestrzeni oraz wynikających z tego nowych zadań i obowiązków JST. Część respondentów wskazała bowiem, że nie ma dokumentu polityki cyberbezpieczeństwa także dlatego, że w urzędzie nie istnieje elektroniczny obieg dokumentów. Jednocześnie jest to dowód na to, że polskie gminy dopiero są na drugim z czterech etapów ewolucji cyfrowej administracji wyróżnianych np. przez T. Janowskiego[31] i wiele czasu upłynie zanim cyberbezpieczeństwo będzie funkcją zarządzania.

Niewywiązywanie się z zadań w tej dziedzinie tłumaczy się brakiem zagrożeń, brakiem odpowiedniej kadry lub wystarczających zasobów finansowych[32]. Tymczasem takie zagrożenia jednak istnieją. Ataki i incydenty w cyberprzestrzeni, o różnej skali i konsekwencjach, stały się już rzeczywistością i stanowią realne zagrożenie nie tylko dla wybranych obywateli, przedsiębiorstw, ale także dla JST i państwa. Konieczne jest więc postulowanie upowszechniania wiedzy w tej dziedzinie, uzmysławianie wszystkim zagrożeń ze strony cyberprzestępców[33]. Do sposobów zapewnienia bezpieczeństwa danych należy współpraca z zewnętrznymi audytorami bezpieczeństwa i specjalistami z zakresu ICT, którzy pomogliby ocenić ryzyko cyberataku[34], tym bardziej, że „zarządzanie cyberbezpieczeństwem sprowadza się do zarządzania ryzykiem"[35].

Audyt bezpieczeństwa informacji przeprowadza się z różnych powodów. Po pierwsze, jest obowiązkowy[36], po drugie, aby wdrożyć zabezpieczenie, które jest adekwatne do zagrożeń zidentyfikowanych

---

[31] T. Janowski: *Digital government evolution: From transformation to contextualization*, "Government Information Quarterly" No 32(3)/2015.

[32] Podobne wyjaśnienia składają gminy amerykańskie. Zob.: D. F. Norris, L. Mateczun, A. Joshi, T. Finin: *Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity*, "Journal of Urban Affairs" 2020.

[33] H. de Bruijn, M. Janssen, op.cit.

[34] W. Hatcher, W. Meares, J. Heslen, op.cit.; D. F. Norris, L. Mateczun, A. Joshi, T. Finin: *Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity*, "Public Administration Review" No 79(6)/2019.

[35] A. Wygodny: *Metody prowadzenia audytu cyberbezpieczeństwa*, „Kontrola Państwowa" nr 2/2021, s. 82.

[36] S. Kańduła, J. Przybylska: *Internal Audit of the National Interoperability Framework as a Tool for Assessing Information Security in the Conditions of Economy 4.0*, [in:] Materialy Mizhnarodnoyi naukovo-praktychnoyi konferentsiyi: Innovacijnyj rozvytok ta bezpeka pidpryjemstv v umovah neoindustrial'nogo suspil'stva/ Polinkiewicz O. M., Szostak L. W. (red.), Wschodnioeuropejski Państwowy Uniwersytet im. Lesi Ukrainki w Łucku 2020, ss. 518-520.

w jego trakcie. Inną przyczyną jest dążenie do otrzymania lub utrzymania certyfikatu systemu zarządzania bezpieczeństwem informacji (normy ISO). Jeszcze innym motywem jest chęć wprowadzenia w urzędzie rozwiązań poprawiających bezpieczeństwo informacji. Może ona wynikać z przekonania organu wykonawczego lub pracowników urzędu, może być też pochodną czynników zewnętrznych. Jednym z nich są wymogi nakładane przez organy administracji rządowej na gminy uczestniczące w konkursie Cyfrowa gmina. Warunkiem rozliczenia dotacji na różne zadania z zakresu cyfryzacji gminy jest przeprowadzenie diagnozy (audytu) cyberbezpieczeństwa w terminie do 6 miesięcy od dnia zawarcia umowy o przekazanie środków[37].

Zadania JST w zakresie cyberbezpieczeństwa wykraczają poza możliwości kadrowe, organizacyjne i finansowe poszczególnych gmin. Ograniczenia finansowe są szczególnie widoczne w małych jednostkach. Powodują trudności nie tylko we wdrażaniu podstawowych technicznych środków bezpieczeństwa, ale także w pozyskiwaniu fachowców z zakresu bezpieczeństwa informacji[38]. W krótkim okresie remedium na lukę finansową mogą być nieodpłatne szkolenia i konferencje organizowane przez organy państwa, w tym korzystanie z przygotowanych przez nie oraz placówki naukowe, materiałów informacyjnych[39]. W długim okresie problem można rozwiązać zaliczając cyberbezpieczeństwo do codziennej praktyki zarządzania w samorządzie lokalnym przez odpowiednie kształcenie przyszłych menedżerów i urzędników publicznych[40]. Szkolenia mogłyby być także finansowane ze środków unijnych. Konieczne jest informowanie JST o potencjalnych źródłach finansowania wydatków na cyberbezpieczeństwo, upowszechnienie dobrych praktyk z tym związanych i uproszczenie zasad korzystania z zewnętrznych źródeł finansowania, w tym z budżetu Unii Europejskiej.

W Polsce środki z UE były wydatkowane na podstawie programu operacyjnego Polska Cyfrowa w latach 2014–2020, ale gminy miały utrudniony dostęp do tych funduszy, ponieważ program został zaprojektowany głównie z myślą o jednostkach administracji państwowej[41]. W rezultacie 87% urzędów gmin w Polsce finansuje inwestycje w infrastrukturę zabezpieczającą przed cyberatakami ze środków własnych[42].

---

[37] Regulamin konkursu grantowego Cyfrowa gmina, <https://www.gov.pl/web/cppc/cyfrowa-gmina>, (dostęp 15.11.2021).

[38] L. Eisenstein: *Why Municipalities Should Care About Cybersecurity*, <https://insights.diligent.com/cybersecurity-local-government/why-municipalities-care-cybersecurit> (dostęp 15.6.2021).

[39] KPRM: #*Cyberbezpieczny samorząd*, <https://www.gov.pl/web/baza-wiedzy/cyberbezpieczny-samorzad> (dostęp 23.8.2021).

[40] W. Hatcher, W. Meares, J. Heslen: *The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices*, "Journal of Cyber Policy" No 5(2)/2020.

[41] W dokumentach, na podstawie których udostępnia się fundusze europejskie w latach 2021–2027, w większym stopniu uwzględnia się specyfikę samorządu terytorialnego.

[42] *Jak to jest z cyberbezpieczeństwem w samorządach*?, op.cit.

Odpowiedzią na ograniczone możliwości kadrowe, organizacyjne i finansowe poszczególnych gmin może też być współpraca i wymiana doświadczeń w zakresie cyberbezpieczeństwa w urzędach i ich jednostkach organizacyjnych. Innym sposobem jest nawiązywanie partnerstw z sąsiednimi JST w celu wymiany wiedzy i wspólnego ponoszenia wydatków. Wymiana doświadczeń, wspólne budowanie systemów, a także wykorzystanie efektu ekonomii skali, to najważniejsze aspekty, na które JST powinny zwrócić uwagę rozważając podjęcie współpracy. Nawiązują do tego J. P. Kesan i L. Zhang[43], którzy zauważyli, że w ostatnich latach coraz częściej atakowane są małe jednostki samorządowe. W związku z tym, to właśnie one powinny przeznaczać więcej środków na inwestycje w technologie zabezpieczające przez cyberatakami. Jednocześnie są to również jednostki bardzo często niemające wystarczających funduszy, aby samodzielnie zbudować odpowiedni system zabezpieczeń.

Bariery we współpracy mogą mieć podłoże mentalne i ideologiczne. Jednostki samorządu terytorialnego mają osobowość prawną i zagwarantowaną prawnie samodzielność działania. W sferze cyberbezpieczeństwa powinny jednak współdziałać nie tylko ze sobą, ale również z przedstawicielami administracji państwowej i agencjami rządowymi[44]. Ograniczanie samodzielności gmin i nadmierna ingerencja organów państwa w ich działanie nie są wprawdzie pożądane, ale przyjmując, że cyberbezpieczeństwo jest dobrem publicznym[45], odznaczającym się efektami skali, powinny one dokonywać symulowanych ataków, przeprowadzać wyrywkową kontrolę wykonywania zadań gmin z tego zakresu, identyfikować wszelkie nieprawidłowości (ale nie karać za wykrycie), pomagać w ich wyeliminowaniu i uszczelnić system. Również pod tym względem edukacja ma kluczowe znaczenie nie tylko dla ukazania słabych stron gmin, ale także upowszechnienia dobrych praktyk.

Cyberprzestępcy wykorzystają to, że JST nie są gotowe na atak. Warto więc podkreślić jeszcze raz, że ważne jest wyprzedzanie zdarzeń, podnoszenie świadomości zagrożeń wśród urzędników, opracowanie jasnych standardów i procedur polityki cyberbezpieczeństwa oraz bardziej rygorystyczne egzekwowanie prawa. Jednym ze sposobów zapewnienia większego bezpieczeństwa danych jest nawiązywanie partnerstw z sąsiednimi gminami w celu wymiany wiedzy i ograniczenia kosztów. Innym sposobem może być również korzystanie z usług przetwarzania w chmurze, świadczonych przez certyfikowanych, sprawdzonych przez rząd dostawców. Współpraca dotycząca bezpieczeństwa cyfrowego pomoże JST dysponującym

[43] J. P. Kesan, L. Zhang: *An empirical investigation of the relationship between local government budgets, IT expenditures, and cyber losses,* "IEEE Transactions on Emerging Topics in Computing" 9(2) 2019.
[44] W. Hatcher, W. L. Meares, J. Heslen, op. cit.; J. Wolff, W. Lehr: *When cyber threats loom, what can state and local governments do*?, "Georgetown Journal of International Affairs" No 1/2019.
[45] M. Taddeo: *Is Cybersecurity a Public Good*?, "Minds and Machines" No 29(3)/2019.

ograniczonymi zasobami w tworzeniu skutecznej polityki cyberbezpieczeństwa[46]. Gminy powinny przyjąć jedną z tych strategii w czystej postaci bądź zdecydować się na wybrane z tych propozycji.

Badanie, którego wyniki prezentujemy w tym artykule nie wyczerpuje problematyki cyberbezpieczeństwa w urzędach JST. W dalszych badaniach warto postawić następujące pytania: Czy zarządzanie bezpieczeństwem informacji, w tym stopień przestrzegania przepisów KRI, jest różny w zależności od szczebla samorządu terytorialnego, typu gminy, wielkości JST, liczby pracowników, w tym osób bezpośrednio związanych z ICT, oraz ich wykształcenia? Czy upowszechnienie wiedzy na temat zagrożeń w Internecie zmieniło podejście rządzących i urzędników do bezpieczeństwa samorządowych systemów informatycznych? Czy rosną wydatki JST na zarządzanie cyberbezpieczeństwem? Czy po udostępnieniu Polsce środków z funduszy europejskich zaplanowanych w ramie finansowej Unii Europejskiej na lata 2021–2027 główną przeszkodą w zapewnieniu cyberbezpieczeństwa w dalszym ciągu jest brak funduszy, czy też brak adekwatnych kwalifikacji pracowników?

dr ANETA CHODAKOWSKA
dr hab. SŁAWOMIRA KAŃDUŁA, prof. UEP
dr JOANNA PRZYBYLSKA,
Uniwersytet Ekonomiczny w Poznaniu,
Katedra Finansów Publicznych

[46] W. Hatcher, W. Meares, J. Heslen, op.cit.

Projekt finansowany w ramach programu Ministra Nauki i Szkolnictwa Wyższego pod nazwą „Regionalna Inicjatywa Doskonałości" w latach 2019–2022, nr projektu 004/RID/2018/19, kwota finansowania 3 000 000 zł.

Słowa kluczowe: cyberbezpieczeństwo w gminach, zarządzanie bezpieczeństwem informacji w urzędzie, cyberprzestępczość, cyberataki

Bibliografia:

1. Chatfield, A. T., Reddick, C. G.: *A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government*, "Government Information Quarterly" No 36(2)/2019, pp. 346–357.
2. de Bruijn, H., M. Janssen, M.: *Building Cybersecurity Awareness: The need for evidence-based framing strategies*, "Government Information Quarterly" No 34(1)/2017.
3. Dębicka, A. J.: *Sprawne państwo*. Wolters Kluwer Polska, Warszawa 2008.

4. Hatcher, W., Meares, W., Heslen, J.: *The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices*, "Journal of Cyber Policy" No 5(2)/2020.
5. Janowski, T.: *Digital government evolution: From transformation to contextualization*, "Government Information Quarterly" No 32(3)/2015.
6. Jatkiewicz, P.: *Wdrożenie wybranych wymagań dotyczących systemów informatycznych oraz Krajowych Ram Interoperacyjności w jednostkach samorządu terytorialnego. Raport z badań*, Wyd. Polskie Towarzystwo Informatyczne, Warszawa 2016.
7. Kaczyńska, A. Kańduła, S., Przybylska, J.: *Transformacja cyfrowa z punktu widzenia samorządu terytorialnego - wybrane zagadnienia*, „Nierówności Społeczne a Wzrost Gospodarczy" nr 65(1)/2021.
8. Kańduła S., Przybylska J.: *Cybersecurity in local government: Essence, tasks and threats*, "Digital Transformation of the Financial Sector of Economy".
9. Kańduła S., Przybylska J.: *Internal Audit of the National Interoperability Framework as a Tool for Assessing Information Security in the Conditions of Economy 4.0*, [w:] Materialy Mizhnarodnoyi naukovo-praktychnoyi konferentsiyi: Innovacijnyj rozvytok ta bezpeka pidpryjemstv v umovah neoindustrial'nogo suspil'stva / Polinkiewicz O. M., Szostak L. W. (red.), Wschodnioeuropejski Państwowy Uniwersytet im. Lesi Ukrainki w Łucku, 2020.
10. Kesan, J.P., L. Zhang, L.: *An empirical investigation of the relationship between local government budgets, IT expenditures, and cyber losses*, "IEEE Transactions on Emerging Topics in Computing" No 9(2) 2019.
11. Krawiec, J., Ożarek, G.: *Certyfikacja w informatyce*, Polski Komitet Normalizacyjny, Warszawa 2014.
12. Lisiak-Felicka, D., Schmit, M.: *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, European Association for Security, Kraków 2016.
13. Lisiak-Felicka, D., Pytko, M.: *Cyberbezpieczeństwo urzędów gmin w województwie łódzkim*, „Przedsiębiorczość i Zarządzanie" nr 18(4)/2017.
14. Lisiak-Felicka, D.: *Cyberbezpieczeństwo urzędów administracji samorządowej - wyniki badań*, „IT w administracji" nr 10(143)/2019.
15. Magdziarczyk, M.: *Wdrożenie i realizacja przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 przez jednostki samorządu terytorialnego – na przykładzie gminy*, „Samorząd Terytorialny" nr 4/2021.
16. Norris, D. F., Mateczun, L., Joshi, A., Finin, T.: *Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity*, "Public Administration Review" No 79(6)/2019.
17. Norris, D. F., Mateczun, L., Joshi, A., Finin, T.: *Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity*, "Journal of Urban Affairs" 2020.
18. Salminen, M., Hossain, K.: *Digitalisation and human security dimensions in cybersecurity: An appraisal for the European High Nort*h, "Polar Record" No 54(2)/2018.
19. Schallbruch, M., I. Skierka, I.: *Cybersecurity in Germany.* Springer International Publishing, Nowy Jork 2018.

20. Świtała, K.: *Obowiązki jednostek samorządu terytorialnego w krajowym systemie cyberbezpieczeństwa*, [w:] K. Czaplicki, A. Gryszczyńska, G. Szpor (red.): *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.
21. Taddeo, M.: *Is Cybersecurity a Public Good?*, „Minds and Machines" No 29(3)/2019.
22. Ruohonen, J.: *An Acid Test for Europeanization: Public Cyber Security Procurement in the European Union*, "Europan Journal for Security Research" No 5(2)/2020.
23. Wolff, J., Lehr, W.: *When cyber threats loom, what can state and local governments do?*, "Georgetown Journal of International Affairs" No 1/2019.
24. Wygodny, A.: *Metody prowadzenia audytu cyberbezpieczeństwa*, „Kontrola Państwowa" nr 2/2021.

ABSTRACT

How Polish Local Authorities Deal with Cybersecurity – Results of Own Research

Cybersecurity is an important and complex issue that should be of interest to all levels of public administration. However, to date little research has been dedicated to this issue at the level of local government. The problem of cybersecurity of municipalities in Poland has not been well recognised so far. A gap has been diagnosed in the existing literature: there are no reports on whether Polish municipalities have adopted cybersecurity policies, whether such policies are applied in practice, and what they are about. This research is an attempt to fill in this gap. To collect the data, a CAWI method was used. The questionnaire was sent to all Polish municipalities. The research shows that the majority of them have documents describing their security policy, but they do not always apply them in practice. The awareness of counteracting cyber-attacks is not high, so more emphasis should be placed on the integration of cybersecurity policies with the management of municipality offices, emerging attacks, consultations with security auditors and increasing the number of training in cybersecurity management. The research described in the article partially fills in the knowledge gap on how to prepare to prevent cyber-attacks in Polish municipalities.

Aneta Chodakowska, PhD, **Sławomira Kańduła**, PhD, **Joanna Przybylska**, PhD, Poznań University of Economics and Business, Department of Public Finance

Key words: cybersecurity, local government, public sector, information security, Poland