Ewa Maria Włodyka*

Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa

Streszczenie

Pandemia koronawirusa w 2020 roku pokazała, że dotychczasowe schematy społeczno-gospodarcze i polityczne nie sprawdziły się w nowej rzeczywistości zarówno w sektorze gospodarczym, jak i publicznym. Jednakże to dla sektora publicznego w dobie ograniczeń spowodowanych pandemią niezbędne okazało się zapewnienie szybkiej i adekwatnej reakcji administracji publicznej na potrzeby obywateli. Wszak dostępność usług w ramach e-administracji stale się powiększa, a w związku ze skierowaniem wielu pracowników, także samorządowych, do pracy zdalnej wprowadzono w urzędach m.in. elektroniczny obieg dokumentów czy dostęp do wspólnych zasobów w chmurze. Nieprawdą byłoby wskazanie pandemii jako jedynej przyczyny digitalizacji wielu procesów administracyjnych. Sytuacja ta wymusiła jedynie przyspieszenie procesów cyfryzacji. Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne obowiązuje od 2005 roku, nowelizacje wprowadzające m.in. obowiązek rejestrowania cyfrowego obrad sesji rady gminy, powiatu czy sejmiku wojewódzkiego – od 20018 roku. Ustawa o krajowym systemie cyberbezpieczeństwa weszła w życie w 2018 roku, tzw. ustawy samorządowe regulujące zasady ustrojowe jednostek samorządu terytorialnego w trójstopniowym podziale – od roku 1999. Czy przez te ponad 20 lat jednostki samorządu terytorialnego przygotowały się na kolejne, dodatkowe, oprócz licznych zadań własnych czy zleconych, zadania związane z cyberbezpieczeństwem w związku chociażby z przytoczonymi ustawami? Hipoteza wynikająca z analizy wniosków po kontroli Najwyższej Izby Kontroli w kwestii zapewnienia bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych nie napawa optymizmem.

Słowa kluczowe: cyberbezpieczeństwo, samorząd terytorialny, e-administracja, administracja publiczna

* Dr Ewa Maria Włodyka, Wydział Humanistyczny, Politechnika Koszalińska, e-mail: ewa.wlodyka@tu.koszalin.pl, ORCID: 0000-0002-8229-342X.

Wstęp

W artykule wykorzystałam techniki badawcze adekwatne do przedmiotu i charakteru badań. Do weryfikacji tezy badawczej posłużyłam się poniższymi, odpowiednimi dla nauk o polityce i administracji metodami badawczymi, tj.: porównawczą, opisową i przede wszystkim analizą dokumentów. Przyjęta metodologia badań z wykorzystaniem materiału teoretycznego i empirycznego, z uwzględnieniem doktryny i orzecznictwa, pozwoliła na przedstawienie prognoz i wysnucie wniosków potwierdzających lub negujących postawione tezy badawcze: 1) jednostki samorządu terytorialnego (JST) podlegają tym samym przepisom, mimo że ich możliwości organizacyjne i finansowe są niezwykle zróżnicowane. Nawet małe gminy mają bardzo duży katalog zadań własnych, zbierają dane osobowe z wielu dziedzin; 2) występuje współzależność samorządu terytorialnego z cyberprzestrzenią w funkcjonowaniu administracji publicznej front office oraz back office[1]; 3) oprócz usprawnień w funkcjonowaniu e-administracji obywatele oczekują zapewnienia, że wszelkie dane będące w posiadaniu administracji publicznej są właściwie zabezpieczone przed dostępem osób nieupoważnionych; 4) cyberbezpieczeństwo nie odnosi się tylko do zapewnienia poufności danych przetwarzanych w systemach teleinformatycznych, jest zagadnieniem znacznie pojemniejszym; 5) zagrożenia związane z cyberbezpieczeństwem mogą mieć swoje konsekwencje fizyczne, także w rzeczywistości, nawet dla osób, które nie korzystają bezpośrednio m.in. z e-usług; 6) na jednostki samorządu terytorialnego zostały nałożone nowe obowiązki dotyczące cyberbezpieczeństwa; mogą one wpłynąć na wzrost poziomu cyberbezpieczeństwa w administracji samorządowej; 7) to człowiek jako część systemu społecznego jest obecnie najsłabszym ogniwem systemu cyberbezpieczeństwa w administracji publicznej (w tym w JST) w porównaniu z możliwościami infrastrukturalnymi. Powinno być szczególnie stosowane podejście human firewall; 8) funkcjonuje wsparcie infrastrukturalne oraz edukacyjne na poziomie organów centralnych, otoczenia nauki i biznesu oraz sektora pozarządowego dla bezpiecznego funkcjonowania JST w cyberprzestrzeni.

1 Rodzaj podziału organizacji pracy instytucji zaczerpnięty z nauk o zarządzaniu. Front office oznacza tę część administracji danej firmy, która ma najbardziej bezpośredni kontakt z klientami, oferuje klientom (petentom) administracji publicznej e-usługi publiczne (tzw. systemy front office). Z kolei back office oznacza systemy wspomagające procesy wewnętrzne w jednostkach administracji publicznej (tzw. systemy back office).

Na powyższy temat brakuje najnowszych opracowań naukowych o charakterze interdyscyplinarnym, mając na uwadze dynamikę zagadnienia i jego uregulowania prawne. Publikacja nie wyczerpuje wszystkich poruszonych kwestii, niemniej jednak może być przyczynkiem do dalszej dyskusji nad postawioną tezą. Pokazuje jak aktualny jest to temat.

Miejsce samorządu terytorialnego w cyberprzestrzeni

Samorząd terytorialny jest definiowany z punktu widzenia wielu teorii, koncepcji czy funkcjonujących modeli w różnorodny sposób[2]. Jednakże wspólne są pewne jego cechy, tj.: samorządność, wielość zadań własnych, niezwykle duży ich zakres tematyczny[3], który określają przede wszystkim tzw. ustawy samorządowe: z 8 marca 1990 roku o samorządzie gminnym[4], z 5 czerwca 1998 roku o samorządzie powiatowym[5] i z 5 czerwca 1998 roku *o samorządzie województwa*[6]. W ustroju politycznym Rzeczypospolitej Polskiej jego zadania zostały określone w art. 166 Konstytucji RP jako zadania publiczne służące zaspokajaniu potrzeb wspólnoty samorządowej (zadania własne) oraz inne zadania publiczne (zadania zlecone). Jednostki samorządu terytorialnego jako efekt decentralizacji administracji publicznej, w wyniku trójstopniowego podziału samorządu terytorialnego, wykonują powyższe zadania samodzielnie lub pośrednio, m.in. poprzez spółki komunalne, związki i stowarzyszenia JST czy też w formie zlecania i powierzania.

2 Główne teorie samorządu terytorialnego: naturalistyczna, państwowa, polityczna.

3 Tak zwane ustawy samorządowe zawierają długą listę zadań własnych samorządu terytorialnego, które zostały ujęte w cztery podstawowe grupy: 1) infrastruktura techniczna (drogi, wodociągi, komunikacja publiczna); 2) infrastruktura społeczna (szkolnictwo podstawowe, ochrona zdrowia, opieka społeczna); 3) porządek i bezpieczeństwo publiczne (ochrona przeciwpożarowa, sanitarna); 4) ład przestrzenny i ekologiczny (gospodarka terenowa i ochrona środowiska).

4 Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym, Dz.U. 1990, nr 16, poz. 95.

5 Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym, ibidem 1998, nr 91 poz. 578.

6 Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa, ibidem, poz. 576.

Do bogatej listy zadań realizowanych przez JST należałoby dołożyć ich pokaźną liczbę –2807[7], przy czym każda jest utożsamiana, na potrzeby artykułu, z konkretnym urzędem[8].

Ogólnoświatowe trendy w gospodarce z charakterystycznymi dla kolejnych etapów jej rozwoju (aktualnie: Przemysł 4.0 czy też rewolucja społeczna w kontekście rozwoju społeczeństw) mają swoje przełożenie na funkcjonowanie administracji publicznej. Zwiększający się udział technologii informatycznych w życiu codziennym obywateli oraz oczekiwania społeczne co do ułatwienia i przyspieszenia procedur usług realizowanych przez samorządy spowodowały wzrost wykorzystywania w coraz większym stopniu nowoczesnych technologii informacyjno-komunikacyjnych, tzw. ICT. Zmianie ulegają procesy organizacji pracy urzędów nie tylko front office, lecz także back office. Zjawisko cyfryzacji administracji publicznej starały się regulować kolejne ustawy[9]: z 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne

7 Według stanu na 1 stycznia 2021 r. w Polsce mamy: 16 województw, 314 powiatów i 66 miast na prawach powiatu oraz 2477 gmin. Zob. *Podział administracyjny Polski*, https://stat.gov.pl/statystyka-regionalna/jednostki-terytorialne/podzial-administracyjny-polski/ [dostęp: 1.02.2022].

8 Urzędy będące aparatem pomocniczym organu wykonawczego JST to: urząd gminy/miasta na poziomie samorządu gminnego, urząd starostwa powiatowego na poziomie samorządu powiatowego, urząd marszałkowski na poziomie samorządu wojewódzkiego.

9 Jest to jedynie przykład aktów prawnych odnoszących się do powszechnie pojętej informatyzacji, cyfryzacji, cyberbezpieczeństwa przestrzeni publicznej. Regulacje prawne obszernie definiują oraz określają obowiązki podmiotów publicznych w zakresie cyberbezpieczeństwa. Między innymi art. 2 ust. 1b ustawy z 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. 2002, nr 156 poz. 1301) stanowi, że cyberprzestrzeń to „przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Zgodnie z art. 13 ust. 1 ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne „podmiot publiczny używa do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności". Zgodnie z rozporządzeniem KRI „podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji". Zadania mające na celu zapewnienie ochrony danych osobowych zostały określone w nowym unijnym rozporządzeniu RODO, które weszło w życie 25 maja 2018 r. i ujednoliciło przepisy dotyczące ochrony danych osobowych dla wszystkich państw członkowskich UE. Celem RODO było także unowocześnienie regulacji o ochronie danych osobowych, które obowiązywały od 1995 r. i w dobie cyfrowej rewolucji miały coraz mniejsze zastosowanie praktyczne. Jednocześnie RODO zostało zredagowane tak, żeby było zawsze aktualne niezależnie od rozwoju technologii.

(tzw. Krajowe Ramy Interoperacyjności)[10]; z 2018 rok – nowelizacje ustaw samorządowych wprowadzające m.in. obowiązek rejestrowania cyfrowego obrad sesji rady gminy, powiatu czy sejmiku wojewódzkiego; rozporządzenie o ochronie danych (RODO)[11]. W 2018 roku weszła w życie ustawa o krajowym systemie cyberbezpieczeństwa[12], która wyznaczyła jednostkom samorządu terytorialnego dodatkowe zadania dotyczące cyberbezpieczeństwa.

Z roku na rok z powodu wielu czynników[13] stopień wykorzystywania przez JST usług e-administracji[14] rośnie. W 2020 roku usługi elektroniczne oferowało obywatelom 99,3% jednostek administracji publicznej, w tym wszystkie urzędy powiatowe i marszałkowskie[15]. Wykorzystanie szerokopasmowych łączy jest podstawowym warunkiem prawidłowego funkcjonowania sprawnej administracji w cyberprzestrzeni – w 2020 roku dostęp do Internetu poprzez łącze w technologii DSL zadeklarowało 99,9% JST[16]. W tym czasie jedynie dwie trzecie jednostek administracji publicznej przeprowadziło audyt bezpieczeństwa systemu informacyjnego, 86,9% zapewniało swoim pracownikom urządzenia przenośne pozwalające na mobilne łączenie się z Internetem w celach służbowych, a 80,7% deklarowało korzystanie z elektronicznego zarządzania dokumentacją. Wsparcie technologiczne dla JST w postaci przeznaczonej do tych celów aplikacji i programów e-administracji można przedstawić jako te, które realizują zadania w konkretnej dziedzinie (m.in. generator wniosków i e-deklaracji, poboru opłat i podatków lokalnych, systemy monitoringu sesji rad organów uchwałodawczych, systemy planowania przestrzennego) lub kompleksowe (front office wraz z back office), systemy IT do obsługi zadań zleconych (e-PUAP, SSDIP, CEIDG, Źródło/SRP, Emp@tia, EMUiA, Besti@).

10 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005, nr 64, poz. 565.

11 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych RODO), Dz. Urz. UE 2016, L 119.

12 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018, poz. 1560.

13 Wymienić należy nie tylko skutki przyspieszenia tychże procesów ICT w wyniku pandemii wirusa COVID-19, lecz także celowe kierunku polityki państwa.

14 Rozumianej jako część zarówno „front office", jak i „back office" wykorzystującą cyberprzestrzeń w realizacji zadań JST.

15 *Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej w 2020 r.*, Warszawa 2021.

16 Ibidem.

Samorządy powszechnie korzystają z różnego rodzaju systemów informatycznych[17] do gromadzenia i przetwarzania danych w związku z realizowanymi przez nie zadaniami, którym to systemom muszą zapewnić bezpieczeństwo[18].

Na podstawie powyższych rozważań można stwierdzić, że istnieje współzależność między samorządem terytorialnym a cyberprzestrzenią. Obracanie się w niej wiąże się nie tylko z korzyściami dla jej podmiotów, lecz także z wieloma zagrożeniami. Nie udaje się ich uniknąć nawet tym większym JST – o większych zasobach finansowych, kadrowych, większej liczbie mieszkańców. Przykładem złamania zasad cyberbezpieczeństwa jest tu chociażby wyciek danych z gminy liczącej 470 tys. mieszkańców miasta Gdańska, gdzie przez ponad kwartał w systemie budżetu obywatelskiego można było podejrzeć dane osobowe (imię i nazwisko oraz numer PESEL) prawie 100 mieszkańców popierających wybrane projekty. Dotyczyło to także osób, które nie wyraziły zgody na udostępnienie danych[19]. Innym przykładem niebezpieczeństwa związanego z obecnością w cyberprzestrzeni jest gmina Kościerzyna[20] (15 tys. mieszkańców) oraz samorząd województwa małopolskiego (prawie 3,5 mln mieszkańców) [21], od których zażądano w 2021 roku okupu za odszyfrowanie

17 Świadczenie usługi drogą elektroniczną to „[...] wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy" – zob. Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, Dz.U. 2004, nr 171, poz. 1800. Przykłady e-administracji, gdzie administratorem narzędzi i aplikacji jest administracja centralna: e-PUAP, Profil zaufany, mObywatel, Konto pacjenta.

18 Tendencją, oprócz sektora gospodarczego, w administracji publicznej jest już nie tylko zbieranie i ochrona danych, lecz także analiza i przetwarzanie danych (tzw. business intelligence).

19 Do ujawnienia danych mieszkańców doszło dzięki możliwości pobrania z systemu budżetu obywatelskiego skanu list zawierających ich imiona i nazwiska, adresy oraz podpisy. Dane dostępne były od 3 października 2021 do 9 stycznia 2022 r. Naruszenie zostało zgłoszone do UODO i – według Urzędu Miasta w Gdańsku – usunięte. Zob. *Wyciekły dane z systemu budżetu obywatelskiego w Gdańsku. Miasto wcześniej zaprzeczało*, https://cyberdefence24.pl/cyberbezpieczenstwo/wyciekly-dane-z-systemu-budzetu-obywatelskiego-w-gdansku-miasto-wczesniej-zaprzeczalo [dostęp: 20.01.2022].

20 J. Surażyńska, *Haker zaszyfrował dane. Teraz żąda okupu od gminy. Mieszkańcy są pełni obaw*, https://koscierzyna.naszemiasto.pl/haker-zaszyfrowal-dane-teraz-zada-okupu-od-gminy-mieszkancy/ar/c1-7462597 [dostęp: 20.01.2022].

21 Doszło do naruszenia bezpieczeństwa danych osobowych m.in. klientów instytucji. Sprawa została zgłoszona do Agencji Bezpieczeństwa Wewnętrznego oraz Policji, zawiadomiono także Prezesa Urzędu Ochrony Danych Osobowych oraz Naukową i Akademicką Sieć Komputerową (NASK). Zob. *Cyberprzestępcy żądają okupu za odszyfrowanie serwerów małopolskiego urzędu marszałkowskiego*, https://samorzad.pap.pl/kategoria/e-urzad/

sparaliżowanej przez złośliwe oprogramowanie znacznej części systemu IT urzędu. Tylko w 2021 roku zespół CERT Polska odnotował aż 525 incydentów w JST[22]. O innych przykładach informuje w swoich komunikatach Najwyższa Izba Kontroli[23].

Jednostki samorządu terytorialnego a krajowy system cyberbezpieczeństwa

Jednostki samorządu terytorialnego jako część administracji publicznej są podmiotem krajowego systemu cyberbezpieczeństwa (KSC). Ustawa o KSC w rozdziale piątym określa obowiązki podmiotów publicznych oraz JST, które pojawiły się wraz z ustawą i funkcjonują aktualnie czwarty rok. Na podstawie art. 4 pkt 7 rzeczonej ustawy w związku z art. 9 pkt 2 ustawy o finansach publicznych[24] do podmiotów objętych KSC należą JST oraz ich związki. W ustawie o KSC zapisano: „Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa"[25].

Jednakże między ust. 1 a ust. 3 zachodzi różnica: „Jednostka samorządu terytorialnego może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa

cyberprzestepcy-zadaja-okupu-za-odszyfrowanie-serwerow-malopolskiego-urzedu [dostęp: 20.01.2022].

22 Zespół CERT Polska działa w strukturach NASK – państwowego instytutu badawczego prowadzącego od 1996 r. działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty.

23 W latach 2013–2014 hakerzy okradli pięć polskich gmin, w tym gminę Jaworzno na prawie milion złotych. W 2014 r. z Urzędu Miejskiego w Przemyślu wyciekły dane dzieci. W 2017 r. z Urzędu Miasta Łodzi wyciekły dane z tzw. deklaracji śmieciowych, dzięki czemu bez problemu można było poznać dane właścicieli łódzkich nieruchomości. W 2018 r. wyciekły dane części posiadaczy karty krakowskiej. Zob. *Żeby elektronicznie znaczyło bezpiecznie. NIK o zarządzaniu bezpieczeństwem informacji w jednostkach samorządu terytorialnego*, https://www.nik.gov.pl/aktualnosci/zeby-elektronicznie-znaczylo-bezpiecznie.html [dostęp: 20.01.2022].

24 Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych, Dz.U. 2019, poz. 869.

25 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa..., art. 21, ust. 1.

w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jej jednostki organizacyjne”[26].

Nie chodzi jedynie o podmiotowość powyższych ustępów, ale i o ich przedmiotowość – wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa dla podmiotów publicznych jest obligatoryjne, dla JST zaś jedynie fakultatywne. Stąd pośrednio wynika brak konsekwencji za niewyznaczenie osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa. Kwestią z obszaru filozofii prawa byłoby dywagowanie, czy takowa dobrowolność wpisuje się w podstawowe koncepcje samorządu terytorialnego – jego samostanowienia tej samorządności. Jednakże, czy jest to zadowalający argument braku obligatoryjności, biorąc pod uwagę wzrost znaczenia cyberbezpieczeństwa administracji publicznej? Należałoby się posłużyć pełnymi wynikami badań faktycznego utworzenia omawianego stanowiska kontaktowego. Z przeprowadzonych przeze mnie badań cząstkowych wynika, że w praktyce w czasie obowiązywania ustawy o KSC bardzo często zdarza się łączenie w JST stanowisk inspektora RODO i ds. kontaktów z CSIRT NASK. Rozwiązanie to ma swoje uzasadnienie z racji obowiązków na tych stanowiskach, lecz znane są takie uchybienia w funkcjonowaniu inspektora RODO w JST, jak: brak stanowiska inspektora RODO[27], łączenie stanowiska inspektora RODO ze stanowiskiem informatyka lub pod kątem zakresu zadań z odległymi innymi stanowiskami. W niektórych jednostkach samorządowych często jest to spowodowane niskim wynagrodzeniem na stanowisku inspektora RODO, co prowadzi do niepożądanych sytuacji. Dość powszechnym zjawiskiem jest to, że jeden inspektor danych osobowych obsługuje na podstawie umowy zlecenia nawet kilka podmiotów lub jest inspektorem „korespondencyjnym” albo „widmo” (nie pojawia się w urzędzie JST bezpośrednio, a świadczy usługi jedynie online). W kontekście prawidłowości wypełniania zaleceń ustawy o KSC (skoro mowa o fakultatywności zapisów art. 22 ust. 3 ustawy o KSC) zasadne jest pytanie nie tylko o dobrowolność wyznaczania osoby kontaktowej w JST, ale i o łączenie tego

26 Ibidem, art. 21, ust. 3.

27 Na przykład zarzut wobec starostwa we Wschowie braku formalnego (np. w drodze zarządzenia, aktu powołania) wyznaczenia przez administratora danych osobowych (starostę) osoby na stanowisko inspektora ochrony danych osobowych. Ponadto w obowiązującym „Regulaminie organizacyjnym starostwa” nie wyodrębniono tego stanowiska (brak jakichkolwiek zapisów dotyczących IOD). Zob. *Wdrożenie przez jednostki samorządu terytorialnego z województwa lubuskiego regulacji dotyczących ochrony danych osobowych nr I/19/003*, Warszawa 2019.

stanowiska z innymi w danym urzędzie. Należałoby tu wziąć pod uwagę charakter i możliwości finansowo-organizacyjne JST (małe, mniej zasobne urzędy gmin, a urzędy marszałkowskie dysponujące rozbudowaną strukturą biurokratyczną).

Zarządzanie incydentem[28], które jest drugim wskazanym w ustawie o KSC zadaniem JST, w myśl art. 22 ust. 1[29] obejmuje: zgłaszanie i obsługę incydentu. Obsługa ta definiowana jest jako „[...] czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu"[30].

Wraz z wejściem w życie ustawy o krajowym systemie bezpieczeństwa na NASK został nałożony obowiązek pełnienia funkcji jednego z trzech CSIRT poziomu krajowego[31]. CSIRT NASK przyjmuje, analizuje i podejmuje działania oraz koordynuje reakcje na incydenty dotyczące bezpieczeństwa cywilnej cyberprzestrzeni Polski, w tym na incydenty w podmiocie publicznym i JST oraz na incydenty związane z nielegalnymi treściami publikowanymi w Internecie i zagrażającymi bezpieczeństwu dzieci.

Znów pojawia się pytanie o fakultatywność pewnych działań, zwłaszcza o rejestrowanie zgłaszanych incydentów przez CSIRT NASK, ponieważ

28 „Incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15" – zob. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa..., art. 2, ust. 9.

29 „Podmiot publiczny […] realizujący zadanie publiczne zależne od systemu informacyjnego: 1) zapewnia zarządzanie incydentem w podmiocie publicznym; 2) zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV; 3) zapewnia obsługę incydentu w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe; 4) zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej; 5) przekazuje do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV dane osoby, o której mowa w art. 21, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany" – zob. ibidem, art. 22, ust. 1.

30 Ibidem, art. 2, ust. 10.

31 W polskim systemie cyberbezpieczeństwa działają trzy zespoły Computer Security Incident Response Team (CSIRT) odpowiedzialne za poszczególne dziedziny funkcjonowania państwa. Do CSIRT NASK incydenty zgłasza większość operatorów usług kluczowych, dostawcy usług cyfrowych, samorząd terytorialny oraz pozostałe podmioty, których nie obsługują CSIRT GOV i MON. Incydenty mogą także zgłaszać obywatele.

z zapisów ustawy o KSC nie wynika wprost prowadzenie rejestru incydentów przez JST. Wobec tego można postawić hipotezę, że JST nie ponoszą odpowiedzialności za brak rejestru incydentów. W tym miejscu należałoby wspomnieć o kolejnej tendencji w obszarze gromadzenia informacji, zaczerpniętej z sektora gospodarczego – zbierane informacje są nie tylko celem samym w sobie, lecz także narzędziem podejmowania decyzji, analizy, mogą być chociażby źródłem profilaktyki cyberbezpieczeństwa. W związku z tym, czy JST faktycznie, skoro jest to jedynie ich fakultatywność, będą takie rejestry prowadziły? Hipoteza ta jest doskonałym zagadnieniem do badań kolejnych, ale poniższe wyniki pozwolą udzielić choć cząstkowej odpowiedzi na powyższe pytanie.

Najwyższa Izba Kontroli – wnioski po kontrolach w jednostkach samorządu terytorialnego

Kontrole przeprowadzone przez Najwyższą Izbę Kontroli[32] w wybranych JST już w 2014 roku[33] i 2016 roku[34] ujawniły istotne nieprawidłowości w zapewnieniu bezpieczeństwa systemów informatycznych i zgromadzonych w nich danych o mieszkańcach poszczególnych urzędów. Wskazywano w nich na brak systemowego podejścia kierowników urzędów do zarządzania bezpieczeństwem informacji oraz właściwego zabezpieczenia danych będących w posiadaniu urzędów. Pomimo upływu kilku lat nadal nie nastąpiła poprawa w tym zakresie, co – zdaniem NIK – rodzi obawy o bezpieczeństwo danych w sytuacji rozwoju e-usług administracji publicznej i gromadzenia i przetwarzania przez nią coraz większej ilości danych w postaci elektronicznej. W wyniku przeprowadzonej w 2014 roku kontroli wdrażania wybranych wymagań wobec systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności nieprawidłowości w zapewnieniu bezpieczeństwa systemów informatycznych stwierdzono w 87% skontrolowanych urzędów miast. Kontrola NIK z 2016 roku dotycząca systemu rejestrów

32 Misją Najwyższej Izby Kontroli jest dbałość o gospodarność i skuteczność w służbie publicznej dla Rzeczypospolitej Polskiej

33 *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*, Warszawa 2014.

34 *Świadczenie usług publicznych w formie elektronicznej na przykładzie wybranych jednostek samorządu terytorialnego*, Warszawa 2016.

państwowych[35] wykazała, że kierownicy kontrolowanych urzędów na ogół nie przywiązywali dostatecznej wagi do zapewnienia bezpieczeństwa przetwarzania informacji z wykorzystaniem tego systemu, w którym przetwarzane są istotne dane o obywatelach (m.in.: imię, nazwisko, nr PESEL, adres)[36].

Tabela 1. Wnioski po kontroli i przykłady uchybień w JST w zakresie ochrony informacji i danych osobowych wykazane przez Najwyższą Izbę Kontroli

Rodzaj uchybienia	Przykłady uchybienia/wniosek	Procent urzędów JST
Niekompletne procedury ochrony danych	brak systemowego podejścia do zapewnienia bezpieczeństwa informacji, o którym mowa w par. 20 ust. 1 rozporządzenia KRI – opracowane i wdrożone regulacje dotyczyły głównie danych osobowych i nie obejmowały bezpieczeństwa innych informacji	61
	nie ustanowiono polityk bezpieczeństwa informacji	61
Niedostosowanie wewnętrznych regulacji do przepisów RODO	brak wdrożenia aktualizacji uregulowań wewnętrznych w zakresie ochrony danych osobowych w związku z wejściem w życie przepisów RODO	26
Realizacja przez inspektora danych osobowych innych zadań mogących wywoływać konflikt interesów	we wszystkich jednostkach został powołany inspektor danych osobowych, ale inne zadania i obowiązki wykonywane przez osobę pełniącą funkcję IOD mogły powodować konflikt interesów, o którym mowa w art. 38 ust. 6 RODO	22
Brak informacji lub niepełna informacja o posiadanych zasobach informatycznych	brak prowadzonej na bieżąco inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji pod kątem ich rodzaju i konfiguracji	74
	zgromadzone dane w tym zakresie były nierzetelne	29
	nie zidentyfikowano wszystkich zbiorów danych będących w posiadaniu urzędu lub sporządzony wykaz aktywów informacyjnych nie był prowadzony rzetelnie	26

35 *System rejestrów państwowych – bezpieczeństwo, funkcjonowanie i użyteczność*, Warszawa 2016.

36 W 62% skontrolowanych urzędów miast nie opracowano i nie wdrożono polityk bezpieczeństwa informacji, w 38% wystąpiły nieprawidłowości w blokowaniu lub odbieraniu dostępu do systemu byłym pracownikom, a w 23% nie przeprowadzano obowiązkowego corocznego audytu bezpieczeństwa informacji. W związku z powyższym podjęto decyzję o przeprowadzeniu w urzędach JST kontroli bezpieczeństwa informacji oraz działań związanych z zapewnieniem wdrożenia niektórych wymogów RODO. Najwyższa Izba Kontroli negatywnie oceniła wykonywanie przez blisko 70% skontrolowanych urzędów JST zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji w okresie objętym kontrolą. Zob. ibidem.

Rodzaj uchybienia	Przykłady uchybienia/wniosek	Procent urzędów JST
Niewłaściwe zarządzanie uprawnieniami użytkowników systemów informatycznych	nie opracowano i nie wdrożono pisemnych procedur zarządzania uprawnieniami użytkowników w systemach informatycznych	17
	brak dokumentowania czynności związanych z zarządzaniem uprawnieniami użytkowników	22
	w przypadku 23 osób, spośród 157, które zakończyły zatrudnienie, stwierdzono, że ich konta nie zostały zablokowane i pozostawały wciąż aktywne	30
	użytkownicy posiadali na swoich komputerach uprawnienia administratora systemu, w związku z tym mieli możliwość zainstalowania dowolnego oprogramowania	52
Stosowanie niewłaściwych haseł do systemów	stosowanie przez użytkowników haseł dostępu do systemów informatycznych krótszych niż wymagane	57
	nie korzystano z istniejących w oprogramowaniu funkcji, które wymuszają stosowanie zasad dotyczących złożoności haseł ustanowionych w urzędzie (m.in. wartość „-1" daty obowiązywania zmiany hasła, hasła od 2013 r.)	57
Nieustanowienie zasad pracy mobilnej	nie określono szczegółowych zasad i procedur korzystania przez pracowników z urządzeń przenośnych poza ich siedzibami, gwarantujących bezpieczną pracę podczas przetwarzania mobilnego i pracy na odległość	35
Niewłaściwe zabezpieczenie danych zgromadzonych na urządzeniach mobilnych	nie stosowano szyfrowania dysków twardych komputerów przenośnych	70
Niewłaściwe zabezpieczenie serwerowni	zastosowano zabezpieczenia fizyczne serwerowni, które w niewystarczającym stopniu chroniły te pomieszczenia	43
Brak zapisów dotyczących zachowania poufności informacji w umowach serwisowych	w umowach na zakup lub serwis sprzętu komputerowego/oprogramowania objętych badaniem stwierdzono brak zapisów gwarantujących zabezpieczenie poufności informacji uzyskanych przez wykonawców w związku z realizacją tych umów	52
Wykorzystywanie oprogramowania nieposiadającego wsparcia producenta	wykorzystywanie komputerów z zainstalowanym systemem operacyjnym nieposiadającym już wsparcia producenta	56
Niewłaściwe tworzenie kopii zapasowych	nie powadzono okresowych analiz ryzyka utraty integralności, poufności, dostępności	48
	nie przeprowadzono analizy procesów przetwarzania danych osobowych i nie dokonano oceny stopnia zapewnienia ich bezpieczeństwa w odniesieniu do stwierdzonych ryzyk, o których mowa w art. 32 ust. 1 RODO	30

Rodzaj uchybienia	Przykłady uchybienia/wniosek	Procent urzędów JST
Procedury dotyczące incydentów bezpieczeństwa	ustanowiono i wprowadzono procedury wewnętrzne zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji przewidziane w par. 20 ust. 2 pkt 13 rozporządzenia KRI	78
	urzędy opracowały i stosowały uregulowania dotyczące zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu	99
Nieprzeprowadzanie audytów bezpieczeństwa informacji	w 2017 r. nie przeprowadzono obowiązkowego audytu bezpieczeństwa informacji	70
Zapewnienie szkoleń z bezpieczeństwa informacji i RODO	zorganizowano dla pracowników szkolenia dotyczące bezpieczeństwa informacji	83
	zapewniono szkolenia z zakresu ochrony i przetwarzania danych osobowych uwzględniające przepisy RODO	91%
Niewiele kontroli bezpieczeństwa informatycznego w JST przeprowadzonych przez wojewodów	od 1 stycznia 2016 do końca lutego 2018 r. przeprowadzono łącznie 40 kontroli w 12 województwach, kontroli takich nie przeprowadzono w czterech województwach	cztery województwa bez kontroli bezpieczeństwa informatycznego przez wojewodów

Źródło: opracowanie własne na podstawie: *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego. Informacja o wynikach kontroli*, Warszawa 2019.

W 61% skontrolowanych urzędów[37] JST brak było systemowego podejścia do zapewnienia bezpieczeństwa informacji[38]. W 74% nie prowadzono 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 26% stwierdzono niedostosowanie uregulowań wewnętrznych dotyczących ochrony danych osobowych do przepisów RODO. W 22% jednostek

37 Kontrole przeprowadzono w 23 jednostkach – w 9 starostwach powiatowych oraz 14 urzędach miast i gmin. Zob. *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego. Informacja o wynikach kontroli*, Warszawa 2019.

38 Ibidem.

samorządów osoby pełniące funkcję inspektora ochrony danych wykonywały inne zadania i obowiązki, które mogły powodować konflikt interesów. W wielu skontrolowanych urzędach nie dostrzegano występujących zagrożeń. W 48% nie przeprowadzono analiz ryzyka, a w 70% – obowiązkowego corocznego audytu bezpieczeństwa informacji. Stąd brak cyklicznych analiz ryzyka i audytów bezpieczeństwa nie pozwalał na wskazanie istotnych ryzyk związanych z bezpieczeństwem informacji. W ponad 80% skontrolowanych JST wystąpiły nieprawidłowości w zarządzaniu uprawnieniami użytkowników w systemach informatycznych. W wyniku przeprowadzonego badania blokowania lub odbierania dostępu do systemów informatycznych 157 osobom, które zakończyły zatrudnienie w kontrolowanych urzędach, stwierdzono, że 23 byłym pracownikom (tj. 15%) z siedmiu urzędów konta nie zostały zablokowane i wciąż były aktywne. Było to niezgodne z par. 20 ust. 2 pkt 5 rozporządzenia Krajowych Ram Interoperacyjności stanowiącym, że zarządzanie bezpieczeństwem informacji jest realizowane w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających wykonanie i egzekwowanie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji[39]. Wobec 12 urzędów sformułowano również uwagi dotyczące niepotrzebnego udostępnienia wszystkim pracownikom szczegółowych procedur stosowanych rozwiązań technicznych oraz zabezpieczeń.

We wnioskach po kontroli organów wykonawczych JST zawarto wiele zaleceń wprowadzenia zmian we wskazanych kwestiach[40]. W związku

39 Przykłady: w Urzędzie Miasta Brańsk jednemu pracownikowi zablokowano dostęp do systemu informatycznego po ponad 11 latach od ustania zatrudnienia, dopiero w trakcie kontroli NIK. W Starostwie Powiatowym w Piasecznie 12 spośród 14 osób, które od 1 czerwca 2017 do 4 czerwca 2018 r. zakończyły pracę w urzędzie, miało aktywne uprawnienia do systemów informatycznych takich, jak: Elektroniczne Zarządzanie Dokumentacją, Kataster OnLine, Ośrodek, aplikacja do informacji przestrzennej GIS, Ekoportal. Jednej z tych osób nie zablokowano konta umożliwiającego dostęp do systemu operacyjnego. Starosta wyjaśnił m.in., że w okresie objętym kontrolą uprawnienia odbierano na podstawie karty obiegowej, ale nie zawsze było to przestrzegane.

40 „Po kontroli NIK wnioskowała o: 1) prowadzenie okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI; 2) opracowanie i wdrożenie oraz aktualizowanie Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z § 20 ust. 1 rozporządzenia KRI; 3) prowadzenie aktualnej i kompletnej elektronicznej ewidencji sprzętu informatycznego, obejmującej jego rodzaj i konfigurację, zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI; 4) wdrożenie rozwiązań zapewniających odpowiednie zabezpieczenie pomieszczeń serwerowni, zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI; 5) zapewnienie prowadzenia przynajmniej raz w roku okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 14

z uchybieniami wykazanymi podczas kontroli była planowana pomoc o charakterze edukacyjnym na poziomie administracji centralnej oraz Komisji Wspólnej Rządu i Samorządu Terytorialnego[41].

Co ciekawe, organy wykonawcze JST najczęściej wskazywały, że przyczyną tych nieprawidłowości były błędy popełnione przez człowieka a nie brak sprzętu i oprogramowania. Tłumaczono je m.in.: natłokiem obowiązków, brakiem specjalistycznego oprogramowania, a także częstą rotacją pracowników, niedopatrzeniem zatrudnionych na stanowisku informatyka[42]. Jest to zresztą zgodne z ogólnoświatowymi wynikami wskazującymi przyczyny łamania procedur cyberbezpieczeństwa – w 95% uskutecznionych cyberataków przyczyna leży po stronie człowieka, a nie systemu[43]. Dlatego na popularności zyskuje koncepcja tzw. human firewall[44], która uwzględnia człowieka jako niezwykle istotny element firewall (rozumianego jako zaporę sieciową pod postacią oprogramowania wraz lub osobno z urządzeniem sieciowym, które monitorują

rozporządzenia KRI; 6) zapewnienie dokumentowania procesu nadawania uprawnień użytkowników systemów informatycznych; 7) przyznawanie pracownikom urzędów uprawnień w systemach informatycznych adekwatnych do realizowanych zadań, zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI; 8) dostosowanie uregulowań wewnętrznych w zakresie danych osobowych do wymogów RODO; 9) prowadzenie rejestru czynności przetwarzania danych, o którym mowa w art. 30 RODO; 10) przeprowadzenie analizy i oceny procesów przetwarzania danych o których mowa w art. 32 ust. 1 RODO" – zob. ibidem, s. 11.

41 Mowa o działaniach takich, jak: zaangażowanie JST w ćwiczenia ogólnokrajowe dotyczące cyberbezpieczeństwa; dystrybucja gotowych narzędzi (tzw. toolboxy) przygotowanych przez specjalistów z NASK; akcje informacyjne dla kierowników jednostek o obowiązkach wynikających z przepisów prawa wraz z poradami jak je realizować z wykorzystaniem dostępnych środków; utworzenie platformy e-learningowej. W dalszej kolejności, w miarę możliwości organizacyjnych i finansowych, planowane są następujące działania: wdrożenie systemu szkoleń dla osób zajmujących kierownicze stanowiska w JST, w szczególności w okresie po wyborach samorządowych, gdy następują zmiany na tych stanowiskach; przygotowanie scenariuszy szkoleniowych podnoszących świadomość wśród szeregowych pracowników (tzw. cyberhigiena); organizacja wsparcia w budowie systemów zarządzania bezpieczeństwem, w tym standaryzacja dokumentacji normatywnej SZBI, metodyk zarządzania ryzykiem, planowania ciągłości działania, procedur operacyjnych; agregacja nadzoru nad cyberbezpieczeństwem w JST w postaci regionalnych centrów operacyjnych. Odpowiedź ministra cyfryzacji Marka Zagórskiego na interpelację poselską zob. M. Zagórski, *Dot. pisma z 22 maja br. posła na Sejm RP Pana Adama Ołdakowskiego w sprawie podatności administracji publicznej na ataki hakerskie (interpelacja nr 31486)*, Warszawa, 10 czerwca 2019, https://orka2.sejm.gov.pl/INT8.nsf/klucz/ATTBD3HT8/%24FILE/i31486-o1.pdf [dostęp: 20.01.2022].

42 *Zarządzanie bezpieczeństwem informacji…*, s. 25.

43 www.netpresenter.com [dostęp: 20.02.2022].

44 Więcej zob. A. Belaz, S. Zsolt, *The human firewall – the human side of cybersecurity*, 2020, https://www.researchgate.net/publication/344541190_THE_HUMAN_FIREWALL_the_human_side_of_cybersecurity [dostęp: 2.02.2022].

wchodzący i wychodzący ruch sieciowy i podejmują decyzje o identyfikacji zagrożenia z sieci zewnętrznej, np. Internet). Wdrożenie metodyki mogłoby polegać m.in.: na określeniu miejsca i roli informatyka oraz inspektora danych osobowych w JST, podejściu tychże organów JST do prowadzenia polityki cyberbezpieczeństwa, szkolenia i uświadamianie pracowników samorządowych.

Oprócz wymienionych wcześniej rozwiązań w praktyce funkcjonuje, nie tylko w polityce cyberbezpieczeństwa, wsparcie infrastrukturalne (m.in. NASK[45], e-administracja centralna), a także o charakterze edukacyjnym na poziomie organów centralnych, otoczenia nauki i sektora biznesu oraz sektora pozarządowego (m.in. Stowarzyszenie „Miasta w Internecie"[46]) dla bezpiecznego funkcjonowania JST w cyberprzestrzeni.

Zakończenie

Wraz z wkraczaniem gospodarki w erę Przemysłu 4.0 i z rewolucją cyfrową społeczeństw w administracji publicznej rosną procesy cyfryzacyjne. Oczekiwania obywateli dotyczą już nie tylko usprawnień w funkcjonowaniu e-administracji i powiększania katalogu e-usług, lecz także zapewnienia, że wszelkie dane tak powszechnie zbierane i przechowywane będą dostatecznie zabezpieczone przed cyberatakami i dostępem osób nieupoważnionych. Występuje współzależność między samorządem terytorialnym a cyberprzestrzenią w funkcjonowania administracji publicznej front office oraz back office.

Jednostki samorządu terytorialnego obowiązują te same przepisy, choć ich możliwości organizacyjne i finansowe są niezwykle zróżnicowane. Nawet

45 NASK jest państwowym instytutem badawczym nadzorowanym przez Kancelarię Prezesa Rady Ministrów. W zakresie cyberbezpieczeństwa i ochrony użytkowników kluczowym polem aktywności NASK są działania związane z zapewnieniem bezpieczeństwa Internetu. Zob. www.nask.pl [dostęp: 20.02.2022].

46 Stowarzyszenie „Miasta w Internecie" jest ekspercką organizacją pozarządową działającą od 1998 r. na rzecz rozwoju cyfrowego samorządów oraz wspierania rozwoju kompetencji cyfrowych. Wspiera polskie gminy i regiony, inicjuje i realizuje innowacyjne projekty, bada cyfrową rzeczywistość w Polsce. Od 24 lat organizuje konferencje nt. „Miasta w Internecie" – spotkania przedstawicieli środowisk samorządowych w Polsce. Jest think tankiem mającym mocne zaplecze badawcze oraz umiejętności i możliwości wykorzystania najlepszej europejskiej wiedzy. To także organizacja wdrażająca wyniki badań i eksperymentów w praktyce inwestycji samorządowych zarówno lokalnych, jak i regionalnych. Jedną z podstawowych pól aktywności jest doradzanie samorządom (studia wykonalności, strategie, konsultacje) w zakresie realizacji projektów informatycznych i edukacyjnych. Zob. https://www.mwi.pl [dostęp: 20.02.2022].

małe gminy mają bardzo duży katalog zadań własnych, zbierają dane osobowe z wielu dziedzin, a wszystkie są narażone na cyberprzestępczość i dlatego powinny tworzyć politykę cyberbezpieczeństwa i uwzględniać ją w trakcie wykonywania zadań. Jej realizacja odbywa się m.in. poprzez wyznaczenie pewnych, choć częściowo fakultatywnych zadań w ustawie o krajowym systemie cyberbezpieczeństwa (wyznaczanie osoby odpowiedzialnej za kontakty z podmiotami systemu cyberbezpieczeństwa oraz zarządzanie incydentami). Obywatele oprócz usprawnień w funkcjonowaniu e-administracji oczekują bezpieczeństwa pozyskiwanych i przechowywanych danych osobowych. Samo cyberbezpieczeństwo nie odnosi się tylko do zapewnienia poufności danych przetwarzanych w systemach teleinformatycznych, jest bowiem zagadnieniem znacznie pojemniejszym, a zagrożenia z nim związane i jego konsekwencje w przypadku JST mogą być fizyczne również w rzeczywistości, nawet dla osób, które nie korzystają bezpośrednio m.in. z e-usług[47]. Do działań zapobiegawczych i naprawczych należy wsparcie infrastrukturalne oraz edukacyjne na poziomie organów centralnych, nauki i biznesu oraz sektora pozarządowego na rzecz bezpiecznego funkcjonowania JST w cyberprzestrzeni. Należy mieć na uwadze, że to człowiek, jako część systemu społecznego, jest obecnie najsłabszym ogniwem systemu cyberbezpieczeństwa w administracji publicznej (w tym JST) w porównaniu z możliwościami i rozwiązaniami infrastrukturalnymi. Dlatego w sposób szczególny powinno być stosowane podejście human firewall.

Bibliografia

Belaz A., Zsolt S., *The human firewall – the human side of cybersecurity*, 2020, https://www.researchgate.net/publication/344541190_THE_HUMAN_FIREWALL_the_human_side_of_cybersecurity [dostęp: 2.02.2022].

Cyberprzestępcy żądają okupu za odszyfrowanie serwerów małopolskiego urzędu marszałkowskiego, https://samorzad.pap.pl/kategoria/e-urzad/cyberprzestepcy-zadaja-okupu-za-odszyfrowanie-serwerow-malopolskiego-urzedu [dostęp: 20.01.2022].

Podział administracyjny Polski, https://stat.gov.pl/statystyka-regionalna/jednostki-terytorialne/podzial-administracyjny-polski/ [dostęp: 1.02.2022].

Surażyńska J., *Haker zaszyfrował dane. Teraz żąda okupu od gminy. Mieszkańcy są pełni obaw*, https://koscierzyna.naszemiasto.pl/haker-zaszyfrowal-dane-teraz-zada-okupu-od-gminy-mieszkancy/ar/c1-7462597 [dostęp: 20.01.2022].

47 Niewłaściwe zarządzanie bezpieczeństwem informacji może doprowadzić do wycieku, utraty lub sfałszowania danych posiadanych przez urząd. Możliwy jest także całkowity paraliż pracy urzędu poprzez nie tylko wyciek, lecz także całkowitą utratę zarządzanych danych, ich wykorzystanie w celu np. fałszywego udzielenia pożyczki na podstawie danych mieszkańca, który w sposób bezpośredni – bez korzystania z e-usług – udostępnił swoje dane.

System rejestrów państwowych – bezpieczeństwo, funkcjonowanie i użyteczność, Warszawa 2016.
Świadczenie usług publicznych w formie elektronicznej na przykładzie wybranych jednostek samorządu terytorialnego, Warszawa 2016.
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, Warszawa 2014.
Wdrożenie przez jednostki samorządu terytorialnego z województwa lubuskiego regulacji dotyczących ochrony danych osobowych nr I/19/003, Warszawa 2019.
Wyciekły dane z systemu budżetu obywatelskiego w Gdańsku. Miasto wcześniej zaprzeczało, https://cyberdefence24.pl/cyberbezpieczenstwo/wyciekly-dane-z-systemu-budzetu-obywatelskiego-w-gdansku-miasto-wczesniej-zaprzeczalo [dostęp: 20.01.2022].
Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej w 2020 r., Warszawa 2021.
Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego. Informacja o wynikach kontroli, Warszawa 2019
Żeby elektronicznie znaczyło bezpiecznie. NIK o zarządzaniu bezpieczeństwem informacji w jednostkach samorządu terytorialnego, https://www.nik.gov.pl/aktualnosci/zeby-elektronicznie--znaczylo-bezpiecznie.html [dostęp: 20.01.2022].

Ready – steady – go? A contribution to the discussion on local government cyber security readiness

Abstract

The 2020 coronavirus pandemic has shown that previous socio-economic and political patterns have not worked in the new reality-both in the economic and public sectors. However, it was essential for the public sector, in an era of pandemic-induced constraints, to ensure a rapid and adequate public administration response to citizens' needs. After all, the range of services available within the framework of e-government is steadily growing, and in connection with the fact that many employees, including local government employees, have moved to remote work, offices have introduced, among others, electronic document circulation or access to shared resources in the cloud. However, it would be wrong to point to the pandemic as the only reason for the digitalisation of many administrative processes. This situation only forced the acceleration of digitisation processes: The Act on Informatisation of the Activities of Entities Performing Public Tasks has been in force since 2005, amendments introducing, among others, the obligation to digitally record the sessions of a commune, county or voivodship assembly – since 20018. Similarly, the Act on the National Cyber Security System came into force in 2018. The so-called Local Government Acts, regulating the political system of local government units in a three-tier division – since 1999. However, have these slightly more than twenty years prepared local government units for further, additional to numerous own or commissioned tasks, tasks related to the issue of cyber security in the face of, for example, the cited acts? The hypothesis resulting from the analysis of post-control conclusions of the Supreme Chamber of Control in the matter of ensuring the security of operation of IT systems used for the implementation of public tasks is not optimistic.

Key words: cyber security, local government, e-government, public administration