Centrum Ekspertyzy Lokalnej

Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego

OPINIE I KOMENTARZE FRDL

SAMORZĄD TERYTORIALNY NA ŚWIECIE

nr 1/2026

DOŚWIADCZENIA JEDNOSTEK SAMORZĄDU TERYTORIALNEGO W STANACH ZJEDNOCZONYCH I W POLSCE W ZAKRESIE CYBERBEZPIECZEŃSTWA

Dr hab. Grażyna Piechota, prof. UAFM, Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie

Dr hab. Robert Rajczyk, prof. UŚ, Uniwersytet Śląski w Katowicach

Wprowadzenie

Ostatnie lata dowodzą rosnącej potrzeby cyfryzacji usług sektora publicznego, również na poziomie lokalnym. Funkcjonowanie jednostek samorządu terytorialnego (JST) w cyberprzestrzeni stanowi szansę na zmianę postrzegania instytucji publicznych – jako upraszczających i usprawniających dostęp obywateli do oferowanych usług, ale jednocześnie generujących zagrożenia w zakresie ochrony danych. Cyberzagrożenia są zjawiskiem coraz powszechniejszym i ich wzrost następuje wprost proporcjonalnie do ewolucji e-administracji. Gromadzenie i przechowywanie danych stanowią zatem nie lada wyzwanie dla podmiotów, w dyspozycji których informacje i dane wrażliwe się znajdują, oraz tych, które funkcjonują, wykorzystując sieci informatyczne.

Cyberbezpieczeństwo to kluczowa strategia organizacji, która umożliwia ochronę sieci, komputerów i wykorzystywanego oprogramowania oraz posiadanych danych przed atakami, uszkodzeniami lub nieautoryzowanym dostępem osób nieuprawnionych. Amerykański Narodowy Instytut Standardów i Technologii (NIST) zdefiniował cyberbezpieczeństwo jako proces ochrony danych poprzez zapobieganie atakom, wykrywanie takowych oraz reagowanie na nie. Inny z pod-miotów międzynarodowych – Międzynarodowa Organizacja Normalizacyjna (ISO) cyberbezpieczeństwo identyfikuje z ochroną społeczeństwa, ludzi, organizacji i narodów przed cyberzagrożeniami.

Istotnym zagadnieniem wymagającym wyjaśnienia na wstępnym etapie rozważań jest zależność pomiędzy pojęciami „cyberbezpieczeństwo” i „bezpieczeństwo informacyjne”. Często te pojęcia są mylone, a pomimo istnienia między nimi wielu podobieństw terminy mają różne znaczenia. Cyberbezpieczeństwo stanowi element bezpieczeństwa informacji i dotyczy zarządzania ryzykiem bezpieczeństwa informacji przechowywanych, przesyłanych i przetwarzanych w formatach cyfrowych. Natomiast bezpieczeństwo informacyjne jest pojęciem szerszym. Polega na zachowaniu poufności, integralności i dostępności do informacji. Poufność oznacza, że dane nie są

ujawniane osobom nieuprawnionym; integralność polega na dokładności i kompletności informacji, dostępność zaś to udostępnianie informacji na żądanie podmiotów uprawnionych.

Niniejszy artykuł został poświęcony zilustrowaniu zagrożeń dla cyberbezpieczeństwa informacyjnego zidentyfikowanych w literaturze naukowej i badaniach empirycznych prowadzonych w USA i w Polsce. W szczególności autorzy skoncentrowali się na wskazaniach potencjalnych zagrożeń dla samorządu lokalnego, ale również identyfikacji tych obszarów, które wymagają poprawy poziomu zabezpieczenia dysponowania danymi. W artykule celowo nie zaprezentowano katalogu aktów prawnych regulujących zagadnienia związane z cyberbezpieczeństwem, poniższa analiza odnosi się bowiem do praktyki zagrożeń oraz przeciwdziałania im. Wskazując sposoby i narzędzia najczęściej wykorzystywane przez cyberprzestępców, w tekście zawarto katalog działań, które może podjąć każda JST, aby skuteczniej zabezpieczyć wykorzystywane systemy i sieci informatyczne.

Wybór kontekstu porównawczego amerykańskich i polskich doświadczeń również nie jest przypadkowy. Stany Zjednoczone są państwem, gdzie od dłuższego czasu istnieje możliwość wy-korzystania zaawansowanych technologii informacyjno-komunikacyjnych. Tym samym potencjalnie i teoretycznie e-administracja może wdrażać nowatorskie rozwiązania co do zabezpieczeń przez atakami cybernetycznymi. Polskie samorządy, choć w ostatnich latach, zwłaszcza podczas pandemii koronawirusa, poczyniły znaczne postępy we wdrażaniu technologii w administracji, wciąż są na etapie rozwoju. Porównanie doświadczeń w samorządach terytorialnych w obu państwach stanowi zatem interesujący przegląd sposobów implementacji rozwiązań w celu zapewnienia cyberbezpieczeństwa na poziomie lokalnym.

Cyberbezpieczeństwo w amerykańskich jednostkach samorządu terytorialnego

Wprowadzanie e-administracji i jej sukcesywny rozwój doprowadziły do gromadzenia danych bezpośrednio odnoszących się do obywateli, ale także dotyczących innych podmiotów związanych z funkcjonowaniem jednostek samorządu terytorialnego. Zapewnienie bezpieczeństwa cybernetycznego ma zatem bezpośredni związek z gwarancją zabezpieczenia informacji i zgromadzonych w jednostkach danych obywateli oraz innych podmiotów. Analizy związane z bezpieczeństwem in-formacyjnym są coraz częściej łączone z powstawaniem miast kreatywnych – smart cities . Trans-formacja miast w podmioty kreatywne wynika przede wszystkim z wykorzystania w procesach zarządzania technologii informacyjno-komunikacyjnych. Wdrażanie zaawansowanych technologii, w tym Internetu Rzeczy (IoT) , który według danych w 2019 roku znajdował zastosowanie niemal w 30 proc. smart cities, czy sztucznej inteligencji (AI), niesie za sobą zarówno szanse na inteligentny i kreatywny rozwój, jak i zagrożenia, w tym cyberzagrożenia. Z jednej strony procesy transformacji w samorządach uczyniły pracę jednostek bardziej efektywną, umożliwiając w krót-kim czasie reagowanie na potrzeby obywateli, z drugiej strony jednak wdrażanie rozwiązań opar-tych na technologiach stanowi wyzwanie wobec ochrony danych, szczególnie tych wrażliwych lub poufnych, które cyberprzestępcy uważają za szczególnie atrakcyjne.

Jak zauważyli badacze pod kierownictwem Hossaina , analizy cyberbezpieczeństwa w jednostkach samorządu terytorialnego na świecie wciąż są na niskim poziomie zaawansowania, rozproszone i fragmentarycznie prowadzone. Grupa badaczy skoncentrowała się na opracowaniu metaanalizy opartej na dotychczas opublikowanej literaturze. Ambicją Hossaina i pozostałych było podjęcie próby zidentyfikowania kluczowych elementów cyberbezpieczeństwa w perspektywie lokalnej. Wśród problemów generujących wzrost zagrożeń cyberbezpieczeństwa badacze, analizujący

wcześniejsze ustalenia empiryczne, wskazali: deficyt specjalistycznej kadry, brak adekwatnych przepisów prawnych lub ich ignorowanie, wreszcie brak priorytetyzacji cyberbezpieczeństwa przez odpowiednie organy i kierujących konkretnymi jednostkami samorządowymi. Badania empiryczne, ale i codzienne doniesienia medialne, wskazują na systematyczny wzrost zagrożeń cyberatakami, na co jednostki samorządu i ich pracownicy nie są przygotowani. Przykładem z polskich doświadczeń JST jest Kraków, gdzie w 2025 roku w jednej z instytucji miejskich pracownik otworzył link z obcej, zewnętrznej wiadomości. W wyniku tego doszło do kilkudniowego paraliżu działania elektronicznego systemu biletowego w mieście, co wygenerowało jednocześnie określone straty finansowe i wizerunkowe dla Krakowa.

Badania nad odpornością systemów na cyberataki w Stanach Zjednoczonych są zaawansowane. Norris wraz z grupą badaczy zrealizowali pierwsze badania cyberbezpieczeństwa w samorządzie lokalnym w 2016 roku i sukcesywnie co kilka lat je powtarzają. Analiza poziomu zarządzania bezpieczeństwem informacji dowiodła, że samorządy lokalne niewystarczająco radzą sobie w tym zakresie. Podobne wnioski płyną z innej analizy, zrealizowanej w 2019 roku również przez Norrisa i kierowaną przez niego grupę badaczy. W tym badaniu wykazano, że samorządy są stale narażone na cyberataki, a mimo to poziom cyberbezpieczeństwa jest wciąż na relatywnie niskim poziomie. Zilustrowano stan faktyczny, z którego wynikało, że prawie połowa badanych samorządów doświadczała cyberataków co najmniej codziennie, jednocześnie jedna trzecia stwierdziła, że w ogóle nie wie, czy jest atakowana. Natomiast prawie dwie trzecie badanych JST ujawniło, że nie wie, czy ich systemy informatyczne zostały naruszone w wyniku ataków .

Inne badania w 2019 roku przeprowadzono wśród urzędników pracujących w samorządach amerykańskich miast. W ich wyniku ustalono, że w gminach istnieją formalne polityki dotyczące cyberbezpieczeństwa, zauważalne są jednak problemy w procesach integrowania owych polityk z codziennymi działaniami urzędników. Stwierdzono m.in. brak śledzenia danych, deficyty w konsultowaniu się z zewnętrznymi audytorami ds. bezpieczeństwa oraz nieprowadzenie szkoleń dla kadry kierowniczej w zakresie zarządzania i ochrony danych . Tym samym w.w. projekty badawcze ujawniały podobny poziom deficytów w zakresie zarządzania cyberbezpieczeństwem w JST.

Inna perspektywa badawcza skupia się na ustaleniu poziomu przygotowania kadr zarządzających w amerykańskich JST. W 500 miastach w Stanach Zjednoczonych, w których przeprowadzono badania, ujawniono, że zaangażowanie i percepcja menedżerów koncentrują się głównie na aspektach technicznych. W wyniku wyjaśniania zgłaszanych incydentów cybernetycznych zaistniałych w administracji publicznej menedżerowie podejmowali działania zabezpieczające w obszarze technicznym. Z mniejszą uwagą podchodzono do kwestii społecznej percepcji i edukacji . Zestawiając wyniki tych kilku badań, w kolejnym artykule zwrócono uwagę na konieczność wypracowania tzw. kultury cyberbezpieczeństwa w organizacji (to zagadnienie zostanie omówione w dalszej części niniejszego opracowania). Kultura cyberbezpieczeństwa to typ kultury opartej na wdrażaniu polityk bezpieczeństwa w JST. Tych w Stanach Zjednoczonych jest ponad 90 tys., z czego prawie 39 tys. to gminy, hrabstwa, miasta i miasteczka. Kultura cyberbezpieczeństwa oznacza zatem, że wszystkie podmioty w pełni rozumieją i wspierają bezpieczeństwo cybernetyczne, i to na wszystkich szczeblach funkcjonowania samorządu terytorialnego.

Analizy zrealizowane w Stanach Zjednoczonych, na które powołują się Hossain i pozostali badacze, dowiodły, że częstotliwość ataków jest znacząca: 28 proc. samorządów lokalnych w Stanach Zjednoczonych doświadcza cyberataków co godzinę lub częściej, a 19 proc. zgłasza co najmniej jeden atak dziennie. Liczne badania prowadzone nie tylko w Stanach Zjednoczonych, lecz także w innych państwach, w tym w Polsce, potwierdziły, że pomimo wzrostu zagrożeń istnieje wciąż pod-stawowy problem w zabezpieczeniach przed atakami cybernetycznymi. Jest nim deficyt wiedzy lokalnych kadr administracyjnych na temat wyzwań, możliwych rodzajów cyberataków

i technik w nich stosowanych. Powyższe ustalenia potwierdzają również analizy przeprowadzone przez Ocampo, który skoncentrował się na wewnętrznym funkcjonowaniu samorządów i wskazał, że źródłem problemów w zakresie zarządzania cyberbezpieczeństwem w amerykańskich JST jest brak nadzoru, współpracy oraz zasobów, które pozwalałyby na implementację skutecznych rozwiązań .

Wreszcie najnowsze badania, ponownie zrealizowane w skali ogólnokrajowej przez Norrisa i Ma-teczun i opublikowane w 2025 roku, potwierdzają, że pomimo upływu czasu (wcześniejsze analizy w analogicznej skali ogólnokrajowej zrealizowano w 2020 roku), a także zwiększenia zagrożenia cyberatakami i podejmowania coraz częstszych prób ataków przez hakerów JST wciąż nie radzą sobie z zarządzaniem cyberbezpieczeństwem. Wyniki ogólnokrajowych badań ujawniły, że: 4,5 proc. JST zgłosiło odpowiednim podmiotom naruszenia cyberbezpieczeństwa w ciągu ostatniego roku; nie wzrosła świadomość zagrożeń wśród pracowników; nie podniesiono znacząco budżetów JST przeznaczonych na cyberbezpieczeństwo; wreszcie w JST wciąż zauważalny jest deficyt wyszkolonych i doświadczonych specjalistów z zakresu cyberbezpieczeństwa. Procesy zarządzania ochroną danych przed cyberatakami są realizowane w niespełna 34 proc. badanych JST. Te dane, wynikające z prowadzonych cyklicznie od 2016 roku analiz, jednoznacznie potwierdzają, że pomimo wzrostu zagrożeń nie zmienia się w sposób znaczący podejście w ame-rykańskim samorządzie do wypracowania kultury cyberbezpieczeństwa, już na etapie opracowania strategii, a następnie jej skutecznej implementacji.

Znaczącym okresem związanym z rozszerzaniem usług e-administracji w USA był czas pandemii, kiedy to wiele jednostek samorządu terytorialnego wdrażało i rozwijało rozwiązania cyfrowe dla efektywnej obsługi interesantów. Grupa badaczy, analizując zagadnienia cyberbezpieczeństwa na poziomie stanowym w kontekście legislacyjno-porównawczym po pandemii COVID-19, ujawniła, że: w ok. 34 proc. administracji stanowych wdrożono odpowiednie polityki; niemal każdy stan przyjął co najmniej jedną politykę dotyczącą cyberbezpieczeństwa; zaimplementowane polityki obejmują kwestie zarządzania, finansowania oraz wymogów co do zabezpieczeń przed cyberatakami. Badania przeprowadzono, uwzględniając dane urzędowe za okres 2019–2022. Analiza dokumentów wykazała aktywność legislacyjną związaną z uchwalaniem ustaw dotyczących cyberbezpieczeństwa. Ustalono, że większość stanów przyjęła jeden albo dwa akty prawne regulujące cyberbezpieczeństwo (Wisconsin, Karolina Południowa, Pensylwania, Nowy York, Idaho, Massachusetts, Hawaje, Kolorado i Alabama), takie stany, jak: Maryland, Floryda, Teksas, Luizja-na, Wirginia i Vermont przyjęły co najmniej sześć aktów prawnych w ciągu roku, Nebraska i Wyoming zaś nie uchwaliły żadnego aktu prawnego w zakresie cyberbezpieczeństwa (badacze wskazali, że nie podjęto w analizowanym okresie nawet prób ustawodawczych w zakresie uregulowania cyberbezpieczeństwa). Te dane jednoznacznie ilustrują w ujęciu porównawczym, w których stanach USA zagadnienia związane z cyberbezpieczeństwem są traktowane priorytetowo, a gdzie ta tematyka nie stanowi istotnej funkcji zarządzania .

Zidentyfikowanym problemem wynikającym z nieznajomości potencjalnych zagrożeń jest również brak opracowanych standardów i merytorycznego przygotowania wszystkich pracowników administracji lokalnych w kwestii rozpoznania źródeł potencjalnych ryzyk. Brak odpowiednich strategii działania w przypadku ataków cybernetycznych prowadzi do rozlicznych negatywnych konsekwencji w samorządach. Do nich zaliczyć należy: ujawnienie wrażliwych i prawnie chronionych danych, utratę wiarygodności, reputacji i zaufania do lokalnej administracji samorządowej czy wreszcie wysokie koszty usuwania skutków skutecznych cyberataków. Brak standardów działania w przypadku wystąpienia cyberataku oraz regularnego testowania mechanizmów obrony przez takimi próbami rodzi kosztowne konsekwencje dla konkretnych jednostek samorządu terytorialnego.

Badacze zidentyfikowali sposoby, którymi cyberprzestępcy atakują sieci lokalnych samorządów. Badania zrealizowane w stanie Floryda ujawniły, że cyberataki najczęściej polegały na przesyłaniu linków zawierających wirusy i robaki, następnie na phishingu, oprogramowaniu szpiegującym i wykorzystaniu nazw domen. Inne badania, przeprowadzone w 11 miastach Stanów Zjednoczonych, wskazały, że cyberataki są prowadzone poprzez phishing (85 proc.) lub spear phishing, ujawniono także ataki typu zero-day czy brute force. Wreszcie ogólnokrajowe badania zrealizowane w Stanach Zjednoczonych na poziomie samorządów jako najczęstszą formę cyberataków wskazały ransomware.

Cyberbezpieczeństwo w polskim samorządzie

Po przeprowadzeniu powyższych analiz w zakresie cyberbezpieczeństwa w JST w Stanach Zjednoczonych w kolejnej części artykułu poddano analizie ustalenia empiryczne związane z cyberbezpieczeństwem w polskich JST.

Jak wskazuje Ewa Maria Włodyka , wzrost znaczenia e-administracji jest pochodną wdrażania polityk publicznych, ale też upowszechnienia trendów społecznych, związanych z oczekiwaniami ułatwień funkcjonowania administracji lokalnej przez różne podmioty. Rozwój e-administracji, zdaniem Włodyki, stanowi zatem odpowiedź ze strony administracji na oczekiwania dotyczące usprawnienia i poprawy jakości funkcjonowania administracji publicznej. Jako że w polskim systemie prawnym obywatele najczęściej kontaktują się z podmiotami administracji publicznej na poziomie lokalnym, to właśnie zabezpieczenie danych oraz dostępu do nich stanowi podstawowe wyzwanie dla podmiotów lokalnych w zapewnieniu bezpieczeństwa cyfrowego. Na dowód tych stwierdzeń Włodyka przedstawia dane Najwyższej Izby Kontroli (NIK) z 2020 roku, z których wynika, że 99,3 proc. jednostek administracji publicznej oferowało podmiotom indywidualnym i instytucjonalnym usługi e-administracji. Warunkiem prawidłowego działania wprowadzonych rozwiązań e-administracji jest dostęp do szerokopasmowego Internetu (w 2020 roku posiadało takowy 99,9 proc. samorządów). NIK ustaliła, że w momencie dokonywania kontroli tylko nieco ponad 60 proc. jednostek administracji przeprowadzało regularnie audyty bezpieczeństwa systemów informatycznych. Włodyka, prezentując dane z kontroli NIK z 2020 roku, podkreśla przede wszystkim korelację zachodzącą pomiędzy wielkością jednostki samorządu a poziomem zabezpieczeń danych. Te ustalenia ujawniają, że wielkość JST determinuje, czy takowa posiada wyznaczoną osobę odpowiedzialną wyłącznie za zabezpieczenia systemów. Problemem, który zwykle warunkuje podejście mniejszych jednostek do cyberbezpieczeństwa, są również ograniczone środki finansowe, które umożliwiłyby zapewnienie odpowiedniego poziomu bezpieczeństwa cyfrowego.

Kolejne badania NIK zrealizowane w 2025 roku ujawniły, że: „Większość skontrolowanych samorządów nie podejmowała skutecznych i rzetelnych działań na rzecz bezpieczeństwa informacji. NIK negatywnie oceniła przygotowanie do zapewnienia ciągłości działania systemów informatycznych w 71 procentach urzędów, a istotne nieprawidłowości w tym zakresie wystąpiły w 23 z 24 badanych jednostek”.

Jednocześnie NIK wskazała konieczne działania, które zalecono władzom lokalnym do przeprowadzenia. Do nich należało:

- opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji;
- zapewnienie wykonywania okresowego przeglądu i aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji;

- ustanowienie polityk ciągłości działania oraz opracowanie i wdrożenie planów zapewnienia ciągłości działania urzędów, planów odtworzeniowych oraz zapewnienie ich okresowego testowania;
- prowadzenie okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji;
- wdrożenie rozwiązań zapewniających odpowiednie zabezpieczenie pomieszczeń serwerowni;
- regularne testowanie kopii zapasowych oraz przechowywanie ich poza miejscem wytworzenia;
- zapewnienie prowadzenia przynajmniej raz w roku okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji;
- objęcie nadzorem oprogramowania instalowanego na urządzeniach mobilnych.

W ostatnich latach w Polsce, w związku z zagrożeniami związanymi z hybrydowymi działaniami wojennymi, ochrona danych i dostępu do nich stanowi kluczowe wyzwanie dla całej administracji. Brak odpowiednich gwarancji ochrony danych obywateli i niezapewnienie sprawnego funkcjonowania e-administracji przekładają się wprost na poziom zaufania do działań administracji publicznej. Rola audytu polegającego na zapewnieniu prawidłowości ochrony danych oraz wskazaniu obszarów wymagających poprawy nabiera zatem kluczowego znaczenia.

W innej ze swoich prac poświęconych cyberbezpieczeństwu Włodyka zauważa, że to pandemia koronawirusa w latach 2020–2022 istotnie wpłynęła na rozwój e-administracji. Z jednej strony urzędnicy, podobnie jak i pracownicy w innych sektorach, przeszli do pracy zdalnej, z drugiej – obywatele nadal oczekiwali sprawnej obsługi w zakresie realizacji ich potrzeb. Odpowiadając na zmiany, wdrożono elektroniczny obieg dokumentów oraz pracę urzędników w chmurze. Natomiast w celu usprawnienia obsługi klientów dokonano digitalizacji procesów administracyjnych.

Znaczenie audytu dla ochrony danych podkreślają również Marcin Janik i Stanisław Hady-Głowiak . Zwracają oni uwagę na znaczenie tego procesu, jako powtarzalnego i systematycznie realizowanego, dla zwiększenia efektywności zarządzania danymi i podniesienia poziomu bezpieczeństwa w kontekście zagrożeń cybernetycznych. Wśród działań, na które powinni zwrócić szczególną uwagę kierownicy jednostek samorządu terytorialnego, wskazali przede wszystkim dobór właściwych osób odpowiedzialnych za cyberbezpieczeństwo. Jak piszą Janik i Hady-Głowiak: „Brak zapewnienia skuteczności i efektywności systemu zarządzania bezpieczeństwem informacji w jednostce może powodować straty finansowe i wizerunkowe lub utrudniać utrzyma-nie ciągłości działania i realizację założonych celów i zadań”.

Z badań zrealizowanych w 2021 roku w polskich gminach przez grupę badaczy wynika, że w 76,9 proc. samorządów opracowano i wdrożono system polityki bezpieczeństwa informacji; w 75 proc. gmin przeprowadzany jest coroczny audyt bezpieczeństwa informacji. Te dane ilustrują zarazem, że w ok. 35 proc. samorządów w Polsce w 2021 roku podejmowane działania nie były wystarczające, aby skutecznie zapobiegać incydentom cybernetycznym. Równie niepokojące są ustalenia wynikające z kolejnych danych. Tylko połowa gmin uczestniczących w badaniu przeprowadziła szkolenia dla pracowników z zakresu cyberbezpieczeństwa, w 9 proc. zaś przesz-kolona była wyłącznie kadra kierownicza. Do rzadkości należy także ubezpieczanie się gmin od ryzyka cyberataków, mimo że – jak ujawniły badania – w 66 proc. badanych gmin potwierdzono, że zagrożenie cyberprzestępstwami jest obarczone średnim lub wysokim poziomem ryzyka.

Analiza przeprowadzona przez Chodakowską i pozostałych członków zespołu ujawniła, że w obszarze samorządu najbardziej zagrożone cyberatakami są dane osobowe, które gminy gromadzą i którymi dysponują. Mimo iż badania zrealizowane w 2021 roku nie ujawniły w polskich gminach znacznej liczby ataków cybernetycznych (blisko 87 proc. zadeklarowało, że nie wystąpiły żadne incydenty), jednocześnie poziom przygotowania samorządów do takich zagrożeń, przy świadomości wzrostu ryzyka ich występowania, nie zmienił się. Nie podjęto kroków prowadzących do implementacji dodatkowych zabezpieczeń. Zdecydowana większość JST nie dokonuje również zgłoszeń do odpowiednich organów państwa zaistniałych incydentów i prób naruszenia bezpieczeństwa w wyniku cyberataków. Ustalenia płynące z badań zrealizowanych w JST w 2021 roku potwierdziły, że polityka cyberbezpieczeństwa wciąż nie stanowi przedmiotu objętego funkcją zarządzania. Należy zwrócić uwagę na to, że analizy przeprowadzono w drugim roku funk-cjonowania administracji w obliczu pandemii koronawirusa, co niejako zmusiło administracje samorządów do zwiększenia aktywności w cyberprzestrzeni.

Problem z ochroną systemów informatycznych przed cyberzagrożeniami występuje przede wszystkim w małych JST. Wynika to z kumulacji kilku przyczyn: braku wystarczających środków finansowych, deficytu odpowiednio przeszkolonych pracowników i poziomu wiedzy kadry zarządzającej co do cyberzagrożeń. Chodakowska i pozostali badacze zaproponowali, odnosząc się do małych JST w Polsce, kilka zaleceń możliwych do zastosowania wobec deficytów kadrowych oraz finansowych determinujących poziom odporności na cyberzagrożenia. Wskazali m.in. korzystanie z dobrych praktyk i ich implementację oraz współpracę i nawiązywanie partnerstw przez małe JST sąsiadujące ze sobą w celu wymiany wiedzy oraz wspólnego ponoszenia wydatków związanych z tworzeniem odpowiednich systemów zabezpieczeń. Twórcy raportu zwracają jednak uwagę na utrudnienia we współpracy wynikające z różnych przesłanek. Piszą: „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 ”.

Reasumując, należy podkreślić, że zarówno amerykański, jak i polski samorząd podchodzą do zarządzania cyberbezpieczeństwem w podobny sposób. Jednostki samorządu terytorialnego w obu państwach, mając świadomość rosnących zagrożeń co do potencjalnych cyberataków, jednocześnie z podobnych powodów nie podejmują wystarczających działań zabezpieczających systemy i sieci, w których funkcjonują. Liczba zagrożeń atakami cybernetycznymi przy zwiększających się możliwościach działań cyberprzestępców będzie rosła. Oznacza to, że w najbliższych latach cyberbezpieczeństwo stanie się kluczowym wyzwaniem w samorządach.

Badania prowadzone w tożsamym interwale czasowym w Polsce i w Stanach Zjednoczonych dowiodły istnienia podobnych przesłanek deficytu cyberbezpieczeństwa w każdym z państw. Do tychże należy zaliczyć: brak świadomości i wiedzy co do znaczenia implementacji polityk cyberbezpieczeństwa w organizacji oraz brak wystarczających środków finansowych na wdrożenie i regularny audyt narzędzi cyberbezpieczeństwa. Istotną przesłanką wpływającą na poziom zabezpieczenia organizacji przed cyberryzykami należy zaliczyć cyberhigienę, której nie przestrzegają zarządzający JST, co bezpośrednio oddziałuje na niepromowania cyberbezpieczeństwa jako priorytetu wśród pracowników JST.

Kultura cyberbezpieczeństwa w samorządzie terytorialnym

Pojęcie kultury cyberbezpieczeństwa pojawiło się już wcześniej, wraz z wyjaśnieniem samego terminu „cyberbezpieczeństwo". Odwołując się do wcześniej opisanego stanu faktycznego w zakresie cyberbezpieczeństwa w amerykańskich i polskich JST, w tej części opisano zarówno potencjalne narzędzia stosowane przez cyberprzestępców w celu przejęcia danych lub włamania do sieci organizacji, jak i powody zaniedbań w zakresie wypracowania kultury cyberbezpieczeństwa w samorządzie. W analizie, która powstała na podstawie dotychczasowych doświadczeń JST, zidentyfikowano zabezpieczenia, których wprowadzenie do strategii zarządzania cyberbezpieczeństwem może zminimalizować negatywne konsekwencje cyberzagrożeń dla organizacji oraz wspierać kreowanie kultury cyberbezpieczeństwa.

Do zabezpieczeń tych zaliczono:

1. politykę dopuszczalnego użytkowania – definiuje to, w jaki sposób i w jakim zakresie pracownicy korzystają z zasobu danych w JST;

2. politykę bezpieczeństwa informacji – określa sposób, w jaki są tworzone, wymieniane i przechowywane informacje w systemie informatycznym JST, w tym konieczność szyfrowania danych przez cały czas ich przechowywania;

3. politykę prywatności – reguluje sposób, w jaki lokalne witryny internetowe gromadzą, wykorzystują, przechowują i udostępniają informację podmiotom zewnętrznym;

4. politykę zarządzania tożsamością i dostępem – obejmuje proces tworzenia i usuwania kont użytkowników (ich kategorii) oraz uprawnień przypisanych użytkownikom, zależnie od ich funkcji w organizacji;

5. politykę obsługi incydentów – opisuje sposób, w który JST reaguje na różne formy ataków cybernetycznych, ze wskazaniem, jakie funkcje i usługi mogą zostać zagrożone, zakłócone lub wyłączone;

6. politykę odzyskiwania informacji (po awarii lub przerwaniu ciągłości działania) – opisuje mechanizmy, które są stosowane przez JST w reakcji na kryzysy (zarówno cyberataki, jak i zagrożenia losowe);

7. politykę zdalnego dostępu – opisuje sposób udzielania i cofania dostępu do systemu informatycznego JST;

8. politykę przynoszenia własnych urządzeń – zawiera regulacje dotyczące określenia, kiedy i w jaki sposób pracownicy mogą korzystać z własnych urządzeń przez ich podłączenie do systemów informatycznych JST;

9. politykę korzystania z poczty elektronicznej – reguluje sposób, w jaki pracownik JST może korzystać z oficjalnej poczty elektronicznej do innych celów niż służbowe;

10. politykę mediów i komunikacji – zawiera procedury określające, kto może kontaktować się ze środkami masowego przekazu w przypadku powstania naruszeń w zakresie bezpieczeństwa in-formacyjnego;

11. politykę zarządzania zmianami – określa proces zmiany systemu informatycznego w JST;

12. politykę zarządzania odpornością – obejmuje procedurę obsługi zagrożeń technologicznych ujawnionych w wykorzystywanych przez JST aplikacjach;

13. politykę tworzenia kopii zapasowych – opisuje częstotliwość i metody tworzenia kopii zapasowych systemów informatycznych w JST.

W celu faktycznego zabezpieczenia podmiotu przez atakami cybernetycznymi niezbędne jest nie tylko opracowanie strategii (enumeratywnie zaproponowano jej zawartość), lecz także jej wdrożenie oraz regularny audyt, umożliwiający identyfikację i usunięcie zagrożeń na etapie testowania systemów. Ciągły monitoring skuteczności ujętych w strategii metod i narzędzi jest konieczny, aby proces zarządzania i ochrony danych był efektywny. Wówczas można uznać, że w danej JST została wdrożona kultura cyberbezpieczeństwa.

Na podstawie wymienionych polityk Hossain i pozostali autorzy opracowali także szczegółowe zalecenia, których zaimplementowanie pozwoli na efektywne zwiększenie bezpieczeństwa cybernetycznego w JST.

Wśród zaleceń znalazły się:

1. opanowanie podstaw cyberbezpieczeństwa przez pracowników i kadrę kierowniczą – poprzez realizację okresowych szkoleń wewnętrznych, finansowanie zewnętrznych kursów, udział w konferencjach branżowych i inne narzędzia zwiększające poziom wiedzy, zwłaszcza odnośnie do nowych technik stosowanych przez hakerów;

2. zadbanie o finansowanie cyberbezpieczeństwa oraz odpowiedniego wsparcia działów IT, głównie poprzez wyszczególnienie dedykowanego dla IT budżetu celowego;

3. zatrudnienie wykwalifikowanej kadry – zalecenie to dotyczy nie tylko odpowiedniego pozio-mu kwalifikacji osób, lecz także odpowiedniej liczby pracowników, tak aby wdrożyć i utrzymać system na wysokim poziomie zabezpieczenia przed cyberatakami;

4. kształtowanie świadomości wszystkich pracowników, że cyberzagrożenia to de facto ryzyko utraty bezpieczeństwa, które stanowi funkcję zarządzania ryzykami w każdej organizacji – tym samym ten szczególny komponent bezpieczeństwa powinien być zabezpieczony przed wszelkimi działaniami wymierzonymi w JST;

5. regularne testowanie systemów i badanie reakcji urzędników JST na zagrożenia różnymi for-mami cyberataków, a także włączenie cyberbezpieczeństwa do zarządzania sytuacjami kryzysowymi w organizacji;

6. rozwijanie i utrzymywanie kultury cyberbezpieczeństwa w całej organizacji, również poprzez wsparcie przez kadrę zarządzającą procesów zabezpieczania i ochrony danych;

7. centralizacja działań we wszystkich aspektach cyberbezpieczeństwa – ulokowanie odpowie-dzialności za tę funkcję zarządzania w obowiązkach konkretnej osoby spośród kadry zarządzającej;

8. analiza dobrych praktyk stosowanych w innych JST i ich wdrażanie, tak aby maksymalizować ochronę przed cyberzagrożeniami – w tej kwestii za pożądane można uznać także zbudowanie relacji pomiędzy JST w zakresie wymiany doświadczeń, dobrych praktyk i wzajemnego wsparcia.

Podsumowanie

Opracowanie i wdrożenie strategii cyberbezpieczeństwa, a następnie zastosowanie mechanizmów upraktycznienia zapisów strategii prowadzą do efektywnego ukształtowania kultury cyberbezpieczeństwa. To nie gwarantuje braku zagrożeń, ale pozwala zminimalizować skutki ich wystąpienia oraz ułatwia usuwanie negatywnych konsekwencji, zarówno finansowych, jak i wizerunkowych. Przy rosnącej liczbie podmiotów o różnych motywacjach i rozbudowywanym kata-logu narzędzi cyberataki

będą coraz powszechniejsze. Zidentyfikowane motywacje hakerów podejmujących ataki na systemy informatyczne w JST to: chęć nielegalnego uzyskania informacji o mieszkańcach (dane osobowe); żądanie okupu, aby JST mogła odzyskać dane lub dostęp do nich; motywy polityczne lub ideologiczne (haktywizm), szpiegostwo, osobista zemsta i chęć odwetu (motywacja towarzyszy często pracownikom albo obywatelom, którzy czują się pokrzywdzeni decyzjami lub działaniami samorządu). Wśród motywacji zdarzają się także zupełnie prozaiczne powody cyberataków, jak chęć wykazania się w środowisku hakerów, wyrządzenie szkód bez wy-raźnego powodu, chęć zademonstrowania własnych umiejętności. Wszystkie wymienione motywacje, jeśli przeradzają się w konkretne działania, finalnie prowadzą do zakłócenia usług świadczonych przez samorządy online, utraty zaufania obywateli oraz strat finansowych i wizerunkowych. Celem aktywistów podejmujących cyberataki może być również narażenie JST na śmieszność, np. poprzez publikację w kontencie stron internetowych czy oficjalnych witryn samorządu kompromitujących lub ośmieszających treści. Coraz częściej ataki cybernetyczne są przejawem terroryzmu. Jako takie mają na celu wzbudzanie strachu i zakłócenie normalnego funkcjonowania lokalnej wspólnoty.

Porównanie odporności JST na cyberzagrożenia w Stanach Zjednoczonych i w Polsce ujawniło podobieństwa, głównie w obszarze implementacji kultury cyberaktywizmu i objęcia ryzyk cybernetycznych procesami zarządzania. Szczególnie narażone na cyberataki są małe samorządy (w oby państwach), z uwagi na ograniczone zasoby finansowe oraz deficyty wykwalifikowanej kadry. Tymczasem rosnąca liczba ataków hakerskich, przy wykorzystaniu coraz obszerniejszego katalogu narzędzi umożliwiających cyberataki motywowane różnymi powodami, powinna prowadzić do objęcia cyberbezpieczeństwa funkcją zarządzania w JST.

Bibliografia:

- Chodakowska A., Kańduła S., Przybylska J., *Jak polskie gminy radzą sobie z cyberbezpieczeństwem*, 2022, https://www.nik.gov.pl/2022/01/jak-polskie-gminy-radza-sobie-z-cyberbezpieczenstwem-wyniki-badan-wlasnych.html [data dostępu 26.08.2025].
- Frandell A., Feeney M., *Cybersecurity Threats in Local Government: A Sociotechnical Perspective*, „The American Review of Public Administration" 2022, vol. 52, iss. 8, https://doi.org/10.1177/02750740221125432.
- Ganapati S., Franco L.O., Le A.N., *American State Government Cybersecurity Policies. Proceedings of the 24th Annual International Conference on Digital Government Research*, 2023, https://doi.org/10.1145/3598469.3598540 [data dostępu: 26.08.2025].
- Hatcher W., Meares W.L, Heslen J., *The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices*, „Journal of Cyber Policy" 2020, vol. 5, iss. 2, s. 302–325, https://doi.org/10.1080/23738871.2020.1792956.
- Hossain S.T., Yigitcanlar T., Nguyen K., Xu Y., *Cybersecurity in Local Governments: A Review and Framework of Key Challenges*, https://ssrn.com/abstract=4631885; http://dx.doi.org/10.2139/ssrn.4631885 [data dostępu: 8.09.2025].
- Hossain S.T., Yigitcanlar T., Nguyen K., Xu Y., *Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework*, „Applied Sciences" 2024, vol. 14, iss. 13, 5501, https://doi.org/10.3390/app14135501.
- Janik M., Hady-Głowiak S., *Bezpieczeństwo informacji jako zadanie jednostek sektora finansów publicznych*, „Studia Prawnoustrojowe" 2023, nr 62, s. 285–302.
- Norris D.F., Mateczun L.K., *Adoption of Cybersecurity Policies by Local Governments 2020*, „Journal of Cybersecurity Education, Research and Practice" 2023, no. 2.
- Norris D.F., Mateczun, L.K., *Managing Cybersecurity in local governments: 2022*, „Journal of Cybersecurity Education, Research and Practice" 2025, no. 1.
- 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" 2019, vol. 79, iss. 6, s. 895–904.
- 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 vol. 43, iss. 8, s. 1173–1195, https://doi.org/10.1080/07352166.2020.1727295.
- Ocampo H.R., *Municipal Governments and the Need for Cybersecurity*, 2021, https://uh-ir.tdl.org/server/api/core/bitstreams/b3d2a292-620b-492e-9638-a1b577fcf0fd/content [data dostępu: 8.09.2025].
- Piechota G., *Ewolucja miasta. Od miasta tradycyjnego do innowacyjnego „smart city"*, „Analizy Celowe" 2024, nr 8, https://frdl.org.pl/publikacje/analizy-celowe/ewolucja-miasta-od-miasta-tradycyjnego-do-innowacyjnego-smart-city [data dostępu 28.08.2025].
- Włodyka E.M., *Samorządowa administracja publiczna wobec cyberprzestrzeni: bezpieczeństwo informacji a praktyka zgłaszania w samorządzie terytorialnym osób do kontaktu z CSIRT NASK*, „Studia Gdańskie. Wizje i rzeczywistość" 2021, t. 18, s. 301–314.
- Włodyka E.M., *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa*, „Cybersecurity and Law" 2022, vol. 7(1), s. 202–219.

O AUTORZE

Dr hab. Grażyna Piechota – prawniczka, doktor nauk humanistycznych w dziedzinie socjologii, doktor habilitowana nauk społecznych w dyscyplinie nauki o komunikacji społecznej i mediach. Pracuje na Wydziale Zarządzania, Mediów i Technologii Uniwersytetu im. Andrzeja Frycza Modrzewskiego w Krakowie. Specjalizuje się w zagadnieniach społeczeństwa obywatelskiego, komunikacji politycznej, nowych ruchów społecznych i technologii informacyjno-komunikacyjnych (ICT).

Dr hab. Robert Rajczyk – doktor habilitowany nauk o polityce i administracji, pracownik naukowy Instytutu Dziennikarstwa i Komunikacji Medialnej Uniwersytetu Śląskiego w Katowicach. Swoje zainteresowania badawcze koncentruje m.in. wokół problematyki funkcjonowania administracji publicznej i sa-morządu terytorialnego, w tym także w państwach Europy Środkowej i Wschodniej, oraz procesów współczesnego oddziaływania perswazyjnego i komunikacji społecznej.

STRESZCZENIE

Cyberzagrożenia stanowią jedno z podstawowych wyzwań stojących przed samorządami terytorialnymi w erze technologii informacyjno-komunikacyjnych. Celem artykułu jest wskazanie podejścia samorządów do cyberbezpieczeństwa w dwóch państwach. Przedstawiona analiza umożliwia zapoznanie się z wynikami badań empirycznych zrealizowanych w Stanach Zjednoczonych i w Polsce w analogicznym okresie. Badania ujawniają gotowość administracji samorządowych do minimalizowania ryzyk wystąpienia skutecznych cyberataków. W tekście zaprezentowano istniejące w obu państwach deficyty związane z polityką cyberbezpieczeństwa w jednostkach samorządu terytorialnego. Nadto wskazano, jakimi motywami kierują się cyberprzestępcy i przy użyciu jakich narzędzi podejmują próby ataków cybernetycznych. Artykuł odpowiada na pytanie, czy można skutecznie przygotować się do zminimalizowania zagrożeń cybernetycznych oraz jakie elementy należy zawrzeć w strategii bezpieczeństwa cyfrowego tak, aby ta sprzyjała wykreowaniu kultury cyberbezpieczeństwa w JST.

Słowa kluczowe:

cyberbezpieczeństwo, kultura cyberbezpieczeństwa, strategia cyberbezpieczeństwa, cyberbezpieczeństwo w administracji samorządowej, cyberzagrożenia

...

Warszawa, czerwiec 2025

Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego

ul. Edwarda Jelinka 6, 01-646 Warszawa

WWW.FRDL.ORG.PL