WOJEWODA PODKARPACKI
ul. Grunwaldzka 15
35-959 Rzeszów

OA-IV.431.3.2025 Rzeszów, 2025-08-14

Pan
Krzysztof Szpyt
Burmistrz Lubaczowa

Na podstawie art. 46 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, w związku ze zrealizowaną w dniach 8 i 9 lipiec 2025 r. u Burmistrza Lubaczowa (Urząd Miejski w Lubaczowie, ul. Rynek 26, 37-600 Lubaczów) kontrolą problemową[1], której przedmiotem była ocena działania systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej z minimalnymi wymaganiami dla systemów teleinformatycznych - przekazuję niniejsze **wystąpienie pokontrolne.**

Kontrolę przeprowadził zespół kontrolerów: Alicja Trygar (starszy inspektor wojewódzki), Tomasz Szmigiel (zastępca kierownika) na podstawie imiennych upoważnień do kontroli (pisma z dnia 01.07.2025 r., znak OA-IV.431.3.2025) udzielonych przez działającego z upoważnienia Wojewody Podkarpackiego – Dyrektora Wydziału Organizacyjno-Administracyjnego.

Ustalenia kontrolne dokonane zostały w oparciu o stan faktyczny istniejący od 1stycznia 2024 r. do dnia realizacji czynności kontrolnych włącznie.

W toku kontroli - w oparciu o kontrolowane dokumenty (przy zastosowaniu metody niestatystycznej, losowy dobór próby) - ustalono, iż pracownicy Urzędu Miejskiego w Lubaczowie prawidłowo realizowali swoje zadania. Stwierdzone uchybienia w swych skutkach nie miały charakteru kluczowego (strategicznego) dla funkcjonowania kontrolowanej jednostki. W dużej mierze miały one charakter formalny, przejawiając się odstępstwami od stanu pożądanego, nie powodując jednak negatywnych następstw dla kontrolowanej działalności.

Kontrola nie wykazała okoliczności wskazujących na popełnienie przestępstwa, wykroczenia, naruszenia dyscypliny finansów publicznych lub innych czynów, za które ustawowo przewidziana jest odpowiedzialność prawna.

[1] W oparciu o zatwierdzony w dniu 7 stycznia 2025 r. „Planu zewnętrznej działalności kontrolnej Podkarpackiego Urzędu Wojewódzkiego w Rzeszowie na 2025 rok").

W oparciu o poczynione ustalenia, stosownie do skali ocen przyjętej w „Programie kontroli problemowej realizowanej u Burmistrza Lubaczowa”[2], **działalność w ww. zakresie należy ocenić pozytywnie z uchybieniami**.

Na podstawie analizy dokumentacji źródłowej zespół kontrolny sformułował następującą ocenę kontrolowanych obszarów:

1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną – pozytywnie;
2. Wdrożenie systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych – pozytywnie z uchybieniami;
3. Dostosowanie systemów informatycznych do standardu WCAG 2.0 – pozytywnie.

Kontekst organizacyjny

Funkcję kierownika w Urzędzie Miejskim w Lubaczowie pełnił Burmistrz: Pan Krzysztof Szpyt.

Funkcję Inspektora Ochrony Danych (IOD) pełnił pracownik zatrudniony w Urzędzie Miejskim w Lubaczowie - Pani Magda Fusińska, powołana Zarządzeniem Nr 114/2018 Burmistrza Miasta Lubaczowa z dnia 24 maja 2018 r. w sprawie wyznaczenia wspólnego inspektora ochrony danych w Urzędzie Miejskim w Lubaczowie oraz w Miejskim Ośrodku Sportu i Rekreacji.

Wsparcie informatyczne zapewnione było przez dwóch informatyków, pracowników Urzędu Miasta Lubaczowa. Pod ich opieką znajdowały się: środowiska sprzętowo-programowe, sieć lokalna, serwerownia, systemy i aplikacje centralne oraz własne, usprawniające pracę pracownikom Urzędu Miejskiego w Lubaczowie.

Zostały wyznaczone osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa na podstawie Zarządzenia nr 165/2022 Burmistrza Miasta Lubaczowa z dnia 23 listopada 2022 r. Następnie, zostało dokonane zgłoszenie tych osób do CSIRT NASK w dniu 24 listopada 2022 r.

Funkcja Administratora Systemów Informatycznych (ASI) na podstawie Zarządzenia Nr 187/2012 Burmistrza Miasta Lubaczowa z dnia 20 sierpnia 2012 r. w sprawie wyznaczenia Administratora Bezpieczeństwa Informacji oraz Administratora Systemu Informatycznego została powierzona osobie zatrudnionej na stanowisku informatyka.

W okresie objętym kontrolą w Urzędzie Miejskim w Lubaczowie funkcjonowały systemy teleinformatyczne własne - zakupione przez urząd oraz centralne m.in.:

a) systemy centralne:

[2] Stosownie do § 37 ust. 2 zarządzenia Nr 1/14 Wojewody Podkarpackiego z dnia 2 stycznia 2014 r. w sprawie szczegółowych warunków i trybu prowadzenia kontroli (z późn. zm.) w ramach realizacji czynności kontrolnych stosowana była 4-stopniowa skala ocen, tj. ocena pozytywna, pozytywna z uchybieniami, pozytywna z nieprawidłowościami, negatywna.

- System Rejestrów Państwowych (SRP) - dane o obywatelach zgromadzonych w poszczególnych rejestrach (rejestr PESEL, rejestr Dowodów Osobistych, rejestr Stanu Cywilnego);

- Elektroniczna Platforma Usług Administracji Publicznej (ePUAP);
- Centralna Ewidencja Działalności Gospodarczej (CEIDG);
- eDoręczenia.

b) systemy własne lub zakupione:
- PB_EWID, PB_EWID_SRP (System Ewidencji Ludności i Obsługi wyborów samorządowych) – firmy TECHNIKA IT sp. z o.o.,
- Ewidencja zwrotów podatku akcyzowego – firmy Biuro Usług Komputerowych SOFTRES sp. z o.o.,
- Proton - Elektroniczny Obieg Dokumentów firmy Sputnik wdrożony w ramach projektu PSeAP (Podkarpacki System E-Administracji Publicznej),
- poczta elektroniczna,

- strona www,
- BIP.

Podstawą oceny są następujące ustalenia kontroli:

1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną

1.1. Usługi elektroniczne

Urząd Miejski w Lubaczowie udostępniał elektroniczną skrzynkę podawczą (dalej: ESP) na platformie ePUAP oraz adres do eDoręczeń. Na stronie BIP kontrolowanej jednostki znajdowała się informacja o **elektronicznej skrzynce podawczej i adresie do eDoręczeń,** które pozwalały na przesłanie drogą elektroniczną pism skierowanych do Urzędu, w tym pism ogólnych, skarg, wniosków, zapytań itp.
Korespondencja z ePUAP oraz z eDoręczeń była odbierana przez używany system obiegu dokumentów - PROTON. W przypadku problemów z komunikacją występowała konieczność pobierania korespondencji bezpośrednio z portalu np. eDoręczeń.
Na stronie www Urzędu oraz na BIP znajdowała się informacja o adresie eDoręczeń i **elektronicznej skrzynki podawczej**.

1.2. Współpraca systemów teleinformatycznych z innymi systemami

Pracownicy Urzędu Miejskiego w Lubaczowie posiadali dostęp do rejestrów publicznych takich jak: SRP Źródło, CEIDG.

System PB_EWID komunikował się z usługami sieciowymi Systemu Rejestrów Państwowych w celu pobierania danych dzięki modułowi PB_EWID_SRP odpowiadającemu za transmisję danych z SRP do Systemu Ewidencji Ludności.

1.3. Obieg dokumentów

W Urzędzie Miejskim w Lubaczowie był wdrożony System Elektronicznego Zarządzania Dokumentacją PROTON umożliwiający zarządzanie dokumentami i wykonywanie czynności kancelaryjnych. Obecnie każda wpływająca korespondencja była rejestrowana i dekretowana w systemie PROTON.

2. Wdrożenie systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z § 19 ust. 1 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zwanego dalej 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 z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Wymaga to opracowania dokumentacji SZBI, w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Dokumentacja jest warunkiem niezbędnym dla możliwości skutecznego zarządzania bezpieczeństwem informacji.

W zakresie bezpieczeństwa teleinformatycznego w badanej jednostce został ustanowiony System Zarządzania Bezpieczeństwem Informacji (SZBI) w 2022 roku według wymogów rozporządzenia KRI.

Oprócz dokumentów i procedur wchodzących w skład SZBI zostały wprowadzone również dokumenty z zakresu ochrony danych osobowych. Pomimo, iż dokumentacja była ustanowiona i aktualizowana, brak było w niej spójności i jednolitości, dodatkowo dużo zapisów zostało powielanych w poszczególnych dokumentach oraz nie wszystkie załączniki zostały wdrożone.

W Urzędzie Miasta Lubaczów ustanowiono:

- System Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Lubaczowie - Zarządzenie nr 138/2022 Burmistrza Miasta Lubaczowa z dnia 30 września 2022 r.;
- Polityka Bezpieczeństwa Informacji (PBI) w Urzędzie Miejskim w Lubaczowie wraz z załącznikami stanowiąca Załącznik nr 1 do Zarządzenia nr 138/2022 Burmistrza Miasta Lubaczowa z dnia 30 września 2022 r.;
- Polityka Bezpieczeństwa Teleinformatycznego w Urzędzie Miejskim w Lubaczowie wraz z załącznikami stanowiąca Załącznik do Zarządzenia nr 138/2022 Burmistrza Miasta Lubaczowa z dnia 30 września 2022 r.;
- Polityka Bezpieczeństwa Fizycznego w Urzędzie Miejskim w Lubaczowie wraz z załącznikiem stanowiąca Załącznik do Zarządzenia nr 138/2022 Burmistrza Miasta Lubaczowa z dnia 30 września 2022 r.;

- Procedura Zarządzania Incydentami Bezpieczeństwa Informacji w Urzędzie Miejskim w Lubaczowie stanowiąca Załącznik do Zarządzenia nr 138/2022 Burmistrza Miasta Lubaczowa z dnia 30 września 2022 r.;
- Procedura Inwentaryzacji i Klasyfikacji Informacji SZBI w Urzędzie Miejskim w Lubaczowie stanowiąca Załącznik do Zarządzenia nr 138/2022 Burmistrza Miasta Lubaczowa z dnia 30 września 2022 r.;
- Polityka Ochrony Danych Osobowych w Urzędzie Miejskim w Lubaczowie wraz z załącznikami, stanowiąca Załącznik Nr 1 do Zarządzenia Nr 116/2018 Burmistrza Miasta Lubaczowa z dnia 25 maja 2018 r.;
- Instrukcja Zarządzania Systemem Informatycznym w Urzędzie Miejskim w Lubaczowie (IZSI) stanowiąca Załącznik Nr 14 do Polityki Ochrony Danych;
- Regulamin Ochrony Danych Osobowych w Urzędzie Miejskim w Lubaczowie stanowiąca Załącznik Nr 14 do Polityki Ochrony Danych;
- Identyfikacja, ocena oraz określenie metod przeciwdziałania ryzyku – załącznik nr 2 do procedury zarządzania ryzykiem;
- Regulamin funkcjonowania monitoringu wizyjnego Urzędu Miasta w Lubaczowie – Zarządzenie nr 89/2019 Burmistrza Miasta Lubaczowa z dnia 28 maja 2019 r.

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Na analizę ryzyka składają się: identyfikacja, szacowanie a następnie określenie sposobu postępowania z ryzykiem oraz deklaracja stosowania zabezpieczeń będących podstawą podejmowania wszelkich działań minimalizujących ryzyko stosownie do przeprowadzonej analizy.

Zarządzanie bezpieczeństwem przetwarzania danych w Urzędzie Miasta w Lubaczowie opierało się na zarządzaniu ryzykiem, które polegało na przeprowadzaniu okresowej analizie ryzyka i oceny skutków dla przetwarzania danych. Identyfikacja, ocena oraz określenie metod przeciwdziałaniu ryzyku przeprowadzana była corocznie w odniesieniu do poprawy bezpieczeństwa ochrony informacji, w tym zapewnienia ochrony danych osobowych przetwarzanych wewnątrz Urzędu oraz tych przekazywanych na zewnątrz.

Wyniki analizy ryzyka mają wpływać na decyzje odnośnie podniesienia bezpieczeństwa funkcjonowania jednostki, np. poprzez wzmocnienie kontroli zarządczej, system zastępstw na strategicznych stanowiskach, szkolenia pracowników w stosunku do zagrożonych obszarów eksploatacji systemów informatycznych.
Dokonując analizy ryzyka warto wziąć pod uwagę utratę integralności, dostępności lub poufności wszystkich informacji, nie tylko tych związanych z danymi osobowymi.
Analiza ryzyka powinna obejmować największe zagrożenia dla cyberbezpieczeństwa oraz stanowić fundament skutecznego cyberbezpieczeństwa.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

Zarządzanie infrastrukturą informatyczną wymaga utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. W praktyce oznacza to zapewnienie funkcjonowania rejestru zasobów teleinformatycznych zawierającego informacje o wszystkich

zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, parametrach, aktualnej konfiguracji, oprogramowaniach, środkach komunikacji, a także rodzaju relacji między elementami konfiguracji oraz użytkownikiem.

Regulacje wewnętrzne, w Polityce Bezpieczeństwa Informacji, zawierały zapisy dotyczące inwentaryzacji i identyfikacji zasobów informacyjnych. Dodatkowo w Załączniku nr 1 do Polityki Bezpieczeństwa Teleinformatycznego została zawarta Lista Gestorów Systemów Informatycznych i usług IT.
W Instrukcji Zarządzania Systemem Informatycznym wskazany został sposób zabezpieczenia systemu informatycznego (punkt 8), w tym zabezpieczenie infrastruktury IT i zabezpieczenie aplikacji.

Jednostka dysponowała zakupionym i wdrożonym oprogramowaniem ESET Protect Advenced pozwalającym na identyfikację oprogramowania i komputerów w sieci.

W urzędzie do pracy bieżącej, użytkowane były komputery stacjonarne oraz laptopy, a do eksploatacji dopuszczone było tylko oprogramowanie autoryzowane przez ASI.

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Istotnym elementem polityki bezpieczeństwa informacji jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie dostępem ma zapewnić, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, a w przypadku zmiany zadań następuje również zmiana ich uprawnień.
W Urzędzie Miejskim, w badanym okresie, zarządzanie uprawnieniami dostępu do przetwarzania danych regulowały: Polityki Bezpieczeństwa Teleinformatycznego, Polityka Ochrony Danych Osobowych i Instrukcja Zarządzania Systemem Informatycznym.
Dodatkowo w Polityce Ochrony Danych Osobowych zostały zawarte procedury i zasady nadawania i odbierania upoważnień do przetwarzania danych osobowych (punkt 5).
Dokumentacja powyższa szczegółowo opisywała sposób dostępu do obszarów chronionych, sieci i systemów teleinformatycznych oraz nadawania, zmiany i odbierania uprawnień użytkownikom w systemach informatycznych funkcjonujących w jednostce.
Pracownicy uzyskiwali dostęp do zasobów informatycznych po przyznaniu zakresu obowiązków i nadaniu unikalnego identyfikatora i hasła w systemie teleinformatycznym.
W przypadku konieczności zmiany i odbioru uprawnień dla użytkownika w systemach informatycznych informacja przekazywana była przy pomocy Wniosku o nadanie/usunięcie/dodanie uprawnień dla użytkownika w systemie informatycznym podpisanego przez bezpośredniego przełożonego.
Zakres uprawnień użytkowników badanych systemów uniemożliwiał wykonywanie przez nich działań zastrzeżonych dla administratorów systemów w przypadku komputerów stacjonarnych podłączonych do Active Directory. Jednakże laptopy znajdujące się w posiadaniu kierownictwa nie zawsze były objęte podłączeniem do Active Directory.
W okresie objętym badaniem konta byłych pracowników urzędu były sukcesywnie blokowane w systemach informatycznych. Na bieżąco odbywało się monitorowanie dostępu do zasobów informatycznych zgodnie z wymaganiami § 19 ust. 2 pkt 4 rozporządzenia KRI.

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Istotnym elementem SZBI jest świadomość pracowników współodpowiedzialności za bezpieczeństwo informacji, zagrożeń i konsekwencji zaistnienia incydentów związanych z naruszeniem bezpieczeństwa.

Szkolenia z zakresu bezpieczeństwa informacji powinny obejmować wszystkie osoby uczestniczące w procesie przetwarzania informacji oraz dostarczać aktualnej wiedzy o nowych zagrożeniach, adekwatnych zabezpieczeniach oraz skutkach ewentualnych incydentów związanych z bezpieczeństwem informacji.

Dokumentacja wewnętrzna (Polityka Ochrony Danych Osobowych) Urzędu Miasta w Lubaczowie regulowała zakres przeszkolenia osób przed dopuszczeniem do pracy. Również w zakresie zwiększenia świadomości pracowników przynajmniej raz w roku powinno być organizowane szkolenie przypominające zasady ochrony informacji.

Nie przedstawiono informacji o ostatnim takim szkoleniu.

W Urzędzie Miejskim w Lubaczowie podejmowane były działania podnoszące świadomość pracowników: został udostępniony folder na zasobie dyskowym zawierający ustanowione dokumenty w zakresie ochrony danych osobowych i informacji oraz prezentację dotyczącą ochrony danych osobowych, a także poradnik podstawowych zasad cyberbezpieczeństwa w Urzędzie Miejskim w Lubaczowie.

Pomimo tych działań można było zauważyć, że pracownicy przechowywali hasła do komputera w widocznym miejscu.

2.6. Praca na odległość i mobilne przetwarzanie danych

Wobec możliwości technicznych związanych z telepracą (pracą poza siedzibą podmiotu publicznego z wykorzystaniem urządzeń mobilnych takich jak laptopy, tablety, smartfony) pojawiają się nowe zagrożenia bezpieczeństwa informacji. Konieczne jest opisanie zasad określających sposoby zabezpieczenia urządzeń mobilnych i danych w nich zawartych przed kradzieżą i nieuprawnionym dostępem poza siedzibą jednostki, a także zasady korzystania z ogólnodostępnych sieci.

W obowiązujących dokumentach były zawarte ogólne zasady zarządzania bezpieczną pracą na komputerach przenośnych i sposoby zabezpieczenia tych urządzeń (Polityka Bezpieczeństwa Teleinformatycznego, Instrukcja Zarządzania Systemem Informatycznym – punkt 8: Bezpieczeństwo przetwarzania danych poza organizacją). W Urzędzie Miasta Lubaczowa nie funkcjonował Regulamin pracy zdalnej.

Laptopy nie były szyfrowane. Pracownicy nie wynosili przenośnych komputerów poza siedzibę jednostki.

2.7. Serwis sprzętu informatycznego i oprogramowania

W przypadku systemów informatycznych o znaczeniu istotnym dla jednostki niezbędne jest objęcie tych systemów (w zakresie oprogramowania użytkowego, systemowego, sprzętu i rozwiązań telekomunikacyjnych) stosownymi umowami serwisowymi, gwarantującymi odpowiednio szybkie uruchomienie pracy systemu w przypadku awarii. Umowy powinny posiadać klauzule prawne zabezpieczające ochronę informacji w przypadku wejścia w ich posiadanie przez firmy serwisujące.

W procedurach wewnętrznych m.in. w: Polityce Bezpieczeństwa Informacji, Polityce Bezpieczeństwa Teleinformatycznego zostały określone zasady współpracy z podmiotami

trzecimi w zakresie korzystania z usług firm zewnętrznych przy rozwoju i utrzymaniu systemów teleinformatycznych oraz przy przetwarzania danych osobowych.
Dodatkowo poziom bezpieczeństwa regulowały umowy zawierane z firmami zewnętrznymi, w przypadku serwisowania sprzętu lub oprogramowania (udostępniono umowę licencyjną z Biurem Usług komputerowych SOFTRES Sp. z o.o. – 2024 r., z Nefeni Sp. z o.o. – z 2022 r., DMK STUDIO Maciejewska, Klonowski Spółka Jawna – z 2025 r. i 2024 r., EXTRANET Joanna Październierska – 2025 r.).
W przypadku systemów informatycznych istotnych dla jednostki zostały zawarte także umowy powierzenia przetwarzania danych osobowych.

2.8. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji
Zostały określone zasady postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa informacji w Procedurze Zarządzania Incydentami Bezpieczeństwa Informacji w Urzędzie Miejskim w Lubaczowie.
Rejestr incydentów i działań korygujących w Urzędzie Miejskim w Lubaczowie nie został przedstawiony.
2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji
Audyt z zakresu bezpieczeństwa informacji nie rzadziej niż raz na rok, w rozumieniu § 19 ust. 14 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych nie był wykonany w 2024 roku. Warto zwrócić uwagę, że celem audytów jest ewentualne ujawnienie słabości systemów, a także słabości zabezpieczeń lub ich stosowania. Uregulowania wewnętrzne nie zawierały zapisów dotyczących konieczności audytowania i sprawdzeń w zakresie bezpieczeństwa informacji.

Wyniki audytu powinny wpłynąć na doskonalenie tych zabezpieczeń, sposobów ich stosowania, a także na program szkoleń z bezpieczeństwa informacji.

W 2023 roku była wykonana kontrola przez Inspektora Ochrony Danych w zakresie prawidłowości postepowania pracowników w przypadku wystąpienia zagrożeń związanych z utratą, zgubieniem lub uszkodzeniem danych osobowych.

2.10. Kopie zapasowe
Wykonywanie kopii zapasowych zapobiega utracie informacji w wyniku awarii.
Kopie powinny być właściwie tworzone, przechowywane i testowane.
W okresie objętym kontrolą w zakresie wykonywania kopii zapasowych w Urzędzie Miejskim w Lubaczowie obowiązywały wymagania określone w Polityce Ochrony Danych Osobowych i Polityce Bezpieczeństwa Teleinformatycznego (punkt 5.8 Procedury tworzenia oraz sposób, miejsce i okres przechowywania kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania).
Kopie folderów, maszyn wirtualnych były wykonywane według harmonogramu ustalonego przez ASI oraz przechowywane na serwerze Synology.
Wykonywanie odtworzenia systemów z kopii zapasowych było testowana oraz odbywało się w razie potrzeby.
Przechowywanie kopii zapasowej poza siedzibą Urzędu nie zostało uregulowane i opisane.

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

W Urzędzie Miejskim w Lubaczowie proces administrowania technicznego i monitorowania określonych obszarów systemów, aplikacji, danych, infrastruktury sieciowej i stacji roboczych był wykonywany przez informatyków, co pozwalało na przewidywanie i zapobieganie ewentualnym problemom związanym z awariami, wyciekami bądź utratą danych.

Systemy centralne, w ramach kontroli podlegały badaniu w ograniczonym zakresie, ze względu na centralne polityki, procedury, wdrożenia i dostępy.

Wybrane systemy własne lub zakupione podlegały sprawdzeniu w zakresie zgodności z rozdz. IV rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Najistotniejsze systemy były objęte opieką na podstawie umów opieki autorskiej lub serwisowej.

W przypadku problemów z systemami centralnymi, np. eDoręczenia i CEIDG były dokonywane zgłoszenia na udostępnione portale help desk. W przypadku systemów zakupionych należy pamiętać, aby w umowach z firmami trzecimi zawrzeć odpowiednie zapisy dotyczące kanałów komunikacji i czasów reakcji.

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji. Zastosowane zabezpieczenia powinny być adekwatne do poziomu ryzyka wynikającego z analizy ryzyka bezpieczeństwa informacji.
Szereg zabezpieczeń techniczno-organizacyjnych dostępu do informacji opisano w Polityce Bezpieczeństwa Teleinformatycznego i Polityce Ochrony Danych Osobowych oraz w Polityce Bezpieczeństwa Fizycznego w Urzędzie Miejskim w Lubaczowie.
Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami realizowana była przez:

a) zabezpieczenie dostępu do informacji poprzez wymuszone logowanie użytkowników za pomocą kart lub poprzez podanie unikalnego hasła do badanych systemów;
b) kontrolę i monitorowanie zabezpieczenia fizycznego dostępu do pomieszczeń;
c) podejmowanie czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez monitorowanie infrastruktury teleinformatycznej, kontrolę wejść i wyjść do pomieszczeń serwerowni uprawnionych osób;
d) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji poprzez system autoryzacji dostępu do systemów operacyjnych, sieci i aplikacji, stosowania systemów antywirusowych i antyspamowych.

Urząd Miejski w Lubaczowie posiadał pomieszczenia biurowe zlokalizowane w jednym budynku.

Obiekt był objęty systemem alarmowym ochrony fizycznej oraz był objęty systemem monitoringu na zewnątrz i wewnątrz budynku. Do otwierania głównych drzwi budynku oraz rozbrajania systemu alarmowego byli upoważnieni wyznaczeni pracownicy.
Klucze do pomieszczeń biurowych pracownicy wynosili z sobą poza budynek Urzędu, pomimo funkcjonowania portierni.
W budynku oprócz systemu alarmowego były również w niektórych częściach czujki pożarowe.
Urząd Miejski dysponował jedną główną serwerownią. Dostęp do serwerowni był ograniczony i możliwy jedynie dla upoważnionych pracowników Urzędu. Ważnym elementem ochrony było asystowanie osobom wchodzącym i wykonującym prace serwisowe.

Serwerownia znajdowała się w pomieszczeniu zaadaptowanym na ten cel. Pomieszczenie nie do końca zostało przystosowane do pełnienia funkcji serwerowni.
Serwerownia nie posiadała systemu kontroli wejść. Występowało monitorowanie tylko niektórych parametrów środowiskowych w serwerowni (temperatury i wilgotności). Pomieszczenie było klimatyzowane. Zapewniono redundancję klimatyzatorów ze względu na bardzo małe pomieszczenie i możliwość jego mocnego nagrzewania (brak rolet i izolacji w oknie dachowym). Na ścianach były widoczne ślady zalania od klimatyzatorów.
Ponadto uchylne okno dachowe nie posiadało wzmocnień i zabezpieczeń (od pożaru, zalania, uderzenia). Drzwi do serwerowni były pokryte blachą, natomiast zamki nie posiadały wzmocnień i atestów.
W serwerowni znajdowały się UPSy, który podtrzymywały pracę serwera i urządzeń sieciowych.
W pomieszczeniu nie były przechowywane materiały łatwopalne.
Urząd nie dysponował drugim pomieszczeniem, mogącym pełnić funkcję serwerowni zapasowej.
Zapewniono redundancję łączy internetowych od niezależnych dostawców.

Bazy danych z kopiami nie były umieszczone w innej lokalizacji.
Podstawowe urządzenie infrastruktury informatycznej: serwer, urządzenia sieciowe były zakupione w ramach Projektu.
Monitorowanie ruchu wchodzącego i wychodzącego realizowane było przez maszyny sprzętowe UTM Fortigate 100f.

Wszystkie komputery oraz urządzenie sieciowe posiadały oprogramowanie systemowe zaktualizowane do wersji posiadających wsparcie producenta.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Stosowanie zabezpieczeń techniczno-organizacyjnych również powinno wynikać z analizy ryzyka i powstałego w jej wyniku planu postępowania z ryzykiem i deklaracji stosowania zabezpieczeń.
Poziom bezpieczeństwa systemów teleinformatycznych zapewniono poprzez:
a) aktualizację oprogramowania oraz redukcję ryzyk wynikających z wykorzystywania opublikowanych podatności technicznych systemów teleinformatycznych (w tym oprogramowania antywirusowego);

b) minimalizację ryzyka utraty informacji w wyniku awarii oraz ochronę przed błędami, utratą i nieuprawnioną modyfikacją, a także zapewnienie bezpieczeństwa plików systemowych, zastosowania systemu kopii zapasowych, systemu kontroli dostępu do zasobów informatycznych, systemu monitorowania funkcjonowania systemów teleinformatycznych i sieci.
Była wdrożona usługa katalogowa Active Directory, która pozwalała na zarządzanie tożsamościami i relacjami w sieci, przez co umożliwiała sprawniejszą kontrolę nad całą siecią oraz użytkownikami.
Kontrolujący zwrócili uwagę, że w folderze udostępnionym dla wszystkich pracowników mogły być umieszczane informacje nadmiarowe i bez nadzoru.

2.14. Rozliczalność działań w systemach informatycznych
Przetwarzanie informacji w systemach wymagało dostępu do danych przez uprawnionych użytkowników. Wszelkie działania związane z przetwarzaniem informacji, a także działania administratorów muszą podlegać dokumentowaniu w postaci zapisów w dziennikach systemów (logi), co zapewnia rozliczalność operacji. Informacje zawarte w logach (tj. kto, kiedy i co wykonał w systemie teleinformatycznym) powinny być regularnie przeglądane w celu wykrycia działań niepożądanych i muszą być przechowywane w bezpieczny sposób, co najmniej dwa lata. Świadomość użytkowników, że żadne działanie nie zostanie anonimowe podnosi poziom bezpieczeństwa informacji.

Urząd Miejski w Lubaczowie dysponował regulacjami wewnętrznymi, w których określone byłyby zasady polityki zarządzania logami oraz rozliczalności działań poszczególnych obiektów Instrukcja Zarządzania Systemem Informatycznym – punkt 8 Zabezpieczenia aplikacji.
Sprawdzane systemy informatyczne użytkowe miały udokumentowaną rozliczalność.
Warto w celu zapewnienia rozliczalności każdemu użytkownikowi przypisać indywidulane konto, w szczególności dla administratorów, (w tym z firm zewnętrznych) oraz zdeponować hasła administratorów do najważniejszych systemów i urządzeń w bezpiecznym miejscu w powiązaniu z procedurą ciągłości działania.

3. Zapewnienie dostępności informacji zawartych na stronie BIP oraz internetowej urzędów dla osób niepełnosprawnych

W udostępnianych systemach teleinformatycznych powinny zostać zastosowane rozwiązania techniczne umożliwiające osobom niedosłyszącym lub niedowidzącym zapoznanie z treścią informacji m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu, czy też odsłuchanie wyświetlanej treści – zgodnie ze standardem WCAG 2.0.

Systemy informatyczne wspomagające realizację zadań Urzędu nie były objęte wymogami WCAG 2.0 w zakresie dostępności ze względu na brak interakcji z klientami za pośrednictwem sieci publicznej.
Analizując poprawność kodu strony BIP poprzez walidator dostępny pod adresem: https://validator.utilitia.pl/ badana strona uzyskała wynik 5,5 pkt na 10 możliwych, natomiast strona www uzyskała wynik 3,2 pkt na 10 możliwych.

Ww. ustalenia, w tym ocena kontrolowanej działalności, zostały udokumentowane w aktach kontroli, na które składają się kopie dokumentów.

Przy czym do ww. ustaleń kontrolnych (przekazanych do wiadomości w dniu 29 lipca 2025 r.) przysługiwało Panu, na podstawie ww. ustawy o kontroli w administracji rządowej, prawo zgłoszenia umotywowanych pisemnych zastrzeżeń, z którego Pan nie skorzystał.

W związku z powyższym, stosownie do art. 46 ust. 1 ustawy o kontroli w administracji rządowej, sporządzono niniejsze wystąpienie pokontrolne, obejmujące m.in. treść projektu wystąpienia pokontrolnego.

Zgodnie z wymogami § 19 ust. 1-14 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych:

1. Dążyć do wzmocnienia zabezpieczeń techniczno-organizacyjnych (drzwi, okno, system ppoż.) pomieszczenia pełniącego rolę serwerowni.
2. Kopie zapasowe przechowywać w innej lokalizacji niż Urząd.
3. Niezbędne jest uporządkowanie, a następnie eksploatowanie, monitorowanie, przeglądanie i doskonalenie pełnego systemu zarządzania bezpieczeństwem informacji uwzględniającego zarządzanie ryzykiem (wziąć pod uwagę utratę integralności, dostępności lub poufności wszystkich informacji oraz ciągłość działania systemu bezpieczeństwa informacji).
4. Dokonać szyfrowania urządzeń przenośnych.
5. Wprowadzić pełną rozliczalność w zakresie kont indywidualnych oraz dostępów w systemach.

O sposobie wykonania powyższych wniosków pokontrolnych, bądź działaniach podjętych w celu ich realizacji, oczekuję od Pana odpowiedzi na piśmie wraz ze skanami dokumentów lub innych potwierdzeń dotyczących sposobu wdrożenia zaleceń, w terminie 21 dni od dnia otrzymania niniejszego wystąpienia.

WOJEWODA PODKARPACKI

(-)

Teresa Kubas-Hul

(Podpisane bezpiecznym podpisem elektronicznym)