

**WOJEWODA PODKARPACKI**

ul. Grunwaldzka 15

35-959 Rzeszów

OA-VII.431.2.2021 Rzeszów, 2021-05-25

**Pan**

**Waldemar Góra**

**Burmistrz Strzyżowa**

Na podstawie art. 46 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, w związku ze zrealizowaną w dniu 30 marca 2021 r. oraz przy użyciu środków komunikacji elektronicznej u Burmistrza Strzyżowa (Urząd Miejski w Strzyżowie, ul. Przecławczyka 5, 38-100 Strzyżów) kontrolą problemową[[1]](#footnote-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 (kierownik) na podstawie imiennych upoważnień do kontroli (pisma z dnia 22.03.2021 r., znak OA-VII.431.2.2021) udzielonych przez działającego z upoważnienia Wojewody Podkarpackiego – Dyrektora Wydziału Organizacyjno-Administracyjnego.

Ustalenia kontrolne dokonane zostały w oparciu o stan faktyczny istniejący od 1 stycznia 2019 r.do dnia realizacji czynności kontrolnych włącznie.

Kontrola obejmuje priorytet Prezesa Rady Ministrów na 2021 r. pn. „Bezpieczeństwo teleinformatyczne oraz cyfryzacja usług i procesów w administracji”.

W toku kontroli - w oparciu o kontrolowane dokumenty (przy zastosowaniu metody niestatystycznej, losowy dobór próby) - ustalono, iż pracownicy Urzędu Miasta Strzyżów 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.

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

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 Strzyżowie pełnił Burmistrz: Pan Waldemar Góra.

Funkcję Inspektora Ochrony Danych (IOD) powierzono wykonawcy zewnętrznemu na podstawie zawartej umowy.

Wsparcie informatyczne zapewnione było przez pracownika urzędu zatrudnionego jako informatyk. Pod jego opieką znajdowały się: środowiska sprzętowo-programowe, sieć lokalna i serwerownia, systemy i aplikacje centralne oraz własne, usprawniające pracę pracownikom Urzędu Miejskiego w Strzyżowie.

Informatyk pełnił funkcję Administratora Systemów Informatycznych (ASI).

W okresie objętym kontrolą w Urzędzie Miejskim w Strzyżowie użytkowane były systemy teleinformatyczne zakupione przez urząd oraz tzw. centralne m.in.:

a) systemy centralne:

- 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)

- SIO (System Informacji Oświatowej)

b) systemy własne lub zakupione:

- Lokalny Rejestr Mieszkańców wraz z modułem ImportSRP – firmy Clanet – Klaudiusz Gatys

- Proton - Elektroniczny Obieg Dokumentów firmy Sputnik wdrożony w ramach projektu PSeAP (Podkarpacki System E-Administracji Publicznej)

- Ewidencja wniosków o Zwrot Podatku Akcyzowego (AKC) – Biura Usług Komputerowych „Softres” sp. z o.o.

- pozostałe moduły firmy „Softres” sp. z o.o.

- 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. Usługi elektroniczne

Urząd Miejski w Strzyżowie udostępniał elektroniczną skrzynkę podawczą (dalej: ESP) na platformie ePUAP, która pozwalała na przesłanie drogą elektroniczną pism kierowanych do urzędu, w tym pism ogólnych, skarg, wniosków, zapytań itp. System Proton nie komunikowały się z systemem zewnętrznym ePUAP w celu odbierania i wysyłania korespondencji w postaci elektronicznej. Korespondencja wpływająca przez ESP odbierana była bezpośrednio w ePUAP, a następnie rejestrowana w systemie Proton i kierowana do kierowników wydziałów lub pracowników.

Na stronie głównej oraz na stronie BIP kontrolowanej jednostki nie było informacji o adresie **elektronicznej skrzynki podawczej.**

* 1. Obieg dokumentów

W Urzędzie Miejskim w Strzyżowie funkcjonował system – Proton (w ramach projektu PSeAP) umożliwiający zarządzanie dokumentami i wykonywanie czynności kancelaryjnych. Był to system pomocniczy w sposobie dokumentowania przebiegu załatwiania spraw. Obecnie jest rozważana możliwość przejścia na inny system obsługujący elektroniczny obieg dokumentów.

* 1. Współpraca systemów teleinformatycznych z innymi systemami

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

System ImportSRP komunikował się z usługami sieciowymi Systemu Rejestrów Państwowych w celu pobierania danych dzięki modułowi odpowiadającemu za transmisję danych z SRP do Lokalnego Rejestru Mieszkańców.

1. **Wdrożenie systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych**
   1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarzadzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji. 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 i wprowadzony System Zarządzania Bezpieczeństwem Informacji (SZBI).

Kluczowe dokumenty związane z wdrożeniem SZBI to:

* Polityka Bezpieczeństwa Informacji stanowiąca załącznik do Zarządzenia Nr 11/18 Burmistrza Strzyżowa z dnia 7 grudnia 2018 r. w sprawie ustanowienia i wdrożenia Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Strzyżowie;
* Procedura Dotycząca Zarządzania Systemem Informatycznym na potrzeby Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Strzyżowie stanowiąca Załącznik nr 1 do Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Strzyżowie;
* Procedura Zarządzania Sprzętem i Oprogramowaniem na potrzeby Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Strzyżowie stanowiąca Załącznik nr 2 do Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Strzyżowie;
* Procedura Wykonywania i Testowania Kopii Bezpieczeństwa na potrzeby Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Strzyżowie stanowiąca Załącznik nr 3 do Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Strzyżowie;
* Procedura Identyfikacji, Szacowania oraz Sposobu Postępowania z Ryzykiem w Systemie Informacyjnym na potrzeby Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Strzyżowie stanowiąca Załącznik nr 4 do Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Strzyżowie;
* Plan Zachowania Ciągłości Działania na potrzeby Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Strzyżowie stanowiąca Załącznik nr 5 do Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Strzyżowie;
* Procedura Rozwoju Zasobów Informacyjnych oraz Systemów Informatycznych na potrzeby Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Strzyżowie stanowiąca Załącznik nr 6 do Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Strzyżowie;
* Instrukcja Bezpieczeństwa Danych Osobowych - Urząd Miejski w Strzyżowie stanowiąca załącznik do Zarządzenia Nr 113/20 z dnia 6 lipca 2020 r. w sprawie określenia wprowadzenia instrukcji bezpieczeństwa danych osobowych w Urzędzie Miejskim w Strzyżowie;
* Regulamin wykonywania pracy zdalnej przez pracowników Urzędu Miejskiego w Strzyżowie stanowiący załącznik do Zarządzenia Nr 41/20 Burmistrza Strzyżowa z dnia 24 marca 2020 r. oraz Zasady Bezpieczeństwa Informacji przy wykonywaniu pracy zdalnej (załącznik Nr 3).

Za wdrożenie dokumentacji SZBI, jej monitorowanie i poddawanie przeglądom odpowiedzialny był powołany przez Burmistrza Gminy Strzyżów tzw. Komitet Bezpieczeństwa Informacji (KBI), w skład którego wchodził: Administrator Systemu Informatycznego, Inspektor Ochrony Danych oraz Sekretarz Gminy.

* 1. 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.

W Urzędzie Miejskim w Strzyżowie przyjęty był, wraz z Polityką Bezpieczeństwa Informacji, proces zarządzania ryzykiem zgodnie z Procedurą Identyfikacji, Szacowania oraz Sposobu Postępowania z Ryzykiem w Systemie Informacyjnym.

Dokumentacja analizy poufności, integralności i rozliczalności systemów informatycznych zawierała:

- zasoby

- rodzaje zagrożeń występujące w zasobach

- podatność systemu na zagrożenia

- zabezpieczenia planowane

- zabezpieczenia wdrożone.

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.

Arkusz okresowej analizy ryzyka sporządzany był corocznie.

* 1. Inwentaryzacja sprzętu i oprogramowania informatycznego

Regulacje wewnętrzne zawierały zapisy dotyczące konieczności rejestru zasobów teleinformatycznych, w tym: podstawowej konfiguracji komputera.

Ewidencja sprzętu, oprogramowania oraz podzespołów prowadzona była przez informatyka na kartach technicznych oprogramowania i komputera. W jednostce, do pracy bieżącej, użytkowane były komputery stacjonarne oraz laptopy.

* 1. Zarządzanie uprawnieniami do pracy w systemach informatycznych

W badanym okresie zarządzanie uprawnieniami dostępu do przetwarzania danych w Urzędzie Miejskim regulowały:

* Polityka Bezpieczeństwa Informacji
* Procedura Dotycząca Zarządzania Systemem Informatycznym
* Procedura Zarządzania Sprzętem i Oprogramowaniem.

Dokumentacja powyższa szczegółowo opisywała sposób 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 loginu i hasła w systemie teleinformatycznym.

Zakres uprawnień użytkowników badanych systemów uniemożliwiał wykonywanie przez nich działań zastrzeżonych dla administratorów systemów.

W okresie objętym badaniem konta byłych pracowników urzędu były sukcesywnie blokowane w systemach informatycznych.

W przypadku konieczności zmiany i odbioru uprawnień dla użytkownika w systemach informatycznych informacja przekazywana była ustnie.

Na bieżąco odbywało się monitorowanie dostępu do zasobów informatycznych zgodnie z wymaganiami § 20 ust. 2 pkt 4 rozporządzenia KRI.

* 1. 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 Urzędu Miejskiego w Strzyżowie regulowała zakres podnoszenia świadomości pracowników poprzez konieczność zapoznania każdego nowego pracownika z treścią polityk, instrukcji, a także o zobowiązaniu się do ich przestrzegania.

Dokumentacja także regulowała sprawę nadzoru przez Komitet Bezpieczeństwa Informacji nad koniecznością przeprowadzenia cyklicznych szkoleń w tym zakresie.

W Urzędzie były przeprowadzane szkolenia dla pracowników w 2019 r. głównie z RODO. Natomiast na bieżąco pracownicy byli powiadamiani o nowych zagrożeniach poprzez system mailowy.

* 1. Praca na odległość i mobilne przetwarzanie danych

W obowiązującej Polityce Bezpieczeństwa Informacji były zawarte podstawowe zasady zarządzania zabezpieczeniem komputerów przenośnych (Rozdział XII). Zasady pracy zdalnej oraz zabezpieczenia wynoszonych urządzeń określone zostały w Regulaminie wykonywania pracy zdalnej przez pracowników Urzędu Miejskiego w Strzyżowie.

Pracownicy Urzędu korzystali z laptopów przy pracy zdalnej, które nie były szyfrowane. Praca wykonywana była na zasobach serwerowych, bez umieszczania danych na dyskach laptopów.

Sprawdzane umowy serwisowe zawierane z wykonawcą zewnętrznym nie zawsze miały określone zasady bezpiecznych połączeń zdalnych na wypadek wykonywania usługi opieki przez takie połączenie.

* 1. Serwis sprzętu informatycznego i oprogramowania

W przypadku systemów informatycznych o znaczeniu krytycznym 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.

Jednak nie wszystkie umowy o asystę i opiekę autorską lub serwisową z firmami zewnętrznymi miały określone SLA (Service Level Agreement), czyli gwarantowany poziom świadczenia usług oraz czas i sposób reakcji na zgłaszane problemy.

W przypadku systemów informatycznych istotnych dla jednostki zostały zawarte umowy powierzenia przetwarzania danych osobowych.

* 1. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Zostały określone zasady Zarządzania incydentami związanymi z bezpieczeństwem informacji w Polityce Bezpieczeństwa Informacji (rozdział XIII).

* 1. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Audyt z zakresu bezpieczeństwa informacji nie rzadziej niż raz na rok, w rozumieniu § 20 ust. 14 rozporządzenia Rady Ministrów z dnia 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych był wykonany w 2019 r. i 2020 r. pn. „System Zarządzania Bezpieczeństwem Informacji w Systemach Teleinformatycznych Urzędu”.

Warto zwrócić uwagę, że celem audytów jest ewentualne ujawnienie słabości systemów, a także słabości zabezpieczeń lub ich stosowania.

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

* 1. Kopie zapasowe

Wykonywanie kopii zapasowych zapobiega utracie informacji w wyniku awarii.

Kopie powinny być właściwie tworzone, przechowywane i testowane.

W zakresie wykonywania kopii zapasowych w Urzędzie Miejskim w Strzyżowie obowiązywały wymagania określone w Procedurze Wykonywania i Testowania Kopii Bezpieczeństwa na potrzeby Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Strzyżowie (Załącznik nr 3 do Polityki Bezpieczeństwa Informacji).

Kopie wykonywane były w sposób automatyczny według zdefiniowanego kalendarza przy pomocy specjalistycznego oprogramowania do tworzenia kopii zapasowych i odzyskiwania danych po awarii. Na bieżąco analizowane były raporty z wykonywania kopii zapasowych.

Nośniki kopii zapasowych były przechowywane w innym pomieszczeniu niż serwerownia.

Wykonywanie odtworzenia systemów z kopii zapasowych występowało w razie potrzeby.

* 1. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

W Urzędzie Miejskim w Strzyżowie proces administrowania technicznego i monitorowania określonych obszarów systemów, aplikacji, danych, infrastruktury sieciowej i stacji roboczych był wykonywany przez informatyka, 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 12 kwietnia 2012 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.

Pracownicy nie zgłaszali problemów z funkcjonalnością badanych systemów.

* 1. 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 Informacji w Urzędzie Miejskim w Strzyżowie.

Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami realizowana była przez:

1. zabezpieczenie dostępu do informacji poprzez wymuszone logowanie u użytkowników za pomocą kart lub poprzez podanie unikalnego hasła do badanych systemów;
2. kontrolę i monitorowanie zabezpieczenia fizycznego dostępu do pomieszczeń;
3. podejmowanie czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez monitorowanie infrastruktury teleinformatycznej, kontrolę wejść i wyjść do pomieszczeń serwerowni uprawnionych osób;
4. 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 Strzyżowie posiadał lokalizację w jednym budynku.

Obiekt był objęty systemem monitoringu. Był także objęty systemem alarmowym ochrony fizycznej.

Urząd Miejski w Strzyżowie dysponował jedną serwerownią, która znajdowała się w pomieszczeniu zaadaptowanym na ten cel. Urząd był w trakcie dostosowywania drugiego pomieszczenia, znajdującego się obok na potrzeby serwerowni. Dodatkowo niektóre urządzenia struktury IT znajdowały się w pokoju informatyka.

Dostęp do serwerowni był ograniczony i możliwy jedynie dla upoważnionych pracowników urzędu. Ważnym elementem ochrony było asystowanie osobom wchodzącym i wykonującym prace serwisowe.

W serwerowni nie zostało wdrożone monitorowanie parametrów środowiskowych (np. temperatury, wilgotności). Drzwi do serwerowni nie posiadały atestowanych wzmocnień i zamków.

W serwerowni przechowywane były serwery i urządzenia sieciowe. Nośniki z kopiami zapasowymi były umieszczone w innym miejscu niż serwerownia.

W serwerowni znajdował się UPS, który podtrzymywał pracę serwerów i urządzeń sieciowych. Strategiczne stanowiska komputerowe nie były wyposażone w urządzenia UPS podtrzymujące pracę komputera podczas zaników prądu. Podstawowe urządzenia sieciowe posiadały tzw. zapas.

W pomieszczeniu nie były przechowywane materiały łatwopalne.

Stosowane zapory sieciowe typu firewall były skonfigurowane przez informatyka we współpracy z firmą zewnętrzną.

Konfiguracja pozostałych urządzeń była przemyślana i aktualizowana w zależności od posiadanej wiedzy.

Zastosowane zabezpieczenia techniczno-organizacyjne wynikały częściowo z analizy ryzyka i planu postępowania z ryzykiem.

* 1. 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:

1. aktualizację oprogramowania oraz redukcję ryzyk wynikających z wykorzystywania opublikowanych podatności technicznych systemów teleinformatycznych (w tym oprogramowania antywirusowego);
2. 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.

Nie było wdrożonej usługi katalogowej Active Directory, która pozwalałaby na zarządzanie tożsamościami i relacjami w sieci, przez co umożliwiałaby kontrolę nad całą siecią.

* 1. 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.

W Polityce Bezpieczeństwa Informacji, w sposób ogólny określone były zasady rozliczalności działań wykonywanych w systemach informatycznych (Rozdział XI). Podczas kontroli przedstawiono kontrolującym zasady rozliczalności w następujących systemach: BIP i Zwrot Podatku Akcyzowego (AKC).

1. **Zapewnienie dostępności informacji zawartych na stronach internetowych 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 3,2 pkt na 10 możliwych, podobnie strona www.

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

Przy czym do ustaleń kontrolnych (przekazanych do wiadomości w dniu 12 maja 2021 r.) została dosłana procedura nie przedstawiona wcześniej w czasie kontroli problemowej, dotycząca zasad organizacji pracy zdalnej (pismo OR.1710.1.2021.MM z dnia 18.05.2021 r.). Wystąpienie pokontrolne oraz dokumentacja kontrolna zostały uzupełnione o to zagadnienie.

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.

Przedstawiając powyższe uwagi i oceny, dokonane m.in. w oparciu o projekt wystąpienia pokontrolnego oraz ww. akta kontroli, w celu usunięcia stwierdzonych uchybień oraz usprawnienia badanej działalności, przekazuję Panu następujące wnioski, zalecenia pokontrolne:

1. We wszystkich umowach serwisowych ze stronami trzecimi zawierać zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, w tym połączeń zdalnych i określić poziom SLA.
2. Wdrożyć szyfrowanie wszystkich urządzeń przenośnych.
3. Pomieszczenia z ważnymi danymi (serwerownia, pokój informatyka) zabezpieczyć w stopniu odpowiadającym zasadom bezpieczeństwa. Wszystkie urządzenia sieciowe powinny być umieszczone w pomieszczeniach odpowiadającym zasadom bezpieczeństwa.

Należy rozważyć montaż urządzeń badających warunki środowiskowe (temperatura, wilgotność, dym, otwarcie drzwi serwerowni). Urządzenia te można skonfigurować tak, aby informacje o wystąpieniu w pomieszczeniu serwerowni niekorzystnych warunków środowiskowych wysyłane były poprzez np. e-mail, SMS.

1. Wdrożyć usługę katalogową Active Directory, która pozwala na zarządzanie tożsamościami i relacjami w sieci, przez co umożliwia kontrolę nad całą siecią.
2. Na stronie głównej oraz na stronie BIP kontrolowanej jednostki uzupełnić informację o adresie **elektronicznej skrzynki podawczej.**

O sposobie wykonania powyższych wniosków pokontrolnych, bądź działaniach podjętych w celu ich realizacji, oczekuję od Pana odpowiedzi na piśmie, w terminie **30 dni** od dnia otrzymania niniejszego wystąpienia.

**WOJEWODA PODKARPACKI**

**(-)**

**Ewa Leniart**

(Podpisane bezpiecznym podpisem elektronicznym)

1. W oparciu o zatwierdzony w dniu 21 grudnia 2020 r. „Plan zewnętrznej działalności kontrolnej Podkarpackiego Urzędu Wojewódzkiego w Rzeszowie na 2021 rok”. [↑](#footnote-ref-1)
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. [↑](#footnote-ref-2)