

**WOJEWODA PODKARPACKI**

ul. Grunwaldzka 15

35-959 Rzeszów

OA-IV.431.3.2022 Rzeszów, 2022-12-08

**Pan**

**Wilhelm Woźniak**

**Wójt Gminy Krasne**

Na podstawie art. 46 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, w związku ze zrealizowaną w dniach 12 i 18 maj 2022 r. u Wójta Gminy Krasne (Urząd Gminy Krasne, Krasne 121, 36-007 Krasne) 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 07.09.2022 r., znak OA-IV.431.3.2022) udzielonych przez Wojewodę Podkarpackiego.

Ustalenia kontrolne dokonane zostały w oparciu o stan faktyczny istniejący od 1 stycznia 2021 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 Gminy Krasne 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 Wójta Gminy Krasne”[[2]](#footnote-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 Gminy Krasne pełnił Wójt: Pan Wilhelm Woźniak.

Funkcję Inspektora Ochrony Danych (IOD) pełnił Pan Daniel Panek, powołany na podstawie Zarządzenia NR 0050.43.2017 Wójta Gminy Krasne z dnia 25.05.2018 r. w sprawie określenia zasad bezpieczeństwa danych osobowych w Urzędzie Gminy Krasne.

Jest to wykonawca zewnętrzny świadczący usługę w ramach zawartej umowy.

Wsparcie informatyczne zapewnione było przez pracowników Urzędu Gminy. Pod ich opieką znajdowały się: środowiska sprzętowo-programowe, sieć lokalna i serwerownia, systemy i aplikacje centralne oraz własne, usprawniające pracę pracownikom Urzędu Gminy Krasne.

Funkcję Administratora Systemów Informatycznych (ASI) pełnił wyznaczony informatyk na podstawie Zarządzenia NR 0050.119.2018 Wójta Gminy Krasne z dnia 23.10.2018 r. w sprawie wdrożenia systemu zarządzania bezpieczeństwem informacji w Urzędzie Gminy Krasne oraz w jednostkach organizacyjnych Gminy Krasne.

W okresie objętym kontrolą w Urzędzie Gminy Krasne funkcjonowały systemy teleinformatyczne własne - zakupione przez urząd oraz 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 Gminy Krasne 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. Korespondencja odbierana była bezpośrednio w ePUAP.

Na stronie głównej kontrolowanej jednostki znajdowała się informacja o adresie **elektronicznej skrzynki podawczej**.

* 1. Współpraca systemów teleinformatycznych z innymi systemami

Pracownicy Urzędu Gminy Krasne 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. Obieg dokumentów

W Urzędzie Gminy Krasne funkcjonował system Proton umożliwiający zarządzanie dokumentami i wykonywanie czynności kancelaryjnych. Był to system pomocniczy w sposobie dokumentowania przebiegu załatwiania spraw.

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 zarządzania 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 System Zarządzania Bezpieczeństwem Informacji (SZBI) na podstawie Zarządzenia NR 0050.119.2018 Wójta Gminy Krasne z dnia 23.10.2018 r. w sprawie wdrożenia systemu zarządzania bezpieczeństwem informacji w Urzędzie Gminy Krasne oraz w jednostkach organizacyjnych Gminy Krasne.

Zostały równocześnie ustanowione dokumenty pełniący kluczową rolę w zakresie ochrony informacji i danych osobowych, były to:

* Polityka Bezpieczeństwa Informacji wprowadzona Zarządzeniem NR 0050.119.2018 Wójta Gminy Krasne z dnia 23.10.2018 r. w sprawie wdrożenia systemu zarządzania bezpieczeństwem informacji w Urzędzie Gminy Krasne oraz w jednostkach organizacyjnych Gminy Krasne wraz z załącznikami:
* Polityka zarządzania zasobami ludzkimi (Załącznik numer 1)
* Polityka zarządzania kontami dostępowymi (Załącznik numer 2)
* Regulamin zarządzania hasłami dostępu (Załącznik numer 3)
* Regulamin ochrony przed złośliwym oprogramowaniem (Załącznik numer 4)
* Regulamin wykorzystania komunikacji elektronicznej (Załącznik numer 5)
* Regulamin pracy z siecią lokalną (Załącznik numer 6)
* Regulamin wykorzystania sieci Internet (Załącznik numer 7)
* Regulamin wykorzystania dostępu zdalnego (Załącznik numer 8)
* Regulamin wykorzystania urządzeń mobilnych (Załącznik numer 9)
* Regulamin dostępu do wydzielonych pomieszczeń (Załącznik numer 10)
* Polityka archiwizacji informacji (Załącznik numer 11);
* Instrukcja Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Krasne stanowiąca Załącznik Nr 1 do Zarządzenia Nr 0050.119.2018 Wójta Gminy Krasne z dnia 23 października 2018 r.;
* Polityka Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Krasne stanowiąca Załącznik Nr 1 do Zarządzenia Nr 0050.43.2018 Wójta Gminy Krasne z dnia 25 maja 2018 r.;
* Instrukcja zarządzania zdarzeniami, mającymi negatywny wpływ na cyberbezpieczeństwo stanowiąca załącznik nr 1 do Zarządzenie nr 120.20.2022 r. Wójta Gminy Krasne z dnia 02.08.2022 r. w sprawie wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz wprowadzenia instrukcji zarządzania zdarzeniami, mającymi negatywny wpływ na cyberbezpieczeństwo.
  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 Gminy Krasne wprowadzone zostało Zarządzanie Ryzykiem Danych Osobowych (Rozdział XIII Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Krasne).

Plan postępowania z ryzykiem, jego ocena, decyzja władz Urzędu oraz monitorowanie realizacji planu dokumentowane są zgodnie Planem Postępowania z Ryzykiem będącego załącznikiem numer 8 do Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Krasne.

Poza planem postępowania z ryzykiem na potrzeby danych osobowych kontrolującym nie przedstawiono pozostałych analiz.

W wyniku zaistniałego incydentu, który zbiegł się z terminem kontroli w urzędzie została przeprowadzona ponowna analiza ryzyka dla przypadku objętego zdarzeniem, zgodnie z procedurą Zarządzania Ryzykiem Danych Osobowych.

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.

* 1. 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, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku.

Regulacje wewnętrzne nie zawierały wprost zapisów dotyczących sposobu zarządzania sprzętem informatycznym i oprogramowaniem (w tym licencjami na oprogramowanie) oraz wymogów co do funkcjonowania rejestru zasobów teleinformatycznych.

Regulamin pracy z siecią lokalną Urzędu Gminy Krasne zawierał zapisy, według których ASI jest zobowiązany do ewidencjonowania stacji roboczych w zarządzanej przez niego sieci. W Regulaminie wykorzystania urządzeń mobilnych Urzędu Gminy Krasne w ramach zasad dotyczących sposobu zarządzania sprzętem informatycznym i oprogramowaniem na urządzeniach mobilnych oddanych do czasowej dyspozycji użytkownika „zezwala się wykorzystywać wyłącznie oprogramowanie wpisane do Rejestru oprogramowania dopuszczonego do użytku oraz wpisanego do Karty ewidencyjnej komputera”. Karta ewidencyjna komputera to dokument zawierający pełny wykaz sprzętu i oprogramowania stacji roboczej.

Ewidencja poszczególnych podzespołów oraz oprogramowania prowadzona była przez informatyków przy pomocy arkusza kalkulacyjnego.

* 1. 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 badanym okresie zarządzanie uprawnieniami dostępu do przetwarzania danych w Urzędzie Gminy regulowały: Polityka zarządzania kontami dostępowymi, będąca Załącznikiem numer 2 do Polityki Bezpieczeństwa Informacji Urzędu Gminy Krasne, Regulamin zarządzania hasłami dostępu (Załącznik numer 3 do Polityki Bezpieczeństwa Informacji) oraz Polityka Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Krasne.

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.

Uprawnienia w systemie informatycznym nadawane były przez Administratora Systemu Informatycznego na podstawie Upoważnienia do przetwarzania danych osobowych.

Dostęp do zasobów informatycznych zależny był od zakresu obowiązków.

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 nadania, zmiany i odbioru uprawnień dla użytkownika w systemach informatycznych informacja przekazywana była ustnie, pomimo powołania się w dokumentach na wprowadzenie wzoru wniosku o konto dostępowe (Załącznik 1 do Polityki zarządzania kontami dostępowymi).

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, taka jak: Polityka zarządzania zasobami ludzkimi (Załącznik numer 1 do Polityki Bezpieczeństwa Informacji Urzędu Gminy Krasne) szczegółowo regulowała zakres podnoszenia świadomości pracowników poprzez: podejmowanie działań przed zatrudnieniem oraz w trakcie zatrudnienia, a także z pracownikami firm zewnętrznych. W przypadku osób zatrudnionych konieczne było podpisanie oświadczenia określającego role i obowiązki w zakresie bezpieczeństwa informacji.

Wszyscy pracownicy mający dostęp do informacji powinni raz w roku przechodzić szkolenie z zakresu bezpieczeństwa informacji, za które odpowiadał Inspektor Ochrony Danych (IOD). IOD w formie mailowej przekazywał na bieżąco pracownikom urzędu informacje dotyczące tematów z bezpieczeństwa informatycznego oraz współczesnych zagrożeń.

* 1. 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.

Został ustanowiony Regulamin wykorzystania dostępu zdalnego (Załącznik numer 8 do Polityki Bezpieczeństwa Informacji Urzędu Gminy Krasne), który określał szczegółowe zasady takiej pracy poprzez mechanizm VPN.

W innym dokumencie Regulamin wykorzystania urządzeń mobilnych (Załącznik numer 9 Polityki Bezpieczeństwa Informacji Urzędu Gminy Krasne) wskazano, że na urządzeniach mobilnych oddanych do czasowej dyspozycji użytkownika obowiązują te same wymagania bezpieczeństwa jak na urządzeniach stacjonarnych. Celowość zastosowania dodatkowych środków bezpieczeństwa jest określana przez ASI.

Według Regulaminu urządzenia mobilne i nośniki informacji są oddawane do dyspozycji użytkowników, na wniosek kierownika komórki organizacyjnej. Ta procedura przekazania użytkownikowi urządzeń mobilnych lub nośników informacji nie do końca przebiegała zgodnie z zapisami w Regulaminie.

Pracownicy wynosili przenośne urządzenia poza siedzibę jednostki, jednak nie były one szyfrowane (laptopy, pendrive).

* 1. 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 ogólnie określono zasady współpracy z podwykonawcami w zakresie przetwarzania informacji i serwisu autorskiego. Załącznik 1 do Polityki zarządzania zasobami ludzkimi w Urzędzie Gminy Krasne określał zalecane elementy umowy o poufności, dotyczące m.in. zachowania poufności i nieujawniania informacji przez pracowników firm zewnętrznych. Niemniej w umowach serwisowych z firmami trzecimi nie zawsze były zawarte te wymagania (np. z firmą Clanet), jak i nie było określonego SLA (Service Level Agreement), czyli gwarantowanego poziomu świadczenia usług oraz czas i sposób reakcji na zgłaszane problemy.

* 1. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Zasady postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych zostały określone w Polityce Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Krasne (Rozdział XV), a w przypadku pozostałych incydentów i naruszeń – w Instrukcji zarządzania zdarzeniami, mającymi negatywny wpływ na cyberbezpieczeństwo (tzw. incydentami).

W miesiącu październik b.r. w urzędzie miał miejsce incydent, który został zgłoszony do Urzędu Ochrony Danych Osobowych w dniu 04.10.2022 r. Zdarzenie polegało na przejęciu usługi skrzynki pocztowej [kontakt@gminakrasne.pl](mailto:kontakt@gminakrasne.pl), administrowanej przez pracowników urzędu, i wykorzystaniu jej przez „boota” do rozsyłania spamu, w związku z tym podlegał pod kategorię „Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń”. Incydent został zgłoszony również do CSIRT NASK.

* 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 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 był wykonywany w 2020 roku przez firmę zewnętrzną. Sprawozdanie „Raport z Audytu Zgodności z Rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności oraz z ogólnym Rozporządzeniem o Ochronie Danych (2016/679)” zawierał opis niezgodności audytowanego obszaru a także obszarów wymagających poprawy.

W 2022 roku na potrzeby projektu „Cyfrowa Gmina” było wykonane sprawdzenie związane z przeprowadzeniem diagnozy cyberbezpieczeństwa.

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.

Zakres wykonywania kopii zapasowych był określony w wewnętrznej dokumentacji: Polityka archiwizacji informacji Urzędu Gminy Krasne (Załącznik numer 11 do Polityki Bezpieczeństwa Informacji Urzędu Gminy Krasne). Zapisy odbiegały od rzeczywistego sposobu wykonywania kopii zapasowych dlatego niezbędne jest zaktualizowanie dokumentacji w tym zakresie.

Wykonywanie odtworzenia systemów z kopii zapasowych występowało w razie potrzeby.

* 1. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

W Urzędzie Gminy Krasne proces administrowania technicznego i monitorowania określonych obszarów systemów, aplikacji, danych, infrastruktury sieciowej i stacji roboczych był wykonywany przez zatrudnionych 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 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 wprowadzonej Zarządzeniem NR 0050.119.2018 Wójta Gminy Krasne z dnia 23.10.2018 r. w sprawie wdrożenia systemu zarządzania bezpieczeństwem informacji w Urzędzie Gminy Krasne oraz w jednostkach organizacyjnych Gminy Krasne wraz z załącznikami, a także w Instrukcji Bezpieczeństwa Danych Osobowych i Polityce Bezpieczeństwa Danych Osobowych.

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 Gminy Krasne posiadał lokalizację w jednym budynku.

Obiekt był objęty systemem monitoringu (na zewnątrz) oraz był objęty systemem alarmowym ochrony fizycznej, natomiast system zadymienia obejmował tylko serwerownię.

Klucze do budynku były zabezpieczone i przechowywane przez pracowników uprawnionych do otwierania budynku oraz rozkodowywania systemu alarmowego.

W tym samym budynku miał również siedzibę Gminny Ośrodek Pomocy Społecznej.

Urząd Gminy dysponował jedną serwerownią, która umieszczona była w pomieszczeniu zaadaptowanym na ten cel. Do tego pomieszczenie możliwe było wejście tylko przez pokój informatyków. Dostęp do serwerowni był ograniczony i możliwy jedynie dla upoważnionych pracowników urzędu. Ważnym elementem ochrony było asystowanie osobom wchodzącym i wykonującym prace serwisowe.

Serwerownia posiadała podłogę techniczną oraz wzmocnione i ognioodporne drzwi. Występowało monitorowanie parametrów środowiskowych w serwerowni (np. temperatury, wilgotności) oraz był zainstalowany system alarmowy. Pomieszczenie było klimatyzowane przez dwa urządzenia.

Bazy danych z kopiami były umieszczone w tym samym miejscu.

W serwerowni znajdował się UPS, który podtrzymywał pracę serwera i urządzeń sieciowych. Strategiczne stanowiska komputerowe także wyposażone były w urządzenia UPS podtrzymujące pracę komputera podczas zaników prądu.

Podstawowe urządzenie infrastruktury informatycznej posiadały zabezpieczenie przed awariami prądu, jednak warto rozważyć dodatkowe zabezpieczenie na wypadek awarii.

W ramach zabezpieczenia dostępu stosowana była zapora sieciowa typu firewall z aktualną licencją.

Do połączeń internetowych było wykorzystywane jedno łącze główne, brakowało drugiego łącza jako zapasowego.

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

W pomieszczeniu, w okolicy urządzeń sieciowych, nie były przechowywane materiały łatwopalne.

Sprzęt komputerowy był ubezpieczony.

W urzędzie była wykorzystywana sieć bezprzewodowa. Dostęp do niej możliwy był po zalogowaniu.

* 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.

Była wdrożona usługa katalogowa Active Directory, która pozwalała na zarządzanie tożsamościami i relacjami w sieci, przez co umożliwiała 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 Regulaminie pracy z siecią lokalną Urzędu Gminy Krasne (Załącznik numer 6 do Polityki bezpieczeństwa Informacji Urzędu Gminy Krasne) zostały określone zasady monitorowania zdarzeń sieciowych w sieci LAN/VLAN. Wykaz zdarzeń, które podlegały protokołowaniu określał ASI. Uzyskane w ten sposób elektroniczne dzienniki zdarzeń były używane do analizy pracy sieci, a także mogły służyć jako dowód bezprawnych działań użytkowników.

Pozostałe regulacje wewnętrzne nie określały konieczności zasady rozliczalności działań wykonywanych w systemach informatycznych.

Sprawdzane systemy informatyczne użytkowe miały udokumentowaną rozliczalność.

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 i strony www poprzez walidator dostępny pod adresem: https://validator.utilitia.pl/ badane strony uzyskały wynik 5,5 pkt na 10 możliwych.

Ww. ustalenia, w tym ocena kontrolowanej działalności, zostały udokumentowane w aktach kontroli, na które składają się również przesyłki drogą elektroniczną ePUAP.

Przy czym do ww. ustaleń kontrolnych (przekazanych do wiadomości w dniu 10 listopada 2022 r.) przysługiwało Panu, na podstawie ww. ustawy o kontroli w administracji rządowej, prawo zgłoszenia umotywowanych pisemnych zastrzeżeń, z których Pan nie skorzystał. W ramach ww. uprawnienia nie skorzystał Pan również z prawa skierowania wniosku o przedłużenie terminu do złożenia zastrzeżeń.

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. Nośniki kopii zapasowych przechowywać w innym pomieszczeniu niż serwerownia.
2. Zgodnie z wymogami § 20 ust. 1-3 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 niezbędne jest monitorowanie, przeglądanie i doskonalenie pełnego systemu bezpieczeństwa informacji wraz ze sprawdzeniem i ujednoliceniem dokumentacji.
3. Przeprowadzić okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji oraz utworzyć plan zachowania ciągłości działania.
4. Wdrożyć podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, takie jak: ewidencja, zabezpieczenie i szyfrowanie urządzeń przenośnych.
5. Wdrożyć i ujednolicić zasady nadawania uprawnień do pracy w systemach informatycznych.

O sposobie wykonania powyższych wniosków pokontrolnych, bądź działaniach podjętych w celu ich realizacji, oczekuję od Pana odpowiedzi na piśmie, w terminie **21dni** od daty otrzymania niniejszego wystąpienia.

**WOJEWODA PODKARPACKI**

**(-)**

**Ewa Leniart**

(Podpisane bezpiecznym podpisem elektronicznym)

1. W oparciu o zatwierdzony w dniu 22 grudnia 2021 r. „Plan zewnętrznej działalności kontrolnej Podkarpackiego Urzędu Wojewódzkiego w Rzeszowie na 2022 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)