WOJEWODA ŚWIĘTOKRZYSKI

Kielce, 03.02.2016

Znak sprawy: OK.V.431.2.2015

Pan
Szczepan Skorupski
Wójt Gminy
Zagnańsk

WYSTĄPIENIE POKONTROLNE

Zakres kontroli: Przedmiotem kontroli jest działanie systemów teleinformatycznych używanych do realizacji zadań publicznych zgodnie z Rozporządzeniem 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 (Dz. U. z dnia 16 maja 2012 r. poz. 526) wydanym na podstawie ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64 poz. 565, z późn. zm.).

Okres objęty kontrolą: Od 01.01.2014 r. do dnia kontroli.

Zespół kontrolerów:

- Marek Rak, Informatyk Wojewódzki – Kierownik Oddziału ds. Informatyki w Wydziale Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego - Przewodniczący Zespołu Kontrolnego – upoważnienie do kontroli nr 1013/2015 z dnia 30 listopada 2015r.
- Maciej Terek Główny Specjalista Oddziału ds. Informatyki w Wydziale Organizacji i Kard Świętokrzyskiego Urzędu Wojewódzkiego - Członek Zespołu Kontrolnego – upoważnienie do kontroli nr 1012/2015 z dnia 25 listopada 2015r.

Termin przeprowadzenia kontroli: Od 7 do 9 grudnia 2015 r.

Kierownik jednostki kontrolowanej: Kierownikiem Jednostki kontrolowanej jest Pan Szczepan Skorupski wybrany w wyborach bezpośrednich w dniu 5 grudnia 2010r.

Podstawa prawna do przeprowadzenia kontroli:	Kontrolę przeprowadzono na podstawie art. 28 ust. 1 pkt. 2 ustawy *o Wojewodzie i administracji rządowej w województwie*[1] oraz art. 6 ust. 4 pkt. 2 ustawy *o Kontroli w administracji rządowej*[2]. Projekt wystąpienia pokontrolnego przekazano zgodnie z przepisami art. 38 ustawy *o Kontroli w administracji rządowej*.
Ocena stanu faktycznego wynikająca z ustaleń kontroli:	Pozytywnie z nieprawidłowościami ocenia się działanie systemów teleinformatycznych wykorzystywanych w Urzędzie Gminy w Zagnańsku do realizacji zadań zleconych z zakresu administracji rządowej w latach 2014-2015. Ocena ogólna ustalona została w oparciu kryteria zawarte w programie kontroli zatwierdzonym przez Dyrektora Wydziału Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach.

W toku przeprowadzonej kontroli ustalono, że:

Projektowanie, wdrażanie i eksploatacja systemu teleinformatycznego:	Kontrolą objęto dwa systemy informatyczne MikroPESEL (system wspomagający procedury wyborcze) oraz system centralny Źródło (wykorzystywany w USC).
Ocena cząstkowa:	Pozytywnie ocenia się działalność Jednostki w zakresie wdrożenia i eksploatacji systemu.
Zarządzanie usługami realizowanymi przez systemy teleinformatyczne	Urząd Gminy w Zagnańsku nie zarządza systemami informatycznymi w modelu usługowym, w związku z powyższym obszar ten nie został poddany ocenie kontrolerów.
Ocena cząstkowa:	W zawiązku z brakiem realizacji usługi nie sformułowano w tym obszarze oceny cząstkowej .
System zarządzania bezpieczeństwem informacji:	Zarządzeniem Wójta Nr 172/2014 z dnia 29 grudnia 2014 roku w jednostce wdrożono System Zarządzania Bezpieczeństwem Informacji. Jednostka nie ma zatrudnionego audytora wewnętrznego, korzysta z usług audytora zewnętrznego. W okresie objętym kontrolą tj. lata 2014-2015 nie został przeprowadzony audyt wewnętrzny w zakresie bezpieczeństwa informacji co jest niezgodne z § 20 ust.2

[1] Ustawa z dnia 23 stycznia 2009 r., o *Wojewodzie i administracji rządowej w województwie* (Dz. U. nr 31, poz. 206 z późn. zm.).

[2] Ustawa z dnia 15 lipca 2011 r. *o Kontroli w administracji rządowej* (Dz. U. Nr 185, poz. 1092).

[3] Rozporządzenie 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 (Dz. U. z dnia 16 maja 2012 r. poz. 526) wydanym na podstawie ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64 poz. 565, z późn. zm.)

pkt. 14 z wyżej wymienionego rozporządzenia[3]. Jedynie w aneksie do planu audytu na rok 2015 wprowadzono zadanie audytowe pt.: „Ocena realizacji zadań w zakresie zarządzania aktywami informatycznymi”.

Wójt Gminy powołał a następnie zgłosił do GIODO, Administratora Bezpieczeństwa Informacji w osobie Pani Jolanty Borkowskiej-Słoń. Kontrolujący stwierdzili, jednak że Administrator Bezpieczeństwa Informacji w Urzędzie Gminy nie złożył oświadczenia o zapoznaniu się z Polityką Bezpieczeństwa Informacji co jest niezgodne z § 20 ust. pkt. 4 wspomnianego wyżej rozporządzenia[3]. Takiego oświadczenia również nie złożył Wójt Gminy Zagnańsk Pan Szczepan Skorupski.

Czynności kontrolne wykazały także, że Urząd Gminy nie posiada dokumentów świadczących o przeprowadzaniu okresowej samooceny funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji jak i o przeprowadzeniu okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, co zalecono w § 20 ust.1 i ust.3 w/w rozporządzenia[3].

Kontrolujący ustalili, że Urząd Gminy zapewniał szkolenia zewnętrzne i wewnętrzne dla pracowników zaangażowanych w proces przetwarzania informacji w okresie poddanym kontroli.

Kontrolowana jednostka prawidłowo zapewnia ochronę przetwarzanych informacji przed ich kradzieżą, awarią nieuprawnionym dostępem stosując następujące zabezpieczenia :

- monitoring wizyjny,
- alarm przeciwwłamaniowy, przeciwpożarowy,
- zabezpieczenia wejść wybranych pomieszczeń drzwiami antywłamaniowymi pokój nr 7 (serwerownia),
- system monitorowania temperatury, okna zabezpieczone dodatkowym zamkiem na klucz w pomieszczeniu nr 7,
- stosowanie szaf na klucz do przechowywania dokumentów i nośników danych,
- systemów awaryjnego zasilania (UPS),
- Active Directory do kontroli dostępu do danych,
- urządzenia UTM do zabezpieczeni sieci Urzędu Gminy,
- regularne sporządzanie kopii zapasowych danych przechowywanych na serwerach.

Niezależnie od powyższego Kontrolujący stwierdzili rozbieżności pomiędzy zapisami Polityki Bezpieczeństwa Informacji dotyczącymi zabezpieczenia systemów teleinformatycznych hasłami (w PBI długość haseł została określona na minimum 8 znaków, hasło powinno składać się z trzech rodzajów znaków) a rzeczywistymi ustawieniami

[3] Rozporządzenie 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 (Dz. U. z dnia 16 maja 2012 r. poz. 526) wydanym na podstawie ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64 poz. 565, z późn. zm.)

w systemie operacyjnym serwera, bowiem długość haseł na działającym serwerze została zdefiniowana na 5 znaków, a opcja dotycząca złożoności haseł została wyłączona.

W Polityce Bezpieczeństwa Informacji Urzędu Gminy są określone zasady zapewniające minimalizację występowania ryzyka kradzieży.

Urząd Gminy w Zagnańsku nie wykorzystuje urządzeń mobilnych do wykonywania obowiązków służbowych poza siedzibą Urzędu. W „Systemie Zarządzania Bezpieczeństwem Informacji" w punkcie 15 (Polityka dostępu do systemów informatycznych) podpunkt 15.2 jest napisane iż „dostęp zdalny do systemów informatycznych jest stosowany w przypadku dostępu m.in. serwisowego, inicjowanego przez pracowników Urzędu".

Kontrolowana jednostka zapewnia aktualizację oprogramowania na bieżąco. W umowach serwisowych firm współpracujących z Urzędem Gminy są zapisy zapewniające aktualizację oprogramowania. Ryzyko wynikające z wykorzystania opublikowanych podatności technicznych systemów jest minimalizowane. W dokumencie opisującym System Zarządzania Bezpieczeństwem Informacji w rozdziale 23.1 w punkcie 3 jest mowa o tym iż osoby nie będące pracownikami Urzędu Gminy przed uzyskaniem dostępu do systemów informatycznych urzędu muszą podpisać zobowiązanie do przestrzegania zasad bezpieczeństwa oraz zachowania poufności (załącznik nr 1). Żadna z osób reprezentujących firmy współpracujące tj. CANEA, mikroPESEL, FORTES oraz audytor zewnętrzny nie podpisały wyżej wspomnianego załącznika nr 1.

W Urzędzie Gminy są stosowane mechanizmy kryptograficzne w sposób adekwatny do zagrożeń i wymogów prawa. Bezpieczeństwo plików systemowych zostało również zapewnione zgodnie zapisami Polityki Bezpieczeństwa Informacji.

W Polityce Bezpieczeństwa Informacji Urzędu Gminy są opisane procedury postępowania na wypadek zaistnienia incydentu. Ze względu na brak zarejestrowanych incydentów kontrolerzy nie są w stanie ocenić funkcjonowania związanych z tym procedur.

-

Ocena cząstkowa: Pozytywnie z nieprawidłowościami ocenia się działalność jednostki w zakresie systemu zarządzania bezpieczeństwem informacji.

Rozliczalność: W kontrolowanej jednostce rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów. System gromadzenia, przechowywania i analizy logów działa dopiero od początku listopada 2015 i za taki okres logi są gromadzone, przechowywane i analizowane przy użyciu specjalistycznego oprogramowania.

-

W jednostce kontrolowanej kopie dzienników są systematycznie składowane na karcie SD, natomiast kopie zapasowe danych i kopie zapasowe systemów są przechowywane na przenośnym dysku zewnętrznym poza pomieszczeniem serwerowni w oddzielnym pomieszczeniu (pokój numer 3) zabezpieczonym zwykłymi drzwiami z zamkiem, w zwykłej szafie biurowej zabezpieczonej zamkiem. Kontrolerzy stwierdzili niezgodność co do miejsca przechowywania kopii zapasowych, która w dokumencie pt. „System Zarządzania Bezpieczeństwem Informacji" w punkcie 12 podpunkt l) jest określona jako „przechowywanie kopii zapasowych w bezpiecznej lokalizacji (inny budynek Urzędu)" a w rzeczywistości są przechowywane w tej samej lokalizacji w pokoju numer 3. Nie stwierdzono prowadzenia dzienników systemowych na nośniku papierowym.

Nie stwierdzono prowadzenia dzienników systemowych na nośniku papierowym.

Zakresy uprawnień pracowników w kontrolowanych systemach informatycznych (Źródło i mikroPESEL) odpowiadały uprawnieniom opisanym w dokumencie pt. „Ewidencja osób upoważnionych do przetwarzania danych osobowych".

Inwentaryzacja sprzętu i oprogramowania prowadzona jest na bieżąco w systemie informatycznym i obejmuje jedynie informacje o miejscu rozlokowania sprzętu. Natomiast pozostałe niezbędne informacje np. o wersji systemu operacyjnego, zainstalowanym oprogramowaniu biurowym, antywirusowym czy chociażby podstawowe informacje o samym sprzęcie komputerowym nie są gromadzone i nie znajdują się na przedłożonym wydruku z systemu komputerowego.

Ocena cząstkowa: Pozytywnie z nieprawidłowościami ocenia się działalność Jednostki w zakresie rozliczalności systemów teleinformatycznych.

Zalecenia:

W związku z powyższym uprzejmie proszę Wójta o rozważenie możliwości podjęcia następujących działań w celu niedopuszczenia do powstania podobnych nieprawidłowości w przyszłej działalności podległej Panu jednostce. W szczególności należy zadbać o :

1. zapewnienie zgodności zastosowanych zabezpieczeń z przepisami wewnętrznymi regulującymi zasady funkcjonowania Systemu Zarządzania Bezpieczeństwem (długości i złożoności haseł, lokalizacja kopii zapasowych),
2. coroczne szacowanie i analizę ryzyka posiadanych systemów teleinformatycznych zgodnie z przyjętą w jednostce metodą,
3. zapewnienie raz do roku audytu w zakresie bezpieczeństwa informacji,
4. aktualizacje dokumentów i wykazów dotyczących zobowiązań pracowników firm współpracujących z urzędem gminy

do przestrzegania zasad bezpieczeństwa informacji oraz zachowania poufności. (Załącznik nr 1 do dokumentu opisującego system zarządzania bezpieczeństwem informacji).

Jednocześnie proszę poinformować Wojewodę Świętokrzyskiego, w terminie 30 dni od daty otrzymania niniejszego wystąpienia pokontrolnego o sposobie wykorzystania wyżej wymienionych uwag i wniosków oraz zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań. Ponadto informuj, iż zgodnie z art. 48 ustawy z dnia 15 lipca 2011 roku *o Kontroli w administracji rządowej* od niniejszego wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Z upoważnienia
Wojewody Świętokrzyskiego

Edyta Suchoń
Dyrektor Wydziału
Wydział Organizacji i Kadr