ORP.1720.1.2016

ORP
01.07.2016

3 0 -06- 2016
6359

Sprawozdanie z zadania zapewniającego
Nr 6/2016

***I. Temat zadania**: Audyt polityki bezpieczeństwa danych w jednostkach organizacyjnych Gminy Żmigród wskazanych w upoważnieniu Burmistrza Gminy Żmigród.*

II. Oznaczenie zadania: *6/2016*

III. Data rozpoczęcia zadania zapewniającego: 12.05.2016

IV. Data sporządzenia sprawozdania: 28.06.2016

V. Jednostki Gminy Żmigród, w których przeprowadzono zadanie:

- *Zespół Szkół Dwujęzycznych w Żmigrodzie,*
- *Szkoła Podstawowa w Żmigrodzie,*
- *Miejski Zakład Gospodarki Komunalnej w Żmigrodzie,*

Środowiskowy Dom Samopomocy w Żmigrodzie

VI. Imię i nazwisko audytora: *Mariusz Więch*

VII. Upoważnienie do przeprowadzenia audytu: *Burmistrza Gminy Żmigród*

VIII. Cel zadania zapewniającego: *Ocena ustanowienia kontroli zarządczej w ramach Grupy Standardów C Mechanizmy kontroli, a w szczególności w zakresie standardu ochrona zasobów oraz standardu mechanizmy kontroli dotyczące systemów informatycznych, w kontekście warunków wynikających z § 20 ust. 2 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 (Dz. U. 2012, poz. 526 zmiany Dz.U. z 2014 r. poz. Dz.U. 2014 r. poz. 1671).*

IX. Przedmiotowy zakres zadania zapewniającego:

Zakres przedmiotowy zadania audytowego objął obszar wskazany w § 20 ust. 2 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 (Dz. U. 2012, poz. 526 zmiany Dz.U. z 2014 r. poz. Dz.U. 2014 r. poz. 1671), gdzie wskazuje się, iż zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu

publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

- Zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia,
- Utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację,
- Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowane są działania minimalizujące to ryzyko, stosownie do wyników przeprowadzonej analizy,
- Przeprowadzanie działań zapewniających, 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 mających na celu zapewnienie bezpieczeństwa informacji,
- Zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
- Zagrożenia bezpieczeństwa informacji,
- Skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
- Stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich,
- Zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, niuprawnionym dostępem, uszkodzeniami lub zakłóceniami przez:
- monitorowanie dostępu do informacji,
- czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
- zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji
- Ustanowienie podstawowych zasad gwarantujących bezpieczna pracę przy przetwarzaniu mobilnym i pracy na odległość,
- Zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie modyfikację, usuniecie lub zniszczenie,
- Zawieranie w umowach serwisowych (dotyczących sprzętu lub zakupionego oprogramowania), podpisanych ze stronami trzecimi, zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
- Ustalenie zasad postępowania z informacjami, zapewniającymi minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych,
- Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
  - dbałości o aktualizację oprogramowania,

- minimalizowaniu ryzyka utraty informacji w wyniku awarii,
- ochronie przed błędami, utratą nieuprawnioną modyfikacją,
- stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa,
- zapewnieniu bezpieczeństwa plików systemowych,
- redukcji ryzyka wynikającego z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
- niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
- kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

- Bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

X. Podjęte czynności i zastosowane techniki przeprowadzenia zadania.

1. *Przegląd sprawozdań z poprzednich audytów,*
2. *Zapoznanie się z celami jednostki audytowanej,*
3. *Zapoznanie się z systemem kontroli zarządczej,*
4. *Typowanie,*
5. *Uzyskiwanie informacji i wyjaśnień od pracowników,*
6. *Formularz listy weryfikacyjnej,*
7. *Porównanie określonych zbiorów danych,*
8. *Wstępny przegląd,*
9. *Analiza dokumentacji.*

XI. Termin, w którym przeprowadzono zadanie: 12.05-28.06.2016 r.

XII. Zwięzły opis działań jednostki w obszarze objętym zadaniem:

Przepis § 20 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 (Dz. U. 2012, poz. 526 zmiany Dz.U. z 2014 r. poz. Dz.U. 2014 r. poz. 1671) określa ciążące na kierownictwie podmiotu publicznego obowiązki związane z systemem zarządzania bezpieczeństwem informacji. Wymienione w § 20 ust. 1 i 2 rozporządzenia obowiązki, stanowią podstawowe kryterium oceny ustaleń stanu faktycznego.

W podmiotach, w których system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, zgodnie z § 20 ust. 3 wymagania określone w rozporządzeniu uznaje się za spełnione.

Polityka bezpieczeństwa informacji jest zbiorem spójnych, precyzyjnych reguł i procedur, według których dana organizacja zarządza, chroni i dystrybuuje zasoby i systemy informacyjne oraz informatyczne.

Istotne jest, aby polityka bezpieczeństwa była dokumentem opracowanym w sposób pisemny, znanym (zrozumianym) oraz przestrzeganym przez pracowników organizacji korzystających z zasobów informatycznych. Polityka powinna precyzować zasoby i sposób ich ochrony, jak również powinna obejmować wskazanie możliwych rodzajów naruszenia bezpieczeństwa (jak np. utrata danych, nieautoryzowany dostęp), scenariusze postępowania w takich sytuacjach i działania, które pozwolą uniknąć powtórzenia się danego incydentu.

XIII. Ustalenia stanu faktycznego wraz ze sklasyfikowanymi wynikami ich oceny:

Podstawowym warunkiem oceny ustaleń stanu faktycznego w odniesieniu do kryterium adekwatności, było dostosowanie funkcjonowania jednostek organizacyjnych Gminy Żmigród w zakresie systemów zarządzania bezpieczeństwem informacji, do wymogów określonych w:

1. Rozporządzeniu 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. 2012, poz. 526 zmiany Dz.U. z 2014 r. poz. Dz.U. 2014 r. poz. 1671),
2. Komunikacie nr 23 Ministra Finansów z dnia 16.12.2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych, w szczególności: Standardu 13 (Ochrona zasobów) oraz Standardu 15 (Mechanizmy kontroli dotyczące systemów informatycznych).

Ponadto przedmiotowe zagadnienie zweryfikowane zostało w oparciu o przepisy:

I. Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2014 poz.1182, zm. Dz.U. z 2014 poz. 1662).

II. Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz.U. z 2014 r. poz.1934).

III. Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 105 r. poz.745).

IV. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11.12.2008 r. w sprawie wzoru zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r. nr 229, poz. 1536),

V. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024).

W audytowanych jednostkach nie wdrożono systemu zarządzania jakością bezpieczeństwem informacji według normy *PN-ISO/IEC 27001*.

Budynki posiadały ochronę fizyczną i zabezpieczenia dostępu do zbiorów. Dostęp do wydzielonych stref jest ograniczony. Zgodnie z § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024), jednostka winna posiadać dokumentację regulującą ochronę danych osobowych, na którą składają się: polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Z przeprowadzonego badania audytowego wynika, że jednostki audytowane posiadały wymaganą dokumentację, bowiem stosują niezbędne procedury chroniące dane osobowe.

XIV. Określenie oraz analiza przyczyn uchybień:

BRAK

XV. Wskazanie słabości kontroli zarządczej:

BRAK

XVI. Skutki lub ryzyka wynikające ze wskazanych słabości kontroli zarządczej:

BRAK

XVII. Zalecenia:

BRAK

XVIII. Opinia audytora wewnętrznego w sprawie adekwatności, skuteczności i efektywności kontroli zarządczej w obszarze ryzyka objętym zadaniem zapewniającym:

System kontroli zarządczej w obszarze ryzyka objętym zadaniem zapewniającym działa prawidłowo.

28.06.2016 r.

data

podpis audytora