Raport

z przeprowadzonego audytu przeglądowego działań w zakresie bezpieczeństwa przetwarzania informacji oraz zarządzania usługami IT w Starostwie Powiatowym w Kielcach

Warszawa, dnia 4 stycznia 2014 roku

INTEGRACJA • PRZEDSIĘBIORCZOŚĆ • EDUKACJA

KRS 0000175468, NIP 1181711922, REGON 015580537
02-784 Warszawa, ul. Janowskiego 22, tel. 0-667 157 666, e-mail: jacek.suwara@bezpieczenstwo.org

Warszawa, dnia 4 stycznia 2014 roku

Raport
z przeprowadzonego audytu przeglądowego działań Starostwa Powiatowego w Kielcach w zakresie bezpieczeństwa przetwarzania informacji oraz zarządzania usługami IT

Celem głównym audytu było potwierdzenie, że audytowana organizacja skutecznie podejmuje działania w zakresie ochrony informacji oraz tworzy podstawy do systemowego podejścia do ochrony i bezpieczeństwa informacji a tym samym spełnia warunki niezbędne do przedłużenia ważności Certyfikatu Bezpieczny Urząd Związku Powiatów Polskich.

Jako podstawę wymagań audytowych zgodnie z nowelizowanymi zasadami przyznawania Certyfikatu Bezpieczny Urząd Związku Powiatów Polskich zostały przyjęte wybrane elementy:

1) międzynarodowej normy ISO/IEC 27001:2005 (edycja polska wersja z 2007) „Technika informatyczna Techniki bezpieczeństwa Systemy zarządzania bezpieczeństwem informacji"
2) międzynarodowej normy ISO/IEC 20000-1 „Technika informatyczna. Zarządzanie usługami".

Audyt został przeprowadzony na wybranej próbie audytowej co oznacza, że nie wszystkie obszary audytowanej organizacji uczestniczyły w procesie audytu. Ponieważ Starostwo posiada ważny, certyfikowany system zarządzania bezpieczeństwem informacji audyt dotyczył wyłącznie obszarów związanych z prowadzeniem szkoleń dla nowych pracowników, wybranych elementów w zakresie zarządzania usługami IT i audytów wewnętrznych.

Audyt został przeprowadzony w dniu 23 grudnia 2013 roku przez audytora:
Krzysztof Wertejuk
Raport przygotował:
Krzysztof Wertejuk

Kolejny audyt przeglądowy powinien być przeprowadzony, zgodnie wytycznymi regulującymi przyznawanie i odnawianie Certyfikatu Bezpieczeństwa Związku Powiatów Polskich, nie później niż w ciągu roku od daty ostatniego audytu przeglądowego.

W ramach audytu odbyły się konsultacje z pracownikami wsparcia IT i na ich podstawie zostały sformułowane wnioski w zakresie zabezpieczeń systemów przetwarzania, przeprowadzania audytów w ramach tych systemów oraz zarządzania usługami informatycznymi.

Obserwacje dotyczące zabezpieczeń w audytowanym obszarze.

1. Starostwo posiada certyfikowany system w zakresie normy ISO/IEC 27001.
2. Starostwo posiada grupę bardzo dobrze przygotowanych pracowników wsparcia IT. Pracownicy ci maja kompletną i ugruntowaną wiedze z zakresu wymagań normy ISO/IEC 27001 oraz zasad audytowania systemów informatycznych.
3. Starostwo posiada 16 audytorów wewnętrznych którzy co najmniej raz w roku przeprowadzają audyty we wszystkich obszarach Organizacji.
4. W Starostwie istnieje sprawny system monitorowania ruchu sieciowego i zabezpieczeń.
5. Stosowany jest system nadzoru nad zasobami Ewida.
6. System separacji sieci wewnętrznej od sieci zewnętrznej daje duże możliwości ochrony.
7. Dokumentacja systemowa jest dobrze dostosowana do specyfiki Organizacji. Istnieją odpowiednie dokumenty np. Podręcznik Bezpieczeństwa Informacji.
8. Dokumentacja systemu bezpieczeństwa informacji jest zintegrowana z wymaganiami w zakresie prowadzenia dokumentacji dotyczącej ochrony danych osobowych.
9. Śledzone są incydenty bezpieczeństwa informacji i wyciągane są wnioski w zakresie doskonalenia systemu bezpieczeństwa informacji.
10. Starostwo przykłada dużą uwagę do właściwego przeszkolenia Pracowników w zakresie spełnienia wymagań normy ISO 27001 oraz wymagań ochrony informacji. Wszyscy nowo zatrudnieni pracownicy przechodzą stosowne szkolenia w zakresie ochrony informacji. Istnieje plan szkoleń. Szkolenia są przeprowadzane w zakresie wymagań normy ISO/IEC 27001 ale również w zakresie podnoszenia wiedzy Pracowników w zakresie sprawności korzystania z systemów i aplikacji.
11. Dla specjalistycznych aplikacji są podpisane umowy serwisowe na wsparcie oraz rozwój i utrzymanie aplikacji.
12. Zostało przeprowadzone szkolenie dla nowych pracowników i stażystów. Tematem szkolenia były ogólne zaganiania związane wymaganiami zawartymi w Roz. Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, ochroną

informacji, przepisami prawa w zakresie ochrony danych osobowych oraz przepisów dotyczących praw autorskich oraz praw pokrewnych ze szczególnym uwzględnieniem zasad legalnego wykorzystania plików multimedialnych na terenie i przy użyciu sprzętu należącego do Starostwa Powiatowego w Kielcach.

Obserwacje dotyczące możliwości poprawy.

Zasadne jest wprowadzenie następujących działań doskonalących systemy ISO/IEC 27001:2005 (edycja polska wersja z 2007) „Technika informatyczna Techniki bezpieczeństwa Systemy zarządzania bezpieczeństwem informacji" oraz normy ISO/IEC 20000-1 „Technika informatyczna. Zarządzanie usługami" :

1. Wprowadzenie oceny skuteczności szkoleń.
2. Przygotowanie szkoleń w formie e-learningu.
3. Przeprowadzanie szkoleń przez osoby merytoryczne (doświadczonych użytkowników – liderów odpowiednich aplikacji) a nie tylko pracowników wsparcia IT.
4. Ustalenie poziomów dostępnych zasobów w ramach systemów przetwarzania od których będzie uruchamiane raportowanie o przekroczeniu poziomu dostępności zasobów.
5. Konieczne jest uruchomienie wdrożenia system ISO/IEC 20000-1 „Technika informatyczna. Zarządzanie usługami". Jako pierwszy element wdrożenia sugeruje się uruchomienie systemu ticeket'owego wykorzystywanego przy zgłaszaniu usterek sprzętu informatycznego ale też zapewniającego rozliczalność usług IT. Zgodnie z wymaganiami normy oraz Roz. 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 do 12 kwietnia 2015 roku taki system powinien działać. W/w rozporządzenie oraz norma ISO/IEC 20000-1 stawia konkretne wymagania dla systemów zarządzania usługami IT. W celu systematyzowania podejścia do wdrożenia tego systemu zasadne jest podzielenie wdrożenia na następujące obszary zaproponowane jako kamienie milowe w nowej edycji wymagań Certyfikatu Bezpieczny Urząd ZPP:
   - ✓ opracowanie zakresu i głównych założeń systemu oraz polityki zarządzania usługami IT. Zakres i założenia powinny być zatwierdzone przez najwyższe kierownictwo,
   - ✓ udokumentowanie programu szkoleń, ścieżek rozwoju zawodowego oraz potwierdzenia odbytych szkoleń poprzez wykazanie się certyfikatami lub innymi zapisami potwierdzającymi ukończenie szkoleń przez osoby podejmujące decyzje w zakresie planowania budżetu IT, zarządzające obszarem IT, realizujące usługi IT,

- ✓ posiadanie i praktyczne stosowanie procedur planowania i wdrażania nowych lub zmienionych usług, implementacji mechanizmów i narzędzi zarządzania usługami IT oraz monitorowania, pomiarów i przeglądu skuteczności działania usług IT,
- ✓ posiadanie dokumentacji zawierającej takie elementy jak: katalog usług, zasady planowania zarządzania usługami, zasady zarządzania potencjałem wykonawczym, zasady kontroli jakości usług, zarządzania ciągłością i dostępnością usług, planowanie budżetu i rozliczanie usług IT, zarządzanie bezpieczeństwem informacji. Posiadanie narzędzi wspomagających proces dostarczania usług IT,
- ✓ posiadanie zdefiniowanych oraz zapisanych wymagań w zakresie procesów związków pomiędzy usługami IT i oczekiwaniami odbiorców z uwzględnieniem relacji z poddostawcami (przegląd usług, zarządzanie poddostawcami i zarządzanie kontraktami),
- ✓ posiadanie zasad i działających mechanizmów zarządzania incydentami i problemami w obszarze usług IT. Zasady te i mechanizmy powinny dawać gwarancje, że incydenty i problemy będą właściwie obsłużone,
- ✓ posiadanie procedur do procesów zarządzania konfiguracją, kontroli konfiguracji, sprawozdawczości statusu konfiguracji, raportów i audytu konfiguracji. Posiadanie zapisów z przebiegu tego procesu takich jak: zatwierdzenie konfiguracji, karta konfiguracji urządzenia, wyniki audytów konfiguracji,
- ✓ zapewnienie właściwego nadzoru nad procesem wydawania zmian w środowisku informatycznym (polityka wydawania zmian, zasady opracowania lub nabywania oprogramowania, weryfikacja i akceptacja wydawania, instalacja oprogramowania i przekazanie do użytkowania).