



P.M. Socha
06.02.2013
yph

06.02.2013
yph
Strona 1 z 3

Warszawa, dnia 10 stycznia 2013 roku

Raport

z przeprowadzonego audytu przeglądownego działań Starostwa Powiatowego w Kielcach w zakresie bezpieczeństwa przetwarzania informacji

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 Bezpieczeństwa Związku Powiatów Polskich.

Jako podstawę wymagań audytowych zostały przyjęte wybrane elementy międzynarodowej normy ISO/IEC 27001:2005 (edycja polska wersja z 2007) „Technika informatyczna Techniki bezpieczeństwa Systemy zarządzania bezpieczeństwem informacji”. 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 zabezpieczeń sieci oraz stosowanej dokumentacji systemowej.

Audyt został przeprowadzony w dniu 14 grudnia 2011 roku przez audytora:

Krzysztof Wertejuk

Raport przygotował:

Krzysztof Wertejuk

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



Obserwacje dotyczące zabezpieczeń w audytowanym obszarze oraz możliwości poprawy:

1. Starostwo przygotowuje się do certyfikacji w zakresie normy ISO/IEC 27001. Jest to już kolejna certyfikacja.
2. Starostwo posiada grupę bardzo dobrze przygotowanych audytorów wewnętrznych. Pracownicy ci mają kompletną i ugruntowaną wiedzę z zakresu wymagań normy 27001 oraz zasad audytowania systemów bezpieczeństwa informacji.
3. W ramach audytu odbyły się konsultacje z Administratorem Bezpieczeństwa Informacji na ich podstawie zostały sformułowane wnioski w zakresie zabezpieczeń.
4. Istnieje system monitorowania ruchu sieciowego i zabezpieczeń.
5. Instalacja aplikacji odbywa się na koncie administracyjnym natomiast użytkownicy korzystają z kont z ograniczonymi uprawnieniami.
6. W zakresie zabezpieczeń sieci stosowane są mechanizmy domenowe.
7. Starostwo posiada ok. 260 stacji roboczych. Zabezpieczenie przed nieautoryzowanym uruchomieniem systemu zapewnia system operacyjny oraz zarządzanie użytkownikami na poziomie domeny.
8. System separacji sieci wewnętrznej od sieci zewnętrznej daje duże możliwości ochrony.
9. Dokumentacja systemowa jest dobrze dostosowana do specyfiki Organizacji. Istnieją odpowiednie dokumenty np. Podręcznik Bezpieczeństwa Informacji wydanie 2.0 z dnia 14-12-2009 a w nich wymagane procedury. Dokumentacja systemu bezpieczeństwa informacji jest zintegrowana z wymaganiami w zakresie prowadzenia dokumentacji dotyczącej ochrony danych osobowych.
10. Śledzone są incydenty bezpieczeństwa informacji i wyciągane są wnioski w zakresie doskonalenia systemu bezpieczeństwa informacji.
11. Zasadne jest aby była doskonalona analiza ryzyka utraty informacji z uwzględnieniem aspektu istotności informacji.
12. Zasadne jest aby były doskonalone zabezpieczenia w zakresie sieciowych systemów wydruku.
13. Starostwo przykładą 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.



14. Został przeprowadzone szkolenia dla nowych pracowników i stażystów w dwóch grupach. Tematem szkoleń były ogólne zaganiaania związane z ochroną informacji, przepisami prawa w zakresie ochrony danych osobowych oraz przepisy dotyczące 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. Załącznik do raportu zawiera materiały ze szkolenia.

