"Szablon sprawozdania z audytu" podsumowanie prac nad dokumentem i kolejne kroki

Tomasz Wodziński

Chciałbym żyć w cyfrowo bezpiecznym kraju

- Garmin (Lipiec 2020)
- Honda (Czerwiec 2020)
- Przejęcie rosyjskich elektrowni (Czerwiec 2019)
- Norsk Hydro (Marzec 2019)
- Sadara Chemical Company (Sierpień 2017)
- Mersk / InterCars /Reckitt Benckiser (May 2017)
- San Fancisco – system biletowy (Listopad 2016)
- KNF - Atak na strony (Październik 2016)
- Ukraiński system przesyłu prądu (Grudzień 2016)
- Ukraińska firma energetyczna (Grudzień 2015)
- Korea Hydro and Nuclear Power (KHNP) (Grudzień 2014)

Chciałbym żyć w cyfrowo bezpiecznym kraju

- Obserwacja zachowania podmiotów
- Zasoby ludzkie dostępne u podmiotów
- Zasoby ludzkie dostępne w organach właściwych
- Dynamiczna i statyczna analiza
- Platforma 46

Art. 46. 1. Minister właściwy do spraw informatyzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego wspierającego:

1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;

2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;

3) zgłaszanie i obsługę incydentów;

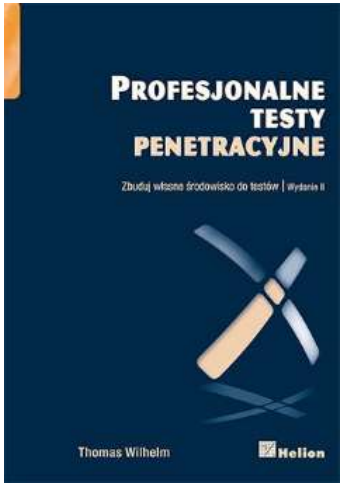
4) szacowanie ryzyka na poziomie krajowym;

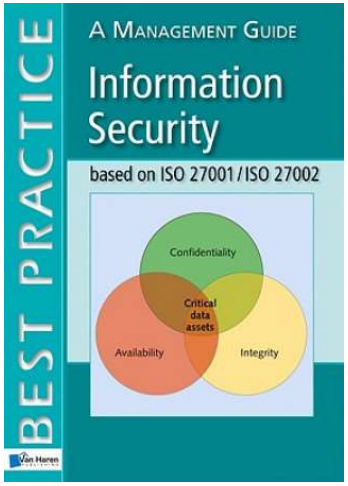
Audyt KSC – czyli CO ?

- Jak go robić ?

Art. 15. 1. Operator usługi kluczowej ma obowiązek zapewnić przeprowadzenie, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, zwanego dalej „audytem".

- Analiza pierwszych OPZ:
  - Audyt KSC zgodnie z ustawą – czyli jak ?





Sprawozdanie z audytu – Art. 15. 5.

5. Na podstawie zebranych dokumentów i dowodów audytor sporządza pisemne sprawozdanie z przeprowadzonego audytu i przekazuje je operatorowi usługi kluczowej wraz z dokumentacją z przeprowadzonego audytu.

7. Operator usługi kluczowej przekazuje kopię sprawozdania z przeprowadzonego audytu na uzasadniony wniosek:

1) organu właściwego do spraw cyberbezpieczeństwa;

2) dyrektora Rządowego Centrum Bezpieczeństwa – w przypadku gdy operator usługi kluczowej jest jednocześnie właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;

3) Szefa Agencji Bezpieczeństwa Wewnętrznego.

Harmonogram prac

- Maj 2019 – deklaracja współpracy przesłana do ministerstwa
- Lipiec 2019 – Pierwsza rozmowa z Ministerstwem Cyfryzacji w zakresie inicjatywy wraz z grupą ekspertów ISSA:
  - Piotr Dzwonkowski
  - Jakub Syta
  - Rafał Krakowski
  - Sebastian Burgemejster
  - Tomasz Wodziński
- Sierpień 2019 – kompletowanie narzędzi wspierających
- Wrzesień 2019 – Przygotowanie inicjalnego dokumentu przez Jakuba Sytę
- Październik 2019 – zaproszenie do współpracy IIA i ISACA
- Listopad 2019 – przygotowanie draftu dla Ministerstwa
- Listopad 2019 – przesłanie do IIA, ISACA Warszawa, ISACA Katowice, ISC2 Chapter Polska, Bezpieczna Cyberprzestrzeń wersji do zaopiniowania
- Grudzień 2019 – marzec 2020 – Prace z organami właściwymi
- Kwiecień 2020 – przyjęcie wersji końcowej (zamrożenie produkcyjnej wersji)

Struktura dokumentu (Metryka)

- Ustrukturyzowane informacje o OUK
- Odpowiedzialności procesowe (formalne i nieformalne) w OUK
- Informacja o audytorach wykonujących
- Niezgodności z poprzednich dwóch audytów UKSC
- Podsumowanie dla kierownictwa

Informacja o audytorach wykonujących

Funkcja Audytowa	Imię i Nazwisko	Potwierdzenie kwalifikacje (certyfikaty, wykształcenie i doświadczenie)	Audytowany obszar
Audytor Wiodący			
Audytor Systemy Operacyjne			
Audytor warstwa aplikacji i baz danych			
Audytor procesów 27001			
Audytor procesów 22301			
Audytor bezpieczeństwa procesów biznesowych			
Audytor systemów typu ICS / SCADA / OT			

Granica konfliktu interesu: Osoby tworzące zespół audytowy i bezpośrednio zaangażowane w weryfikacje zgodności muszą pozostać obiektywne i niezależne. Oznacza, to iż działając w ramach międzynarodowych standardów audytu nie mogą dokonywać oceny obszaru, za który były odpowiedzialne lub prowadziły czynności doradcze. Wszystkie osoby zaangażowane w badanie składają oświadczenie o braku konfliktu interesów, w szczególności w terminie ostatnich 24 miesięcy nie wykonywały osobiście prac doradczych, projektowych, architektonicznych lub implementacyjnych na rzecz audytowanego podmiotu w zakresie audytowanej Usługi kluczowej .

Struktura dokumentu (podział)

- Obszar 1: Organizacja zarządzania bezpieczeństwem informacji
- Obszar 2: Procesy zarządzania bezpieczeństwem informacji
- Obszar 3: Zarządzanie ryzykiem
- Obszar 4: Monitorowanie i reagowanie na incydenty bezpieczeństwa
- Obszar 5: Zarządzanie zmianą
- Obszar 6: Zarządzanie ciągłością działania
- Obszar 7: Utrzymanie systemów informacyjnych
- Obszar 8: Utrzymanie i rozwój systemów informacyjnych (systemy zapewniające bezpieczeństwo)
- Obszar 9: Bezpieczeństwo fizyczne
- Obszar 10: Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług

Obszar 1: Organizacja zarządzania bezpieczeństwem informacji

- Potwierdzenie zgodności z wymaganiami w zakresie stworzenia i utrzymywania systemu zarządzania zapewniającego zgodność z ustawą o Krajowym Systemie Cyberbezpieczeństwa.

- Kontekst w zakresie przepisów i normy
  - Obowiązujące przepisy
  - Wskazanie na punkty normy
- Kontekst w zakresie Decyzji OUK
  - Czynności zgodnie z ustawą

Obszar 1: Organizacja zarządzania bezpieczeństwem informacji

Kontekst w zakresie przepisów i normy

Zakres prac obejmował między innymi adekwatne wymagania:

- Artykułu 8, 9,10, 14, 15 i 16 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 ze zm.);
- Rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. 2019 poz. 2479);
- Rozporządzenia Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080);

Obszar 1: Organizacja zarządzania bezpieczeństwem informacji

Kontekst w zakresie Decyzji OUK

Dokumentacja potwierdzająca wykonane działania zgodnie z harmonogramem wskazanym w ustawie:

- Czynności wykonane w terminie 3 miesięcy
- Czynności wykonane w terminie 6 miesięcy
- Czynności wykonane w terminie 12 miesięcy

Opis Identyfikacji systemu informacyjnego wspierającego Usługę Kluczową:

- lista elementów składowych
- lista osób odpowiedzialnych

Obszar 1: Organizacja zarządzania bezpieczeństwem informacji

Dokumentacja Systemu Informacyjnego wspierającego Usługę Kluczową

1. Raporty z audytów systemów informacyjnych wspierających Usługę Kluczową
2. Potwierdzenie działań wynikających z komunikacji z procesem szacowania ryzyka SI_OUK
3. Dokumentacja architektury zastosowanych zabezpieczeń
4. Dokumentacja architektury sieci
5. Baza danych konfiguracji urządzeń aktywnych
6. Dokumentacja zmian w systemach informacyjnych
7. Dokumentacja dotycząca monitorowania w trybie ciągłym
8. Umowy z dostawcami (wsparcie techniczne) itp.
9. Umowy z dostawcami usług z zakresu cyberbezpieczeństwa
10. Wyniki audytów u dostawców usług cyberbezpieczeństwa
11. Dokumentacja zabezpieczeń fizycznych i środowiskowych
12. Rejestr dostępu do dokumentacji systemu informacyjnego

Obszar 2: Procesy zarządzania bezpieczeństwem informacji

- Potwierdzenie zgodności z wymaganiami bezpieczeństwa informacji w zakresie poprawności ich zdefiniowania, wdrożenia, eksploatacji i nadzorowania procesów zapewniających bezpieczeństwo informacji.

- Kontekst w zakresie przepisów i normy
  Obowiązujące przepisy
  Wskazanie na punkty normy
- Kontekst w zakresie Decyzji OUK
  Czynności zgodnie z ustawą

Obszar 3: Zarządzanie ryzykiem

- Potwierdzeniu zgodności z wymaganiami w zakresie poprawności stosowanej metodyki zarządzania ryzykiem oraz kompletności procesu zarządzania ryzykiem poczynając od identyfikacji ryzyka aż po nadzór nad wprowadzeniem rekomendacji

- Kontekst w zakresie przepisów i normy
  Obowiązujące przepisy
  Wskazanie na punkty normy
- Kontekst w zakresie Decyzji OUK
  Czynności zgodnie z ustawą

Obszar 4: Monitorowanie i reagowanie na incydenty bezpieczeństwa

- Potwierdzenie zgodności z wymaganiami w zakresie stworzenia i utrzymywania systemu zarządzania zapewniającego zgodność z ustawą o Krajowym Systemie Cyberbezpieczeństwa.

- Kontekst w zakresie przepisów i normy
  - Obowiązujące przepisy
  - Wskazanie na punkty normy
- Kontekst w zakresie Decyzji OUK
  - Czynności zgodnie z ustawą

Obszar 5: Zarządzanie zmianą

- Potwierdzenie zgodności z wymaganiami w zakresie identyfikowania potrzeby zmian, ustalania wymagań bezpieczeństwa, wyboru rozwiązań, dokumentowania, testowania i wdrażania zmian.

- Kontekst w zakresie przepisów i normy
  Obowiązujące przepisy
  Wskazanie na punkty normy
- Kontekst w zakresie Decyzji OUK
  Czynności zgodnie z ustawą

Obszar 6: Zarządzanie ciągłością działania

- Potwierdzenie zgodności z wymaganiami w zakresie dokonania analizy i zdefiniowania wymagań dla ciągłości działania, wdrożenia rozwiązań zapasowych i redundantnych, testowaniu zdolności, przygotowania odpowiednich umów z dostawcami oraz nadzorowaniu ich sposobu zapewnienia ciągłości działania.

- Kontekst w zakresie przepisów i normy
  Obowiązujące przepisy
  Wskazanie na punkty normy
- Kontekst w zakresie Decyzji OUK
  Czynności zgodnie z ustawą

Obszar 7: Utrzymanie systemów informacyjnych

- Potwierdzenie zgodności z wymaganiami w zakresie ustalania i nadzorowania wymagań bieżącej eksploatacji systemów informacyjnych

- Kontekst w zakresie przepisów i normy
  - Obowiązujące przepisy
  - Wskazanie na punkty normy
- Kontekst w zakresie Decyzji OUK
  - Czynności zgodnie z ustawą

Obszar 8: Utrzymanie i rozwój systemów informacyjnych

- Potwierdzenie zgodności z wymaganiami w zakresie ustalania i nadzorowania wymagań bieżącej eksploatacji systemów informatycznych wykorzystywanych do zapewniania, monitorowania i reagowania na incydenty bezpieczeństwa.

- Kontekst w zakresie przepisów i normy
  - Obowiązujące przepisy
  - Wskazanie na punkty normy
- Kontekst w zakresie Decyzji OUK
  - Czynności zgodnie z ustawą

Obszar 9: Bezpieczeństwo fizyczne

- Potwierdzenie zgodności z wymaganiami w zakresie skuteczności procesu ochrony fizycznej i środowiskowej.

- Kontekst w zakresie przepisów i normy
  Obowiązujące przepisy
  Wskazanie na punkty normy
- Kontekst w zakresie Decyzji OUK
  Czynności zgodnie z ustawą

Obszar 10: Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług

- Potwierdzenie zgodności z wymaganiami w zakresie definiowania i nadzorowania stosowania wymagań bezpieczeństwa informacji i ciągłości działania przez dostawców usług bezpieczeństwa informacji oraz usług wdrażania i utrzymywania systemów informatycznych wykorzystywanych do świadczenia Usług Kluczowych.

- Kontekst w zakresie przepisów i normy
  - Obowiązujące przepisy
  - Wskazanie na punkty normy
- Kontekst w zakresie Decyzji OUK
  - Czynności zgodnie z ustawą

Dalsze plany ?

Dziękuje

https://github.com/ISSAPolska/Audyt_KSC