Bezpieczeństwo informacji

Audyt bezpieczeństwa informacji jest to proces zbierania i oceniania dowodów w celu określenia czy system informacyjny i związane z nim zasoby właściwie chronią majątek, utrzymują integralność danych i dostarczają odpowiednich i rzetelnych informacji, osiągają efektywnie cele organizacji, oszczędnie wykorzystują zasoby i stosują mechanizmy kontroli wewnętrznej, tak aby dostarczyć rozsądnego zapewnienia, że osiągane są cele operacyjne i kontrolne, oraz że chroni się przed niepożądanymi zdarzeniami lub są one na czas wykrywane, a ich skutki na czas korygowane.

Audyt jest prowadzony w celu stwierdzenia stopnia zgodności ocenianego systemu z określonym standardem lub normą, wybraną jako punkt odniesienia.

System Zarządzania Bezpieczeństwem Informacji jest weryfikowany względem wymagań stawianych przez **Ustawę o krajowym systemie cyberbezpieczeństwa** z dnia 5 lipca 2018 r. (Dz.U. 2018 poz. 1560).

Odbywa się analiza i ocena **dokumentacji** w zakresie bezpieczeństwa informacji, w tym polityk, procedur, zarządzeń, instrukcji, umów oraz innych dokumentów, które zostaną udostępnione do analizy.

Powyższe dokumenty zostają sprawdzone pod kątem aktualności i poprawności względem siebie. Ponadto weryfikowane jest czy wprowadzone w organizacji dokumenty są przestrzegane zgodnie z zawartymi w nich zapisami. Może to oznaczać przegląd wymienionych w dokumentacji rejestrów, list, raportów jak np. dziennik administratora systemu, dziennik wykonywania kopii lub wyniki z przeglądów uprawnień.

Przeprowadzane są również **wywiady z wytypowanymi pracownikami** poszczególnych komórek organizacyjnych w zakresie niezbędnym do ustalenia poziomu stosowania wymagań bezpieczeństwa oraz z wewnętrznymi uregulowaniami, w celu ustalenia faktów niezawartych lub niewynikających wprost z dokumentacji, najczęściej z osobą odpowiedzialną za dział IT – ASI, również IOD, pracownikiem ds. ryzyka, kadrową oraz pracownikami obsługi klienta.

Prowadzone są **obserwacje** budynku, pomieszczeń, działań i zachowań pracowników oraz przeprowadzana jest analiza bezpieczeństwa informacji **w systemach teleinformatycznych**.

Wynikiem audytu jest **raport** zawierający wykryte niezgodności oraz dotyczące ich zalecenia naprawcze.

Zakres usługi dla Operatora usług kluczowych

I. Audyt systemu zarządzania bezpieczeństwem informacji w zakresie systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej

Audyt realizowany jest pod kątem wymagań stawianych przez Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, w oparciu o następujące normy oraz standardy: ISO/IEC 27001:2017-06, PN-ISO/IEC 27005:2014-01, PN-EN ISO 22301:2014-11, PN-ISO/IEC 20000-1:2014-01.

Audyt przeprowadza się na podstawie przeprowadzanych analiz udostępnianej dokumentacji, przekazywanych informacji podczas wywiadów oraz obserwacji audytorów.

Audyt dotyczy systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, wskazanych przez Zleceniodawcę.

1. Audyt obszaru organizacyjnego obejmuje:
   a. Weryfikację procesu zarządzania ryzykiem, w tym:
      - dokumentowania metodologii i wyników szacowania ryzyka;
      - planowania i wdrażania zabezpieczeń na podstawie wyników szacowania ryzyka;
      - systematyczności przeprowadzanego szacowania ryzyka.
   b. Weryfikację dokumentacji sytemu zarządzania bezpieczeństwem informacji, w tym systemu informacyjnego, w zakresie:
      - aktualności względem przepisów Ustawy z dnia 5lipca 2018r.o krajowym systemie cyberbezpieczeństwa;
      - stosowania wersjonowania i archiwizacji;
      - dostępności dla osób uprawnionych;
      - procesu zarzadzania z incydentami.
   c. Weryfikację podziału obowiązków związanych z usługami kluczowymi.
   d. Weryfikację procesów zarządzania ciągłością działania i ciągłością bezpieczeństwa informacji, w tym posiadanych planów ciągłości działania.
   e. Weryfikację zawieranych umów związanych z usługami kluczowymi oraz zasad współpracy z dostawcami.
   f. Weryfikację procesu zarządzania incydentami, w tym
      - dokumentowania zgłoszeń;
      - klasyfikacji incydentów;
      - dalszego postepowania z incydentami.
2. Audyt obszaru fizycznego obejmuje:
   a. Kontrolę dostępu fizycznego, w tym:
      - weryfikację granic obszaru bezpiecznego i jego ochrony;
      - weryfikacja zabezpieczeń wejścia/wyjścia.
   b. Weryfikację stosowanych zabezpieczeń, w tym:
      - systemów zabezpieczeń pomieszczeń i urządzeń;

- zabezpieczeń okablowania strukturalnego;
- systemów chłodzenia i innych zabezpieczeń środowiskowych;
- systemów alarmowych i monitoringu;

3. Audyt obszaru teleinformatycznego obejmuje:
   a. Weryfikację istniejących procedur zarządzania systemami.
   b. Weryfikację zarządzania podatnościami, w tym:
      - ochrony przed oprogramowaniem szkodliwym;
      - zabezpieczania konfiguracji urządzeń i systemów;
      - wykrywaniem i reagowaniem na wykryte podatności;
      - zapewniania aktualności oprogramowania.
   c. Weryfikację zarządzania kopiami zapasowymi.
   d. Weryfikację procesów monitorowania oraz rejestracji błędów.
   e. Weryfikację zabezpieczeń systemów i urządzeń, w tym:
      - poziomu uprawnień w systemach;
      - sposobów uwierzytelniania w systemach;
      - możliwości nieautoryzowanych instalacji oprogramowania;
      - ochrony przed nieuprawnionym dostępem;
      - dostępności nośników wymiennych.
4. Analiza podatności systemów wspomagających świadczenie usług kluczowych.
   a. Testy styku sieci lokalnej z Internetem przeprowadzane ze stacji roboczej podłączonej do sieci Internet
      - Analiza topologii brzegu sieci;
      - Weryfikacja mechanizmów ochronnych;
      - Próba wykrycia usług sieciowych udostępnianych do Internetu;
      - Detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet;
      - Exploitacja dostępnych urządzeń oraz usług wystawionych do sieci Internet;
      - Przedstawienie rozwiązań zwiększających bezpieczeństw styku sieci lokalnej z siecią Internet.
   b. Testy penetracyjne przeprowadzone ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz organizacji
      - Analiza topologii sieci LAN;
      - Weryfikacja mechanizmów ochronnych w sieci;
      - Analiza komunikacji sieciowej;
      - Skanowanie portów TCP/UDP próba wykrycia usług sieciowych;
      - Skanowanie hostów aktywnych w sieci;
      - Exploitacja dostępnych urządzeń oraz usług w sieci LAN;
      - Przedstawienie rozwiązań zwiększających bezpieczeństw sieci LAN.
5. Opracowanie raportów z audytu.

II. Wdrożenie systemu zarządzania bezpieczeństwem informacji w zakresie systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej

1. Udokumentowanie zasad zarzadzania dokumentacją:
   a. Opracowanie zasad wersjonowanie dokumentacji;
   b. Określenie zakresu dostępności i ścieżek dystrybucji dokumentacji;
   c. Udokumentowanie zasad ochrony dokumentacji, w tym jej archiwizacji.
2. Utworzenie dokumentacji zarządzania ryzykiem:
   a. Opracowanie metodologii szacowania ryzyka;
   b. Przeprowadzenie szacowania ryzyka;
   c. Opracowanie proponowanych planów postępowania z ryzykiem.
3. Utworzenie dokumentacji zarządzania zmianami:
   a. Opracowanie zasad planowania zmian;
   b. Opracowanie zasad analizowania zmian pod kątem wpływu na bezpieczeństwo.
4. Udokumentowanie zasad kontroli dostępu i zabezpieczania fizycznego i środowiskowego.
5. Udokumentowanie zasad współpracy z dostawcami:
   a. Opracowanie wymagań dla zawieranych umów;
   b. Opracowanie zasad oceny dostawców.
6. Utworzenie dokumentacji ciągłości działania, w zakresie
   a. Utworzenie planów ciągłości działania usług kluczowych;
   b. Opracowanie zasad utrzymania bezpieczeństwa informacji, zapewniających poufność, integralność, dostępność i autentyczność informacji.
7. Utworzenie dokumentacji zarządzania incydentami:
   a. Opracowanie zasad wewnętrznego zgłaszania zdarzeń;
   b. Opracowanie zasad oceny zgłoszonych zdarzeń;
   c. Opracowanie zasad klasyfikacji incydentów;
   d. Opracowanie zasad postępowania z incydentami;
   e. Opracowanie zasad i zakresu udostępniania informacji o incydentach.
8. Utworzenie dokumentacji zarządzania systemem informacyjnym:
   a. Opracowanie zasad zarządzania podatnościami technicznymi;
   b. Opracowanie zasad aktualizacji oprogramowania;
   c. Opracowanie zasad bezpieczeństwa informacji przetwarzanych w systemie;
   d. Opracowanie zasad monitorowania systemu.
9. Udokumentowanie zasad komunikacji:
   a. Udokumentowanie obowiązków osoby kontaktowej operatora kluczowego
   b. Udokumentowanie sposobów uświadamiania użytkowników końcowych o zasadach bezpieczeństwa i zagrożeniach;
   c. Udokumentowanie zasad kontaktowania się z właściwymi organami.