DATA CENTER

Audyt Bezpieczeństwa Systemów Informatycznych

Zastosowanie ochrony informacji w organizacjach

Czym jest audyt?

Audyt Bezpieczeństwa Systemów Informatycznych polega na analizie zabezpieczeń zastosowanych w organizacji w celu ochrony informacji.

Do potencjalnych zagrożeń związanych z podatnościami systemu należą m.in.: wyciek, utrata lub modyfikacja danych, przejęcie kontroli nad infrastrukturą, a także wykorzystywanie systemu oraz sieci w nieodpowiedni sposób np. do celów przestępczych.

Działania audytu teleinformatycznego polegają na kontrolowaniu poziomu bezpieczeństwa IT, sprawdzaniu integralności, poufności oraz dostępności systemów informatycznych, kontroli jego awaryjności, weryfikacji wiarygodności przetwarzanych danych jak również na spełnianiu wymogów standardów bezpieczeństwa. Audyt obejmuje obszary organizacyjne oraz techniczne.

W przeprowadzanym u klienta audycie stosujemy się m.in. do wytycznych określonych w Audit Guideline Międzynarodowego Stowarzyszenia Audytorów Systemów Informatycznych ISACA.

COIG

Audyt Bezpieczeństwa Systemów Informatycznych polega na analizie zabezpieczeń zastosowanych w organizacji w celu ochrony informacji.

W zakresie organizacyjnym audyt obejmuje:

Procedury, politykę wewnętrzną organizacji oraz stosowanie się do zapisów zawartych w dokumentacji jak i w przepisach prawa.

- przegląd polityki bezpieczeństwa firmy;
- analiza procedur bezpieczeństwa oraz zastosowanie ich w praktyce;
- weryfikacja poprawnego stosowania przepisów ochrony danych osobowych zgodnych z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO);
- weryfikacja zgodności z ustawą o krajowym systemie cyberbezpieczeństwa (dla podmiotów które jej podlegają);
- zarządzanie kopiami zapasowymi;
- administrowanie kontami i hasłami dostępowymi;
- zarządzanie rejestracją błędów.

DATA CENTER

W zakresie technicznym audyt obejmuje techniczne zabezpieczenia wdrożone w organizacji:

- techniczne zabezpieczenia komputerów oraz stacji roboczych;
- techniczne zabezpieczenia poczty elektronicznej;
- techniczne zabezpieczenia ochrony antywirusowej, antyspamowej;
- kontrolę mechanizmów logowania;
- kontrolę weryfikacji i konfiguracji oprogramowania.

Dlaczego audyt jest tak ważny?

W celu ochrony informacji zabezpieczenia zastosowane w organizacji muszą podlegac ciągłej analizie, w związku z potencjanym zagrożeniem, które może zagrozić:

- Wyciekiem danych
- Utratą lub modyfikacją
- Przejęciem kontroli nad infrastrukturą
- Wykorzystywaniem systemu oraz sieci w nieodpowiedni sposób np. do celów przestępczych

10 kroków do skutecznego audytu

01 ocena dokumentacji dotyczącej systemu zarządzania bezpieczeństwem informacji pod kątem spełnienia wymogów normy PN-EN ISO/IEC 27001;

02 ocena poprawności wdrożonych procedur oraz przepisów ochrony danych osobowych zgodnych z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO);

03 ocena zgodności z ustawą o krajowym systemie cyberbezpieczeństwa;

04 analiza podatności systemów teleinformatycznych;

05 przegląd oraz analiza słabych punktów systemów teleinformatycznych;

06 kontrola struktury sieci oraz wewnętrznych i zewnętrznych kanałów komunikacyjnych firmy ;

07 kontrola środowiska Wi-Fi;

08 kontrola bezpieczeństwa fizycznego obiektów;

09 ocena stanu technicznego infrastruktury;

10 stworzenie raportu zawierającego stwierdzone nieprawidłowości oraz wskazówki w zakresie rozwiązań zwiększających bezpieczeństwo.