Opracowanie Kompleksowego Systemu Bezpieczeństwa Informacji dla Wybranej Firmy

Cel zadania: Celem projektu jest stworzenie kompleksowego systemu bezpieczeństwa informacji dla wybranej firmy, obejmującego zarówno aspekty techniczne, jak i organizacyjne. Projekt ma na celu zidentyfikowanie, ocenę oraz skuteczne zarządzanie ryzykiem związanym z bezpieczeństwem informacji w kontekście działalności firmy.

Kroki do wykonania:

1. Identyfikacja Aktywów:
   - Sporządzenie pełnej listy aktywów informacyjnych firmy, takich jak bazy danych, serwery, aplikacje, dane klientów itp.
2. Analiza Zagrożeń:
   - Przeprowadzenie analizy zagrożeń związanych z bezpieczeństwem informacji, uwzględniając ataki zewnętrzne i wewnętrzne.
   - Skoncentrowanie się na identyfikacji potencjalnych źródeł ryzyka, takich jak cyberprzestępcy, błędy ludzkie, awarie sprzętowe itp.
3. Ocena Ryzyka:
   - Przeprowadzenie oceny ryzyka dla zidentyfikowanych zagrożeń, uwzględniając prawdopodobieństwo wystąpienia i potencjalne skutki dla firmy.
   - Hierarchizacja zagrożeń według poziomu ryzyka.
4. Polityka Bezpieczeństwa:
   - Opracowanie polityki bezpieczeństwa informacji, która określi zasady i wytyczne dotyczące ochrony aktywów informacyjnych.
   - Uwzględnienie w polityce aspektów takich jak autentykacja, zarządzanie uprawnieniami, monitorowanie i reagowanie na incydenty.
5. Techniczne Środki Bezpieczeństwa:
   - Propozycja technicznych rozwiązań bezpieczeństwa, obejmujących firewalle, systemy antywirusowe, systemy detekcji intruzów, szyfrowanie danych itp.
   - Opis, jakie technologie zostaną wdrożone, aby chronić infrastrukturę IT firmy.
6. Zarządzanie Dostępem:
   - Projektowanie i wdrożenie systemu zarządzania dostępem (IAM), obejmującego autentykację, autoryzację i audyt dostępu do systemów.
7. Szkolenia dla Pracowników:
   - Opracowanie programu szkoleń dla pracowników firmy dotyczących zasad bezpieczeństwa informacji.

- Uwzględnienie szkoleń z zakresu rozpoznawania zagrożeń, korzystania z narzędzi bezpieczeństwa itp.

8. Monitorowanie i Reagowanie na Incydenty:
   - Wdrożenie systemu monitoringu bezpieczeństwa informacji, umożliwiającego śledzenie aktywności i wykrywanie nieprawidłowości.
   - Opracowanie procedur reagowania na incydenty bezpieczeństwa, w tym planu kontynuacji działania.
9. Zarządzanie Łatkami i Aktualizacje:
   - Utworzenie procedur regularnego aktualizowania oprogramowania i wdrażania łatek bezpieczeństwa.
   - Zapewnienie, że wszystkie systemy są utrzymane w najnowszej, bezpiecznej wersji.
10. Audyt Bezpieczeństwa:
    - Opracowanie planu audytów bezpieczeństwa informacji, obejmującego audyty wewnętrzne i zewnętrzne.
    - Przeprowadzenie regularnych audytów w celu oceny skuteczności systemu bezpieczeństwa.
11. Kontrola Dostawców:
    - Ustalenie standardów bezpieczeństwa dla dostawców i kontrahentów firmy.
    - Opracowanie procedur oceny i monitorowania dostawców pod kątem bezpieczeństwa informacji.
12. Szkolenie Zespołu Bezpieczeństwa:
    - Szkolenie dla zespołu odpowiedzialnego za utrzymanie i monitorowanie systemu bezpieczeństwa.
    - Przygotowanie zespołu do skutecznego reagowania na incydenty.

Ocenianie Projektu: Projekt zostanie oceniony pod kątem kompletności, spójności, zgodności z najlepszymi praktykami bezpieczeństwa informacji oraz oryginalności rozwiązań proponowanych dla firmy. Ocena będzie również obejmować skuteczność strategii minimalizacji ryzyka.