Zasady bezpieczeństwa organizacji

1. Polityka bezpieczeństwa

Polityka bezpieczeństwa to dokument określający zasady i procedury mające na celu ochronę zasobów informacyjnych organizacji. Kluczowe elementy polityki bezpieczeństwa:

1. **Cel i zakres**:
    a. Określenie celu polityki bezpieczeństwa.
    b. Zakres polityki obejmujący wszystkie systemy, sieci i dane organizacji.
2. **Zarządzanie ryzykiem**:
    a. Identyfikacja i ocena ryzyk związanych z bezpieczeństwem informacji.
    b. Opracowanie planów zarządzania ryzykiem.
3. **Zarządzanie dostępem**:
    a. Zasady przyznawania, modyfikowania i odwoływania dostępu do zasobów.
    b. Uwierzytelnianie wieloskładnikowe (MFA) dla krytycznych systemów.
4. **Ochrona danych**:
    a. Szyfrowanie danych w spoczynku i w tranzycie.
    b. Regularne tworzenie kopii zapasowych i testowanie procedur odzyskiwania danych.
5. **Bezpieczeństwo sieci**:
    a. Zasady konfiguracji zapór sieciowych, systemów wykrywania włamań (IDS) i systemów zapobiegania włamaniom (IPS).
    b. Monitorowanie ruchu sieciowego i reagowanie na incydenty.
6. **Szkolenia i świadomość**:
    a. Regularne szkolenia dla pracowników dotyczące najlepszych praktyk bezpieczeństwa.
    b. Kampanie podnoszące świadomość na temat zagrożeń, takich jak phishing i socjotechnika.
7. **Zarządzanie incydentami**:
    a. Procedury zgłaszania i reagowania na incydenty bezpieczeństwa.
    b. Plan ciągłości działania i odzyskiwania po awarii.

Analiza bezpieczeństwa

1. Identyfikacja zasobów

- **Systemy operacyjne**: Windows 10, Windows Server 2019.
- **Aplikacje**: Oprogramowanie biurowe, systemy ERP, CRM.
- **Dane**: Bazy danych klientów, dokumenty wewnętrzne.

2. Ocena ryzyka

- **Zagrożenia**: Ataki DDoS, ransomware, phishing, wewnętrzne zagrożenia.
- **Wrażliwości**: Nieaktualne oprogramowanie, słabe hasła, brak szyfrowania.
- **Skutki**: Utrata danych, przestoje w działalności, naruszenie prywatności klientów.

3. Zalecenia dotyczące bezpieczeństwa sieciowego systemu operacyjnego

- **Aktualizacje**: Regularne instalowanie aktualizacji systemu operacyjnego i oprogramowania.
- **Szyfrowanie**: Wykorzystanie BitLocker do szyfrowania dysków twardych.
- **Uwierzytelnianie**: Wprowadzenie uwierzytelniania wieloskładnikowego (MFA).
- **Monitorowanie**: Implementacja narzędzi do monitorowania i analizy ruchu sieciowego, takich jak Windows Defender ATP.
- **Zarządzanie dostępem**: Stosowanie zasad minimalnych uprawnień (least privilege) i regularne przeglądy uprawnień użytkowników.

Tworzenie bezpiecznego hasła

Aby utworzyć hasło spełniające wymagania bezpieczeństwa, należy przestrzegać następujących zasad:

1. **Długość**: Hasło powinno mieć co najmniej 12 znaków.
2. **Złożoność**: Hasło powinno zawierać kombinację wielkich i małych liter, cyfr oraz znaków specjalnych.
3. **Unikalność**: Hasło nie powinno być używane w innych systemach ani łatwe do odgadnięcia.
4. **Regularna zmiana**: Hasło powinno być zmieniane co 3-6 miesięcy.
5. **Unikanie słów słownikowych**: Hasło nie powinno zawierać słów, które można znaleźć w słowniku.

Przykład bezpiecznego hasła: `P@ssw0rd!2025#Secure`