# Network hardening scenario

Jesteś analitykiem bezpieczeństwa pracującym dla organizacji zajmującej się mediami społecznościowymi. Organizacja doświadczyła ostatnio poważnego naruszenia danych, które zagroziło bezpieczeństwu danych osobowych klientów, takich jak nazwiska i adresy. Twoja organizacja chce wdrożyć silne praktyki wzmacniania sieci, które można konsekwentnie stosować, aby zapobiegać atakom i naruszeniom w przyszłości.

Po sprawdzeniu sieci organizacji odkrywasz cztery główne luki. Cztery luki w zabezpieczeniach są następujące:

1. Hasła współdzielone przez pracowników organizacji.
2. Hasło administratora bazy danych jest ustawione na domyślne.
3. Zapory ogniowe nie mają reguł filtrowania ruchu przychodzącego i wychodzącego z sieci.
4. Uwierzytelnianie wieloskładnikowe (MFA) nie jest używane.

Jeśli nie zostaną podjęte żadne działania w celu usunięcia tych luk, organizacja jest narażona na ryzyko kolejnego naruszenia bezpieczeństwa danych lub innych ataków w przyszłości.

**W folderze znajdziemy pliki pomocnicze**

# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Organizacja powinna wprowadzić:   * Uwierzytelnianie wieloskładnikowe * Polityki haseł * Konserwacja Firewalla |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Organizacja nie stosuje silnych polityk haseł oraz uwierzytelniania wieloskładnikowego, są to proste do wprowadzenia a bardzo skuteczne metody na ograniczenie potencjału zagrożeń. Ograniczą one narażenie na ataki typu Brute force a regularna zmiana haseł związana z silną polityką haseł zminimalizuje ryzyko potencjalnych wycieków.  Ich sieć jest zagrożona przez brak odpowiednich reguł w zaporze ogniowej, proponujemy wprowadzić regularną konserwacje Firewalla która będzie polegała na aktualizowaniu konfiguracji, reguł w celu pozostawiania do przodu przed zagrożeniem.  Te akcje są bardzo tanie, a skuteczne do poprawienia bezpieczeństwa organizacji, proponujemy w późniejszym czasie ciągle rozszerzać zakres zabezpieczeń, aby w pełni implementować koncept głębokiej obrony. |