Zadanie 8: Audyt bezpieczeństwa i monitorowanie logów (Event Viewer)

Przedmiot: Administracja systemami sieciowymi

Klasa: 2 Technikum Informatyczne

Temat: Konfiguracja audytu logowania oraz analiza zdarzeń w Podglądzie zdarzeń.

1. Cel ćwiczenia

Celem zadania jest wdrożenie zasad audytu bezpieczeństwa, które pozwolą rejestrować zdarzenia logowania użytkowników. Dzięki temu administrator będzie w stanie zidentyfikować nieudane próby logowania (np. ataki typu brute-force) oraz przeglądać dzienniki zdarzeń w celu diagnostyki systemu.

2. Wymagania wstępne

- Działający kontroler domeny z zainstalowanymi rolami z poprzednich zadań.
- Klient (Windows 11) dołączony do domeny.

3. Instrukcja krok po kroku

Krok 1: Włączenie polityki audytu przez GPO

1. Otwórz **Zarządzanie zasadami grupy (GPO)** na serwerze.
2. Stwórz nowy obiekt GPO (np. "AudytBezpieczenstwa") i powiąż go z jednostką organizacyjną z komputerami.
3. Edytuj GPO: **Konfiguracja komputera -> Zasady -> Ustawienia systemu Windows -> Ustawienia zabezpieczeń -> Zasady lokalne -> Zasady inspekcji**.
4. Skonfiguruj **Inspekcję zdarzeń logowania** (Audit logon events) na:
    - Sukces (Success)
    - Niepowodzenie (Failure)

5. Zatwierdź i zamknij edytor.

Krok 2: Wymuszenie polityki i generowanie zdarzeń

1. Na kliencie (Windows 11) wykonaj gpupdate /force.
2. Wyloguj się z klienta i spróbuj zalogować się jako użytkownik domeny, wpisując celowo błędne hasło.
3. Zaloguj się poprawnie do systemu.

Krok 3: Analiza w Podglądzie zdarzeń (Event Viewer)

1. Na serwerze (lub na kliencie, jeśli audyt dotyczy lokalnego logowania) otwórz **Podgląd zdarzeń**.
2. Przejdź do **Dzienniki systemu Windows -> Zabezpieczenia**.
3. Poszukaj zdarzeń o identyfikatorze (Event ID) **4625** (nieudane logowanie) oraz **4624** (udane logowanie).

4. Sprawozdanie

Sprawozdanie musi zawierać:

- Zrzut ekranu z edytora GPO pokazujący włączone inspekcje (Sukces/Niepowodzenie).
- Zrzut ekranu z "Podglądu zdarzeń" (Dziennik Zabezpieczenia) z widocznym błędem logowania (Event ID 4625).
- Wnioski: Dlaczego inspekcja niepowodzeń logowania jest tak ważna dla bezpieczeństwa w sieciach firmowych?