Zadanie 3

Celem ćwiczenia jest zapoznanie się z działaniem mechanizmu zarządzania zabezpieczeniami systemów operacyjnych pracujących w usłudze Active Directory.

Ćwiczenie można wykonywać w parach. Dla celów ćwiczenia można wykorzystać utworzone poprzednio maszyny wirtualne (Windows Server + Windows).

Czas przewidziany na wykonanie ćwiczenia – 2 godziny lekcyjne. Dzień tygodnia rozpoczęcia ćwiczenia – 25.11.2019 (oznacza to, że prace powinny być zrobione maksymalnie do 29.11.2019).

Prace powinny być przesłane na pocztę piotr_dobosz@int.pl z tematem zawierającym identyfikator klasy np. **[iib], [2A], [IIh]** itp. Brak opisu w temacie będzie skutkował obniżeniem oceny (ze względu na fakt, że nauczyciel będzie musiał ręcznie segregować pocztę!). Również brak podpisu będzie skutkował obniżeniem oceny (chyba, że pole od kogo zawiera imię i nazwisko osoby).

INFORMACJA! Praca może być wykonana dowolnie jednak MUSI BYĆ CZYTELNA. Jeżeli praca będzie zawierała losowe zrzuty ekranu, praca będzie przesłana jako zrzuty ekranu bez wytłumaczenia (zrzuty można znaleźć np. w serwisach internetowych) to automatycznie zmniejsza to jej szansę na lepszą ocenę. Jeżeli praca nie będzie tematyczna (będzie zrobiona ale kompletnie nie na temat) to oczywiście skończy się to oceną niedostateczną.

ZADANIE

Biuro posiada 3 piony pracownicze – księgowość, kadry, dział inżynierski. Każdy z tych działów posiada pewną liczbę pracowników. Administrator chce wykonać następujące operacje:

a) zarówno księgowość jak i kadry powinny mieć całkowity zakaz dostępu do jakichkolwiek ustawień systemowych (w stylu harmonogram zadań, panel sterowania, rejestr systemowy itp.); W zadaniu należy kierować się swoimi doświadczeniami do jakich ustawień użytkownik nie powinien mieć dostępu (swoje decyzje należy BEZWZGLĘDNIE uzasadnić)

b) księgowość powinna mieć ustawioną tapetę z napisem KSIĘGOWOŚĆ; poniżej na tapecie powinny być imiona i i nazwiska osób wykonujących ćwiczenie. Ponadto księgowość powinna mieć możliwość uruchamiania jedynie programów do edycji tekstu (tylko dostępnych w podstawowym wydaniu systemu Windows)

c) kadry muszą mieć pulpit wykonany analogicznie do księgowości. Ponadto kadry w swojej pracy nie wykorzystują programów graficznych oraz aplikacji biurowych. Należy je zablokować (np. Paint i WordPad)

d) inżynierowie powinni mieć dla odmiany niemal wszystko odblokowane. Jedynie rejestr powinien być dla nich niedostępny oraz harmonogram zadań.

e) konta powinny mieć następujące zabezpieczenia: blokada konta po 5 nieudanych próbach na 1 godzinę, hasło zmieniane do 180 dni z uprzednim powiadomieniem o upływie tegoż terminu na 5 dni przed faktyczną datą. Dodatkowo tylko administratorzy i inżynierowie powinni mieć dostęp do logowania się lokalnie na serwerze – nie powinni mieć tego pozostali użytkownicy. Natomiast wszyscy użytkownicy powinni mieć możliwość logowania się do pulpitu zdalnego.

Należy podać 5 zasad dodatkowych zabezpieczeń, które przełożą się na zminimalizowanie ryzyka włamania się na pulpit serwera i/lub maszyny klienckiej.

Po wykonaniu zadania należy zalogować się na maszynę kliencką i przetestować działanie ustawień. Działania należy udokumentować odpowiednimi zrzutami ekranu!

WAŻNE! Należy utworzyć co najmniej jednego użytkownika każdej kategorii by pokazać efekt działania naszych ustawień. Optymalnie będzie stworzyć co najmniej dwóch użytkowników (celem potwierdzenia, że zasady obowiązują dla całej grupy użytkowników!)

Zadanie na ocenę dopuszczającą (zadanie może być robione w pojedynkę, nie ma możliwości pracy grupowej):

Sporządzić prezentację traktująca o dobrych praktykach zabezpieczenia Windows Server oraz o najważniejszych i najciekawszych zasadach zabezpieczeń dostępnych w systemie Windows Server 2016/2019. Prezentacja musi zawierać co najmniej 25 slajdów.