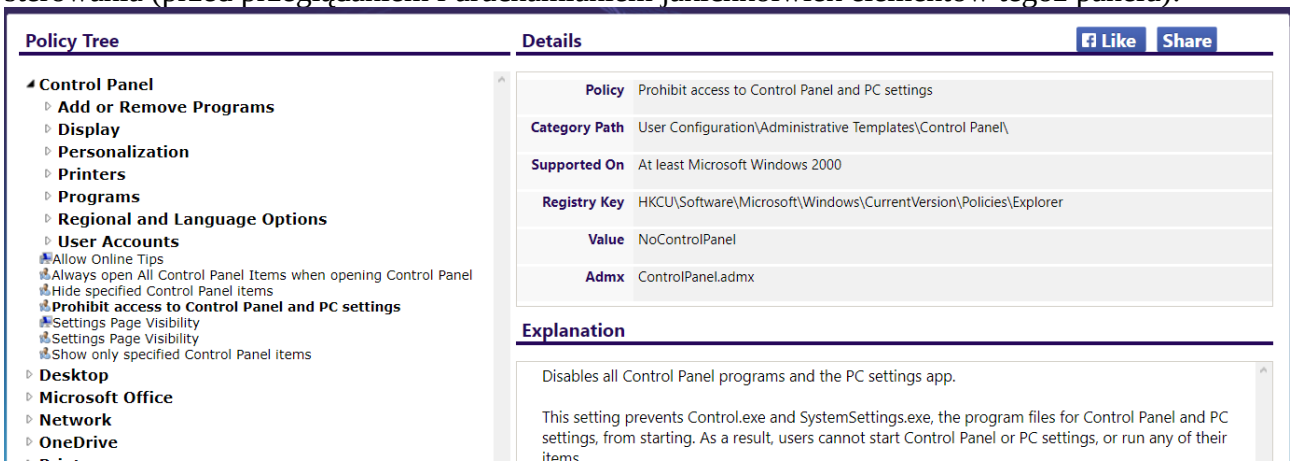
Zasady zabezpieczeń lokalnych w systemie Windows (wersja Pro)

Celem niniejszego ćwiczenia jest zapoznanie się z możliwościami zabezpieczenia systemu operacyjnego poprzez odpowiednie ustawienie zasad bezpieczeństwa.
Systemy z rodziny Windows tego typu zabezpieczenia przechowują w rejestrze systemu Windows. Zabezpieczenia te stosowane są przeważnie wraz z domeną Windows (systemy klienckie pobierają odpowiednie pliki konfiguracyjne bezpośrednio z serwera). Ponadto kopia ustawień gromadzona jest w odpowiednich folderach systemowych Windows w pliku o nazwie Registry.pol. Tego typu pliki można przemieszczać pomiędzy systemami po prostu je kopiując.

Innym sposobem nadawania zabezpieczeń jest bezpośrednia edycja rejestru systemowego systemu Windows. Tego typu rozwiązanie wiąże się jednak z koniecznością przestudiowania dokumentacji tej funkcjonalności systemu Windows. Microsoft udostępnia ją w dość przystępnym miejscu – https://gpsearch.azurewebsites.net. Przykładowe wyniki wyszukiwania dla zabezpieczenia Panelu sterowania (przed przeglądaniem i uruchamianiem jakichkolwiek elementów tegoż panelu):



Pod polem Policy mamy nazwę zabezpieczenia (w wersji angielskiej, w polskiej może się ona różnić niemożliwość tłumaczenia 1:1)

Pole Category Path wskazuje lokalizację zabezpieczenia w narzędziu zabezpieczeń (gpedit). Również po angielsku

Supported On wskazuje, od której wersji (bądź do której wersji) zabezpieczenie działa (w tym wypadku od systemu Windows 2000 wzwyż)

Registry Key wskazuje natomiast, w której gałęzi rejestru systemowego można znaleźć zapis tego zabezpieczenia (HKCU to skrót od HKEY_CURRENT_USER)

Value to nazwa wartości, która musi zostać dodana pod wskazanym kluczem, aby zabezpieczenie zadziałało. Najczęściej nie ma podanego typu wartości, jednak jeżeli nie ma wskazanych konkretnych wartości do ustawienia to można założyć, iż chodzi o wartość DWORD. Ponieważ nazwa wartości to ‘NoControlPanel’ oznacza to, iż musi być ona aktywna by wskazany użytkownik nie miał dostępu do panelu. To oznacza, że wartość dla tego konkretnego ustawienia powinna wynieść 1.

Oczywiście można też ustawić odpowiednie zabezpieczenia poprzez narzędzie gpedit, a później prześledzić ustawienia rejestru. (w odpowiednich gałęziach).

ZADANIA DO WYKONANIA

1. Podać możliwe zastosowania zasad zabezpieczeń lokalnych.
2. W jaki sposób można nadać zasady dla określonych użytkowników systemu operacyjnego i/lub określonych grup użytkowników? (podpowiedź – narzędzie mmc)
3. W których dokładnie folderach gromadzone są pliki Registry.pol? (podpowiedź – po ustawieniu jakichkolwiek zabezpieczeń pliki te są zapisywane w folderze systemu Windows)
4. Czy poprzez zasady zabezpieczeń jest możliwość zablokowanie działania Windows Update dla wszystkich użytkowników? Jeżeli tak należy podać odpowiednie ustawienia.
5. Czy zasady grupy umożliwiają blokadę uruchamiania wybranych programów? Jeżeli tak to proszę podać odpowiednie ustawienia.
6. Czy zasady grupy mogą uniemożliwić zmianę tapety pulpitu? Jeżeli tak to proszę podać odpowiednie ustawienia.
7. Czy istnieje możliwość personalizacji pulpitu (jak paski zadań czy też rozmieszczenia ikon pulpitu)? Jeżeli tak – wskazać możliwe rozwiązanie.
8. Zaproponować dobór ograniczeń dla przeglądarki Internet Explorer/Edge.
9. Dobrać ustawienia zabezpieczeń w taki sposób by z ustawień systemowych można było zarządzać zainstalowanym oprogramowaniem, datą systemową oraz połączeniami sieciowymi. Reszta ustawień ma być niedostępna.
10. W jakiś sposób można wyłączyć podręczne menu w systemie Windows?
11. Zaproponować najlepszy zestaw ustawień zabezpieczających dla eksploratora Windows.
12. W jaki sposób można importować/eksportować ustawienia zabezpieczeń poprzez rejestr (dobre rozwiązanie w przypadku wersji Home).

Przydatne strony WWW:
https://social.technet.microsoft.com/Forums/windowsserver/en-US/46e287c3-a082-422f-a3aa-1f5fbccee2a3/group-policy-registry-settings-not-applying-registrypol-corrupt?forum=winserverGP

https://gpsearch.azurewebsites.net/#4696

http://techgenix.com/windows-group-policy-settings/

https://www.lepide.com/blog/top-10-most-important-group-policy-settings-for-preventing-security-breaches/

https://community.spiceworks.com/topic/805751-gpo-best-practices-and-recommended-implementations

https://support.microsoft.com/en-ca/help/4019502/how-to-use-the-settings-app-group-policy-on-windows-10

https://www.makeuseof.com/tag/12-ways-windows-group-policy-can-make-pc-better/