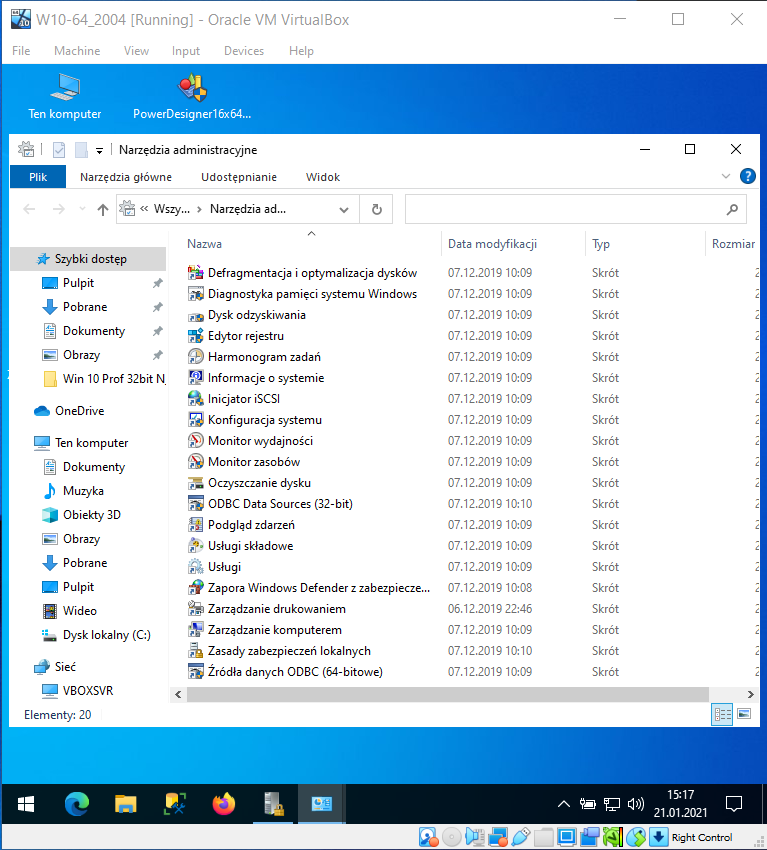


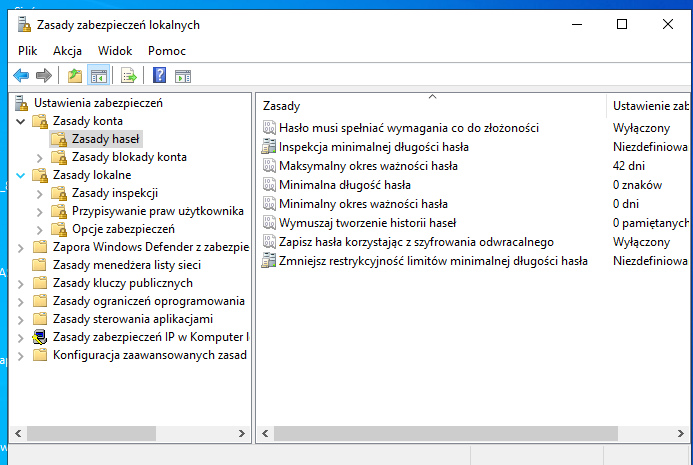
Aby otworzyć to okno trzeba nacisnąć Win + R i wpisać secpol.msc. Za pomocą tej komendy użytkownik z uprawnieniami administratora może dowolnie skonfigurować zasady bezpieczeństwa lokalnego komputera. 

Zasady te podzielono na następujące grupy:

* Zasady konta – do nich zalicza się ustawienia blokady kont oraz zasady haseł
* Zasady lokalne – obejmują zasady inspekcji, opcje zabezpieczeń i ustawienia związane z przypisywaniem praw użytkownikom
* Zasady kluczy publicznych, zawierające ustawienia dotyczące szyfrowania plików
* Zasady ograniczeń oprogramowania, umożliwiające określenie programów, które można uruchamiać na komputerze
* Zasady zabezpieczeń IP – pozwalają zabezpieczyć komunikację sieciową

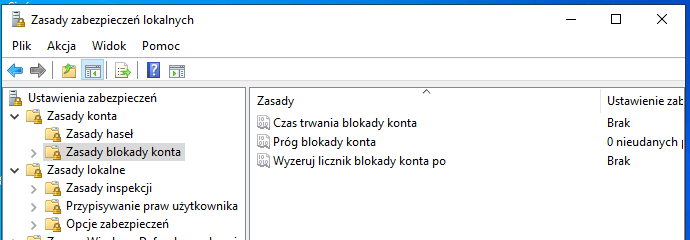
**Możliwości i kompletności zasad zabezpieczeń lokalnych:**

**- Ograniczenia dotyczące haseł użytkowników:**

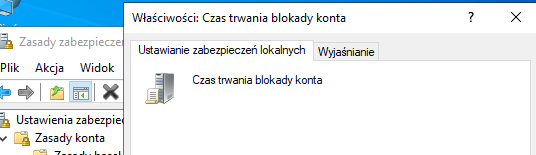


* Wymagania co do złożoności. Włączenie tej opcji pozwala narzucić dodatkowe wymagania na złożonośc hasła.
* Maksymalny okres ważności hasła.
* Minimalna długość hasła
* Minimalny okres ważności hasła.
* Wymuszenie tworzenia historii haseł

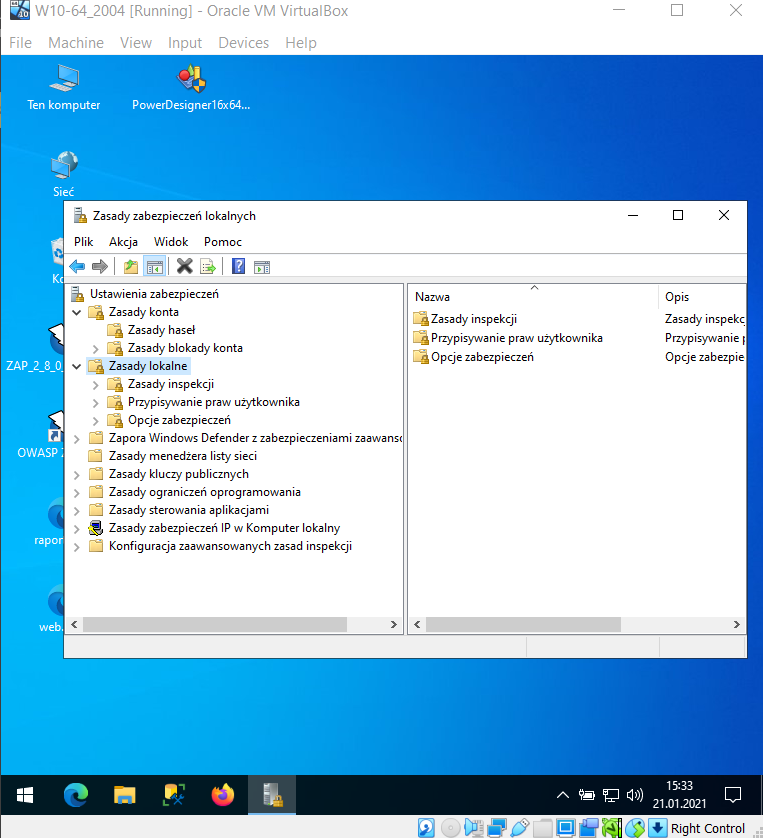
**- Zasady blokady konta**



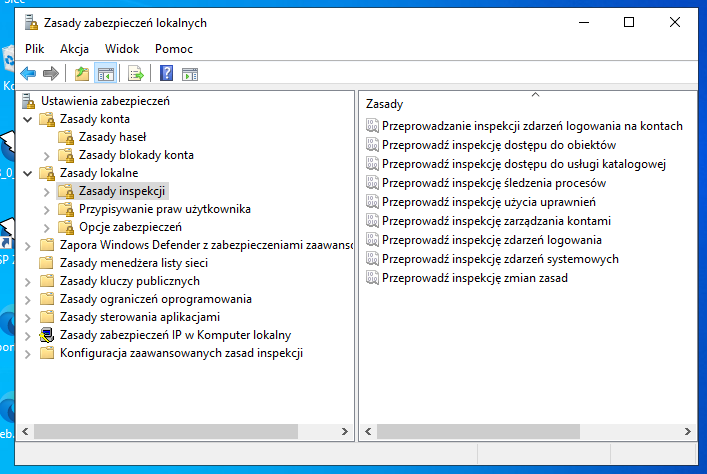
* Czas trwania blokady konta. To ustawienie zabezpieczeń określa liczbę minut, przez jaką konto pozostaje zablokowane, zanim blokada zostanie automatycznie usunięta. Dostępne są wartości przedziału od 0 do 99 999 minut, Jeśli czas trwania blokady konta wynosi 0, konto pozostanie zablokowane do momentu, kiedy administrator sam je odblokuje,



* Próg blokady konta - To ustawienie zabezpieczeń określa liczbę nieudanych prób logowania, która powoduje zablokowanie konta użytkownika. Zablokowanego konta nie można używać do chwili, gdy zostanie ono wyzerowane przez administratora lub gdy upłynie czas blokady. Można ustawić wartość z przedziału od 0 do 999 nieudanych prób logowania. Jeśli zostanie ustawiona wartość 0, konto nigdy nie będzie blokowane. Niepomyślne próby zalogowania do stacji roboczych lub serwerów członkowskich, które zostały zablokowane przez użycie kombinacji klawiszy CTRL+ALT+DELETE lub wygaszaczy chronionych hasłem, nie są traktowane jako nieudane próby logowania.
* Wyzeruj licznik blokady konta po - To ustawienie zabezpieczeń określa liczbę minut, które muszą upłynąć od nieudanej próby logowania, zanim licznik nieudanych prób logowania zostanie wyzerowany i nie będzie wskazywał nieudanych prób logowania. Dostępne są wartości z zakresu od 1 do 99 999 minut. Jeśli jest określona wartość progowa blokady konta, czas wyzerowania musi być krótszy lub taki sam jak Czas trwania blokady konta

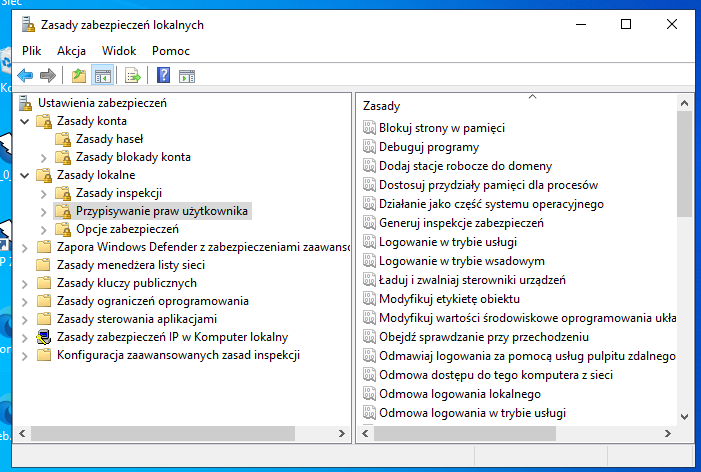


**Opcje zasad lokalnych dzielą się na trzy podfoldery:**

****

* Zasady inspekcji.

Zasady inspekcji pozwalają na inspekcjonowanie konkretnych zdarzeń na komputerze i powiadamianie, gdy zakończą się powodzeniem lub niepowodzeniem. Aby zmienić ustawienia zasady należy nacisnąć prawym przyciskiem myszy na zasadę, otworzyć okno Właściwości i wybrać interesujące nas ustawienia.

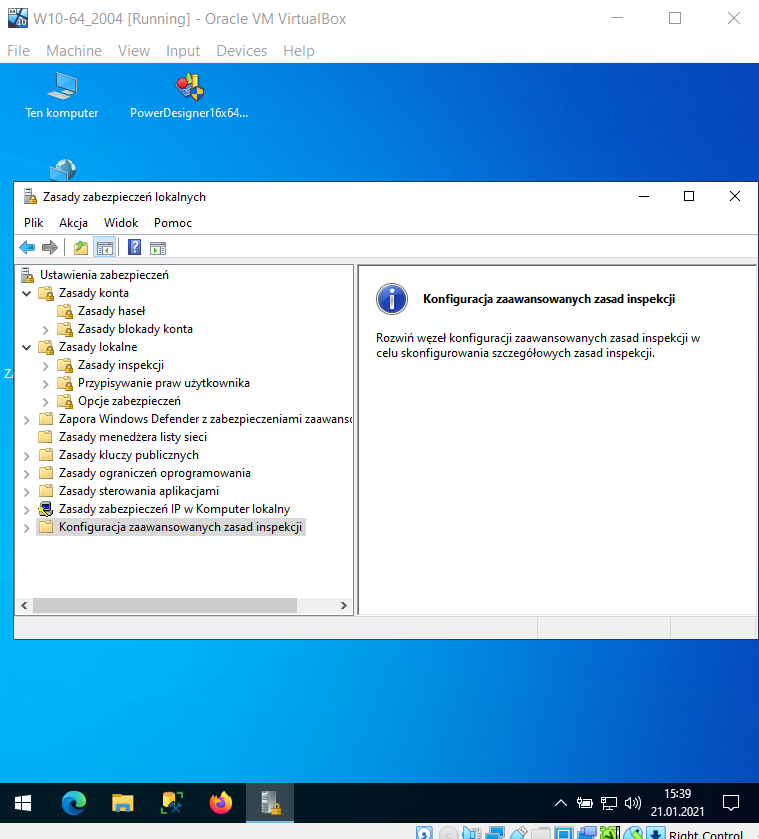


* Przypisywanie praw użytkownika.

Sekcja Przypisywanie praw użytkownika pozwala na nadawanie lub odmawianie określonym użytkownikom lub grupom określonych praw. Aby dodać lub usunąć użytkowników lub grupy z danej zasady należy nacisnąć prawym przyciskiem myszy na zasadę, otworzyć okno Właściwości, a następnie użyć opcji Dodaj użytkownika lub grupę lub Usuń.

* Opcje zabezpieczeń

**Zasady kluczy publicznych**

****

To ustawienie zasad pozwala zezwolić na używanie tej przystawki lub zabronić jej używania.

* Jeśli to ustawienie zasad zostanie włączone, przystawka będzie dozwolona i będzie można ją dodać do programu Microsoft Management Console lub ją uruchomić z poziomu wiersza polecenia jako samodzielną konsolę.

**Zasady Menedżera listy sieci**

Zasady Menedżera listy sieci to ustawienia zabezpieczeń, których można używać do konfigurowania różnych aspektów wyświetlania i wyświetlania sieci na jednym urządzeniu lub na wielu urządzeniach.

Aby skonfigurować zasady Menedżera listy sieci dla jednego urządzenia, można użyć konsoli Microsoft Management Console (MMC) z przystawką Edytor obiektów zasad grupy i edytować zasady komputera lokalnego. Zasady Menedżera list sieci znajdują się w następującej ścieżce w Edytorze obiektów zasad grupy: Konfiguracja komputera | Ustawienia systemu Windows | Ustawienia bezpieczeństwa | Zasady Menedżera list sieci

Aby skonfigurować zasady Menedżera list sieci dla wielu komputerów, na przykład dla wszystkich komputerów domeny w domenie Active Directory, postępuj zgodnie z dokumentacją zasad grupy, aby dowiedzieć się, jak edytować zasady dla wymaganego obiektu. Ścieżka do zasad Menedżera list sieci jest taka sama, jak ścieżka wymieniona powyżej.

**Ocena kompletności zasad zabezpieczeń lokalnych systemu**

Moim zdaniem jest to, że podane grupy zasad są kompletnie satysfakcujące. Czyli użytkownik otrzymuje różne sposoby zabezpieczenia siebie i swego komputera jak w sieci tak i lokalnie.

Zasady ustawień zabezpieczeń służą do zarządzania następującymi aspektami zabezpieczeń: zasadami kont, zasadami lokalnymi, przypisywaniem praw użytkowników, wartościami rejestru, listami kontroli dostępu (ACL) do plików i rejestru, trybami uruchamiania usług i nie tylko.

W ramach strategii zabezpieczeń można tworzyć obiekty zasad grupy z zasadami ustawień zabezpieczeń skonfigurowanymi specjalnie dla różnych ról w organizacji, takich jak kontrolery domeny, serwery plików, serwery członkowskie, klienci itd.

Możesz utworzyć strukturę jednostek organizacyjnych (OU), która grupuje urządzenia według ich ról. Korzystanie z jednostek organizacyjnych to najlepsza metoda rozdzielania określonych wymagań bezpieczeństwa dla różnych ról w sieci. Takie podejście umożliwia również stosowanie niestandardowych szablonów zabezpieczeń do każdej klasy serwerów lub komputerów. Po utworzeniu szablonów zabezpieczeń należy utworzyć nowy obiekt zasad grupy dla każdej jednostki organizacyjnej, a następnie zaimportować szablon zabezpieczeń (plik .inf) do nowego obiektu zasad grupy.

Importowanie szablonu zabezpieczeń do obiektu zasad grupy gwarantuje, że wszystkie konta, do których jest stosowany obiekt zasad grupy, automatycznie otrzymają ustawienia zabezpieczeń szablonu po odświeżeniu ustawień zasad grupy.

**Podsumowanie:**

* Lokalne zasady bezpieczeństwa systemu to zestaw informacji o bezpieczeństwie komputera lokalnego. Informacje o lokalnych zasadach bezpieczeństwa obejmują następujące informacje: Domeny zaufane do uwierzytelniania prób logowania. Które konta użytkowników mogą uzyskiwać dostęp do systemu i jak.