PRZEWODNIK PODSTAWOWYCH ELEMENTÓW BEZPIECZEŃSTWA KOMPUTERÓW PRACUJĄCYCH POD KONTROLĄ SYSTEMU MICROSOFT WINDOWS 7 SP1

Wersja 1.0

OPRACOWANIE POWSTAŁO W RAMACH SECURITY COOPERATION PROGRAM (SCP)

Spis treści

1. Wstęp

Przewodnik Zabezpieczeń systemu Windows 7 SP1 zawiera wybrane i podstawowe instrukcje i rekomendacje, które pomogą ocenić i zweryfikować poziom zabezpieczenia komputerów stacjonarnych i komputerów przenośnych pracujących w grupie roboczej lub pracujących jako samodzielne stanowiska pod kontrolą systemu Windows 7 SP1.

Niniejszy podręcznik stanowi wstęp do zabezpieczenia systemów Windows 7 SP1 i wskazuje w sposób praktyczny, w jaki sposób zweryfikować i skonfigurować podstawowe ustawienia rekomendowane przez firmę Microsoft, zawiera również zalecenia korzystania z wybranych wbudowanych funkcji zabezpieczeń systemu Windows 7 SP1.

2. Automatyczna aktualizacja systemu Windows – usługa Windows Update

Aktualizacja oprogramowania to dowolna aktualizacja, kumulacja aktualizacji, poprawka Service Pack, dodatek Feature Pack, aktualizacja krytyczna, aktualizacja zabezpieczeń lub poprawka, których celem jest ulepszenie lub naprawienie produktu oprogramowania wydanego przez firmę Microsoft. Aktualizacje służą do rozwiązania problemu z produktem lub naprawiają i łatają wykryte luki i podatności na ataki zewnętrzne zwiększając bezpieczeństwo oprogramowania systemu Windows, stanowią kluczowy element bezpieczeństwa każdego systemu komputerowego.

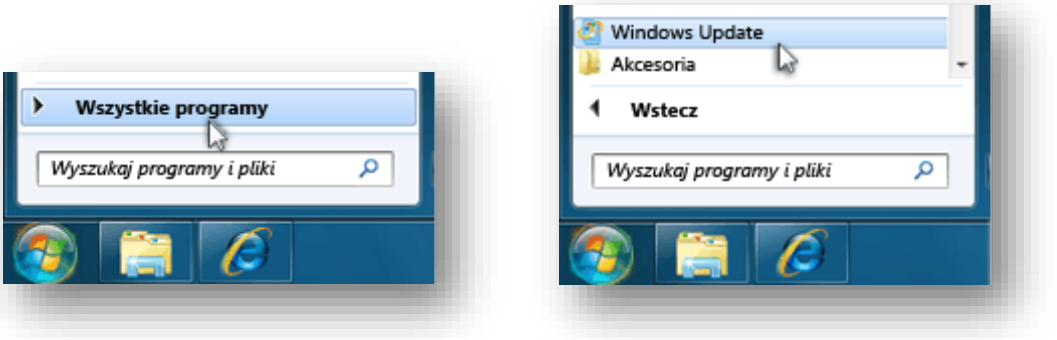
Dzięki automatycznemu aktualizowaniu nie trzeba wyszukiwać aktualizacji w trybie online ani martwić się, że na komputerze może brakować krytycznych poprawek lub sterowników urządzeń dla systemu Windows. Usługa Windows Update automatycznie instaluje ważne aktualizacje natychmiast po ich udostępnieniu. Ponadto można skonfigurować usługę Windows Update do automatycznego instalowania zalecanych aktualizacji lub powiadamiania, że są one dostępne. Można też określić, czy usługa Microsoft Update ma być włączona w celu udostępniania aktualizacji dla innych produktów firmy Microsoft. Aktualizacje opcjonalne, które obejmują pakiety językowe i aktualizacje z witryny Microsoft Update, nie są instalowane automatycznie. Usługa Windows Update nie zainstaluje na komputerze żadnych dodatkowych aplikacji bez zgody Użytkownika ani nie usunie żadnych aplikacji, które już posiada. Więcej informacji na temat usługi Windows Update można uzyskać na stronie - http://windows.microsoft.com/pl-PL/windows7/products/features/windows-update[1]

Usługę Windows Update należy skonfigurować w taki sposób, aby najnowsze aktualizacje były pobierane i instalowane w komputerze automatycznie.

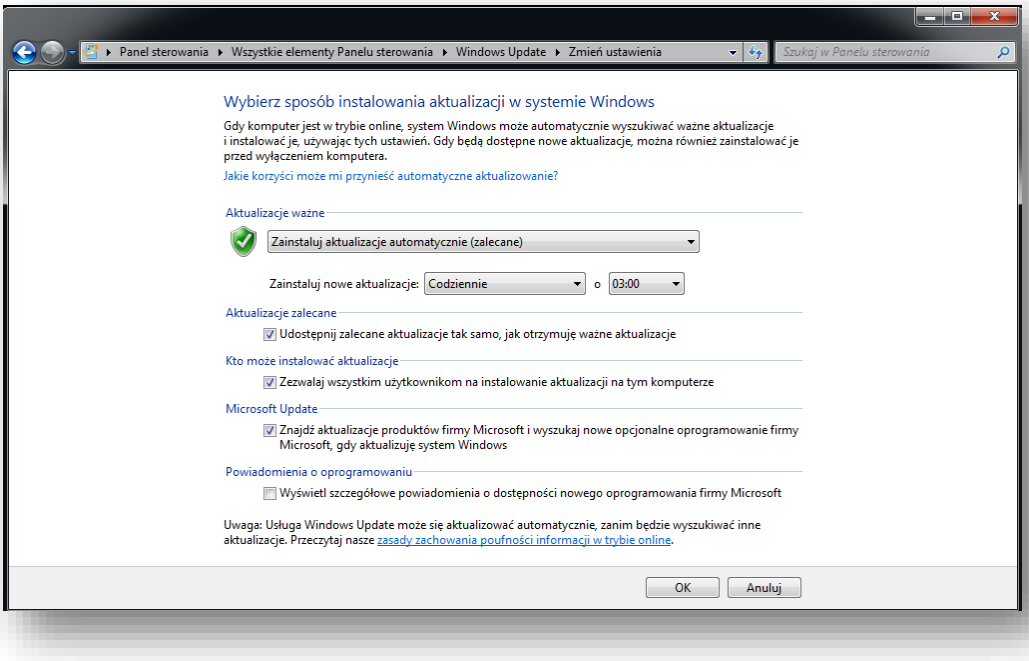
Aby zweryfikować ustawienia lub włączyć aktualizowanie automatyczne systemu Windows należy:

1. Otwórz Usługę **Windows Update** w Panelu Sterowania lub kliknij przycisk **Start**, wskaż polecenie Wszystkie programy, a następnie kliknij polecenie Windows Update

[1] http://windows.microsoft.com/pl-PL/windows7/products/features/windows-update



2. Następnie należy wybrać pozycję **Zmień Ustawienia**, i ustawić rekomendowane ustawienia (przedstawione na poniższym rysunku) i kliknąć przycisk **OK**. Do potwierdzenia wyboru może być wymagane podanie hasła administratora.



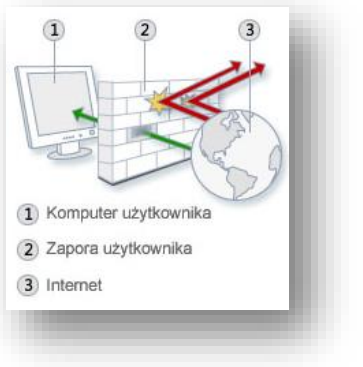
Rys. 2.1 - Widok rekomendowanych ustawień dla usługi Windows Update

3. Zapora systemu Windows

Zapora (ang. firewall) to oprogramowanie lub urządzenie sprawdzające informacje pochodzące z Internetu lub sieci. Zapora blokuje te informacje lub zezwala na ich przesłanie do komputera w zależności od ustawień.

Zapora może uniemożliwić uzyskanie dostępu do komputera przez hakerów lub złośliwe oprogramowanie (takie jak robaki) za pośrednictwem sieci lub Internetu. Zapora może też pomóc w uniemożliwieniu komputerowi wysyłania złośliwego oprogramowania do innych komputerów.

Podobnie jak ceglana ściana może stanowić barierę fizyczną, zapora tworzy barierę między Internetem a komputerem. Sposób działania zapory przedstawiono na poniższej ilustracji.



Rys. 3.1. Sposób działania zapory

Zapora osobista jest krytycznym elementem obrony przed wieloma rodzajami oprogramowania złośliwego. Tak jak w przypadku poprzednich wersji systemu Windows od czasu wydania Windows XP SP2 zapora osobista jest domyślnie włączona w systemie Windows 7 SP1, w celu zapewnienia ochrony komputera użytkownika od momentu jak tylko system operacyjny jest gotowy do pracy.

Zapora osobista w systemie Windows 7 SP1 wykorzystuje ten sam mechanizm ochrony jak w przypadku Windows Vista włączając w to filtrowanie ruchu wchodzącego i wychodzącego dla zapewnienia ochrony poprzez ograniczenie dostępu sieciowego do zasobów systemu operacyjnego.

Rekomendowane domyślne ustawienia zapory:

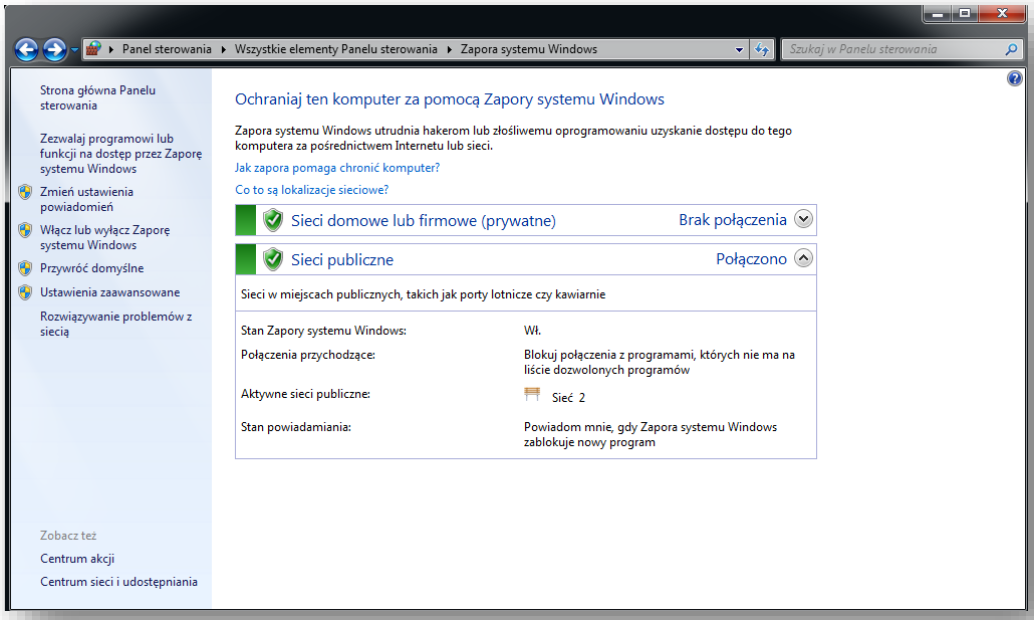
- Zapora włączona.
- Zapora włączona dla wszystkich lokalizacji sieciowych (Dom lub praca, Miejsce publiczne lub Domena).
- Zapora włączona dla wszystkich połączeń sieciowych.
- Zapora blokuje wszystkie połączenia przychodzące z wyjątkiem tych, które określono jako dozwolone.

Więcej informacji na temat **Zapory sytemu Windows** można uzyskać odwiedzając stronę - http://windows.microsoft.com/pl-PL/windows7/products/features/windows-firewall[2] .
Szczegółowe informacje na temat **Zapory systemu Windows z zaawansowanymi zabezpieczeniami** można uzyskać na stronie http://technet.microsoft.com/pl-pl/library/cc754274(v=ws.10).aspx[3]

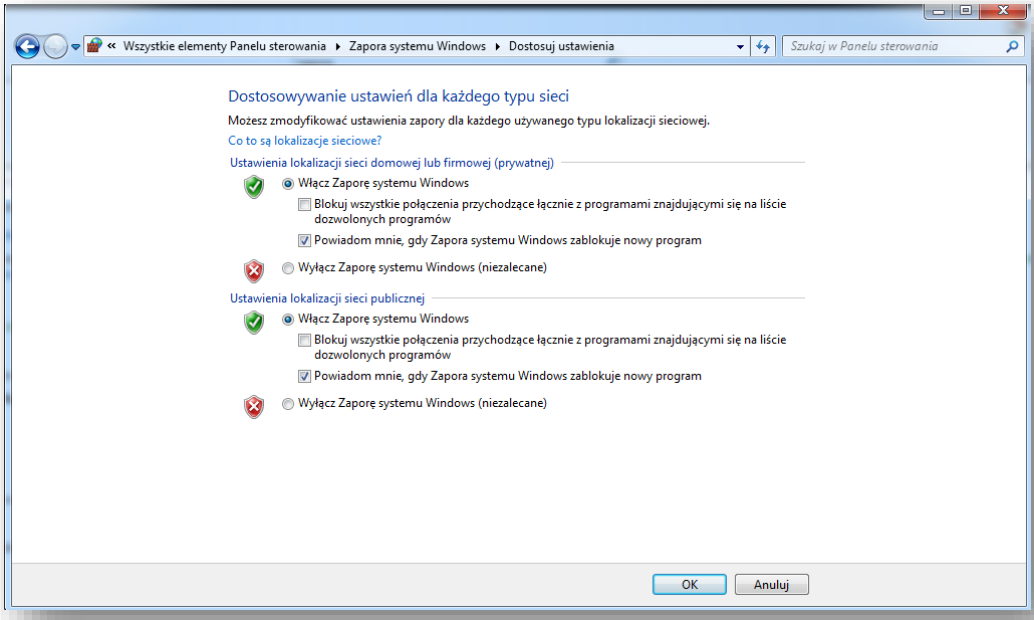
Aby zweryfikować ustawienia lub włączyć zaporę systemu Windows należy:

1. Otwórz Usługę **Zapora systemu Windows** w Panelu Sterowania lub kliknij przycisk **Start** wpisz w oknie „Wyszukaj programy i pliki”: **Zapora systemu Windows**, a następnie kliknij polecenie **Zapora systemu Windows.**

[2] http://windows.microsoft.com/pl-PL/windows7/products/features/windows-firewall
[3] http://technet.microsoft.com/pl-pl/library/cc754274(v=ws.10).aspx



2. Następnie należy wybrać pozycję **Włącz lub Wyłącz Zaporę systemu Windows**, i ustawić rekomendowane ustawienia (przedstawione na poniższym rysunku) i kliknąć przycisk **OK**. Do potwierdzenia wyboru może być wymagane podanie hasła administratora.



4. Oprogramowanie chroniące przed złośliwym oprogramowaniem Windows Defender i oprogramowanie antywirusowe

Usługa Windows Defender jest oprogramowaniem antyszpiegowskim dołączonym do systemu Windows 7 SP1 i uruchamianym automatycznie po włączeniu systemu. Używanie oprogramowania antyszpiegowskiego może pomóc w zapewnieniu ochrony komputera przed programami szpiegującymi i innymi potencjalnie niechcianymi aplikacjami. Program szpiegujący może zostać zainstalowany na komputerze bez wiedzy użytkownika podczas każdego połączenia z Internetem, a ponadto komputer może zostać nim zainfekowany podczas instalowania niektórych programów przy użyciu nośników wymiennych. Usługa Windows Defender oferuje dwa sposoby ochrony komputera przed zainfekowaniem programami szpiegującymi:

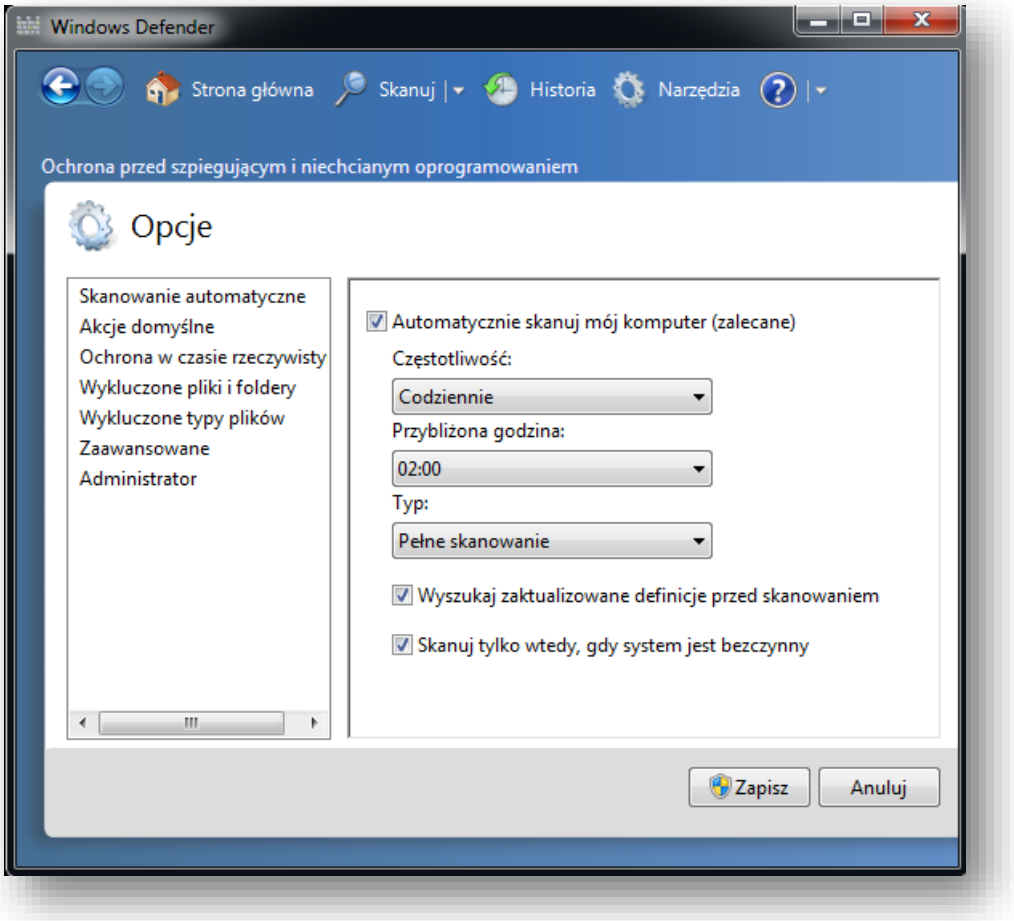
- Ochrona w czasie rzeczywistym. Usługa Windows Defender alarmuje użytkownika w przypadku próby zainstalowania lub uruchomienia programu szpiegującego na komputerze. Użytkownik jest powiadamiany również wówczas, gdy programy próbują zmieniać ważne ustawienia systemu Windows.
- Opcje skanowania. Przy użyciu usługi Windows Defender można skanować komputer w poszukiwaniu programów szpiegujących, które mogły zostać zainstalowane na komputerze. Można także ustalać harmonogram regularnego skanowania oraz automatycznie usuwać dowolne elementy wykryte podczas skanowania.

Na rys. 4.1 przedstawiono rekomendowane ustawienia dla usługi Windows Defender dla komputerów pracujących w systemie Windows 7 SP1.

Aby zweryfikować ustawienia lub ustawić rekomendowane ustawienia Windows Defender należy:

1. Kliknij przycisk **Start**, wpisz w oknie „Wyszukaj programy i pliki”: **Windows Defender**, a następnie kliknij polecenie **Windows Defender.**

2. Następnie należy wybrać pozycję **Narzędzia**, następnie **Opcje** i ustawić rekomendowane ustawienia (przedstawione na poniższym rysunku) i kliknąć przycisk **OK**. Do potwierdzenia wyboru może być wymagane podanie hasła administratora.



Rys. 4.1 – Widok okna ustawień rekomendowanych dla usługi Windows Defender

Oprócz ochrony antyszpiegowskiej zapewnionej przez Windows Defender, wysoce rekomendowana jest instalacja **oprogramowania antywirusowego**, który w dodatkowy sposób rozszerzy ochronę antyszpiegowską i zapewni ochronę przed wirusami, trojanami, robakami oraz innymi zagrożeniami ze strony oprogramowania złośliwego. Na przykład program **Microsoft System Center 2012 Endpoint Protection**[4] zapewnia uniwersalną ochronę przed oprogramowaniem złośliwym, stosowaną na komputerach przenośnych, stacjonarnych oraz serwerach.

Rekomendowane minimalne funkcje oprogramowania antywirusowego:

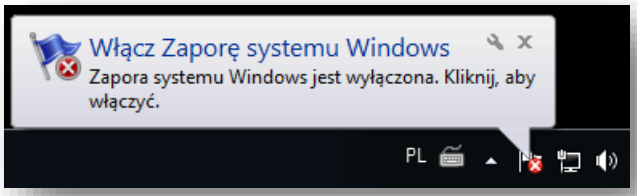
- Ochrona w czasie rzeczywistym
- Automatyczna aktualizacja definicji i sygnatur
- Zaplanowane codzienne skanowanie systemu Windows 7 pod kątem złośliwego oprogramowania i wirusów

Więcej informacji na temat programu Windows Defender można uzyskać na stronie http://windows.microsoft.com/pl-PL/windows7/Using-Windows-Defender

[4] http://www.microsoft.com/en-us/server-cloud/system-center/endpoint-protection-2012.aspx

5. Konsola Centrum Akcji

Centrum akcji to centralne miejsce, gdzie użytkownik może wyświetlać alerty i podejmować działania mające na celu zapewnienie sprawnego funkcjonowania systemu Windows. W Centrum Akcji wyświetlana jest lista ważnych komunikatów dotyczących ustawień zabezpieczeń oraz konserwacji, które wymagają uwagi użytkownika. Kiedy stan monitorowanych elementów się zmienia (na przykład oprogramowanie antywirusowe staje się nieaktualne), Centrum akcji wyświetla komunikat w obszarze powiadomień na pasku narzędzi. Zmienia się też kolor stanu elementu w Centrum akcji w celu odzwierciedlenia ważności komunikatu oraz wyświetlane są informacje o zalecanej akcji.



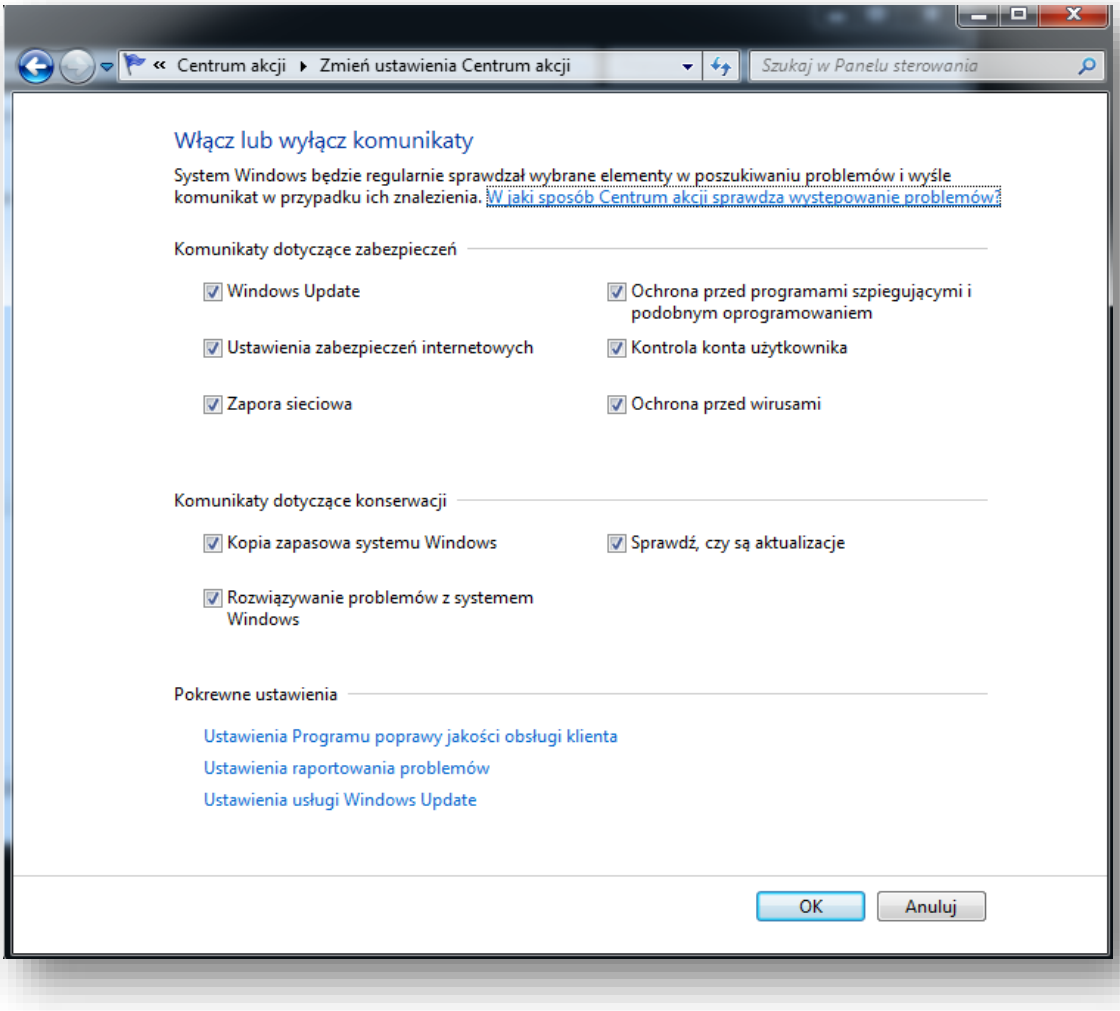
Rys. 5.1. – Przykładowy komunikat o wyłączonej zaporze komunikat w obszarze powiadomień na pasku narzędzi

Zakres wyświetlanych komunikatów, które mogą być wyłączone lub włączone został przedstawiony w ustawieniach konsoli **Zmień ustawienia Centrum Akcji** na rysunku poniżej.

Aby zweryfikować ustawienia wyświetlanych komunikatów Centrum Akcji należy:

1. Otwórz Usługę **Centrum Akcji** w Panelu Sterowania lub kliknij przycisk **Start**, wpisz w oknie „Wyszukaj programy i pliki”: **Centrum akcji**, a następnie kliknij polecenie **Centrum akcji.**

2. Następnie należy wybrać pozycję **Zmień ustawienia Centrum akcji**, i ustawić rekomendowane ustawienia (przedstawione na poniższym rysunku) i kliknąć przycisk **OK**.



Rys. 5.2 - Rekomendowane ustawienia wyświetlanych komunikatów **Centrum Akcji**

Zaleca się **włączenie** wszystkich komunikatów dotyczących zabezpieczeń i konserwacji.

Więcej informacji na temat Centrum akcji w systemie Windows 7 można uzyskać na stronie http://windows.microsoft.com/pl-PL/windows7/products/features/action-center[5]

6. Silne i bezpieczne hasła

Co to jest bezpieczne hasło?

Bezpieczne hasło to jest hasło łatwe do zapamiętania dla użytkownika, a dla innych trudne do odgadnięcia, hasło powinno zawierać odpowiednia liczbę znaków i powinno być złożone.

Jakie hasło nie jest bezpieczne?

- zbyt krótkie - im więcej znaków w haśle tym więcej możliwości kombinacji. Czas potrzebny do złamania hasła zdecydowanie się wydłuża przy dłuższym haśle.

[5] http://windows.microsoft.com/pl-PL/windows7/products/features/action-center

- zawierające znaki tylko jednego rodzaju, np. tylko małe litery. Użycie znaków spośród różnych grup znaków daje możliwości ich skomplikowania i zwiększenia złożoności
- słownikowe, czyli składające się wyłącznie (lub niemal wyłącznie) z nazw własnych, np: krzysztof, krzys12, auto, gruszka, etc. Słów zapisanych od tyłu, częstych błędów ortograficznych i skrótów
- zawierające dane osobiste: imię, data urodzenia, numer dowodu, PESEL lub podobne dane.
- nie zmieniane przez dłuższy czas (np. od ponad 3 miesięcy).

Więcej informacji na temat tworzenia silnych haseł można uzyskać pod adresem http://windows.microsoft.com/pl-PL/windows7/Tips-for-creating-strong-passwords-and-passphrases[6] oraz http://www.microsoft.com/pl-pl/security/online-privacy/passwords-create.aspx[7]

Kluczem do bezpieczeństwa hasła jest jego długość, złożoność i częsta zmiana.

Głównym aspektem bezpieczeństwa każdego systemu jest bezpieczne hasło oraz dobrze dobrana i ustalona polityka dotycząca haseł. Takie elementy jak złożoność haseł, cykliczność zmiany czy świadomość ich przechowywania składają się na ogólną politykę bezpieczeństwa stanowiąc kluczowy aspekt całości. Ustawienia dotyczące polityki haseł znajdują się w zbiorze **Zasady haseł.**

W hasłach mogą być stosowane znaki z czterech grup:

- Wielkie litery
- Małe litery
- Cyfry
- Znaki specjalne

Złożoność hasła (w kontekście zasady „Hasło musi spełniać wymagania co do złożoności") oznacza, że są w nim wykorzystane znaki z co najmniej **trzech** powyższych grup.

Zapewnienie zmiany haseł przez użytkowników tylko w ściśle określonym momencie wymaga ustalenia zasad dotyczących minimalnego i maksymalnego wieku hasła. Dla zasad „Minimalny okres ważności hasła" oraz „Maksymalny okres ważności hasła" obowiązują poniższe zależności.

- Minimalny okres ważności hasła
  Wartość minimalna – 0 – oznacza, że hasło może być zmieniane w dowolnym momencie.
  Wartość maksymalna – 998 – oznacza, że hasło może być zmienione po upływie 998 dni.
- Maksymalny okres ważności hasła
  Wartość minimalna – 0 – oznacza, że ważność hasła nigdy nie wygasa.
  Wartość maksymalna – 999 – oznacza, że ważność hasła wygasa po 999 dniach.

Między zasadami „Minimalny okres ważności hasła" a „Maksymalny okres ważności hasła" obowiązuje zależność:

Maksymalny okres ważności hasła = Minimalny okres ważności hasła + 1

[6] http://windows.microsoft.com/pl-PL/windows7/Tips-for-creating-strong-passwords-and-passphrases
[7] http://www.microsoft.com/pl-pl/security/online-privacy/passwords-create.aspx

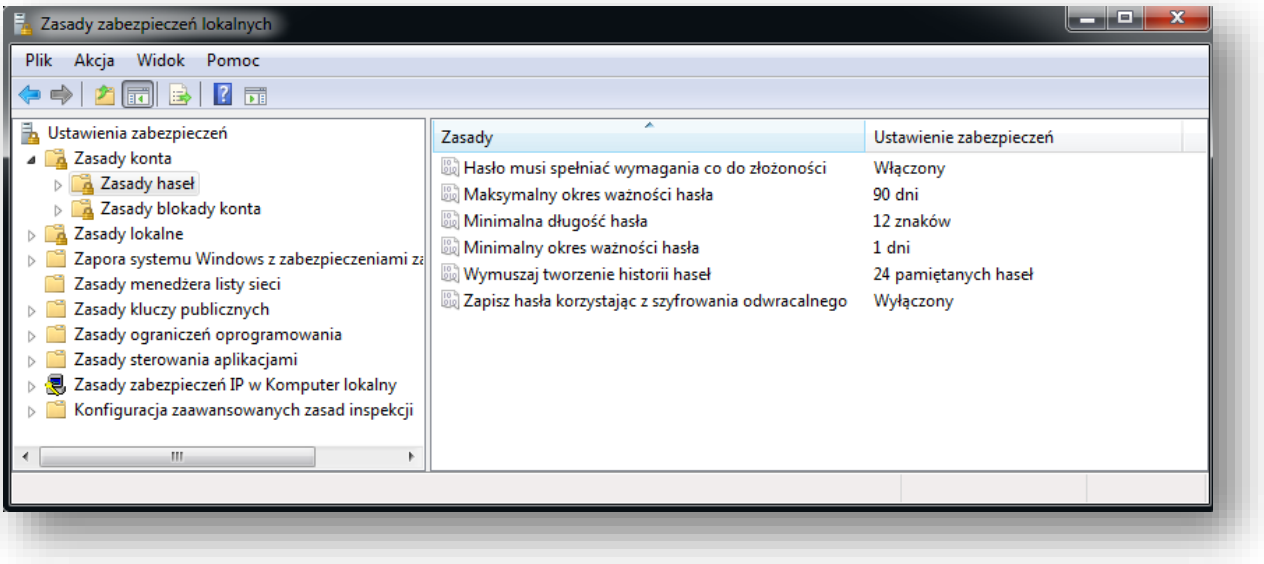
Zasady blokady konta zapewniają ochronę przed próbami odgadnięcia haseł użytkowników. Realizowane to jest przez zliczanie błędnych prób logowania i wykonanie określonej akcji związanej ze stanem konta użytkownika.

Rekomendowana konfiguracja i weryfikacja ustawień dotyczących polityki haseł dla zbioru **Zasady haseł** oraz **Zasady blokady konta**

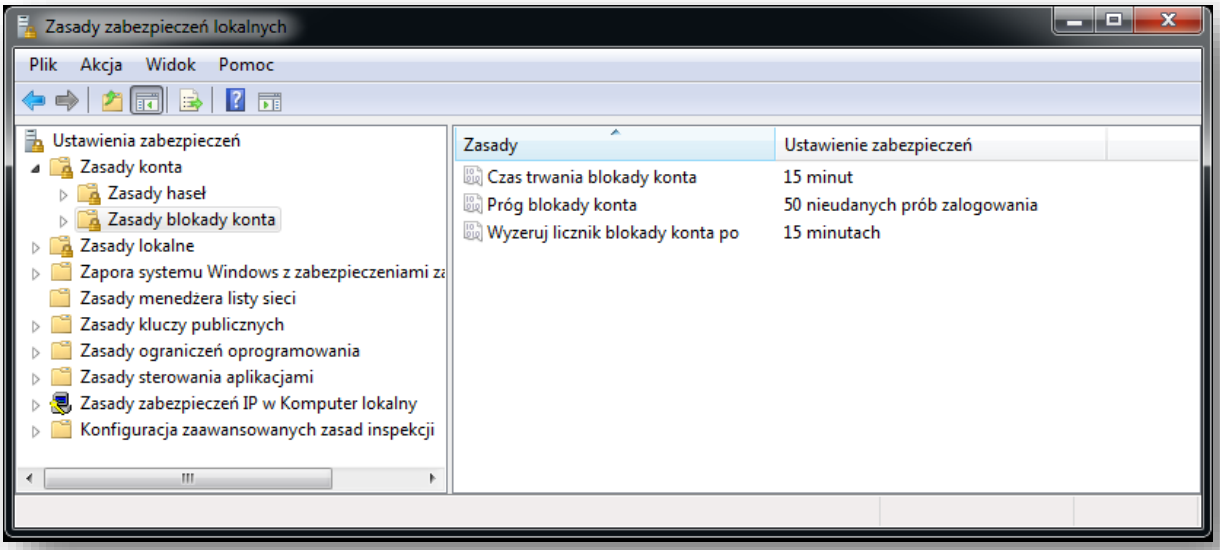
Zasady haseł można ustawić lokalnie na komputerze z zastosowaniem konsoli **Zasady Zabezpieczeń Lokalnych.**

Aby zweryfikować ustawienia lub skonfigurować ustawienia Zasady Konta należy:

1. Otwórz przystawkę **Zasady zabezpieczeń lokalnych**, kliknij przycisk **Start**, wskaż polecenie **Ustawienia**, kliknij polecenie **Panel sterowania**, kliknij dwukrotnie ikonę **Narzędzia administracyjne**, a następnie kliknij dwukrotnie ikonę **Zasady zabezpieczeń lokalnych**.
2. Następnie należy ustawić Zasady konta zgodnie z przedstawionymi poniżej rysunkami.



Rys. 6.1 - Rekomendowane ustawienia dla zbioru zasady haseł



Rys. 6.2 Rekomendowane ustawienia dla zbioru zasady blokady konta

7. Korzystanie ze standardowego konta użytkownika

W systemie Windows 7 SP1 istnieją trzy różne typy kont:

- **Standardowe**
- **Administrator**
- **Gość**

Każdy typ konta przyznaje użytkownikowi różne poziomy kontroli nad komputerem. Konto standardowe to konto do codziennego korzystania z komputera. Konto administratora zapewnia najwyższy poziom kontroli nad komputerem, należy z niego korzystać tylko wtedy, gdy jest to konieczne. Konto gościa jest przeznaczone głównie dla osób potrzebujących tymczasowego dostępu do komputera.

Standardowe konto użytkownika umożliwia korzystanie z większości funkcji komputera. Wprowadzenie zmian dotyczących innych użytkowników lub zabezpieczeń komputera wymaga jednak zgody administratora.

Użytkownik korzystający z konta standardowego może używać większości programów zainstalowanych na komputerze, nie może jednak instalować oprogramowania ani sprzętu, usuwać plików niezbędnych do pracy komputera ani zmieniać ustawień dotyczących innych użytkowników tego komputera. W przypadku korzystania z konta standardowego niektóre programy mogą wymagać podania hasła administratora w celu wykonania określonych zadań.

Dlaczego należy korzystać ze standardowego konta użytkownika zamiast konta administratora?

Konto standardowe może ułatwić ochronę komputera, uniemożliwiając użytkownikom wprowadzanie zmian dotyczących wszystkich użytkowników komputera.

Konto standardowe pozwala na tworzenie i zapis plików, ale nie w kluczowych dla systemu Windows katalogach, jak Windows czy Program Files. Pozwala również na zmianę ustawień systemu, ale tylko tych, które dotyczą danego konta, a nie całego systemu.

Oprogramowanie złośliwe, takie jak wirusy czy programy szpiegowskie, które zwykle wymagają wyższych uprawnień w celu instalacji oraz poprawnego działania oraz próbują odwołać się do globalnych funkcji i konfiguracji systemu, dostępnych tylko z poziomu konta administratora, po prostu nie zadziałają na koncie standardowym.

Atakujący, któremu uda się włamać do komputera uruchomionego na koncie standardowym, nie będzie miał dostępu do dokumentów i plików innych użytkowników. **Zaleca się utworzenie konta standardowego dla każdego użytkownika korzystającego z komputera.**

8. Mechanizm Kontrola Konta Użytkownika (User Account Control – UAC)

System Windows Vista wprowadził mechanizm kontroli konta użytkownika (ang. User Account Control – UAC) w celu ułatwienia wykorzystania konta użytkownika, który nie posiada uprawnień administracyjnych. Gdy na komputerze mają zostać dokonane zmiany wymagające uprawnień na poziomie administratora, funkcja Kontrola Konta Użytkownika powiadamia o tym.

W systemie Windows 7 SP1 można ustawić odpowiedni tryb i częstotliwość powiadamiania użytkownika. Poniżej przedstawiono cztery podstawowe poziomy powiadomień, które można odpowiednio skonfigurować w ustawieniach UAC w Centrum Akcji.

Ustawienie	Opis	Wpływ na bezpieczeństwo
Powiadamiaj zawsze	Użytkownik będzie powiadamiany przed wprowadzeniem przez programy zmian na komputerze lub w systemie Windows wymagających uprawnień administratora. Gdy zostanie wyświetlone powiadomienie, pulpit zostanie przyciemniony, a użytkownik będzie musieć zaakceptować lub odrzucić żądanie w oknie dialogowym funkcji Kontrola konta użytkownika, zanim będzie można zrobić na komputerze cokolwiek innego. Przyciemnienie pulpitu jest nazywane bezpiecznym pulpitem, ponieważ inne programy nie mogą działać, gdy pulpit jest przyciemniony.	Jest to najbezpieczniejsze ustawienie. Po wyświetleniu powiadomienia użytkownik powinien starannie przeczytać zawartość każdego z okien dialogowych, nim zezwoli na wprowadzenie zmian na komputerze.
Powiadamiaj mnie tylko wtedy, gdy programy próbują wprowadzać zmiany na komputerze –	Użytkownik będzie powiadamiany przed wprowadzeniem przez programy zmian na komputerze wymagających uprawnień administratora. Użytkownik nie będzie powiadamiany, gdy sam będzie wprowadzać zmiany w ustawieniach systemu Windows wymagające uprawnień administratora. Użytkownik będzie powiadamiany, gdy program spoza systemu Windows będzie próbował wprowadzić zmiany w ustawieniach systemu Windows.	Użytkownik będzie powiadamiany przed wprowadzeniem przez programy zmian na komputerze wymagających uprawnień administratora. Użytkownik nie będzie powiadamiany, gdy sam będzie wprowadzać zmiany w ustawieniach systemu Windows wymagające uprawnień administratora. Użytkownik będzie powiadamiany, gdy program spoza systemu Windows będzie próbował wprowadzić zmiany w ustawieniach systemu Windows. **Ustawienie domyślne w systemie Windows 7 SP1**

Powiadamiaj mnie tylko wtedy, gdy programy próbują wprowadzać zmiany na komputerze (nie przyciemniaj pulpitu)	Użytkownik będzie powiadamiany przed wprowadzeniem przez programy zmian na komputerze wymagających uprawnień administratora. Użytkownik nie będzie powiadamiany, gdy sam będzie wprowadzać zmiany w ustawieniach systemu Windows wymagające uprawnień administratora. Użytkownik będzie powiadamiany, gdy program spoza systemu Windows będzie próbował wprowadzić zmiany w ustawieniach systemu Windows.	To ustawienie jest identyczne jak „Powiadamiaj mnie tylko wtedy, gdy programy próbują wprowadzać zmiany na komputerze”, ale powiadomienia nie są wyświetlane na bezpiecznym pulpicie. Ponieważ przy tym ustawieniu okno dialogowe funkcji Kontrola konta użytkownika nie znajduje się na bezpiecznym pulpicie, inne programy mogą wpływać na wygląd tego okna. Jest to małe zagrożenie dla bezpieczeństwa, jeśli złośliwy program już działa w komputerze.
Nie powiadamiaj nigdy	Użytkownik nie będzie powiadamiany przed wprowadzeniem jakichkolwiek zmian na komputerze. Jeśli użytkownik jest zalogowany jako administrator, programy mogą bez jego wiedzy wprowadzać zmiany na komputerze. Jeśli użytkownik jest zalogowany jako użytkownik standardowy, wszelkie zmiany wymagające uprawnień administratora zostaną automatycznie odrzucone. W przypadku wybrania tego ustawienia będzie konieczne ponowne uruchomienie komputera w celu ukończenia procesu wyłączania funkcji Kontrola konta użytkownika. Po wyłączeniu funkcji Kontrola konta użytkownika użytkownicy logujący się jako administrator zawsze będą mieć uprawnienia administratora.	Użytkownik nie będzie powiadamiany przed wprowadzeniem jakichkolwiek zmian na komputerze. Jeśli użytkownik jest zalogowany jako administrator, programy mogą bez jego wiedzy wprowadzać zmiany na komputerze. Jeśli użytkownik jest zalogowany jako użytkownik standardowy, wszelkie zmiany wymagające uprawnień administratora zostaną automatycznie odrzucone. W przypadku wybrania tego ustawienia będzie konieczne ponowne uruchomienie komputera w celu ukończenia procesu wyłączania funkcji Kontrola konta użytkownika. Po wyłączeniu funkcji Kontrola konta użytkownika użytkownicy logujący się jako administrator zawsze będą mieć uprawnienia administratora. **Ustawienie niezalecane.**

Tabela 8.1 - Opis ustawień funkcji Kontrola konta użytkownika

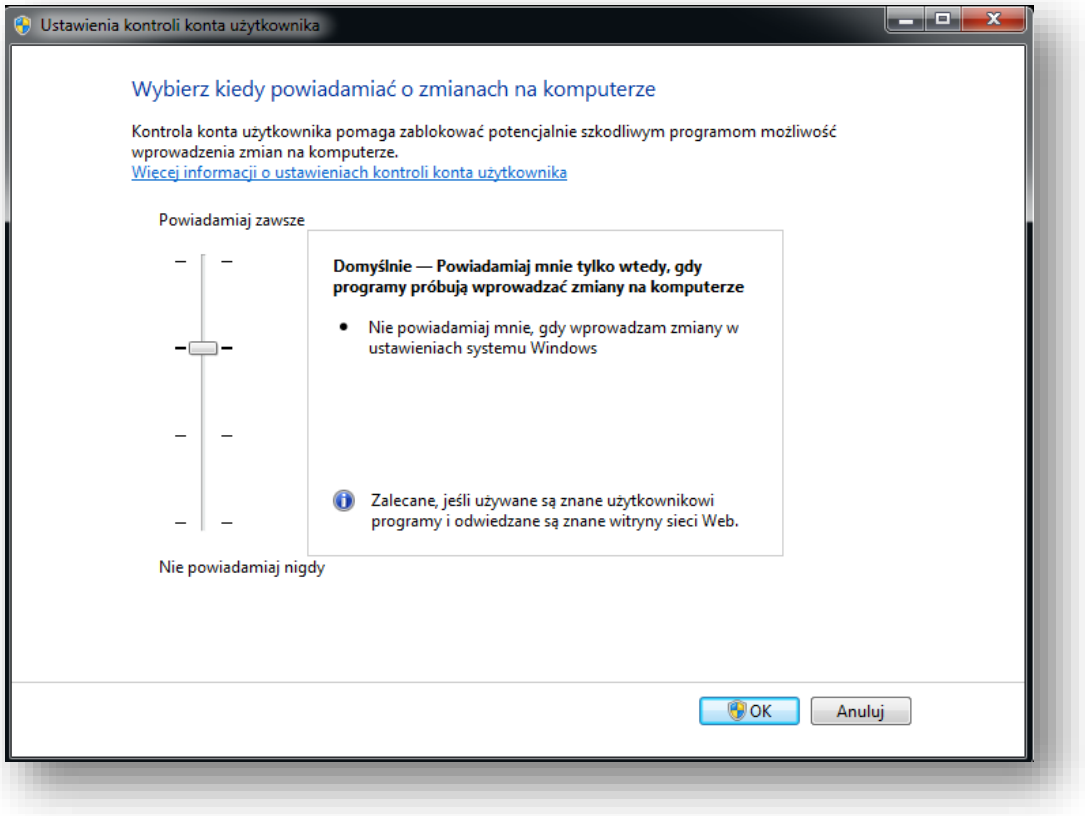
W momencie wprowadzenia technologii UAC, zbyt częste powiadomienia użytkownika systemu, powodowało, że większość użytkowników wyłączyło to ustawienie, zmniejszając w ten sposób poziom bezpieczeństwa komputera. W systemie Windows 7 SP1, liczba pytań o podniesienie poświadczeń została obniżona, tak, aby użytkownik mógł wykonywać więcej zadań, jako standardowy użytkownik.

Rekomendowanym minimalnym ustawieniem UAC jest domyślny poziom **Powiadamiaj mnie tylko wtedy, gdy programy próbują wprowadzać zmiany na komputerze,** ale należy rozważyć ustawienie poziomu **Powiadamiaj zawsze** w środowiskach gdzie użytkownicy komputerów klienckich często podłączają się i korzystają z sieci publicznych lub kiedy wymagany jest wysoki poziom bezpieczeństwa. Zastosowanie pozostałych mniej bezpiecznych poziomów zwiększa prawdopodobieństwo dokonania nieautoryzowanych zmian w komputerze przez oprogramowanie złośliwe.

Aby zweryfikować Ustawienia kontroli konta użytkownika należy:

1. Otwórz Usługę **Centrum Akcji** w Panelu Sterowania lub kliknij przycisk **Start**, wpisz w oknie „Wyszukaj programy i pliki”: **Centrum akcji**, a następnie kliknij polecenie **Centrum akcji.**

2. Następnie należy wybrać pozycję **Zmień ustawienia funkcji Kontrola konta użytkownika**, i ustawić rekomendowane ustawienia za pomocą suwaka (przedstawione na poniższym rysunku) i kliknąć przycisk **OK**.



Rys. 8.1 Rekomendowane ustawienia kontroli konta użytkownika (UAC)

Więcej informacji na temat zagadnienia Kontrola konta użytkownika (UAC) można uzyskać na stronie http://windows.microsoft.com/pl-PL/windows7/products/features/user-account-control[8] a dodatkowo bardzo szczegółowo można zapoznać się z działaniem mechanizmu Kontrola konta użytkownika (UAC) a artykule „Kontrola konta użytkownika Windows 7 od środka" dostępnym pod adresem http://technet.microsoft.com/pl-pl/library/kontrola-konta-uzytkownika-windows-7-od-srodka.aspx [9]

9. Funkcje zabezpieczeń i prywatności w programie Internet Explorer 9

Przeglądarka internetowa stanowi główne źródło zagrożenia dla bezpieczeństwa komputera takie jak: złośliwe witryny, złośliwe skrypty, skrypty, które zwracają IFRAME'y do zainfekowanych witryn oraz złośliwe strony lub pliki. Z jednej strony przeglądarki są głównym narzędziem pracy podczas korzystania z internetu a z drugiej coraz częściej posiadają mechanizmy chroniące użytkownika podczas przeglądania i korzystania z zasobów internetu. Firma Microsoft rekomenduje zainstalowanie i korzystanie z **najnowszej przeglądarki Internet Explorer.**

[8] http://windows.microsoft.com/pl-PL/windows7/products/features/user-account-control
[9] http://technet.microsoft.com/pl-pl/library/kontrola-konta-uzytkownika-windows-7-od-srodka.aspx

Program Microsoft Internet Explorer 9 zawiera następujące wybrane funkcje zabezpieczeń, które chronią użytkownika przed zagrożeniami ze strony oprogramowania złośliwego podczas korzystania z internetu:

- **Filtrowanie formantów ActiveX**, czyli blokowanie formantów ActiveX wszystkich witryn z możliwością zezwolenia na korzystanie z nich tylko zaufanym witrynom.

Formanty ActiveX i dodatki do przeglądarki sieci web to małe programy umożliwiające wyświetlanie zawartości, na przykład wideo, w witrynach sieci web. Mogą one być wykorzystane także do zbierania informacji z komputera, uszkadzania danych na komputerze, instalowania oprogramowania na komputerze bez zgody użytkownika lub przejęcia przez inną osobę zdalnej kontroli nad komputerem.

Aby włączyć filtrowanie formantów ActiveX

1. Otwórz program Internet Explorer, klikając przycisk **Start**. W polu wyszukiwania wpisz tekst **Internet Explorer**, a następnie na liście wyników kliknij pozycję **Internet Explorer**.
2. Kliknij przycisk **Narzędzia**, wskaż polecenie **Bezpieczeństwo**, a następnie kliknij polecenie **Filtrowanie formantów ActiveX**.

- **Wyróżnianie domeny** wyraźnie pokazujące prawdziwych adresów sieci web w odwiedzanych witrynach. Pozwala to unikać witryn sieci web, które używają mylących adresów w celu wprowadzenia użytkownika w błąd, jak witryny wyłudzające informacje. Prawdziwa odwiedzana domena jest wyróżniona na pasku adresu.

- **Filtr SmartScreen** ułatwiający ochronę przed atakami polegającymi na wyłudzaniu informacji w sieci, oszustwami oraz fałszywymi lub złośliwymi witrynami sieci web. Ponadto filtr ten skanuje pobierane pliki i ostrzega, jeśli mogą one być kodem typ malware (złośliwym oprogramowaniem).

Filtr SmartScreen pomaga chronić komputer na trzy sposoby:

- ✓ Podczas przeglądania sieci web analizuje strony sieci web i określa, czy mają one jakiekolwiek cechy charakterystyczne dla podejrzanych stron. W przypadku znalezienia podejrzanych stron sieci web filtr SmartScreen wyświetla komunikat, umożliwiając użytkownikowi wyrażenie opinii i radząc zachować ostrożność.
- ✓ Filtr SmartScreen sprawdza odwiedzane witryny według dynamicznej listy zgłaszanych witryn wyłudzających informacje i zawierających złośliwe oprogramowanie. Jeśli filtr SmartScreen znajdzie witrynę na tej liście, wyświetli ostrzeżenie z informacją, że witryna została zablokowana dla bezpieczeństwa użytkownika.
- ✓ Filtr SmartScreen sprawdza pliki pobrane z sieci web według listy zgłaszanych witryn zawierających złośliwe oprogramowanie i programów uznanych za niebezpieczne. Jeśli filtr SmartScreen znajdzie witrynę na tej liście, wyświetli ostrzeżenie z informacją, że pobieranie zostało zablokowane dla bezpieczeństwa użytkownika. Ponadto filtr SmartScreen sprawdza pobierane pliki według listy plików, które są dobrze znane użytkownikom programu Internet Explorer i przez nich pobierane. Jeśli filtr SmartScreen nie znajdzie pobieranego pliku na tej liście, wyświetli ostrzeżenie.

Używanie filtru SmartScreen jest objęte Umową serwisową firmy Microsoft. Aby uzyskać więcej informacji, przeczytaj umowę serwisową firmy[10] **Microsoft** w trybie online.

Jak wyłączyć lub włączyć filtr SmartScreen?

1. Otwórz program Internet Explorer, klikając przycisk **Start**. W polu wyszukiwania wpisz tekst **Internet Explorer**, a następnie na liście wyników kliknij pozycję **Internet Explorer**.
2. Kliknij przycisk **Bezpieczeństwo**, wskaż polecenie **Filtr SmartScreen**, a następnie kliknij polecenie **Wyłącz filtr SmartScreen** lub **Włącz filtr SmartScreen**.
3. W oknie dialogowym **Filtr SmartScreen firmy Microsoft** kliknij przycisk **OK**.

- **Filtr skryptów między witrynami (ang. Cross-site scripting - XSS)** pozwalający na uniknięcie ataków ze strony nieuczciwych witryn sieci web, które próbują wykraść informacje osobiste i finansowe.

Program Windows Internet Explorer jest wyposażony w filtr XSS, który pomaga zapobiegać dodawaniu przez jedną witrynę sieci Web potencjalnie złośliwego kodu skryptu do innej witryny sieci Web. Filtr XSS analizuje sposób, w jaki współdziałają witryny sieci Web, i gdy rozpozna potencjalny atak, automatycznie blokuje wykonanie kodu skryptu. Gdy taka sytuacja się zdarzy, na pasku powiadomienia zostanie wyświetlony komunikat informujący o zmodyfikowaniu strony sieci Web w celu ochrony prywatności i bezpieczeństwa użytkownika.

Jeśli zmodyfikowana strona sieci Web nie działa prawidłowo, w nowym oknie przeglądarki przejdź do strony głównej tej witryny sieci Web, a stamtąd przejdź bezpośrednio do danej strony sieci Web. Jeśli strona nadal nie działa prawidłowo, skontaktuj się z administratorem witryny sieci Web.

- **128-bitowe połączenie SSL (Secure Sockets layer)** umożliwiające korzystanie z bezpiecznych witryn sieci web. Dzięki temu program Internet Explorer może ustanawiać zaszyfrowane połączenie z witrynami banków, sklepów internetowych, placówek medycznych oraz innych organizacji, które dysponują danymi osobowymi klientów.

Bezpieczna transakcja online to zaszyfrowana wymiana informacji między odwiedzaną witryną sieci Web a programem Windows Internet Explorer 9.

Aby się upewnić, że przeprowadzane transakcje online są bezpieczne, należy zwracać uwagę na następujące elementy:

- ✓ Adres sieci Web musi się zaczynać od prefiksu **HTTPS.** Litera S jest o tyle ważna, że wtedy połączenie z serwerem sieci Web odbywa się za pomocą protokołu szyfrowania SSL (Secure Sockets Layer). Prefiks HTTP (bez S) oznacza, że szyfrowanie nie jest stosowane i transakcja jest mniej bezpieczna.
- ✓ Jeśli na pasku powiadomień zostanie wyświetlony komunikat informujący o tym, że część zawartości nie jest bezpieczna, wtedy strona sieci Web wyświetla zawartość, korzystając zarówno z połączenia HTTPS, jak i HTTP z serwerem sieci Web. Transakcje HTTP (bez S) mogą nie być bezpieczne.
- ✓ Z prawej strony paska adresu musi być wyświetlona ikona kłódki. Kliknij ikonę kłódki, aby wyświetlić certyfikat, który został użyty do zaszyfrowania strony sieci Web. W certyfikacie

[10] http://go.microsoft.com/fwlink/?LinkId=74522

jest podany urząd certyfikacji, który go wystawił, daty ważności certyfikatu i serwer, z którym się komunikujesz. Jeśli cokolwiek w tych informacjach wygląda podejrzanie, skontaktuj się z wystawcą, aby potwierdzić ważność certyfikatu.

- ✓ Jeśli witryna sieci Web ma certyfikat, po kolorze paska adresu można rozpoznać poziom weryfikacji certyfikatu.

Znaczenie kolorów paska adresu jest opisane w poniższej tabeli.

Kolor	Znaczenie
Czerwony	Certyfikat jest nieaktualny, nieważny lub zawiera błędy. Aby uzyskać więcej informacji, zobacz Błędy certyfikatów: często zadawane pytania.
Żółty	Nie można zweryfikować autentyczności certyfikatu lub urzędu certyfikacji, który go wystawił. Może to wskazywać na problem z witryną sieci Web urzędu certyfikacji.
Biały	Certyfikat ma normalną weryfikację. Oznacza to, że komunikacja z tą witryną sieci Web jest szyfrowana.
Zielony	Certyfikat używa rozszerzonej weryfikacji. Oznacza to, że komunikacja między przeglądarką a witryną sieci Web jest szyfrowana, że urząd certyfikacji potwierdził, że usługi są oferowane lub świadczone przez legalny podmiot wskazany w certyfikacie i na pasku stanu zabezpieczeń.

- **Powiadomienia ostrzegające o tym, że ustawienia zabezpieczeń są na poziomie niższym niż zalecany**.

W programie Windows Internet Explorer 9 można zmienić ustawienia zabezpieczeń. Należy wykonać następujące czynności:

1. Otwórz program Internet Explorer, klikając przycisk **Start**. W polu wyszukiwania wpisz tekst **Internet Explorer**, a następnie na liście wyników kliknij pozycję **Internet Explorer**.
2. Kliknij przycisk **Narzędzia**, a następnie kliknij polecenie **Opcje internetowe**.
3. Kliknij kartę **Zabezpieczenia**, a następnie wykonaj jedną lub kilka z następujących czynności:
   - ✓ Aby zmienić ustawienia strefy zabezpieczeń, kliknij ikonę tej strefy, a następnie przesuń suwak do poziomu zabezpieczeń, który ma w niej obowiązywać.
   - ✓ Aby utworzyć własne ustawienia zabezpieczeń danej strefy, kliknij jej ikonę, a następnie przycisk **Poziom niestandardowy**.
   - ✓ Aby przywrócić oryginalne ustawienia wszystkich poziomów zabezpieczeń, kliknij przycisk **Resetuj wszystkie strefy do poziomu domyślnego**.

Cztery strefy zabezpieczeń programu Internet Explorer są opisane w poniższej tabeli.

Strefa	Opis
Internet	Ustawienia strefy zabezpieczeń Internet są stosowane do wszystkich witryn sieci web z wyjątkiem tych, które należą do stref zabezpieczeń Lokalny

	intranet, Zaufane witryny i Witryny z ograniczeniami.
Lokalny intranet	Ustawienia strefy zabezpieczeń Lokalny intranet są stosowane do witryn sieci firmowej i przechowywanej na nich zawartości. Aby zdefiniować, jakie witryny będą należały do tej strefy, lub dodać witryny do tej strefy, kliknij przycisk **Witryny**.
Zaufane witryny	Ustawienia strefy zabezpieczeń Zaufane witryny są stosowane do witryn sieci web, którym ufasz, że nie uszkodzą komputera ani informacji. Aby dodać witryny do tej strefy, kliknij przycisk **Witryny**.
Witryny z ograniczeniami	Ustawienia strefy zabezpieczeń Witryny z ograniczeniami są stosowane do witryn sieci web, które mogą uszkodzić komputer lub informacje. Dodanie witryn do strefy Witryny z ograniczeniami nie blokuje ich, ale nie pozwala im na uruchamianie programów ani jakiejkolwiek zawartości aktywnej. Aby dodać witryny do tej strefy, kliknij przycisk **Witryny**.

- **Ochrona przed śledzeniem**, która służy do ograniczania możliwości komunikacji przeglądarki z pewnymi witrynami sieci web — które są zdefiniowane na liście ochrony przed śledzeniem — aby informacje użytkownika pozostały poufne.

Ochrona przed śledzeniem blokuje tę zawartość z witryn sieci web figurujących na listach ochrony przed śledzeniem. Program Internet Explorer zawiera spersonalizowaną listę ochrony przed śledzeniem, która jest generowana automatycznie na podstawie odwiedzanych stron. Ponadto listy ochrony przed śledzeniem można pobierać, a wtedy program Internet Explorer będzie co pewien czas sprawdzać, czy są dostępne ich aktualizacje.

Aby włączyć ochronę przed śledzeniem

1. Otwórz program Internet Explorer, klikając przycisk **Start**. W polu wyszukiwania wpisz tekst **Internet Explorer**, a następnie na liście wyników kliknij pozycję **Internet Explorer**.
2. Kliknij przycisk **Narzędzia**, wskaż polecenie **Bezpieczeństwo**, a następnie kliknij polecenie **Ochrona przed śledzeniem**.
3. W oknie dialogowym **Zarządzanie dodatkami** kliknij listę ochrony przed śledzeniem, a następnie kliknij przycisk **Włącz**.

- **Przeglądanie InPrivate,** przy użyciu którego można przeglądać sieć web bez zapisywania wynikających z tego danych, jak pliki cookie i tymczasowe pliki internetowe.

Przeglądanie InPrivate powoduje, że program Windows Internet Explorer 9 nie zapisuje danych dotyczących przeglądania w trakcie sesji przeglądania, dzięki czemu inni użytkownicy komputera nie mogą sprawdzić, jakie strony sieci web odwiedzał w trakcie tej sesji dany użytkownik i jaką zawartość oglądał.

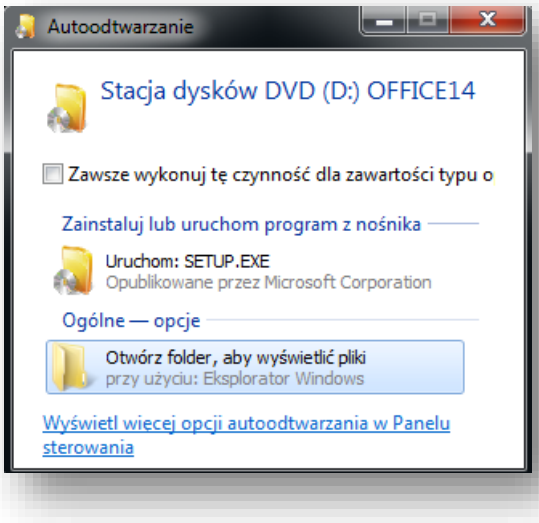
Aby włączyć funkcję Przeglądanie InPrivate

1. Otwórz program Internet Explorer, klikając przycisk **Start**. W polu wyszukiwania wpisz tekst **Internet Explorer**, a następnie na liście wyników kliknij pozycję **Internet Explorer**.
2. Kliknij przycisk **Narzędzia**, wskaż polecenie **Bezpieczeństwo**, a następnie kliknij polecenie **Przeglądanie InPrivate**.

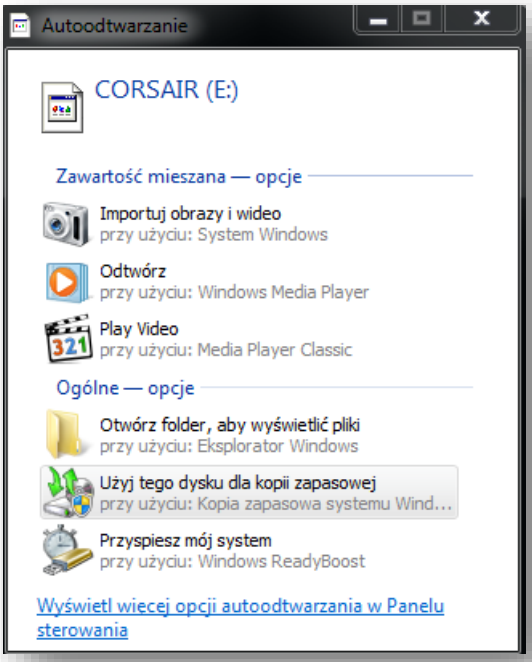
Więcej informacji na temat na temat Internet Explorer 9 oraz jego funkcji zabezpieczeń można uzyskać odwiedzając witrynę http://windows.microsoft.com/pl-PL/windows7/Getting-started-with-Internet-Explorer-9 [11]

10. Kontrola i blokowanie funkcji autostartu i autoodtwarzania

Polecenia autouruchamiania są zazwyczaj przechowywane w plikach **Autorun.inf**. Te polecenia umożliwiają uruchamianie aplikacji, programów instalacyjnych i innych procedur. W wersjach systemu Windows starszych niż Windows Vista oraz Windows 7 włożenie nośnika zawierającego polecenie autouruchamiania powodowało automatyczne uruchomienie programu w systemie bez konieczności interwencji ze strony użytkownika. Ze względu na to, że wykonanie kodu może nastąpić bez wiedzy lub zgody użytkownika, warto rozważyć wyłączenie tej funkcji ze względów bezpieczeństwa. W systemach Windows Windows 7 SP1 domyślnie użytkownikom jest wyświetlany monit z pytaniem, czy uruchomić polecenie autouruchamiania.



[11] http://windows.microsoft.com/pl-PL/windows7/Getting-started-with-Internet-Explorer-9

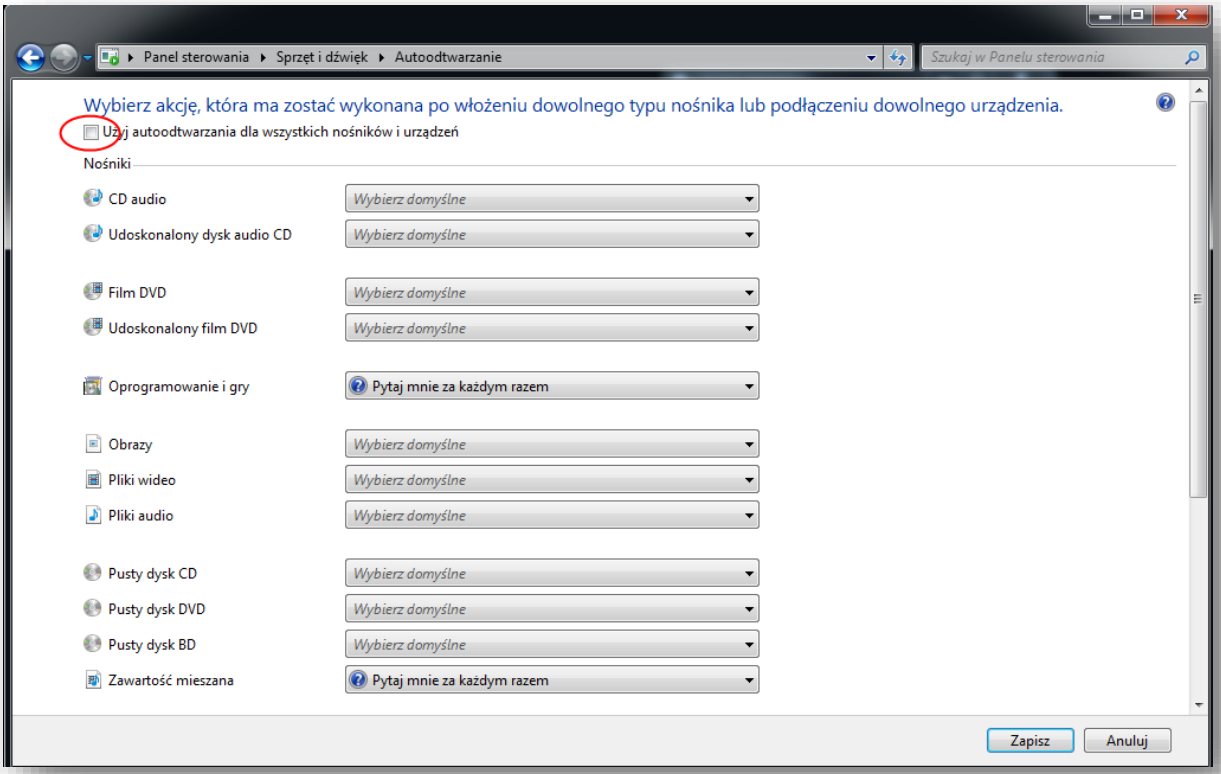


Rys. 10.1 – domyślne zachowanie funkcji Autoodtwarzenie dla nośników pamięci przenośnych USB i płyt CD/DVD.

Z uwagi na popularność nośników pamięci USB w powszechnym stosowaniu i jednocześnie dużym zagrożeniu infekcji oprogramowaniem złośliwym lub szpiegującym zaleca się wyłącznie funkcji Autodotwarzanie.

W celu wyłączenia funkcji Autoodtwarzanie należy:

1. Otwórz aplet **Autoodtwarzanie**, klikając przycisk **Start**, klikając kolejno polecenia **Panel sterowania**, **Sprzęt i dźwięk**, a następnie klikając polecenie **Autoodtwarzanie**.
2. Aby wyłączyć funkcję Autoodtwarzanie, wyczyść pole wyboru **Użyj autoodtwarzania dla wszystkich nośników i urządzeń**.
3. Kliknij przycisk **Zapisz**.



Rys. 10.1 – Wyłącznie funkcji autoodtwarzania dla wszystkich nośników i urządzeń

11. Sprawdzenie stanu zabezpieczeń komputera za pomocą narzędzia MBSA (Microsoft Baseline Security Analyzer)

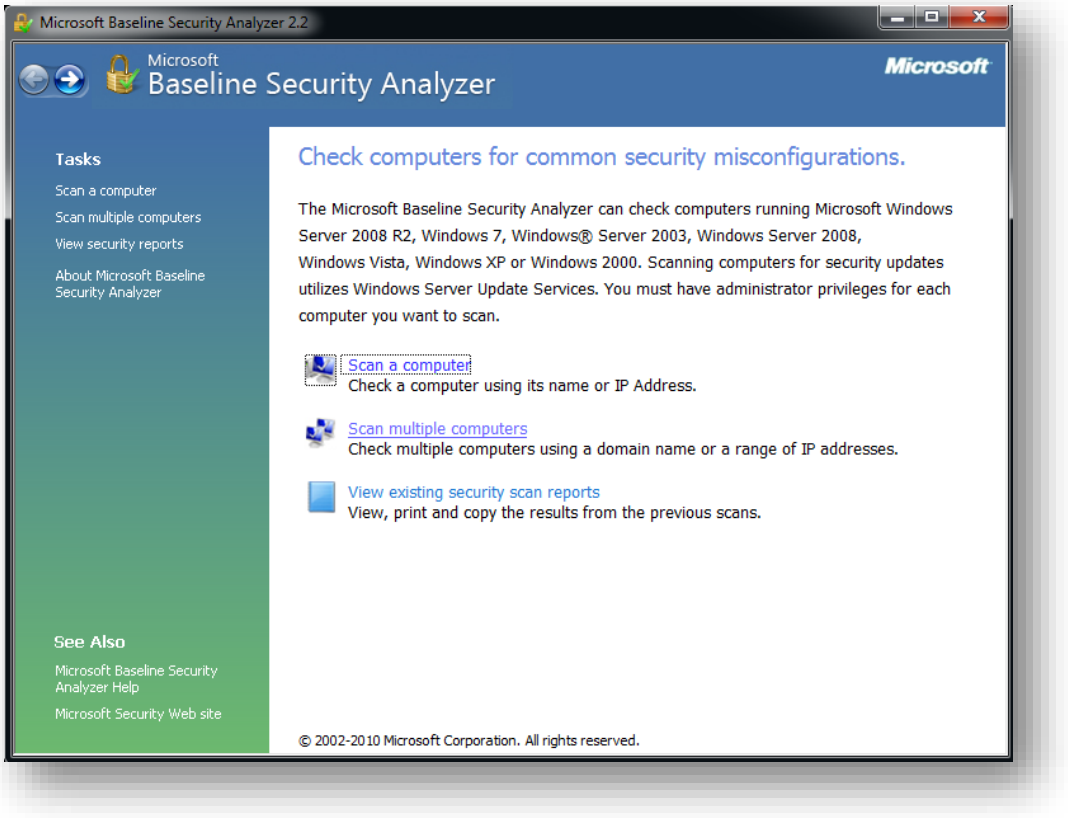
Microsoft Baseline Security Analyzer to bezpłatne narzędzie firmy Microsoft umożliwiające kompleksowe sprawdzenie stanu zabezpieczeń nie tylko systemu Windows, ale również najpopularniejszych aplikacji firmy Microsoft zainstalowanych na komputerze. Oprogramowanie można pobrać z witryny produktu firmy Microsoft. [12] Oprogramowanie dostępne jest w języku angielskim w wersji 32 i 64 bitowej.

MBSA wykrywa podatności między innymi w przeglądarce Internet Explorer i pakiecie Office. Sprawdzenie polega na połączeniu się z usługą Microsoft Update i pobraniu listy dostępnych poprawek, a następnie weryfikacji, które z nich są zainstalowane, a których jeszcze w systemie brakuje i należy je doinstalować. MBSA sprawdza także ustawienia systemowe pod kątem ich zgodności z najlepszymi praktykami bezpieczeństwa – takich jak: spełnienie wymagania złożoności haseł czy stan automatycznych aktualizacji. Po zakończonym skanowaniu użytkownikowi zaprezentowany jest pełny raport wraz z odnośnikami do brakujących poprawek lub informacji na temat usunięcia podatności lub poprawnego skonfigurowania ustawień systemu Windows.

Dużą zaletą programu, zwłaszcza dla specjalistów IT jest możliwość skanowania wielu komputerów za pośrednictwem sieci. MBSA oferuje też opcję uruchomienia z wiersza poleceń w celu automatyzacji

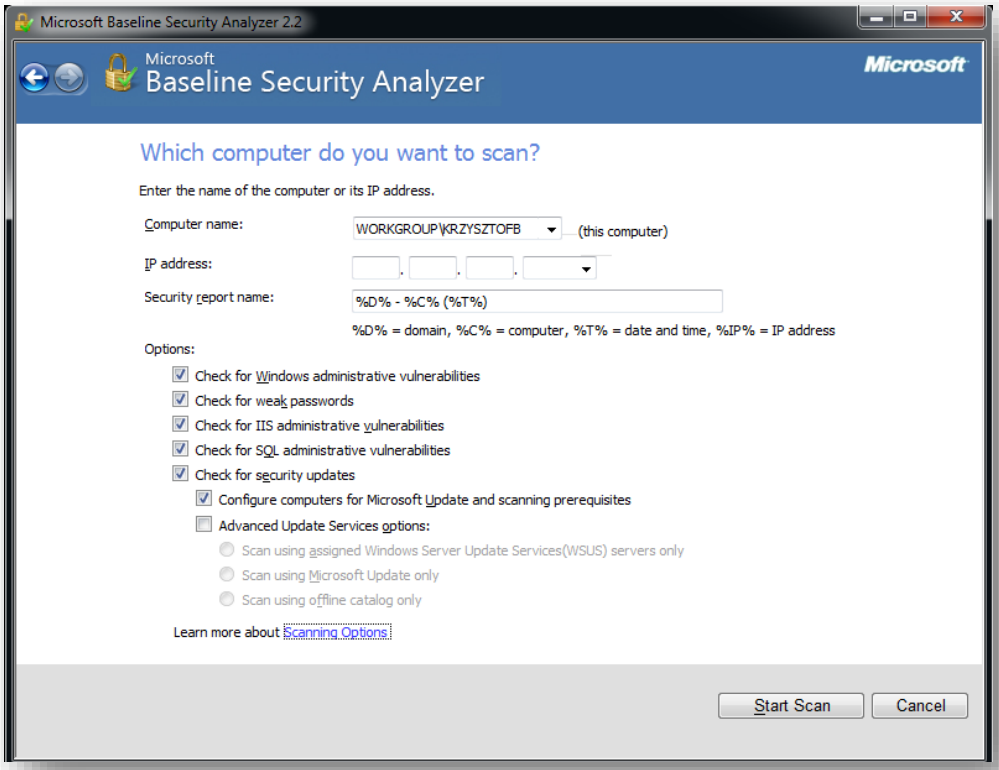
[12] http://www.microsoft.com/en-us/download/details.aspx?id=7558

skanowania komputerów. Program MBSA należy pobrać z witryny Microsoft oraz zainstalować na badanym komputerze lub komputerze Administratora. Widok konsoli głównej programu MBSA przedstawiono na poniższym rysunku.



Rys. 11.1 – Widok konsoli programu MBSA

W celu uruchomienia skanowania komputera należy wskazać pojedynczy komputer lub zakres adresów IP. Po wybraniu rodzaju skanowania, program MBSA pozwoli na wybranie właściwych opcji. Na poniższym rysunku zaprezentowano zalecane ustawienia skanowania komputerów.



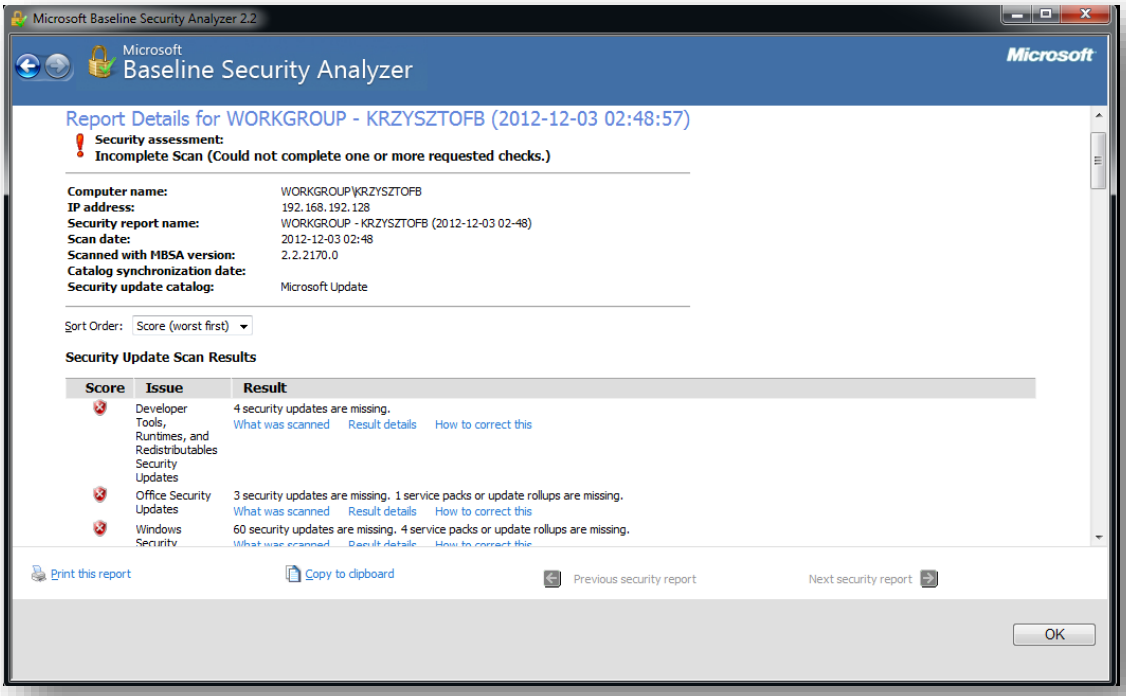
Rys. 11.2 – Funkcja skanowania w programie MBSA

Uwaga: Program wymaga aktywnego połączenia internetowego w celu pobrania listy dostępnych poprawek z witryny Microsoft Update.

Po zakończeniu skanowania MBSA wyświetli raport wskazujący na niewłaściwą konfigurację opcji dotyczących zabezpieczeń oraz informacji na temat brakujących aktualizacji. W przypadku wykrycia brakujących aktualizacji lub niewłaściwej konfiguracji, raport wyświetli informacje na temat każdej podatności:

- What was scaned (Co zostało przeskanowane i zbadane)
- Result details (Szczegółowy wynik skanowania)
- How to correct this (Dokładny opis jak naprawić lub usunąć daną podatność lub niezgodną konfigurację)

Przykładowy raport został zaprezentowany na rysunku poniżej:



Rys. 11.3 – przykładowy raport programu MBSA

Program MBSA jest rekomendowany jako narzędzie pomocnicze w celu określenia stanu zabezpieczeń pojedynczych komputerów orz grupy komputerów wraz z dokładną analizą wyników raportów MBSA oraz możliwością usunięcia wskazanych podatności i ustawienia poprawnej konfiguracji zabezpieczeń systemu Windows 7.

12. Dodatkowe informacje na temat zabezpieczania systemu Windows 7 SP1

Szczegółowe informacje i zaawansowane sposoby zabezpieczania systemu Windows 7 SP1 można uzyskać zapoznając się z przewodnikiem „**PRZEWODNIK ZABEZPIECZEŃ SYSTEMU WINDOWS 7 SP1**” wydanym w języku polskim, opracowanie powstało w ramach SECURITY COOPERATION PROGRAM (SCP) i dostępne jest pod adresem http://www.cert.gov.pl/portal/cer/33/Microsoft_Windows.html http://www.cert.gov.pl/download/3/139/Przewodnik_zabezpieczen_systemu_Windows_7_SP1_SCP.pdf [13]

Przewodnik zabezpieczeń systemu Windows 7 SP1 zawiera instrukcje i rekomendacje, które pomogą wzmocnić poziom zabezpieczenia komputerów stacjonarnych i komputerów przenośnych pracujących pod kontrolą systemu Windows 7 SP1 w domenie Active Directory Domain Services (AD DS).

[13] http://www.cert.gov.pl/download/3/139/Przewodnik_zabezpieczen_systemu_Windows_7_SP1_SCP.pdf

Szczególnie polecanym dodatkowym narzędziem jest Security Compliance Manager (SCM).[14] W połączeniu z „Przewodnikiem zabezpieczeń systemu Windows 7 SP1" zapewnia on możliwość eksportowania wszystkich rekomendowanych ustawień zasad grupowych, aby w praktyczny sposób wykorzystać proponowane rozwiązania we własnym środowisku.

[14] http://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx