PRZEWODNIK ZABEZPIECZEŃ SYSTEMU 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 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).

Dodatkowo w podręczniku tym zostaną zaprezentowane narzędzia, szczegółowe instrukcje, rekomendacje oraz procesy, które w znacznym stopniu usprawnią proces wdrażania systemu Windows 7 SP1.

Publikacja wprowadzi również użytkownika w proces zarządzania zgodnością, a także przedstawi dodatkowe informacje (wraz z odsyłaczami) na temat narzędzi zapewniających zgodność IT oraz zalecenia Microsoft.

Szczególnie polecanym narzędziem jest Security Compliance Manager[1] (SCM). W połączeniu z „Przewodnikiem zabezpieczeń systemu Windows 7 SP1" zapewnia on możliwość eksportowania wszystkich ustawień zasad grupowych, aby w praktyczny sposób wykorzystać proponowane rozwiązania we własnym środowisku.

Autorzy starali się uczynić ten przewodnik:

- **sprawdzonym** – bazującym na zebranym doświadczeniu w tej dziedzinie
- **wiarygodnym** – oferującym najlepsze dostępne dobre praktyki w tym zakresie
- **dokładnym** – przekazującym rozwiązania przetestowane od strony technicznej
- **gotowym do użycia** – prezentującym kroki niezbędne do pomyślnego wdrożenia proponowanych rozwiązań
- **użytecznym** – obejmującym rzeczywiste problemy związane z bezpieczeństwem

W dokumencie zamieszczono najlepsze praktyki stosowane w celu implementacji systemów: Windows 7 SP1, Windows Vista SP2, Windows Server 2003 SP2, Windows Server 2008 SP2 oraz Windows Server 2008 R2 SP1 w różnorodnych środowiskach.

Aby oszacować szanse wdrożenia Windows 7 SP1 we własnym środowisku, można skorzystać z pomocy oferowanej przez narzędzie Microsoft Assessment and Planning Toolkit[2]. Przeprowadzi ono użytkownika przez proces określania gotowości infrastruktury organizacji średniej wielkości do uruchomienia systemu Windows 7 SP1, asystując w inwentaryzacji sprzętu i wyborze scenariusza wsparcia oraz dostarczając niezbędnych informacji i wskazując komputery wymagające aktualizacji sprzętu.

---

[1] http://go.microsoft.com/fwlink/?LinkId=113940
[2] http://go.microsoft.com/fwlink/?LinkId=105520

Niniejszy przewodnik przedstawia funkcjonalności zwiększające poziom bezpieczeństwa systemu Windows 7 SP1. Zawarte informacje zostały sprawdzone i przetestowane na komputerach pracujących w domenie, a także komputerach autonomicznych, niepracujących w domenie.

Uwaga: Wszystkie odniesienia do systemu Windows XP w niniejszym przewodniku dotyczą systemu Windows XP Professional SP3, a odniesienia dotyczące systemu Windows Vista dotyczą systemu Windows Vista SP2.

a. Streszczenie wykonawcze

Niezależnie od wielkości środowiska organizacji, kwestie bezpieczeństwa teleinformatycznego należy traktować priorytetowo.

Wiele organizacji nie docenia ryzyka związanego z możliwościami nowoczesnych technologii informatycznych. Konsekwencje skutecznie przeprowadzonego ataku na serwery organizacji mogą zakłócić codzienne funkcjonowanie organizacji oraz kluczowe procesy biznesowe. Przykładem może być zainfekowanie komputerów klienckich przez oprogramowanie złośliwe we własnej sieci; organizacja może wówczas utracić dane wrażliwe i ponieść koszty związane z przywróceniem stanu sprzed ataku. Atak na firmową witrynę internetową może zaś przyczynić się do jej niedostępności w sieci, narażenia organizacji na straty finansowe, utratę zaufania klientów i osłabienia reputacji marki.

Zgodność z przepisami i standardami staje się kluczową kwestią dla działania organizacji, a organy urzędowe zalecają lub nakazują stosowanie się do wytycznych i zaleceń, których celem jest zapewnienie bezpieczeństwa. Audytorzy, wykonując ocenę dojrzałości organizacji, przeważnie wymagają potwierdzenia podjętych działań i weryfikują, czy spełniono wymagania określone w regulacjach. Brak działań w kierunku zapewnienia zgodności z obowiązującymi wytycznymi i regulacjami może narazić organizację na straty finansowe, utratę reputacji, karę grzywny lub inne kary przewidziane w obowiązującym prawie.

Przeprowadzenie analizy bezpieczeństwa, ewentualnych ryzyk i zagrożeń pozwala na wypracowanie rozsądnego kompromisu pomiędzy odpowiednim poziomem bezpieczeństwa a funkcjonalnością wszystkich systemów informatycznych pracujących w organizacji. Niniejszy przewodnik przedstawi najważniejsze środki zaradcze odnoszące się do kwestii bezpieczeństwa, omówi dostępne funkcjonalności systemu Windows 7 SP1 i wskaże potencjalne zagrożenia, by poprawić bezpieczeństwo organizacji.

Przewodnik bezpieczeństwa w przystępny sposób przedstawia niezbędne informacje oraz narzędzia wspomagające, umożliwiając:

- wdrożenie i zastosowanie ustawień bazowych zapewniających wyższy poziom bezpieczeństwa w środowisku organizacji
- poznanie i wykorzystanie funkcjonalności związanych z bezpieczeństwem systemu Windows 7 SP1 w najczęściej spotykanych sytuacjach
- identyfikację poszczególnych ustawień zabezpieczeń wraz z określeniem ich znaczenia

Aby przeprowadzić testy i wprowadzić ustawienia zabezpieczeń, należy skorzystać z narzędzia Security Compliance Manager (SCM). Narzędzie to ułatwi i zautomatyzuje proces wdrażania bazowych

ustawień bezpieczeństwa. Poradnik, który szczegółowo omawia, jak korzystać z narzędzia SCM, dostępny jest jako dodatek **„Narzędzie Security Compliance Manager (SCM) w praktyce”.**

Choć przewodnik ten skierowany jest przede wszystkim do dużych organizacji, większość zawartych w nim informacji można zastosować dla każdej organizacji – bez względu na jej wielkość. Najlepsze efekty przyniesie lektura całej publikacji, jednak aby zapewnić odpowiedni poziom bezpieczeństwa organizacji i towarzyszących jej celów biznesowych, możliwe jest też zapoznanie się tylko z wybranymi częściami materiału.

b. Zarządzanie bezpieczeństwem i zgodnością ze standardami przy wykorzystaniu technologii

Organizacje wymagają od swoich działów IT, by w sprawny i podlegający kontroli sposób dostarczały bezpieczną infrastrukturę, która będzie zgodna z obowiązującymi regulacjami, standardami certyfikacji oraz najlepszymi praktykami. Dział IT musi dokonywać stałej kontroli owej zgodności, to zaś wymaga ciągłego dostosowywania się do potrzeb nowych technologii.

Aby zapewnić organizacji bezpieczeństwo, konieczne jest wdrożenie efektywnych rozwiązań w zakresie aktualizacji systemów i monitoringu zgodności infrastruktury IT.

Firma Microsoft opracowała zbiór przewodników i narzędzi, które wspierają organizacje – niezależnie od ich wielkości – w zapewnianiu i utrzymywaniu bezpieczeństwa informacji w zarządzanych systemach. Przewodniki te wspomagają zespoły IT w procesach: implementacji, wsparcia i weryfikacji bazowych ustawień systemów wykorzystujących różnorodne produkty Microsoft w swoim środowisku. Niniejszy przewodnik stanowi doskonały punkt wyjścia dla zwiększenia i zapewnienia bezpieczeństwa informacji w zarządzanych systemach.

Ustawienia bazowe są kluczowym pojęciem określającym zbiór rekomendowanych ustawień wykorzystywanych w całym przewodniku oraz innych powiązanych dokumentach i narzędziach wydanych przez Microsoft.

Co oznacza termin ustawienia bazowe (ang. baseline)?

Ustawienia bazowe to zbiór rekomendowanych ustawień funkcji poszczególnych produktów Microsoft, które pomagają zminimalizować określone ryzyka poprzez wykonanie czynności kontrolnych.

Czynności kontrolne wchodzą w zakres obowiązków osób sprawujących funkcje compliance managerów oraz każdej osoby, która – z uwagi na podejmowane działania wymagające określenia zasad zarządzania występującym ryzykiem i sposobów, by je zminimalizować, wykorzystując określone technologie – odpowiada w organizacji za bezpieczeństwo. Firma Microsoft przez wiele lat publikowała zbiory ustawień bazowych, zwracając szczególną uwagę na ustawienia konfiguracji umożliwiające podniesienie poziomu bezpieczeństwa produktów Microsoft. Zbiory te zawierały gotowe rekomendowane ustawienia do bezpośredniego zastosowania przez administratorów IT w środowisku produkcyjnym organizacji.

Po wprowadzeniu produktu IT GRC Process Management Pack dla Manager 2012 opublikowane zostały bazowe ustawienia konfiguracji zapewniające zgodność ze standardami (ang. compliance baselines).

Na potrzeby wytycznych, które opisano w przewodniku, bazowe ustawienia konfiguracji uwzględniają:

- listę rekomendowanych środków zaradczych mających na celu zwiększenie poziomu zabezpieczeń produktów Microsoft

- informacje techniczne niezbędne do implementacji każdego środka zaradczego minimalizującego ryzyko

- informacje techniczne niezbędne do określenia stanu każdego środka zaradczego minimalizującego ryzyko, które pozwolą na automatyczne skanowanie stanu zgodności i tworzenie raportu z przeprowadzonej czynności

- ustawienia zgrupowane w elementy konfiguracji (ang. Configuration Item [CI]), łączące IT Governance, Risk, and Compliance (IT GRC) Process Management Pack (PMP) z czynnościami kontrolnymi

Jak korzystać z bazowych ustawień konfiguracji?

Pierwszym rekomendowanym krokiem jest przeprowadzenie identyfikacji systemów operacyjnych i aplikacji wykorzystywanych we własnej sieci komputerowej; pozwoli to na określenie właściwych ustawień bazowych konfiguracji, które zostaną zaimplementowane. Czynności te można wykonać w kilku etapach:

- inwentaryzacja z wykorzystaniem bezpłatnego narzędzia Microsoft Assessment and Planning Toolkit[3], które uprości i zautomatyzuje proces identyfikacji posiadanych zasobów w sieci
- wybór właściwych bazowych ustawień konfiguracji, korzystając z przygotowanych rozwiązań Microsoft lub innych upoważnionych organizacji
- analiza i korekta bazowych ustawień konfiguracji – tak, aby odpowiadały biznesowym potrzebom organizacji oraz spełniały wymogi organów wydających regulacje. Krok ten można wykonać, korzystając z informacji udostępnionych w narzędziu SCM, przewodnikach zabezpieczeń oraz Information Technology Governance, Risk, and Compliance (IT GRC) Process Management Pack for System Center Service Manager[4]
- zastosowanie celów kontrolnych i czynności kontrolnych w połączeniu z ustawieniami bazowymi w celu właściwej konfiguracji zarządzanych systemów i utrzymania stanu zgodności IT

Konfiguracji ustawień takich produktów Microsoft jak: systemy Windows, Microsoft Office oraz Internet Explorer można dokonywać poprzez wykorzystanie zasad grupowych (Group Policy) w narzędziu SCM. Pozwoli to na dopasowanie ustawień bazowych do własnych potrzeb. Przygotowane ustawienia należy wyeksportować do arkusza kalkulacyjnego Excel i omówić ze stronami zainteresowanymi w całej organizacji. Zatwierdzone ustawienia eksportujemy w postaci kopii

[3] http://go.microsoft.com/fwlink/?LinkId=105520
[4] http://go.microsoft.com/fwlink/?LinkId=201578

zapasowej zasad grupowych i wdrażamy w środowisku testowym, wykorzystując mechanizm zasad grupowych usług katalogowych Active Directory. W przypadku komputerów niepracujących w domenie należy zastosować narzędzie Local Policy Tool, dostępne w SCM (narzędzie to będzie omówione rozdziale 2.5).

1.1. Praca z rekomendowanymi bazowymi ustawieniami konfiguracji (baseline)

Narzędzie SCM zawiera rekomendowane bazowe ustawienia konfiguracji produktów Microsoft, które mogą być zarządzane i dostosowywane do własnych potrzeb. Gdy w bazowych ustawieniach konfiguracji wprowadzimy zmiany, mając na uwadze wymagania organizacji, nowe ustawienia zasad grupowych możemy zweryfikować, generując dla każdego komputera dostosowane ustawienia bazowe w narzędziu SCM.

Utworzenie pakietów Desired Configuration Management (DCM) dla bazowych ustawień, a następnie importowanie tych ustawień do System Center Configuration Managera pozwoli w prosty i zautomatyzowany sposób osiągnąć zgodność ze standardami. Narzędzie SCM pozwala także na eksport bazowych ustawień konfiguracji do formatu Security Content Automation Protocol (SCAP). Format SCAP jest wspierany przez wiele narzędzi służących do zarządzania dostarczonymi przez Microsoft oraz firmy trzecie zabezpieczeniami i danymi konfiguracyjnymi. Aby uzyskać dodatkowe informacje na temat formatu SCAP, należy zapoznać się z informacjami umieszczonymi na stronie National Institute of Standards and Technology (NIST) [5].

Kontroli działań mających na celu zapewnienie zgodności można dokonać poprzez zastosowanie i zintegrowanie produktów: Microsoft System Center Service Manager i IT GRC Process Management Pack. Wspomoże to organizacje we wprowadzaniu zasad ładu korporacyjnego, w skutecznym zarządzaniu ryzykiem i osiągnięciu zgodności ze standardami IT (IT GRC).

Produkt System Center Service Manager umożliwia przygotowanie automatycznych raportów dla kadr kierowniczych, audytorów IT oraz innych osób biorących udział w projekcie. Proces IT GRC zostanie omówiony szerzej w rozdziale drugim – „Ład korporacyjny, zarządzanie ryzykiem oraz zgodność ze standardami w IT (IT GRC)".

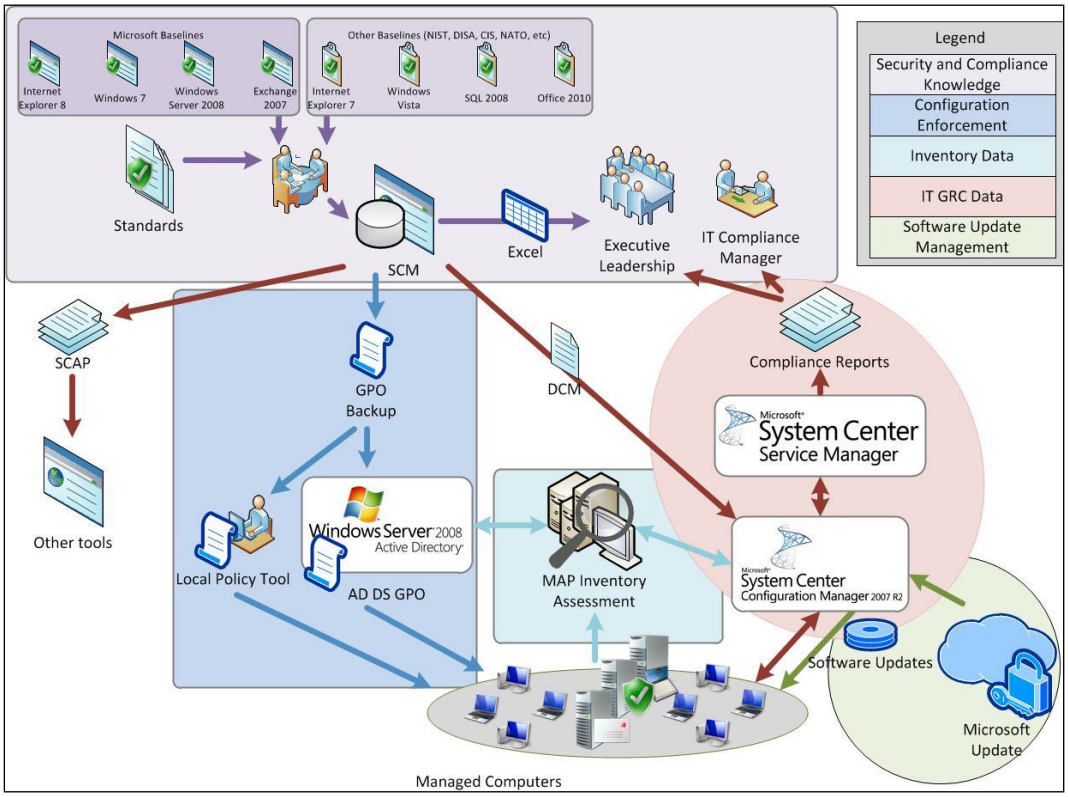
Narzędzie SCM wspomaga zarządzanie bazowymi ustawieniami konfiguracji produktów Microsoft, których nie można konfigurować poprzez zasady grupowe (Group Policy); należy do nich m.in. serwer Microsoft Exchange. SCM zawiera zestaw skryptów PowerShell, które umożliwiają wdrożenie bazowych ustawień konfiguracji dla jednego lub wielu serwerów, korzystając z procesu automatyzacji. Proces ten, dzięki wykorzystaniu skryptów (programów) ułatwiających wykonywanie powtarzających się zadań, redukuje zasoby ludzkie przy realizacji zadań.

Ten sam zestaw skryptów można również wykorzystać do weryfikacji zgodności sprzętu IT. Możliwe jest także skorzystanie z funkcji eksportowania pakietów konfiguracyjnych DCM w narzędziu SCM. W celu uzyskania dodatkowych informacji należy zapoznać się z dokumentem „Exchange Server PowerShell Script Kit User Guide", dostępnym wewnątrz narzędzia SCM (zakładka **Attachments\Guides).**

[5] http://scap.nist.gov/

Na rys. 1.2.1. przedstawiono proces zarządzania bezpieczeństwem i zgodnością ze standardami przy zastosowaniu technologii dla potrzeb organizacji.

Więcej informacji na temat narzędzia SCM znajduje się na stronie Microsoft Security Compliance Manager[6]. Warto również odwiedzić witrynę SCM Wiki[7] na stronach TechNet.



Rys. 1.2.1. Zarządzanie bezpieczeństwem i zgodnością ze standardami przy zastosowaniu technologii dla potrzeb organizacji

1.2. Do kogo skierowany jest ten podręcznik?

Podręcznik przeznaczony jest przede wszystkim dla specjalistów zarządzających bezpieczeństwem, architektów sieciowych, administratorów IT, specjalistów IT oraz konsultantów planujących wdrożenie infrastruktury IT i systemu Windows 7 SP1 na komputerach klienckich w środowiskach domenowym i pozadomenowym.

1.3. Dodatkowe informacje i wskazówki

Poniżej przedstawiono dodatkowe źródła informacji na tematy związane z bezpieczeństwem systemu Microsoft Windows 7 SP1:

- Federal Desktop Core Configuration (FDCC)[8]
- Microsoft Assessment and Planning Toolkit[9]

[6] http://go.microsoft.com/fwlink/?LinkId=113940
[7] http://social.technet.microsoft.com/wiki/contents/articles/microsoft-security-compliance-manager-scm.aspx#comment-2585
[8] http://fdcc.nist.gov/

- Microsoft Security Compliance Manager[10]
- SCM Wiki[11]
- Security and Compliance Management Forum[12]

[9]http://go.microsoft.com/fwlink/?LinkId=105520
[10] http://go.microsoft.com/fwlink/?LinkId=113940
[11] http://social.technet.microsoft.com/wiki/contents/articles/microsoft-security-compliance-manager-scm.aspx#comment-2585
[12]http://social.technet.microsoft.com/Forums/en-us/compliancemanagement/threads

2. Wdrażanie rekomendowanych zasad bezpieczeństwa w kontekście bazowych ustawień systemu Windows 7

2.1. Wprowadzenie

Firma Microsoft wraz z każdym nowo udostępnianym systemem operacyjnym wprowadza ulepszone rozwiązania w zakresie bezpieczeństwa. Ich duża różnorodność w Windows 7 SP1 sprawia, że jest on aktualnie najlepiej zabezpieczonym systemem Windows, jaki został do tej pory wydany. Konfiguracja opcji zabezpieczeń – w odróżnieniu od wcześniejszych wersji Windows – odbywa się obecnie poprzez Zasady polityk grupowych GPO (z ang. Group Policy Object). Mechanizm GPO zapewnia centralną infrastrukturę, która w oparciu o strukturę hierarchiczną umożliwia zarządzanie ustawieniami komputerów i/lub użytkowników, włączając ustawienia zabezpieczeń.

Znane z wcześniejszych wersji systemów Windows kategorie ustawień bezpieczeństwa: Specialized Security – Limited Functionality (SSLF) oraz Enterprise Client (EC) zostały zastąpione poziomami ważności (ang. severity level).

W Windows 7 SP1 stosowane są cztery poziomy ważności:

- Krytyczny

  Ustawienia na tym poziomie w najwyższym stopniu wpływają na bezpieczeństwo komputera i/lub przechowywanych na nim danych. Zaleca się stosowanie wszystkich ustawień krytycznych w organizacji.

- Istotny

  Ustawienia na tym poziomie mają znaczący wpływ na bezpieczeństwo komputera i/lub przechowywanych na nim danych. Są one konfigurowane w organizacjach, które przechowują wrażliwe dane i dbają o ochronę własnych systemów informatycznych.

- Opcjonalny

  Ustawienia na tym poziomie mają niewielki wpływ na bezpieczeństwo, przez co większość organizacji pomija je na etapie projektowania zasad bezpieczeństwa. Nie oznacza to jednak dowolności w zakresie ich stosowania. Dla przykładu: wiele ustawień dotyczących Windows, Internet Explorer czy Office ukrywa elementy interfejsu użytkownika, które upraszczają pracę, a nie mają bezpośredniego wpływu na bezpieczeństwo.

- Niezdefiniowany

  Jest to domyślny poziom ważności w Security Compliance Manager. Ustawienia, które nie były dostępne wcześniej, oznaczane są takim poziomem bezpieczeństwa. Przyjmuje się, że ich znaczenie porównywalne jest z poziomem Opcjonalnym, co oznacza, że mają one bardzo mały lub zerowy wpływ na bezpieczeństwo.

W zależności od wybranego formatu eksportu dla reguł, poziomy ważności przyjmują nazwy zgodnie z poniższą tabelą:

Security Compliance Manager (SCM)	Desired Configuration Management (DCM)	Security Content Automation Protocol (SCAP)
Krytyczny	Krytyczny	Wysoki
Istotny	Ostrzegawczy	Średni
Opcjonalny	Informacyjny	Niski
Niezdefiniowany	Inny	Nieznany

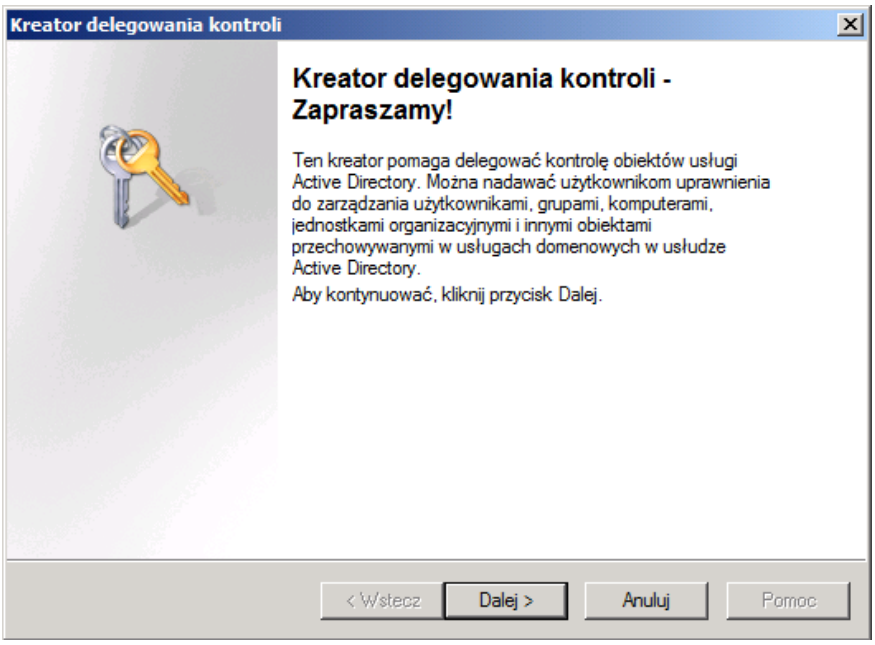
Tab. 2.1.1. Wykaz nazw poziomów ważności w zależności od wybranego formatu eksportu

2.2. Projektowanie struktur jednostek organizacyjnych (OU) ze szczególnym uwzględnieniem zasad bezpieczeństwa

Usługa katalogowa Active Directory umożliwia scentralizowane zarządzanie infrastrukturą przedsiębiorstwa. Stosując hierarchiczną strukturę, można stworzyć model, który będzie uwzględniał narzucone i pożądane aspekty bezpieczeństwa organizacji.

Jednostka organizacyjna OU (z ang. Organizational Unit) jest kontenerem wewnątrz domeny Active Directory Domain Services (AD DS), który może zawierać użytkowników, grupy, komputery oraz inne jednostki organizacyjne. Wyróżniamy nadrzędne oraz podrzędne jednostki organizacyjne.

Jedną z ważnych cech jednostek organizacyjnych jest możliwość dołączania do nich zbiorów zasad grupowych GPO. Dzięki temu zadeklarowane ustawienia mogą być przenoszone do użytkowników i komputerów znajdujących się wewnątrz tych obiektów. Dodatkowo istnieje możliwość delegowania kontroli administracyjnej (rys. 2.2.1) nad jednostkami organizacyjnymi, co znacznie usprawnia proces zarządzania.

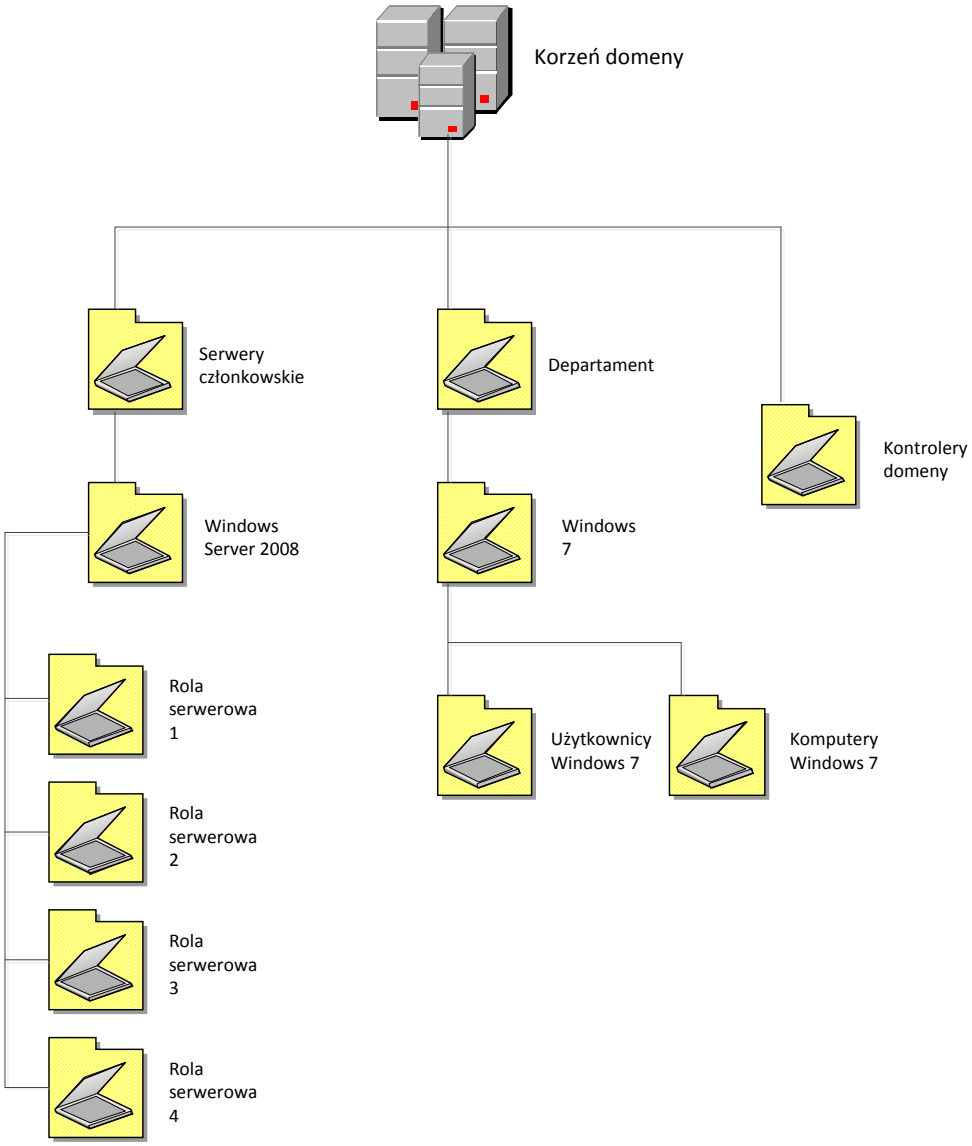


Rys. 2.2.1 Delegation Wizard w ADUC.

Dzięki jednostkom organizacyjnym można również tworzyć granice administracyjne oddzielające użytkowników od komputerów. Takie rozwiązanie idealnie sprawdza się, gdy stosujemy ustawienia dedykowane wyłącznie komputerom oraz wyłącznie użytkownikom.

Najważniejszym celem projektowania struktury jednostek organizacyjnych powinna być możliwość jednolitej implementacji zasad grupowych z uwzględnieniem konieczności spełnienia wszystkich standardów i zaleceń w zakresie bezpieczeństwa.

Na rysunku 2.2.2 zaprezentowana została przykładowa struktura uwzględniająca możliwe do zastosowania poziomy jednostek organizacyjnych w typowych rozwiązaniach usług katalogowych Active Directory.



Rys. 2.2.2. Przykładowa struktura jednostek organizacyjnych dla komputerów oraz użytkowników

Korzeń domeny

Ustawienia, które dotyczą zabezpieczeń całej domeny, można stosować w ramach GPO dołączonego do domeny. Na tym poziomie komputery ani użytkownicy nie podlegają zarządzaniu.

Jednostki organizacyjne

Serwery pełniące role kontrolerów domeny przechowują wiele wrażliwych danych, w tym dane, które kontrolują konfigurację zabezpieczeń ich samych. Stosowanie GPO na poziomie jednostki organizacyjnej Kontrolery domeny umożliwia konfigurację i ochronę kontrolerów domeny.

Serwery członkowskie

Stosowanie zasad GPO do pośredniej jednostki organizacyjnej Serwery członkowskie umożliwia konfigurację stałych opcji dla wszystkich serwerów, bez uwzględniania podziału na pełnione przez nie role.

Role serwerowe

Dobrą praktyką jest tworzenie dedykowanych jednostek organizacyjnych dla wszystkich ról serwerowych w organizacji. Dzięki takiemu rozwiązaniu zachowany zostaje ujednolicony model zarządzania, który umożliwia stosowanie zasad GPO opartych na rolach serwerowych.

Dla serwerów utrzymujących wiele ról można tworzyć dodatkowe jednostki organizacyjne, zgodnie z ich konfiguracją. Do takiej jednostki organizacyjnej dołącza się następnie zbiory GPO dedykowane określonym rolom serwerowym. Należy zwrócić szczególną uwagę na mieszane konfiguracje, aby uwzględnić kolejność przetwarzania zasad GPO, warunkującą uzyskiwane ustawienia końcowe.

Departament

Wymagania w zakresie zabezpieczeń są różne i często zależą od struktury organizacyjnej. Tworzenie jednostek organizacyjnych dla poszczególnych komórek pozwala na stosowanie ustawień zabezpieczeń dla komputerów i użytkowników w zgodzie z celem biznesowym.

Użytkownicy Windows 7

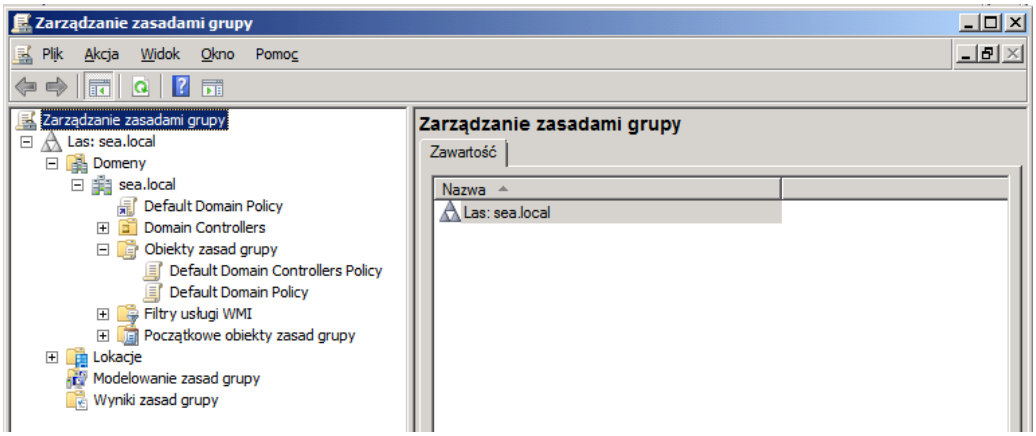
Stosowanie specjalnych jednostek organizacyjnych, w których przechowywane są konta użytkowników, daje możliwość stosowania zasad zabezpieczeń, które są im dedykowane.

Komputery Windows 7

Stosowanie dedykowanych jednostek organizacyjnych, w których przechowywane są konta komputerów, pozwala na stosowanie ustawień zabezpieczeń dla komputerów zarówno stacjonarnych, jak i mobilnych.

2.3. Projektowanie obiektów zasad grupowych (GPO) struktur jednostek organizacyjnych ze szczególnym uwzględnieniem zasad bezpieczeństwa

GPO jest zbiorem zawierającym ustawienia zasad grupowych, który definiuje się w przystawce Zarządzanie zasadami grupy (rys. 2.3.1).



Rys. 2.3.1 Przystawka Zarządzanie zasadami grupy

Zawarte tam ustawienia przechowywane są na poziomie domeny i mogą oddziaływać na użytkowników i/lub komputery w lokacji, domenach i jednostkach organizacyjnych.

Ręczna konfiguracja ustawień zapewniających powyższy efekt może prowadzić do niespójności zarządzania. To zaś w konsekwencji może wymusić konieczność zapewnienia odpowiedniej liczby osób, których zadaniem będzie nadzorowanie jednolitego wdrożenia narzuconych zasad.

Wykorzystanie zasad grupowych – w odróżnieniu od ręcznej konfiguracji ustawień – upraszcza zarządzanie oraz zapewnia natychmiastową aktualizację rozwiązań na wielu komputerach i dla wielu użytkowników. Zasady GPO zdefiniowane w obrębie domeny nadpisują ustawienia zasad lokalnych, co pozwala na utrzymanie centralnego modelu zarządzania konfiguracją.

Kolejność przetwarzania GPO przedstawiona została na rysunku 2.3.2.

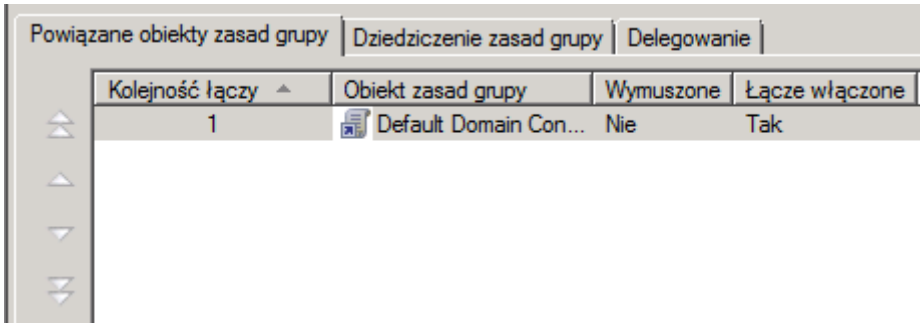
Rys. 2.3.2. Kolejność przetwarzania zasad GPO

Jako pierwsze przetwarzane są zasady lokalne, następnie zaś zasady na poziomach: lokacji, domeny oraz jednostek organizacyjnych. Zbiory znajdujące się na poziomie jednostek organizacyjnych są

przetwarzane hierarchicznie – od OU najwyższego do położonego najniżej. Tym samym zdefiniowane dla komputerów ustawienia znajdujące się na najniższym poziomie hierarchii jednostek organizacyjnych stosowane są jako ostatnie i mają najwyższy priorytet. Takie działanie obowiązuje od systemów: Windows Server 2003 SP2, Windows Server 2008, Windows XP SP3 oraz Windows Vista. Dla użytkowników model przetwarzania zasad jest identyczny.

Istnieje kilka zaleceń związanych z projektowaniem zasad grupowych, o których warto pamiętać.

- W przypadku wielu GPO administrator powinien ustalić kolejność dołączania ich do jednostki organizacyjnej. Domyślnie kolejność ta jest zgodna z porządkiem dołączania poszczególnych elementów na etapie konfiguracji. Zasady, które znajdują się wyżej na liście **Kolejność łączy,** mają wyższy priorytet. W przypadku zdefiniowania takiego samego ustawienia w dwóch zbiorach zasad grupowych, efektywne staje się więc to, które pochodzi ze zbioru mającego wyższy priorytet.



Rys. 2.3.3. Zakładka Powiązane obiekty zasad grupy, definiująca kolejność przetwarzania zasad grupowych

- W ramach konfiguracji GPO dostępna jest opcja **Wymuszone**. Jej zastosowanie sprawia, że zdefiniowane w niej zasady nie będą nadpisywane przez inne zbiory – bez względu na kolejność ich dołączenia.

- Stosowanie ustawień zasad grupowych jest ściśle związane z położeniem obiektów: użytkownik i komputer w AD DS. W niektórych przypadkach pożądane jest jednak stosowanie ustawień dla użytkownika w oparciu o położenie obiektu komputer. W takich sytuacjach przydatna staje się opcja **Tryb przetwarzania sprzężenia zwrotnego zasad grupy użytkownika**. Umożliwia ona stosowanie ustawień konfiguracji użytkownika pochodzącego ze zbioru zawierającego ustawienia konfiguracji komputera.

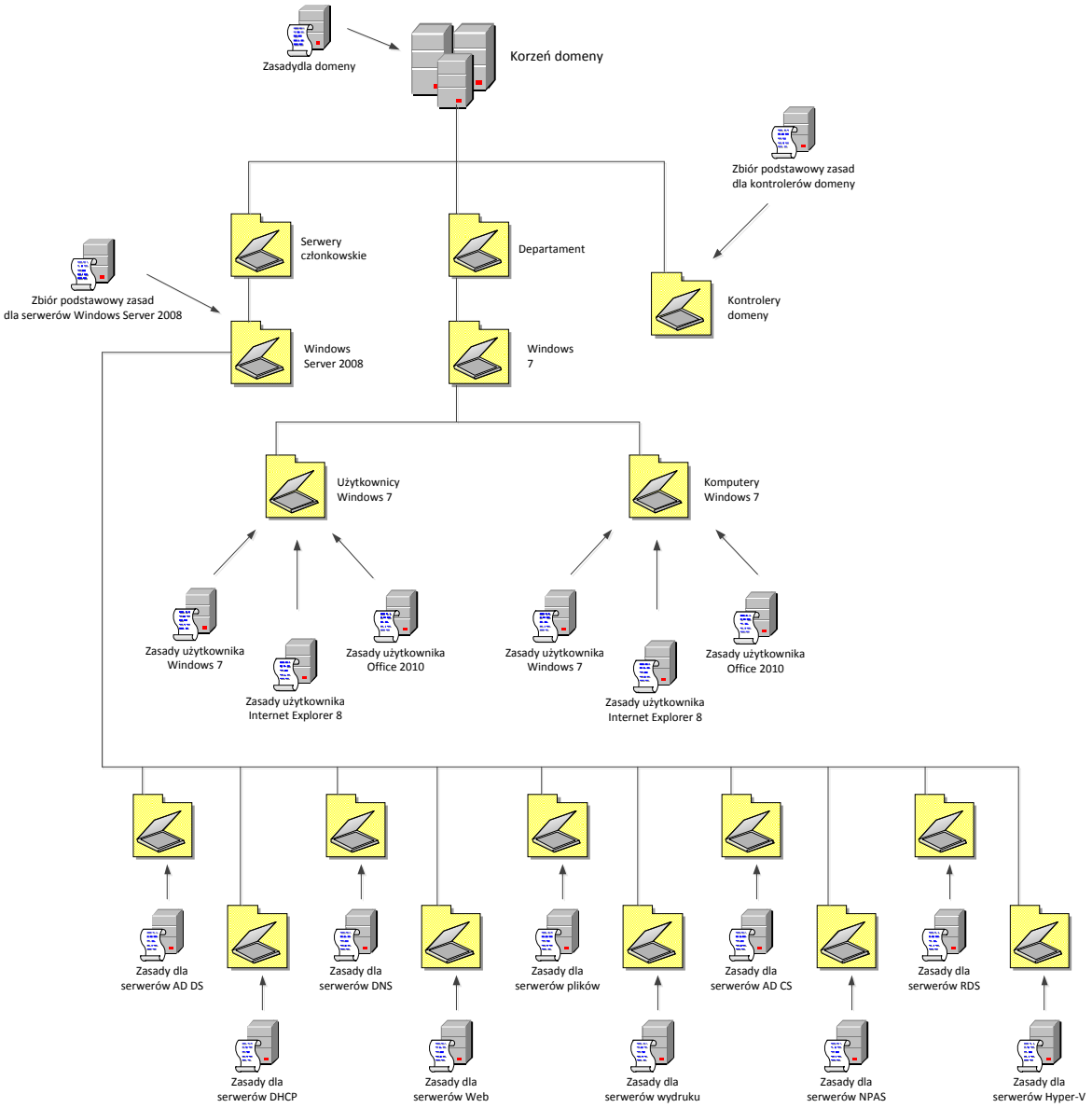
- Na poziomach: lokacji, domeny oraz jednostki organizacyjnej można zastosować opcję **Zablokuj dziedziczenie**. Jej włączenie powoduje, że ustawienia pochodzące od nadrzędnych zbiorów GPO nie są przekazywane do obiektów podrzędnych. Przy konfiguracji zawierającej opcje **Wymuszone** oraz **Zablokuj dziedziczenie** ważniejsza jest opcja **Wymuszone**.

W odniesieniu do wcześniej proponowanej struktury jednostek organizacyjnych (rys. 3.3.2), projekt zakładający wykorzystanie zasad grupowych powinien uwzględnić zbiory GPO zapewniające:

- zasady dla domeny
- zasady dla kontrolerów domeny

- zasady dla serwerów członkowskich
- zasady dla każdej roli serwerowej w organizacji
- zasady dla użytkowników zgromadzonych w jednostce organizacyjne**j Windows 7 SP1**
- zasady dla komputerów znajdujących się w jednostce **organizacyjnej Komputery**

Struktura spełniająca powyższe warunki została przedstawiona na rysunku 2.3.4.



Rys. 2.3.4. Przykładowa struktura jednostek organizacyjnych z dowiązaniami GPO dla infrastruktury Windows 7 SP1 oraz Windows Server 2008 R2

2.4. Zastosowanie filtrowania WMI w celu określenia dokładnej grupy docelowej odbiorców zasad GPO

Filtrowanie oparte o instrumentację zarządzania Windows WMI (z ang. Windows Management Instrumentation) zostało wprowadzone po raz pierwszy w systemach Windows XP i Windows Server 2003. Mechanizm WMI umożliwia dynamiczne sprawdzanie wartości tych atrybutów, na które ma

oddziaływać określony zbiór GPO. Atrybuty to dane konfiguracyjne sprzętu i/lub oprogramowania, na przykład:

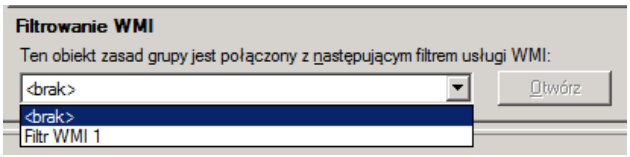
- rodzaj procesora
- wersja Windows
- dane producenta komputera
- wolne miejsce na dysku
- liczba procesorów logicznych
- dane odczytywane z rejestru
- informacje o sterownikach
- elementy systemu plików
- konfiguracja sieciowa
- dane aplikacji

Jeśli ze zbiorem GPO związany jest filtr WMI, na stacji nastąpi jego przetworzenie. Dzięki temu ustawienia GPO zostaną zastosowane tylko po spełnieniu warunków określonych filtrem WMI.

Zapytania WMI tworzone są przy wykorzystaniu języka WQL (z ang. WMI Query Language), który jest językiem podobnym do SQL (z ang. Structured Query Language). Zapytania mogą być łączone operatorami AND i OR – w zależności od potrzeb.

Każde zapytanie WMI jest wykonywane w przestrzeni nazewniczej WMI. Domyślną przestrzenią jest root\CIMv2.

Filtry WMI są oddzielnymi obiektami, niezależnymi od GPO. Aby zastosować filtr WMI, należy dołączyć go do zbioru GPO (rys. 2.4.1).



Rys. 2.4.1 Dołączanie filtru WMI do zbioru GPO.

Każdy zbiór GPO może posiadać tylko jeden filtr WMI. Natomiast pojedynczy filtr WMI może być dołączany do wielu GPO. Filtry WMI oraz powiązane zbiory GPO muszą znajdować się w tej samej domenie.

W tabeli 2.4.2 zawarte zostały przykłady filtrów WMI.

Kryterium	Cel administracyjny	Filtr WMI
Konfiguracja	Blokada możliwości włączania Microsoft Network Monitor (Netmon.exe) na stacjach, które mają włączony ruch grupowy	Select * from Win32_NetworkProtocol where SupportsMulticasting = true
Strefa czasowa	Stosowanie zasad na wszystkich serwerach zlokalizowanych w	Root\cimv2 ; Select * from win32_timezone

	Polsce	where bias =-60
Poprawki	Stosowanie zasad na komputerach z zainstalowaną określoną poprawką	Root\cimv2 ; Select * from Win32_QuickFixEngineering where HotFixID = 'q147222'
Inwentaryzacja oprogramowania	Przypisanie oprogramowania tylko do komputerów, które mają zainstalowany jeden lub więcej określonych pakietów oprogramowania	Root\cimv2;Select * from Win32_Product where name = "MSIPackage1" OR name = "MSIPackage2"
System operacyjny	Zastosowanie zasad wyłącznie na komputerach z Windows XP	Root\CimV2; Select * from Win32_OperatingSystem where Caption = "Microsoft Windows XP Professional"
Zasoby	Zastosowanie zasad wyłącznie na komputerach, które mają co najmniej 600 MB wolnego miejsca na dysku	Root\CimV2; Select * from Win32_LogicalDisk where FreeSpace > 629145600 AND Description <> "Network Connection"

Tab 2.4.2. Przykłady filtrów WMI

Tworzenie i zarządzanie filtrami WMI może być wykonane za pomocą dodatkowych narzędzi:

- WMI Administrative Tools

  http://www.microsoft.com/en-us/download/details.aspx?id=24045

- WMI Code Creator

http://www.microsoft.com/en-us/download/details.aspx?id=8572

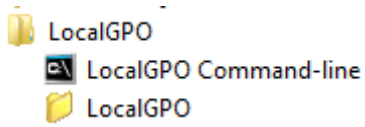
2.5. Omówienie narzędzia Local Policy Tool

Security Compliance Manager zawiera narzędzie tekstowe LocalGPO. Umożliwia ono wykonywanie wielu czynności obsługowych na zbiorach ustawień zasad grupowych, m.in.:

- stosowanie ustawień zabezpieczeń w kontekście lokalnych ustawień zasad grupowych
- eksport lokalnych ustawień zasad grupowych
- tworzenie pakietów zawierających ustawienia, które można stosować na stacjach, na których nie zainstalowano narzędzia LocalGPO
- centralizację lokalnych zbiorów zasad grupowych za pomocą Multiple Local GPO (MLGPO)
- aktualizację interfejsu graficznego potrzebnego do wyświetlenia dodatkowych ustawień zbiorów zasad grupowych w ramach grupy MSS (z ang. Microsoft Solutions for Security)

Narzędzie LocalGPO nie jest automatycznie instalowane wraz z SCM. Aby je zainstalować, należy uruchomić plik **LocalGPO.msi** z lokalizacji **c:\Program Files (x86)\Microsoft Security Compliance Manager\LGPO** i – wykorzystując kreatora – wybrać preferowane opcje instalacji.

Po pomyślnym zainstalowaniu LocalGPO folder narzędzia dostępny będzie w Menu Start:



Rys.2.5.1. Folder LocalGPO w Menu Start

2.6. Omówienie i praktyczne zastosowanie narzędzia Attack Surface Analyzer (ASA)

Firma Microsoft udostępniła narzędzie Attack Surface Analyzer (ASA), które umożliwia określenie zmian dokonywanych na systemie operacyjnym komputera podczas instalacji oprogramowania. Działanie narzędzia ASA poprzedzone jest każdorazowo wykonaniem testu stanu komputera. Po instalacji żądanego oprogramowania wyświetlany jest raport o zmianach w zakresie:

- usług
- sterowników
- uruchomionych procesów
- kontrolek COM
- serwerów DCOM
- zmian dokonanych w zakresie uprawnień domyślnych DCOM
- skojarzeń rozszerzeń plików
- kontrolek Microsoft ActiveX
- Internet Explorer Pluggable Protocol Handlers
- Internet Explorer Silent Elevation Entries
- Internet Explorer Preapproved Controls
- portów
- strumieni nazw
- reguł zapory
- punktów końcowych wywołań RPC
- wpisów ścieżek
- grup i członkostwa w nich
- zasobów sieciowych

Dzięki raportowi, który wykonuje ASA, można łatwo określić wpływ instalacji oprogramowania na funkcje Windows oraz w łatwy sposób go zweryfikować.

2.7. Omówienie mechanizmu kont MSA

Jedną z nowych funkcji w Windows 7 SP1 oraz Windows Server 2008 R2 są konta MSA (z ang. Managed Service Accounts), które pozwalają zmniejszyć ryzyko, które wiąże się z użytkowaniem kont służących do zarządzania usługami. Na stacjach lokalnych administrator może tak skonfigurować poszczególne aplikacje, by były one uruchamiane w powiązaniu z kontami: usługa lokalna, usługa sieciowa lub system lokalny. Rozwiązania tego nie można zastosować w przypadku domeny; zasięg jej działania uniemożliwia wykorzystanie kont.

Stosując standardowe konta użytkowników do uruchamiania aplikacji, należy zadbać o politykę zarządzania hasłami. Konta MSA umożliwiają pełną automatyzację w tym zakresie, a także przypisanie im nazwy głównej usługi SPN (z ang. Service Principal Name) oraz delegowanie zarządzania SPN.

Zarządzanie kontami MSA odbywa się wyłącznie z poziomu PowerShell.

Kontrolery domeny w systemach Windows Server 2008 i Windows Server 2003 posiadają wsparcie dla kont MSA.

2.8. Ustawienia zasad domenowych

Domyślnie do obiektów usługi katalogowej Active Directory Domain Services stosowana jest ograniczona liczba ustawień zabezpieczeń. Są one konfigurowane w obrębie węzła Konfiguracja komputera w ramach zbiorów:

- Zasady haseł
- Zasady blokady konta

Poniżej omówione zostały szczegółowe ustawienia dla tych gałęzi.

Zalecenia dotyczące ustawień znajdują się – w zależności od roli serwerowej – w narzędziu Security Compliance Manager (SCM).

2.8.1. Konfigurowanie ustawień dla zbioru Zasady haseł

Jednym z kluczowych założeń bezpieczeństwa systemów IT jest ustalona i dostosowana polityka dotycząca haseł. Takie elementy jak: złożoność haseł, cykliczność ich zmiany czy świadomość w zakresie ich przechowywania składają się na ogólną politykę bezpieczeństwa.

Zasady dotyczące haseł zorganizowane są w obrębie gałęzi:

Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady konta\Zasady haseł

(Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy)

Zasada	Poziom ważności	Ustawienie domyślne	Ustawienie zalecane przez Microsoft
Wymuszaj tworzenie historii haseł	Krytyczny	0 pamiętanych haseł	24 pamiętane hasła
Maksymalny okres ważności hasła	Krytyczny	42 dni	90 dni
Minimalny okres ważności hasła	Krytyczny	0 dni	1 dzień
Minimalna długość hasła	Krytyczny	0 znaków	12 znaków
Hasło musi spełniać wymagania co do złożoności	Krytyczny	Wyłączone	Włączone

Zapisz hasła dla wszystkich użytkowników w domenie, korzystając z szyfrowania odwracalnego	Krytyczny	Wyłączone	Wyłączone

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.

Aby wymusić na użytkownikach zmianę haseł tylko w ściśle określonym momencie, należy ustalić zasady dotyczące minimalnego i maksymalnego okresu użytkowania 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

2.9. Konfigurowanie ustawień haseł granularnych oraz dla zbioru Zasady blokady konta

Wśród ustawień związanych z hasłami użytkowników istotną rolę pełnią ustawienia haseł granularnych (ang. Fine-Grained Password) oraz Zasady blokady konta.

Hasła granularne to rozwiązanie umożliwiające wdrożenie modelu ustawień zasad haseł, który jest dedykowany określonym użytkownikom lub grupom użytkowników. Jest to możliwe w środowisku domenowym o poziomie funkcjonalności domeny od Windows Server 2008.

Zasady blokady konta zapewniają ochronę przed próbami odgadnięcia haseł użytkowników poprzez zliczanie błędnych prób logowania i wykonywanie określonej akcji związanej ze stanem konta użytkownika. Zasady blokady konta znajdują się w gałęzi:

Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady konta\Zasady blokady konta

(Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy)

Zasada	Poziom ważności	Ustawienie domyślne	Ustawienie zalecane przez Microsoft
Czas trwania blokady konta	Krytyczny	Brak	15 minut
Próg blokady konta	Krytyczny	0 nieudanych prób zalogowania	50 nieudanych prób zalogowania
Wyzeruj licznik blokady konta po upływie...	Krytyczny	Brak	15 minut

2.10. Ustawienia zasad Computer Policy Settings

Ustawienia zabezpieczeń stosowane dla obiektów Komputer skupione są wokół poniższych gałęzi:

- Zasady inspekcji
- Przypisywanie praw użytkownika
- Opcje zabezpieczeń
- Dziennik zdarzeń
- Zapora systemu Windows z zabezpieczeniami zaawansowanymi
- Szablony administracyjne

2.11. Konfigurowanie szczegółowych ustawień zbioru Zasady inspekcji

Zasady inspekcji umożliwiają gromadzenie – w określonych kategoriach – szczegółowych informacji na temat aktywności użytkowników i systemu.

W Windows 7 SP1 uwzględniono 9 kategorii głównych oraz ustawienia podkategorii. Są one dostępne w gałęzi Inspekcja globalnego dostępu do obiektów.

Zasady inspekcji kategorii głównych znajdują się w gałęzi:

Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Zasady inspekcji

(Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy)

- Przeprowadź inspekcję zdarzeń logowania na kontach
- Przeprowadź inspekcję dostępu do obiektów
- Przeprowadź inspekcję dostępu do usługi katalogowej
- Przeprowadź inspekcję śledzenia procesów
- Przeprowadź inspekcję użycia uprawnień
- Przeprowadź inspekcję zarządzania kontami
- Przeprowadź inspekcję zdarzeń logowania
- Przeprowadź inspekcję zdarzeń systemowych

Zasady inspekcji podkategorii znajdują się w gałęzi:

Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Konfiguracja zaawansowanych zasad inspekcji

(Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration)

Zasada	Poziom ważności	Ustawienie domyślne	Ustawienie zalecane przez Microsoft
Przeprowadź inspekcję weryfikacji poświadczeń	Krytyczny	Nie skonfigurowano	Sukces i Niepowodzenie
Przeprowadź inspekcję usługi uwierzytelniania Kerberos	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję operacji biletów usługi Kerberos	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję innych zdarzeń logowania na kontach	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję zarządzania grupami aplikacji	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję zarządzania kontami komputerów	Krytyczny	Nie skonfigurowano	Sukces
Przeprowadź inspekcję zarządzania grupami dystrybucyjnymi	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję innych zdarzeń zarządzania kontami	Krytyczny	Nie skonfigurowano	Sukces i Niepowodzenie
Przeprowadź inspekcję zarządzania grupami zabezpieczeń	Krytyczny	Nie skonfigurowano	Sukces i Niepowodzenie

Przeprowadź inspekcję zarządzania kontami użytkowników	Krytyczny	Nie skonfigurowano	Sukces i Niepowodzenie
Przeprowadź inspekcję działania DPAPI	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję tworzenia procesu	Krytyczny	Nie skonfigurowano	Sukces
Przeprowadź inspekcję zakończenia procesu	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję zdarzeń RPC	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję szczegółowej replikacji usługi katalogowej	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję dostępu do usługi katalogowej	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję zmian usługi katalogowej	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję replikacji usługi katalogowej	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję blokady konta	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję trybu rozszerzonego protokołu IPsec	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję trybu głównego protokołu IPsec	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję trybu szybkiego protokołu IPsec	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję wylogowywania	Krytyczny	Nie skonfigurowano	Sukces

Przeprowadź inspekcję logowania	Krytyczny	Nie skonfigurowano	Sukces i Niepowodzenie
Przeprowadź inspekcję serwera zasad sieciowych	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję innych zdarzeń logowania/wylogowywania	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję logowania specjalnego	Krytyczny	Nie skonfigurowano	Sukces
Przeprowadź inspekcję wygenerowanych przez aplikację	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję usług certyfikacji	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję szczegółowego udziału plików	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję udziału plików	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję systemu plików	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję połączenia platformy filtrowania	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję porzucania pakietów platformy filtrowania	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję manipulowania dojściem	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję obiektu jądra	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję innych zdarzeń dostępu do obiektów	Krytyczny	Nie skonfigurowano	Nie skonfigurowano

Przeprowadź inspekcję rejestru	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję SAM	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję zmiany zasad inspekcji	Krytyczny	Nie skonfigurowano	Sukces i Niepowodzenie
Przeprowadź inspekcję zmiany zasad uwierzytelniania	Krytyczny	Nie skonfigurowano	Sukces
Przeprowadź inspekcję zmiany zasad autoryzacji	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję zmiany zasad platformy filtrowania	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję zmiany zasad na poziomie reguły MPSSVC	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję innych zdarzeń zmiany zasad	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję niepoufnego użycia uprawnień	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję innych zdarzeń użycia uprawnień	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Przeprowadź inspekcję poufnego użycia uprawnień	Krytyczny	Nie skonfigurowano	Sukces i Niepowodzenie
Przeprowadź inspekcję sterownika IPsec	Krytyczny	Nie skonfigurowano	Sukces i Niepowodzenie
Przeprowadź inspekcję innych zdarzeń systemowych	Krytyczny	Nie skonfigurowano	Nie skonfigurowano

Przeprowadź inspekcję zmiany stanu zabezpieczeń	Krytyczny	Nie skonfigurowano	Sukces i Niepowodzenie
Przeprowadź inspekcję rozszerzenia systemu zabezpieczeń	Krytyczny	Nie skonfigurowano	Sukces i Niepowodzenie
Przeprowadź inspekcję integralności systemu	Krytyczny	Nie skonfigurowano	Sukces i Niepowodzenie
System plików	Krytyczny	Nie skonfigurowano	Nie skonfigurowano
Rejestr	Krytyczny	Nie skonfigurowano	Nie skonfigurowano

2.12. Konfigurowanie szczegółowych zasad zbioru Przypisywanie praw użytkownika

Przypisywanie praw użytkownika jest zbiorem ustawień, który można definiować, zapewniając użytkownikom możliwość wykonywania ściśle określonych czynności na systemie operacyjnym.

Zbiór Przypisywanie praw użytkownika znajduje się w gałęzi:

Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Przypisywanie praw użytkownika

(Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment)

Zasada	Poziom ważności	Ustawienie domyślne	Ustawienie zalecane przez Microsoft
Blokuj strony w pamięci	Istotny	-	-
Debuguj programy	Krytyczny	Administratorzy	Administratorzy
Dostosuj przydziały pamięci dla procesów	Istotny	Administratorzy, Usługa lokalna, Usługa sieciowa	Administratorzy, Usługa lokalna, Usługa sieciowa
Działanie jako część systemu operacyjnego	Krytyczny	-	-
Generuj inspekcje zabezpieczeń	Krytyczny	Usługa lokalna, Usługa sieciowa	Usługa lokalna, Usługa sieciowa
Logowanie w trybie usługi	Krytyczny	NT Services\All services	-

Logowanie w trybie wsadowym	Istotny	Administratorzy, Operatorzy kopii zapasowych, Użytkownicy dzienników wydajności	-
Ładuj i zwalniaj sterowniki urządzeń	Istotny	Administratorzy	Administratorzy
Modyfikuj etykietę obiektu	Istotny	-	-
Modyfikuj wartości środowiskowe oprogramowania układowego	Istotny	Administratorzy	Administratorzy
Obejdź sprawdzanie przy przechodzeniu	Krytyczny	Administratorzy, Operatorzy kopii zapasowych, Usługa lokalna, Usługa sieciowa, Użytkownicy, Wszyscy	Administratorzy, Usługa sieciowa, Usługa lokalna, Użytkownicy
Odmawiaj logowania za pomocą usług pulpitu zdalnego	Opcjonalny	-	-
Odmowa dostępu do tego komputera z sieci	Krytyczny	Gość	Goście
Odmowa logowania lokalnego	Krytyczny	Gość	Goście
Odmowa logowania w trybie usługi	Krytyczny	-	-
Odmowa logowania w trybie wsadowym	Krytyczny	-	Goście
Określ konta komputerów i użytkowników jako zaufane w kwestii delegowania	Krytyczny	-	-

Personifikuj klienta po uwierzytelnieniu	Istotny	Administratorzy, Usługa, Usługa lokalna, Usługa sieciowa	Administratorzy, Usługa, Usługa lokalna, Usługa sieciowa
Profiluj pojedynczy proces	Istotny	Administratorzy	-
Profiluj wydajność systemu	Istotny	Administratorzy, NT Service\WdiServiceHost	Administratorzy, NT Service\WdiServiceHost
Przejmij na własność pliki lub inne obiekty	Istotny	Administratorzy	Administratorzy
Przywracaj pliki i katalogi	Istotny	Administratorzy, Operatorzy kopii zapasowych	-
Synchronizuj dane usługi katalogowej	Istotny	-	-
Usuń komputer ze stacji dokującej	Opcjonalny	Administratorzy, Użytkownicy	Administratorzy, Użytkownicy
Utwórz łącza symboliczne	Istotny	Administratorzy	-
Utwórz obiekt tokenu	Istotny	-	-
Utwórz obiekty globalne	Istotny	Administratorzy, Usługa, Usługa lokalna, Usługa sieciowa	Administratorzy, Usługa, Usługa lokalna, Usługa sieciowa
Utwórz plik stronicowania	Krytyczny	Administratorzy	Administratorzy
Utwórz trwałe obiekty udostępnione	Istotny	-	-
Uzyskaj dostęp do Menedżera poświadczeń jako zaufany obiekt wywołujący	Istotny	-	-
Uzyskiwanie dostępu do tego komputera z sieci	Krytyczny	Administratorzy, Operatorzy kopii zapasowych, Użytkownicy, Wszyscy	Administratorzy, Użytkownicy

Wykonuj kopie zapasowe plików i katalogów	Istotny	Administratorzy, Operatorzy kopii zapasowych	-
Wykonuj zadania konserwacji woluminów	Krytyczny	Administratorzy	Administratorzy
Wymuszaj zamknięcie z systemu zdalnego	Krytyczny	Administratorzy	Administratorzy
Zamień token na poziomie procesu	Istotny	Usługa lokalna, Usługa sieciowa	Usługa lokalna, Usługa sieciowa
Zamknij system	Istotny	Administratorzy, Operatorzy kopii zapasowych, Użytkownicy	Administratorzy, Użytkownicy
Zarządzaj dziennikami inspekcji i zabezpieczeń	Krytyczny	Administratorzy	Administratorzy
Zezwalaj na logowanie lokalne	Krytyczny	Administratorzy, Goście, Operatorzy kopii zapasowych, Użytkownicy	Administratorzy, Użytkownicy
Zezwalaj na logowanie za pomocą usług pulpitu zdalnego	Istotny	Administratorzy, Użytkownicy pulpitu zdalnego	-
Zmień czas systemowy	Istotny	Administratorzy, Usługa lokalna	Administratorzy, Usługa lokalna
Zmień strefę czasową	Istotny	Administratorzy, Usługa lokalna, Użytkownicy	Administratorzy, Usługa lokalna, Użytkownicy
Zwiększ priorytet planowania	Istotny	Administratorzy	Administratorzy
Zwiększ zestaw roboczy procesu	Istotny	Użytkownicy	Administratorzy, Usługa lokalna

2.13. Konfigurowanie szczegółowych zasad zbioru Opcje zabezpieczeń

Ustawienia w ramach gałęzi Opcje zabezpieczeń zapewniają szeroki zakres możliwości konfiguracji zabezpieczeń, które są uporządkowane według grup.

Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Opcje zabezpieczeń

(Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options)

Zasada	Poziom ważności	Ustawienie domyślne	Ustawienie zalecane przez Microsoft
Członek domeny: maksymalny wiek hasła konta komputera	Krytyczny	30 dni	30 dni
Członek domeny: podpisuj cyfrowo dane bezpiecznego kanału – gdy to możliwe	Krytyczny	Włączone	Włączone
Członek domeny: szyfruj cyfrowo dane bezpiecznego kanału – gdy to możliwe	Krytyczny	Włączone	Włączone
Członek domeny: szyfruj lub podpisuj cyfrowo dane bezpiecznego kanału – zawsze	Krytyczny	Włączone	Włączone
Członek domeny: wyłącz zmiany hasła konta komputera	Krytyczny	Wyłączone	Wyłączone
Członek domeny: wymagaj silnego klucza sesji (system Windows 2000 lub nowszy)	Krytyczny	Wyłączone	Włączone
DCOM: Ograniczenia dotyczące dostępu do komputera w składni języka SDDL (Security Descriptor Definition Language)	Opcjonalny	Niezdefiniowane	Niezdefiniowane
DCOM: Ograniczenia dotyczące uruchamiania komputera w składni języka SDDL (Security Descriptor Definition Language)	Opcjonalny	Niezdefiniowane	Niezdefiniowane

Dostęp sieciowy: nazwane potoki, do których można uzyskiwać dostęp anonimowo	Istotny	-	Niezdefiniowane
Dostęp sieciowy: nie zezwalaj na anonimowe wyliczanie kont SAM	Krytyczny	Włączone	Włączone
Dostęp sieciowy: nie zezwalaj na anonimowe wyliczanie kont SAM i udziałów	Krytyczny	Wyłączone	Włączone
Dostęp sieciowy: nie zezwalaj na przechowywanie haseł ani poświadczeń do uwierzytelniania sieciowego	Krytyczny	Wyłączone	Niezdefiniowane
Dostęp sieciowy: ogranicz anonimowy dostęp do nazwanych potoków i udziałów	Istotny	Włączone	Włączone
Dostęp sieciowy: ścieżki rejestru, do których można uzyskiwać dostęp anonimowo	Istotny	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion

Dostęp sieciowy: ścieżki rejestru, do których można uzyskiwać dostęp anonimowo i ścieżki podrzędne	Krytyczny	System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog	System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog

Dostęp sieciowy: udostępnianie i model zabezpieczeń dla kont lokalnych	Krytyczny	Klasyczny – uwierzytelnianie użytkowników lokalnych, jako samych siebie	Klasyczny – uwierzytelnianie użytkowników lokalnych, jako samych siebie
Dostęp sieciowy: udziały, do których można uzyskiwać dostęp anonimowo	Istotny	Niezdefiniowane	-
Dostęp sieciowy: zezwalaj na anonimową translację identyfikatorów SID/nazw	Krytyczny	Wyłączone	Wyłączone
Dostęp sieciowy: zezwalaj na stosowanie uprawnień Wszyscy do anonimowych użytkowników	Krytyczny	Wyłączone	Wyłączone
Inspekcja: inspekcjonuj dostęp do globalnych obiektów systemu	Krytyczny	Wyłączone	Niezdefiniowane
Inspekcja: inspekcjonuj użycie prawa do wykonywania kopii zapasowych i przywracania	Krytyczny	Wyłączone	Niezdefiniowane
Inspekcja: wymuś ustawienia podkategorii zasad inspekcji (system Windows Vista lub nowszy), aby zastąpić ustawienia kategorii zasad inspekcji	Krytyczny	Niezdefiniowane	Włączone
Inspekcja: zamknij system natychmiast, jeśli nie można rejestrować wyników inspekcji	Krytyczny	Wyłączone	Wyłączone

Klient sieci Microsoft: podpisuj cyfrowo komunikację (za zgodą serwera)	Krytyczny	Włączone	Włączone
Klient sieci Microsoft: podpisuj cyfrowo komunikację (zawsze)	Krytyczny	Wyłączone	Włączone
Klient sieci Microsoft: wyślij niezaszyfrowane hasło w celu nawiązania połączenia z innymi serwerami SMB	Krytyczny	Wyłączone	Wyłączone
Konsola odzyskiwania: zezwalaj na automatyczne logowanie administracyjne	Krytyczny	Wyłączone	Wyłączone
Konsola odzyskiwania: zezwalaj na kopiowanie na dyskietkę oraz dostęp do wszystkich dysków i folderów	Istotny	Wyłączone	Niezdefiniowane
Konta: ogranicz używanie pustych haseł przez konta lokalne tylko do logowania do konsoli	Krytyczny	Włączone	Włączone
Konta: Stan konta administratora	Krytyczny	Wyłączone	Niezdefiniowane
Konta: Stan konta gościa	Krytyczny	Wyłączone	Wyłączone
Konta: Zmienianie nazwy konta administratora	Krytyczny	Administrator	Niezdefiniowane
Konta: Zmienianie nazwy konta gościa	Istotny	Gość	Niezdefiniowane

Kontrola konta użytkownika: podnoszenie uprawnień tylko tych aplikacji z poziomem UIAccess, które są zainstalowane w bezpiecznych lokalizacjach	Krytyczny	Włączone	Włączone
Kontrola konta użytkownika: podnoszenie uprawnień tylko tych plików wykonywalnych, które są podpisane i mają sprawdzoną poprawność	Krytyczny	Wyłączone	Wyłączone
Kontrola konta użytkownika: przełącz na bezpieczny pulpit przy monitowaniu o podniesienie uprawnień	Krytyczny	Włączone	Włączone
Kontrola konta użytkownika: tryb zatwierdzania przez administratora dla wbudowanego konta administratora	Krytyczny	Wyłączone	Włączone
Kontrola konta użytkownika: uruchamianie wszystkich administratorów w trybie zatwierdzania przez administratora	Krytyczny	Włączone	Włączone
Kontrola konta użytkownika: wirtualizuj błędy zapisu plików i rejestru w lokalizacjach poszczególnych użytkowników	Krytyczny	Włączone	Włączone

Kontrola konta użytkownika: wykrywanie instalacji aplikacji i monitowanie o podniesienie uprawnień	Krytyczny	Włączone	Włączone
Kontrola konta użytkownika: zachowanie monitu o podniesienie uprawnień dla administratorów w trybie zatwierdzania przez administratora	Krytyczny	Monituj o zgodę na pliki binarne niepochodzące z systemu Windows	Monituj o poświadczenia
Kontrola konta użytkownika: zachowanie monitu o podniesienie uprawnień dla użytkowników standardowych	Krytyczny	Monituj o poświadczenia	Automatycznie odrzucaj żądania podniesienia
Kontrola konta użytkownika: zezwalaj aplikacjom z poziomem UIAccess na monitowanie o podniesienie uprawnień bez używania bezpiecznego pulpitu	Krytyczny	Wyłączone	Wyłączone
Kryptografia systemu: użyj zgodnych algorytmów FIPS dla celów szyfrowania, tworzenia skrótu i podpisywania	Istotny	Wyłączone	Niezdefiniowane
Kryptografia systemu: wymuś mocną ochronę klucza dla kluczy użytkowników przechowywanych na komputerze	Istotny	Wyłączone	Niezdefiniowane

Logowanie interakcyjne: liczba poprzednich zalogowań do zbuforowania (w przypadku niedostępności kontrolera domeny)	Krytyczny	10 logowań	2 logowania
Logowanie interakcyjne: monituj użytkownika o zmianę hasła przed jego wygaśnięciem	Krytyczny	14 dni	14 dni
Logowanie interakcyjne: nie wymagaj naciśnięcia klawiszy CTRL+ALT+DEL	Krytyczny	Niezdefiniowane	Wyłączone
Logowanie interakcyjne: nie wyświetlaj nazwy ostatniego użytkownika	Krytyczny	Wyłączone	Włączone
Logowanie interakcyjne: tekst komunikatu dla użytkowników próbujących się zalogować	Krytyczny	Niezdefiniowane	Niezdefiniowane
Logowanie interakcyjne: tytuł komunikatu dla użytkowników próbujących się zalogować	Krytyczny	Niezdefiniowane	Niezdefiniowane
Logowanie interakcyjne: wymagaj karty inteligentnej	Istotny	Wyłączone	Niezdefiniowane
Logowanie interakcyjne: wymagaj uwierzytelnienia kontrolera domeny do odblokowania stacji roboczej	Krytyczny	Wyłączone	Włączone

Logowanie interakcyjne: wyświetlaj informacje o użytkowniku, gdy sesja jest zablokowana	Krytyczny	Niezdefiniowane	Niezdefiniowane
Logowanie interakcyjne: zachowanie przy usuwaniu karty inteligentnej	Istotny	Brak akcji	Zablokuj stację roboczą
Obiekty systemu: wymagaj nierozróżniania wielkości liter dla podsystemów innych niż Windows	Istotny	Włączone	Włączone
Obiekty systemu: wzmocnij uprawnienia domyślne wewnętrznych obiektów systemu (np. łączy symbolicznych)	Krytyczny	Włączone	Włączone
Serwer sieci Microsoft: okres bezczynności wymagany dla wstrzymania sesji	Krytyczny	15 minut	15 minut
Serwer sieci Microsoft: podpisuj cyfrowo komunikację (za zgodą klienta)	Krytyczny	Wyłączone	Włączone
Serwer sieci Microsoft: podpisuj cyfrowo komunikację (zawsze)	Krytyczny	Wyłączone	Włączone
Serwer sieci Microsoft: poziom sprawdzania poprawności docelowej głównej nazwy usługi serwera	Krytyczny	Niezdefiniowane	Niezdefiniowane
Serwer sieci Microsoft: rozłączaj klientów po upływie limitu czasu logowania	Krytyczny	Włączone	Włączone

Urządzenia: ogranicz dostęp do stacji CD-ROM tylko do użytkownika zalogowanego lokalnie	Opcjonalny	Niezdefiniowane	Niezdefiniowane
Urządzenia: ogranicz dostęp do stacji dyskietek tylko do użytkownika zalogowanego lokalnie	Opcjonalny	Niezdefiniowane	Niezdefiniowane
Urządzenia: zapobiegaj instalacji sterowników drukarek przez użytkowników	Istotny	Wyłączone	Włączone
Urządzenia: zezwalaj na oddokowywanie bez potrzeby logowania się	Opcjonalny	Włączone	Niezdefiniowane
Urządzenia: zezwolono na formatowanie i wysunięcie wymiennego nośnika	Istotny	Niezdefiniowane	Administratorzy i użytkownicy interakcyjni
Ustawienia systemowe: opcjonalne podsystemy	Opcjonalny	Posix	Niezdefiniowane
Ustawienia systemowe: użyj reguł certyfikatów do plików wykonywalnych systemu Windows dla Zasad ograniczeń oprogramowania	Istotny	Wyłączone	Niezdefiniowane
Zabezpieczenia sieci: minimalne zabezpieczenia sesji dla klientów opartych na NTLM SSP (włączając secure RPC)	Krytyczny	Wymagaj szyfrowania 128-bitowego	Wymaga zabezpieczeń sesji NTLMv2, Wymagaj szyfrowania 128-bitowego

Zabezpieczenia sieci: minimalne zabezpieczenia sesji dla serwerów opartych na NTLM SSP (włączając secure RPC)	Krytyczny	Wymagaj szyfrowania 128-bitowego	Wymaga zabezpieczeń sesji NTLMv2, Wymagaj szyfrowania 128-bitowego
Zabezpieczenia sieci: nie przechowuj wartości skrótu (hash) programu LAN Manager dla następnej zmiany hasła	Krytyczny	Włączone	Włączone
Zabezpieczenia sieci: poziom uwierzytelniania LAN Manager	Krytyczny	Wyślij tylko odpowiedź NTLMv2	Wyślij tylko odpowiedź NTLMv2. Odmów LM i NTLM.
Zabezpieczenia sieci: wymagania podpisywania klienta LDAP	Krytyczny	Negocjuj podpisywanie	Negocjuj podpisywanie
Zabezpieczenia sieciowe: konfigurowanie typów szyfrowania dozwolonych dla protokołu Kerberos	Istotny	Niezdefiniowane	Niezdefiniowane
Zabezpieczenia sieciowe: Ograniczania ruchu NTLM: Dodaj wyjątki dla serwerów z tej domeny	Krytyczny	Niezdefiniowane	Niezdefiniowane
Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Dodaj wyjątki dla serwerów zdalnych w celu uwierzytelniania NTLM	Krytyczny	Niezdefiniowane	Niezdefiniowane
Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Przeprowadź inspekcję przychodzącego ruchu NTLM	Krytyczny	Niezdefiniowane	Niezdefiniowane

Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Przeprowadź inspekcję uwierzytelniania NTLM w tej domenie	Krytyczny	Niezdefiniowane	Niezdefiniowane
Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Przychodzący ruch NTLM	Krytyczny	Niezdefiniowane	Niezdefiniowane
Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Uwierzytelnianie NTLM w tej domenie	Krytyczny	Niezdefiniowane	Niezdefiniowane
Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Wychodzący ruch NTLM do serwerów zdalnych	Krytyczny	Niezdefiniowane	Niezdefiniowane
Zabezpieczenia sieciowe: Wymuś wylogowanie użytkowników po upłynięciu czasu logowania	Istotny	Wyłączone	Niezdefiniowane
Zabezpieczenia sieciowe: Zezwalaj kontu systemowi lokalnemu na używanie pustych sesji	Istotny	Niezdefiniowane	Niezdefiniowane
Zabezpieczenia sieciowe: Zezwalaj lokalnemu systemowi na uwierzytelnianie NTLM przy użyciu tożsamości komputera	Istotny	Niezdefiniowane	Niezdefiniowane

Zabezpieczenia sieciowe: Zezwalaj na wysyłanie żądań uwierzytelniania PKU2U do tego komputera w celu używania tożsamości online	Istotny	Niezdefiniowane	Niezdefiniowane
Zamknięcie: wyczyść plik stronicowania pamięci wirtualnej	Krytyczny	Wyłączone	Wyłączone
Zamknięcie: zezwalaj na zamykanie systemu bez konieczności zalogowania	Istotny	Włączone	Niezdefiniowane

2.14. Konfigurowanie ustawień MSS

Wśród wielu ustawień zabezpieczeń istnieją takie, które nie mają reprezentacji w postaci zasad GPO. Można je za to definiować poprzez bezpośrednie wpisy w rejestrze. Ustawienia tego typu posiadają prefiks MSS (z ang. Microsoft Solutions for Security).

Ważnym aspektem zarządzania ustawieniami MSS jest to, że nie są kasowane wraz z usuwaniem szablonów zabezpieczeń. To wymusza ich ręczną konfigurację z poziomu rejestru systemu (regedit32.exe).

2.15. Potencjalne zagrożenia związane z zasadami podpisywania cyfrowego pakietów SMB

Protokół SMB (z ang. Server Message Block), znany również jako CIFS (z ang. Common Internet File System), zapewnia metody udostępniania zasobów komputerowych takich jak: pliki, drukarki czy porty szeregowe.

W sytuacji, gdy klient wykorzystujący SMB w wersji 1 nawiązuje połączenie w sesji konta innego niż konto Gość lub loguje się nieanonimowo, kiedy zasady podpisywania SMB są włączone, włącza on podpisywanie cyfrowe komunikacji dla serwera; kolejne nawiązane sesje będą dziedziczyły i stosowały podpisaną cyfrowo komunikację SMB. Aby podwyższyć poziom bezpieczeństwa, w Windows 7 SP1 zasady bezpieczeństwa połączenia uwierzytelnionego przez serwer są chronione przed degradacją do poziomu sesji Gość lub Anonimowe.

Powyższa zasada nie znajduje zastosowania, gdy kontrolery domeny pracują pod kontrolą Windows Server 2003, a stacjami klienckimi są Windows Vista SP2 lub Windows Server 2008.

Mając to na uwadze, aby zachować jednolite zachowanie zasad podpisywania pakietów SMB, należy skonfigurować poniższe ustawienia znajdujące się w gałęzi:

Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Opcje zabezpieczeń

(Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options)

- w zakresie kontrolera domeny pracującego pod kontrolą Windows Server 2003:

Zasada	Poziom ważności	Ustawienie domyślne	Ustawienie zalecane przez Microsoft
Serwer sieci Microsoft: podpisuj cyfrowo komunikację (za zgodą klienta)	Krytyczny	Włączony	Włączony
Serwer sieci Microsoft: podpisuj cyfrowo komunikację (zawsze)	Krytyczny	Włączony	Włączony

- W zakresie komputerów będących członkami domeny pracującymi pod kontrolą Windows Vista SP1 lub Windows Server 2008

Zasada	Poziom ważności	Ustawienie domyślne	Ustawienie zalecane przez Microsoft
Serwer sieci Microsoft: podpisuj cyfrowo komunikację (za zgodą klienta)	Krytyczny	Wyłączone	Włączony
Serwer sieci Microsoft: podpisuj cyfrowo komunikację (zawsze)	Krytyczny	Wyłączone	Włączony

Omawiane problemy zostały rozwiązane w Windows Server 2008 R2 oraz Windows Vista SP2.

2.16. Ograniczenie stosowania mechanizmu uwierzytelnienia NTLM

Uwierzytelnianie NT LAN Manager (NTLM) stosowane jest w wielu sieciach komputerowych – nawet jeśli dostępne są bezpieczniejsze protokoły uwierzytelniania Windows. W Windows 7 SP1 pojawiły się nowe zasady zabezpieczeń, pozwalające na analizę i ograniczanie wykorzystania NTLM w środowisku IT. Funkcje te obejmują zbieranie danych, analizę ruchu NTLM oraz proces metodyczny, który wprowadza ograniczenia w ruchu NTLM na rzecz silniejszych protokołów uwierzytelniania, takich jak

Kerberos. Ograniczenie użycia protokołu NTLM wymaga wiedzy, jak wykorzystywany jest on przez aplikację, oraz znajomości strategii i kroków niezbędnych w konfiguracji infrastruktury do pracy z innymi protokołami.

Zasady umożliwiające audyt oraz ograniczenie wykorzystania ruchu NTLM znajdują się w gałęzi:

Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Opcje zabezpieczeń

(Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options)

i obejmują:

- w zakresie audytu:
  - Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Przeprowadź inspekcję przychodzącego ruchu NTLM
  - Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Przeprowadź inspekcję uwierzytelniania NTLM w tej domenie
- w zakresie ograniczania:
  - Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Przychodzący ruch NTLM
  - Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Uwierzytelnianie NTLM w tej domenie
  - Zabezpieczenia sieciowe: Ograniczanie ruchu NTLM: Wychodzący ruch NTLM do serwerów zdalnych

2.17. Konfigurowanie szczegółowych zasad zbioru Dziennik zdarzeń

Rejestrowanie zdarzeń należy do najważniejszych zadań realizowanych w obszarze bezpieczeństwa Windows, które można przeglądać z poziomu Dziennika zdarzeń. Istotnym aspektem konfiguracji są atrybuty dzienników związane z ich rozmiarem, prawami dostępu oraz metodą nadpisywania zdarzeń.

Zasady umożliwiające konfigurację wymienionych atrybutów znajdują się gałęzi:

Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Dziennik zdarzeń

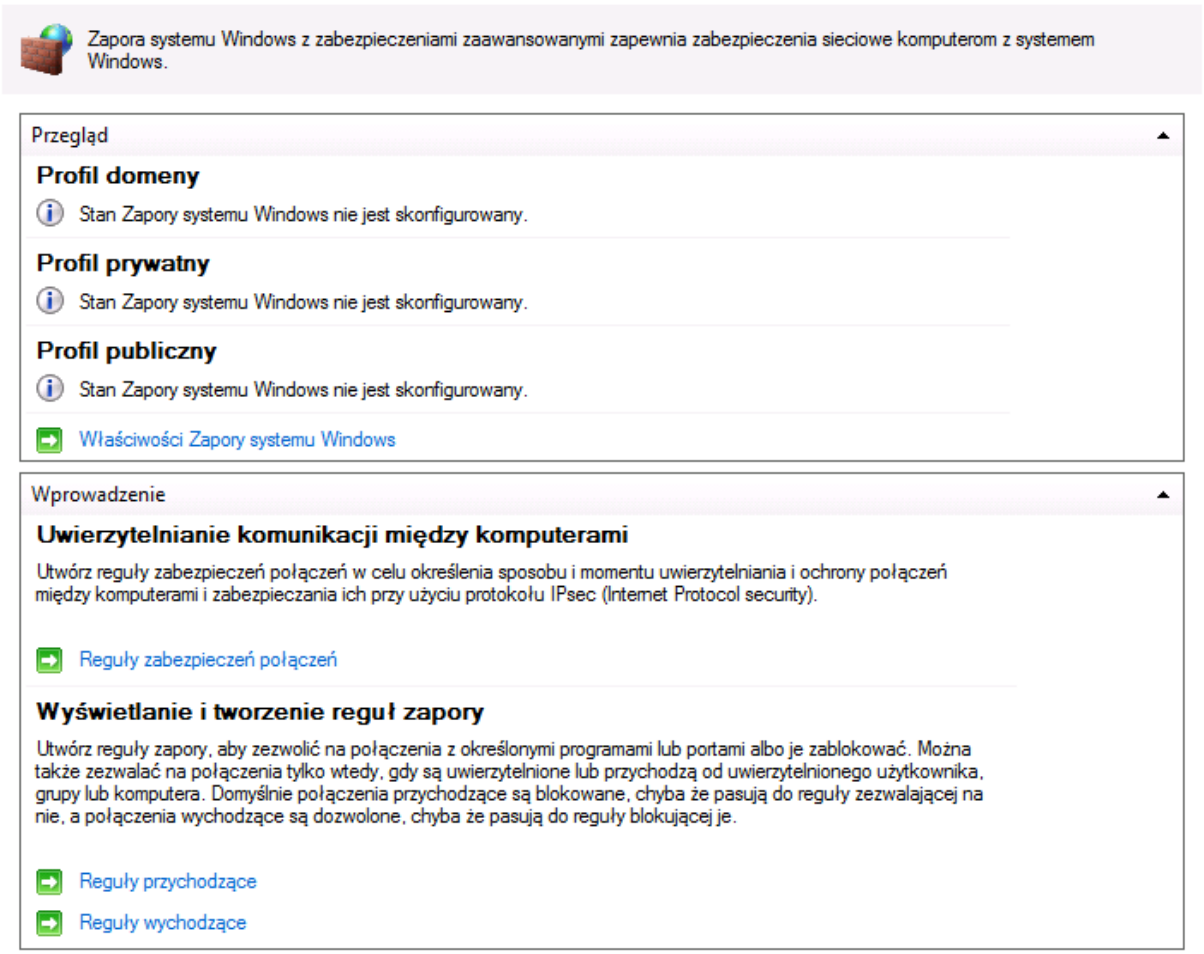
(Computer Configuration\Windows Settings\Security Settings\Event Log)

- Maksymalny rozmiar dziennika aplikacji
- Maksymalny rozmiar dziennika systemu
- Maksymalny rozmiar dziennika zabezpieczeń
- Metoda przechowywania dziennika aplikacji
- Metoda przechowywania dziennika systemu
- Metoda przechowywania dziennika zabezpieczeń
- Odmawiaj dostępu lokalnej grupie gości do dziennika aplikacji
- Odmawiaj dostępu lokalnej grupie gości do dziennika systemu
- Odmawiaj dostępu lokalnej grupie gości do dziennika zabezpieczeń
- Przechowuj dziennik aplikacji przez
- Przechowuj dziennik systemu przez
- Przechowuj dziennik zabezpieczeń przez

2.18. Szczegółowa konfiguracja zapory systemu Windows Firewall with Advanced Security

Precyzyjna konfiguracja narzędzia Zapora systemu Windows z zabezpieczeniami zaawansowanymi jest możliwa z poziomu zasad grupowych w ramach gałęzi:
Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zapora systemu Windows z zabezpieczeniami zaawansowanymi

(Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security)



Rys. 2.18.1. Ustawienia zasad grupowych dla Zapory systemu Windows z ustawieniami zaawansowanymi

W ramach dostępnych ustawień można dokonywać zmian w zakresie:

- ustawień ogólnych zapory dostępnych we właściwościach narzędzia Zapora systemu Windows z zabezpieczeniami zaawansowanymi
- wyświetlania i tworzenia reguł wchodzących i wychodzących zapory
- wyświetlania i tworzenia reguł w zakresie uwierzytelniania komunikacji między komputerami

Przystępując do konfiguracji ustawień, należy sprecyzować profil sieciowy, dla którego będą definiowane ustawienia.

Zapora systemu Windows z zabezpieczeniami zaawansowanymi udostępnia profile sieciowe opisane poniżej:

Profil domenowy
Profil stosowany jest, kiedy komputer został podłączony do sieci oraz nastąpiło uwierzytelnienie do kontrolera domeny, do którego należy komputer. Domyślna konfiguracja profilu umożliwia nawiązywanie sesji Pulpitu zdalnego oraz Pomocy zdalnej.

Profil prywatny
Profil stosowany jest, jeśli użytkownik posiadający poświadczenia lokalnego administratora przypisze go w ramach bieżącego połączenia sieciowego. Zaleca się, by profil prywatny używany był w sieciach zaufanych.

Profil publiczny
Jest to profil domyślny, stosowany, gdy komputer nie jest dołączony do domeny. Profil ten zawiera zbiór najbardziej restrykcyjnych ustawień, w których wyłączona jest komunikacja wchodząca.

2.19. Usługa Windows Update

Usługa Windows Update umożliwia systematyczne sprawdzanie dostępności aktualizacji komponentów systemu Windows. Wszystkie poprawki są dystrybuowane domyślnie poprzez witrynę Windows Update. Istnieje także możliwość lokalnej dystrybucji poprawek z centralną synchronizacją do witryny Windows Update. Taką metodę pozwala zastosować serwer WSUS (z ang. Windows Server Update Services)[13]. Serwer WSUS zapewnia:

- administracyjną kontrolę synchronizacji poprawek z witryny Windows Update, które będą dystrybuowane lokalnie
- lokalny serwer Windows Update
- administracyjną kontrolę nad poprawkami
- automatyczną aktualizację komputerów (stacji roboczych i/lub serwerów)

Konfiguracja klientów serwera WSUS realizowana jest poprzez ustawienia zasad grupowych, dostępne w gałęzi:

Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Usługa Windows Update

(Computer Configuration\Administrative Templates\Windows Components\Windows Update)

- Nie wyświetlaj opcji „Zainstaluj aktualizacje i zamknij system” w oknie dialogowym Zamykanie systemu Windows
- Nie ustawiaj opcji domyślnej na „Zainstaluj aktualizacje i zamknij system” w oknie dialogowym Zamykanie systemu Windows
- Włączanie Opcji zasilania, aby funkcja Windows Update automatycznie wznawiała system w celu zainstalowania zaplanowanych aktualizacji
- Konfigurowanie aktualizacji automatycznych

[13] http://technet.microsoft.com/en-us/windowsserver/bb332157.aspx

- Określ lokalizację intranetowej usługi aktualizującej firmy Microsoft
- Częstotliwość wykrywania aktualizacji automatycznych
- Zezwalaj, aby użytkownicy inni niż administratorzy otrzymywali powiadomienia aktualizacji
- Włącz powiadomienia o oprogramowaniu
- Zezwalaj na natychmiastową instalację aktualizacji automatycznych
- Włącz zalecane aktualizacje za pomocą aktualizacji automatycznych
- Bez automatycznego uruchamiania ponownego dla zaplanowanych instalacji aktualizacji automatycznych przy zalogowanych użytkownikach
- Ponów monit o ponowne uruchomienie komputera z zaplanowanymi instalacjami
- Opóźniaj ponowne uruchomienie komputera dla zaplanowanych instalacji
- Zaplanuj ponownie zaplanowane instalacje aktualizacji automatycznych
- Włącz konfigurowanie docelowej strony klienta
- Zezwalaj na podpisane aktualizacje z intranetowej lokalizacji usługi aktualizacji firmy Microsoft

Do prawidłowego działania klienta z serwerem WSUS należy skonfigurować minimum cztery zasady:

- Określ lokalizację intranetowej usługi aktualizującej firmy Microsoft
- Konfigurowanie aktualizacji automatycznych
- Bez automatycznego uruchamiania ponownego dla zaplanowanych instalacji aktualizacji automatycznych przy zalogowanych użytkownikach
- Zaplanuj ponownie zaplanowane instalacje aktualizacji automatycznych

2.20. Ataki na usługę zintegrowanego uwierzytelniania systemu Windows polegające na przekazywaniu poświadczeń

Poradniki bezpieczeństwa Microsoft – MSA (z ang. Microsoft Security Advisory) – zawierają informację na temat ryzyka ataków związanych z przechwyceniem poświadczeń użytkownika wykorzystującego usługę zintegrowanego uwierzytelniania systemu Windows IWA (z ang. Integrated Windows Authentication). Tego typu naruszenia bezpieczeństwa mogą wystąpić poprzez ataki typu człowiek pośrodku (ang. man-in-the-middle) lub poprzez sprowokowanie użytkownika do uruchomienia konkretnego odnośnika.

Przykłady powyższych typów ataków:

- Przekazanie poświadczeń

  Atak następuje, kiedy przechwycone poświadczenia są wykorzystywane do logowania się do innych usług niż te, do których miała dostęp ofiara ataku.
- Odbicie poświadczeń

  Tego typu atak zakłada wykorzystanie przechwyconych poświadczeń do ponownego logowania się na komputerze ofiary.

Aby zmniejszyć ryzyko tego typu ataków, udostępniono funkcję EPA (z ang. Extended Protection for Authentication). Jest ona zawarta w systemach Windows 7 SP1 oraz w Windows Server 2008 R2 SP1; dla poprzednich wersji Windows można ją pobrać jako aktualizację.

Szczegółowe informacje o konfiguracji EPA dla wcześniejszych wersji Windows znajdują się w KB968389 (http://support.microsoft.com/kb/968389).

W założeniach zintegrowanego uwierzytelniania Windows przyjęto, że niektóre odpowiedzi uwierzytelniania są uniwersalne, co sprawia, że w łatwy sposób mogą zostać powtórne użyte lub przekazane. Dlatego jako minimalne zabezpieczenie zaleca się, by konstrukcja odpowiedzi w komunikacji zawierała określone informacje o kanale komunikacji. Dzięki temu usługi mają zapewnioną rozszerzoną ochronę w zakresie odpowiedzi uwierzytelniania zawierających określone informacje dotyczące usług, takie jak SPN (z ang. Service Principal Name).

3. Sposoby ochrony przed złośliwym oprogramowaniem

Oprogramowanie złośliwe, tzw. malware (ang. **mal**icious soft**ware**), to każdy program komputerowy lub skrypt wykazujący szkodliwe lub złośliwe działanie w stosunku do użytkownika komputera. Przykładami oprogramowania złośliwego są: wirusy, robaki, konie trojańskie, rootkity oraz oprogramowanie szpiegujące (ang. spyware), które gromadzą informacje na temat działalności użytkownika bez uprzedniej zgody użytkownika systemu.

Windows 7 wprowadził nowe technologie, które mogą zostać wykorzystane w celu zapewnienia ochrony przed oprogramowaniem złośliwym na komputerach pracujących pod kontrolą systemu Windows 7 SP1. Rozdział ten zawiera przegląd funkcji zabezpieczeń i rekomendacje dotyczące konfigurowania i stosowania tych technologii.

Rekomendowane ustawienia nowych funkcji zabezpieczeń w systemie Windows 7 SP1 mogą zostać wprowadzone poprzez zastosowanie zasad grupowych, opisanych w rozdziale „Wdrażanie rekomendowanych zasad bezpieczeństwa w kontekście bazowych ustawień systemu Windows 7". W wielu przypadkach wymagane są jednak informacje charakterystyczne dla danego środowiska systemu komputerowego, które ma wpływ na wybór funkcji i ustawień. Dlatego też większość rekomendowanych wartości dla dodatkowych ustawień nie zostało zawartych w niniejszym przewodniku.

Wszystkie opisane funkcje z ustawionymi wartościami domyślnymi zapewniają dodatkowy poziom ochrony komputerów pracujących pod kontrolą systemów Windows 7 SP1. Dostępne są jednak nowe ustawienia zasad grupowych, które mogą – poprzez dostosowanie działań i funkcjonalności poszczególnych komponentów systemu – zapewnić jeszcze lepszą ochronę przed złośliwym oprogramowaniem dla własnego środowiska.

3.1. Wprowadzenie do funkcji zabezpieczeń stosowanych w systemie Windows 7 SP1

System Windows 7 SP1 zawiera następujące nowe i rozszerzone technologie, które zapewniają ochronę przed złośliwym oprogramowaniem:

- Konsola Centrum akcji (ang. Action Center)
- Kontrola konta użytkownika (ang. User Account Control – UAC)
- Zabezpieczenia biometryczne (ang. Biometric Security)
- Windows Defender
- Narzędzie do usuwania złośliwego oprogramowania (ang. Malicious Software Removal Tool)
- Zapora systemu Windows
- AppLocker

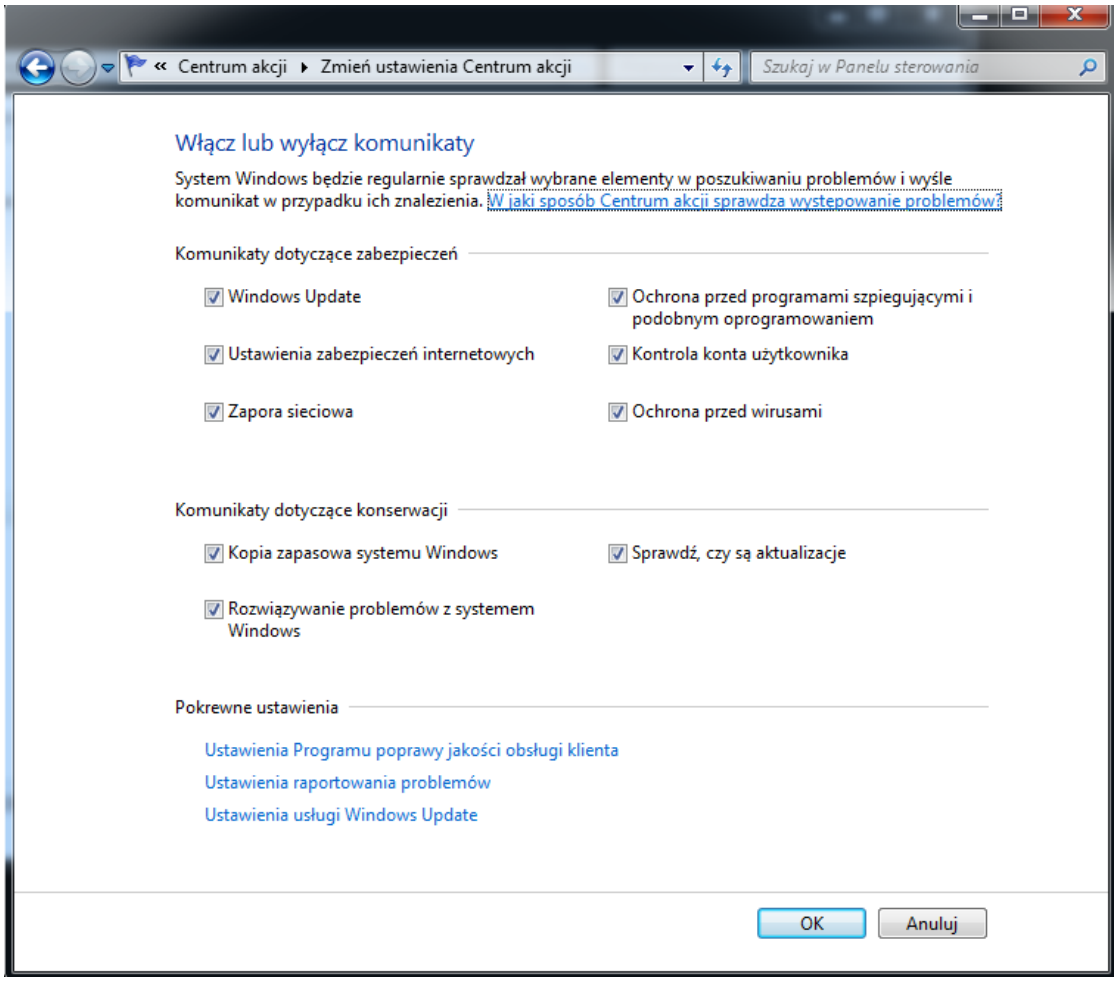
Ponadto w celu zwiększenia bezpieczeństwa rekomenduje się, by logowanie do systemu przebiegało z wykorzystaniem konta zwykłego użytkownika (nieposiadającego uprawnień administracyjnych). Dodatkowo wysoce rekomendowane jest zainstalowanie programu antywirusowego, który zapewnia ochronę w czasie rzeczywistym przez nowymi zagrożeniami, pojawiającymi się każdego dnia.

Przykładem takiego rozwiązania jest System Center 2012 Endpoint Protection[14]. Jeśli dana organizacja stosuje strategię defense-in-depth, zaleca się określenie dodatkowych usług przeszukujących zasoby pod katem zagrożeń. Usługi te mogą być pobrane ze stron firmy Microsoft – jako składnik systemu Windows 7 SP1 lub dodatkowa funkcjonalność w formie programu lub usługi.

Należy podkreślić, iż nawet zastosowanie wszystkich możliwych technologii zabezpieczeń nie uchroni użytkowników komputerów przed ryzykiem niebezpieczeństwa, jeśli w odpowiedni sposób nie zabezpieczymy i nie będziemy kontrolowali dostępu do kont, które posiadają uprawnienia na poziomie administracyjnym, do zabezpieczanych komputerów.

3.2. Konsola Centrum akcji

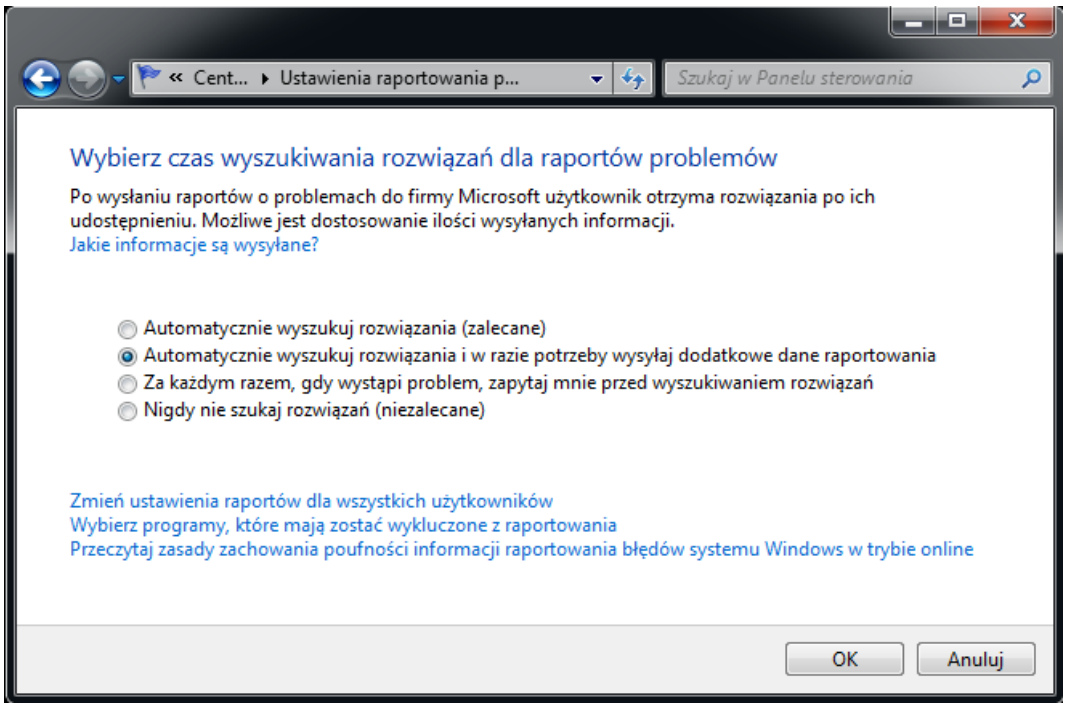
Centrum akcji to centralne miejsce, w którym użytkownik może wyświetlać alerty i podejmować działania mające na celu zapewnienie sprawnego funkcjonowania systemu Windows. W Centrum akcji wyświetlana jest lista ważnych komunikatów dotyczących ustawień zabezpieczeń oraz konserwacji, które wymagają uwagi użytkownika. Zakres wyświetlanych komunikatów, które mogą być wyłączane lub włączane, został przedstawiony na rysunku 3.2.1 (ustawienia konsoli Zmień ustawienia Centrum akcji).



Rys. 3.2.1. Widok okna **Zmień ustawienia Centrum akcji**

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

Konsola Centrum akcji – poza raportowaniem i powiadamianiem użytkowników systemu Windows 7 SP1 o występujących problemach, pozwala na kontrolowanie zakresu informacji wysyłanych do firmy Microsoft w celu wykrycia i rozwiązania problemów. Ustawienia raportowania problemów zostały przedstawione na rysunku 3.2.2.



Rys. 3.2.2. Widok okna **Ustawienia raportowania problemów**

Każdy użytkownik może przejrzeć informacje dotyczące raportowania problemów, które wysyłane są do firmy Microsoft, stosując się do poniższej instrukcji:

1. Otwórz główne okno **Centrum akcji**.
2. Wybierz opcję **Konserwacja**.
3. Kliknij na hiperłącze **Wyświetl historię niezawodności,** znajdujące się poniżej opcji **Wyszukaj rozwiązania dotyczące raportów o problemach.**
4. Na liście historii niezawodności kliknij dwukrotnie na dowolnym zdarzeniu, aby wyświetlić jego szczegóły techniczne.
5. Zdarzenia wyświetlone w sekcji **Informacje** zwykle zawierają szczegóły zmian dokonanych w konfiguracji sprzętu lub oprogramowania.

Aby dowiedzieć się więcej na temat raportowania problemów i zasad zachowania poufności informacji, odwiedź witrynę Microsoft: Usługa raportowania błędów firmy Microsoft — zasady zachowania poufności informacji[15].

[15]http://oca.microsoft.com/pl/dcp20.asp

Zastosowanie ustawień zasad grup w celu minimalizacji ryzyka dla Centrum akcji

Konfiguracja tych ustawień dostępna jest w dwóch lokalizacjach, w gałęziach:

Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Raportowanie błędów systemu Windows
(Computer Configuration\Windows Components\Windows Error Reporting)

Poniższa tabela przedstawia szczegółowe ustawienia zabezpieczeń dla omawianej funkcji, dostępne w systemie Windows 7 SP1.

Ustawienie zasad	***Opis***	***Domyślne ustawienie w systemie Windows 7 SP1***
Wyłącz funkcję Raportowanie błędów systemu Windows	Jeżeli to ustawienie zostanie włączone, funkcja Raportowanie błędów systemu Windows nie będzie wysyłać do firmy Microsoft żadnych informacji o problemach. Ponadto w aplecie Centrum akcji w Panelu sterowania nie będą dostępne informacje dotyczące rozwiązania.	Nie skonfigurowano

Tabela 3.2.1. Ustawienia Centrum akcji w systemie Windows

Konfiguracja użytkownika\Szablony administracyjne\Menu Start i pasek zadań

(User Configuration\Start Menu and Taskbar\)

Poniższa tabela przedstawia szczegółowe ustawienia zabezpieczeń dostępne w systemie Windows 7 SP1 dla omawianej funkcji.

Ustawienie zasad	***Opis***	***Domyślne ustawienie w systemie Windows 7 SP1***
Usuń ikonę Centrum akcji	Zapobiega wyświetlaniu ikony Centrum akcji w obszarze kontroli systemu. Jeżeli to ustawienie zostanie włączone, ikona Centrum akcji nie będzie wyświetlana w obszarze powiadomień systemu. Jeżeli to ustawienie zostanie wyłączone lub nie zostanie skonfigurowane, ikona Centrum akcji będzie wyświetlana w obszarze powiadomień systemu.	Nie skonfigurowano

Tabela 3.2.2. Ustawienia Centrum akcji w systemie Windows

3.3. Mechanizm Kontrola konta użytkownika (User Account Control – UAC)

System Windows Vista wprowadził mechanizm kontroli konta użytkownika (ang. User Account Control – UAC), aby ułatwić korzystanie z oprogramowania użytkownikowi, który nie posiada uprawnień administracyjnych. Funkcja ta powiadomi użytkownika w sytuacji, gdy na komputerze będą miały zostać dokonane zmiany wymagające uprawnień na poziomie administratora. Na mechanizm UAC składa się kilka rozwiązań:

- Konto Protected Administrator (PA)
- Podnoszenie uprawnień (ang. UAC elevation prompts)
- Wirtualizacja rejestru (ang. registry virtualization)
- Wirtualizacja systemu plików (ang. file system virtualization)
- Poziomy integralności Windows (ang. Windows Integrity levels)

Mimo że korzystanie z konta skonfigurowanego w trybie Protected Administrator (PA) wiąże się z nieco wyższym poziomem bezpieczeństwa niż ten, który zapewnia konto administratora niechronionego tym mechanizmem, to w zwykłej, codziennej pracy zaleca się wciąż – jako rozwiązanie najbardziej bezpieczne – korzystanie z konta standardowego użytkownika. Zminimalizuje to ryzyko związane z oprogramowaniem złośliwym, które wykorzystując wysokie uprawnienia użytkownika, potrafi zainstalować niechciane aplikacje lub dokonać nieautoryzowanych zmian w systemie Windows.

W systemie Windows 7 SP1 można ustawić tryb i częstotliwość powiadamiania użytkownika o próbie wprowadzenia zmian na komputerze. 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 zanim programy wprowadzą na komputerze lub w systemie Windows zmiany wymagające uprawnień administratora. Gdy zostanie wyświetlone powiadomienie, pulpit zostanie przyciemniony, a użytkownik – zanim wykona jakąkolwiek inną czynność na komputerze – będzie musiał zaakceptować lub odrzucić prośbę w oknie dialogowym funkcji Kontrola konta użytkownika. Przyciemnienie pulpitu jest nazywane bezpiecznym pulpitem; inne programy nie mogą działać w czasie, gdy pulpit jest przyciemniony.	Jest to najbezpieczniejsze ustawienie. Po wyświetleniu powiadomienia użytkownik powinien uważnie przeczytać treść każdego z okien dialogowych nim zezwoli na wprowadzenie zmian na komputerze.
Powiadamiaj mnie tylko	Użytkownik będzie powiadamiany zanim programy wprowadzą na komputerze lub w	Użytkownik będzie powiadamiany zanim programy wprowadzą na

wtedy, gdy programy próbują wprowadzać zmiany na komputerze	systemie Windows zmiany wymagające uprawnień administratora. Użytkownik nie będzie powiadamiany, gdy w ustawieniach systemu Windows samodzielnie wprowadzi zmiany wymagające uprawnień administratora. Użytkownik będzie powiadamiany, gdy program zewnętrzny – spoza systemu Windows – będzie próbował wprowadzić zmiany w ustawieniach systemu Windows.	komputerze lub w systemie Windows zmiany wymagające uprawnień administratora. Użytkownik nie będzie powiadamiany, gdy w ustawieniach systemu Windows samodzielnie wprowadzi zmiany wymagające uprawnień administratora. Użytkownik będzie powiadamiany, gdy program zewnętrzny – 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 zanim programy wprowadzą na komputerze lub w systemie Windows zmiany wymagające uprawnień administratora. Użytkownik nie będzie powiadamiany, gdy w ustawieniach systemu Windows samodzielnie wprowadzi zmiany wymagające uprawnień administratora. Użytkownik będzie powiadamiany, gdy program zewnętrzny – 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. Stanowi to małe zagrożenie dla bezpieczeństwa, jeśli złośliwy program już działa na komputerze.
Nie powiadamiaj nigdy	Użytkownik nie będzie powiadamiany przed wprowadzeniem jakichkolwiek zmian na komputerze. Jeśli użytkownik jest zalogowany jako administrator, programy mogą bez jego	Użytkownik nie będzie powiadamiany przed wprowadzeniem jakichkolwiek zmian na komputerze. Jeśli użytkownik jest

	wiedzy wprowadzać zmiany na komputerze. Jeśli użytkownik jest zalogowany jako użytkownik standardowy, wszelkie zmiany wymagające uprawnień administratora zostaną automatycznie odrzucone. Po wybraniu tego ustawienia konieczne będzie ponowne uruchomienie komputera w celu ukończenia procesu wyłączania funkcji Kontrola konta użytkownika. Po wyłączeniu funkcji Kontrola konta użytkownika użytkownicy logujący się jako administrator będą mieć zawsze uprawnienia administratora.	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. Po wybraniu tego ustawienia konieczne będzie ponowne uruchomienie komputera w celu ukończenia procesu wyłączania funkcji Kontrola konta użytkownika. Po wyłączeniu funkcji Kontrola konta użytkownika użytkownicy logujący się jako administrator będą mieć zawsze uprawnienia administratora. **Ustawienie niezalecane.**

Tabela. 3.3.1. Opis ustawień funkcji Kontrola konta użytkownika

Gdy technologia UAC została wprowadzona po raz pierwszy, powiadomienia były wysyłane do użytkownika systemu zbyt często. Sprawiło to, że większość użytkowników wyłączyło to ustawienie, zmniejszając w ten sposób poziom bezpieczeństwa komputera. W systemie Windows 7 SP1 prośby o podniesienie poświadczeń wyświetlane są rzadziej – tak, aby umożliwić standardowemu użytkownikowi wykonanie większej liczby zadań. Dodatkowo podczas wykorzystania konta PA niektóre programy zawarte w systemie Windows 7 SP1 mogą automatycznie podnosić poziom uprawnień – bez wyświetlenia powiadomienia.

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

Funkcja zatwierdzania przez administratora (ang. Administrator Approval Mode) w technologii AC zapewnia komputerom z systemami: Windows 7 SP1 oraz Windows Vista Service Pack 1 (SP1) ograniczoną ochronę przed niektórymi typami oprogramowania złośliwego. Większość programów i funkcjonalności w systemie Windows 7 SP1 będzie poprawnie działało na koncie użytkownika standardowego; kiedy zajdzie potrzeba wykonania czynności administracyjnych (np. instalacji

oprogramowania lub modyfikacji ustawień systemu), system powiadomi o tym użytkownika i poprosi go o udzielenie zgody na wykonanie wymaganych zadań. Tryb ten nie zapewnia jednak tego samego poziomu zabezpieczeń, co konto standardowego użytkownika, i nie gwarantuje, iż oprogramowanie złośliwe, które już znajduje się na komputerze, nie będzie mogło skorzystać z możliwości podniesienia uprawnień dla własnej aplikacji, aby wykonać czynności szkodliwych dla komputera, na którym się znajduje.

Ocena ryzyka

Użytkownicy, którzy posiadają uprawnienia administracyjne podczas normalnej pracy w systemie, narażeni są na to, że czynności administracyjne zostaną wykonane bez ich wiedzy – w sposób przypadkowy lub szkodliwy. Poniżej przedstawiono kilka przykładów takich sytuacji:

- Użytkownik pobrał i zainstalował oprogramowanie szkodliwe ze strony internetowej, która została spreparowana, celowo zarażona wirusem lub zaatakowana przez malware.
- Użytkownik został podstępnie zwabiony do otworzenia załącznika z poczty elektronicznej zawierającego oprogramowanie złośliwe, które zainstalowało się w sposób automatyczny i niezauważalny na komputerze użytkownika.
- Nośnik pamięci przenośnej został podłączony do komputera i funkcja autoodtwarzania samoczynnie uruchomiła i zainstalowała oprogramowanie złośliwe.
- Użytkownik zainstalował niewspieraną lub niesprawdzoną aplikację, która wpływa na wydajność komputera i jego awaryjność.

Minimalizacja ryzyka

W codziennych czynnościach wykonywanych na komputerach pod kontrolą systemu Windows rekomendowane jest stosowanie kont użytkownika standardowego bez uprawnień administracyjnych. Podczas wykorzystywania mechanizmu UAC w celu podniesienia uprawnień i wprowadzenia poświadczeń dla konta administratora zaleca się otwarcie innej sesji dla administratora, stosując rozwiązanie umożliwiające szybkie przełączanie użytkowników.

Zagadnienia minimalizacji ryzyka wymagające rozważenia

Mechanizm UAC pomaga zminimalizować zagrożenie zdefiniowane w poprzedniej sekcji („Ocena ryzyka”), jednak ważne jest, aby przed zastosowaniem technologii UAC rozważyć podjęcie poniższych kroków:

- Jeśli wewnętrzny dział programistów dostarcza aplikacje we własnym zakresie, rekomendowane jest zapoznanie się z artykułem "Windows Vista Application Development Requirements for User Account Control Compatibility"[16]. Dokument ten opisuje, w jaki sposób należy projektować i dostarczać aplikacje zgodne z mechanizmem UAC.

- Aplikacje niekompatybilne z technologią UAC mogą spowodować problemy w działaniu domyślnie włączonego trybu UAC. Ważne jest więc, aby przeprowadzić testy aplikacji na zgodność z technologią UAC zanim nowe oprogramowanie zostanie wdrożone w środowisku produkcyjnym. Więcej informacji na temat testów kompatybilności aplikacji znajduje się w rozdziale 6.

[16] http://go.microsoft.com/fwlink/?linkid=104243

- Włączenie UAC znacznie zwiększa liczbę żądań, które dotyczą podniesienia uprawnień lub stosowania kont administracyjnych, podczas normalnych czynności wykonywanych przez użytkowników systemu. Gdy takie działanie wyraźnie wpływa na wydajność pracy administratorów, można rozważyć skonfigurowanie ustawienia zasady grup **Kontrola konta użytkownika: zachowanie monitu o podniesienie uprawnień dla administratorów w trybie zatwierdzania przez administratora,** korzystając z opcji **Podnieś uprawnienia bez monitowania.** Jednakże zmiana ta obniża poziom bezpieczeństwa konfiguracji komputerów i zwiększa ryzyko ataku przez oprogramowanie złośliwe.

- Użytkownik, który posiada uprawnienia administracyjne i posługuje się kontem Protected Administrator (PA), może wyłączyć funkcję zatwierdzania przez administratora (ang. Administrator Approval Mode). Ponadto może on wyłączyć UAC tak, aby system nie powiadamiał o konieczności podnoszenia uprawnień w celu instalacji aplikacji lub dokonania zmian w systemie. Jeśli użytkownicy posiadają uprawnienia administracyjne na komputerach w organizacji, nie można zagwarantować, iż stosowane zasady grup dotyczące mechanizmu UAC będą skuteczne.

- Rekomendowane jest stosowanie dwóch kont dla administratorów systemów. Pierwsze powinno służyć do wykonywania na komputerze wszystkich normalnych czynności i zadań jako standardowy użytkownik, nieposiadający uprawnień administracyjnych. Gdy wymagane jest zastosowanie uprawnień administracyjnych, administratorzy systemu powinni zalogować się, korzystając z drugiego konta, i wykonać na nim określone czynności administracyjne. Po zakończeniu działań należy się wylogować i powrócić do normalnej pracy z wykorzystaniem konta standardowego użytkownika.

- Wskazane w tym przewodniku ustawienia zasad grup nie pozwalają standardowemu użytkownikowi na podnoszenie uprawnień. Rozwiązanie takie jest stosowane na komputerach, które korzystają z domeny Active Directory. Jest to rekomendowane ustawienie, które wymusza, by czynności administracyjne wykonywane były tylko przez użytkowników posiadających konta z przypisanymi uprawnieniami administracyjnymi.

- Jeśli aplikacja zostanie niepoprawnie zidentyfikowana jako aplikacja wymagająca uprawnień administracyjnych lub aplikacja użytkownika, system Windows może uruchomić takie oprogramowanie w złym kontekście zabezpieczeń.

Proces minimalizacji ryzyka

Proces minimalizacji ryzyka należy rozpocząć od zbadania i przetestowania pełnych możliwości mechanizmu UAC. Dodatkowe informacje w tym zakresie można uzyskać na stronach Microsoft: Understanding and Configuring User Account Control in Windows Vista[17] oraz Getting Started with User Account Control on Windows Vista[18].

W celu minimalizacji ryzyka zaleca się wykonanie poniższych działań:

1. Ustalenie liczby użytkowników, którzy wykonują zadania administracyjne.

[17] http://go.microsoft.com/fwlink/?linkid=148165
[18] http://go.microsoft.com/fwlink/?linkid=84129

2. Określenie, jak często wykonywane są zadania administracyjne.
3. Określenie, w jaki sposób czynności administracyjne są wykonywane przez administratorów: prostszy, realizowany poprzez powiadomienie UAC i wyrażanie zgody na wykonanie danej czynności, czy wymagający wprowadzenia określonych poświadczeń w celu wykonania zadań administracyjnych.
4. Określenie, czy standardowi użytkownicy powinni mieć możliwość podniesienia uprawnień w celu wykonania zadań administracyjnych. Zastosowane ustawienia zasad grupowych wskazane w tym przewodniku wyraźnie blokują możliwość podnoszenia uprawnień standardowym użytkownikom.
5. Zidentyfikowanie sposobu obsługi procesu instalacji aplikacji na komputerach.
6. Konfiguracja ustawień zasad grupowych dla UAC dopasowanych do indywidualnych potrzeb i wymagań.

Zastosowanie ustawień zasad grupowych w celu minimalizacji ryzyka dla UAC

Konfiguracja tych ustawień dostępna jest w gałęzi:

Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zasady lokalne\Opcje zabezpieczeń

(Computer Configuration\Windows Settings\Security Settings\Local Policy\Security Options\)

Poniższa tabela przedstawia szczegółowe ustawienia zabezpieczeń dostępne w systemie Windows 7 SP1 dla omawianego zagadnienia:

Ustawienie zasad	***Opis***	***Domyślne ustawienie w systemie Windows 7 SP1***
Kontrola konta użytkownika: tryb zatwierdzania przez administratora dla wbudowanego konta administratora	To ustawienie zasad decyduje o funkjjonalności trybu zatwierdzania przez administratora dla wbudowanego konta administratora.	Wyłączone
Kontrola konta użytkownika: zezwalaj aplikacjom z poziomem UIAccess na monitowanie o podniesienie uprawnień bez używania bezpiecznego pulpitu	To ustawienie zabezpieczeń kontroluje, czy programy z funkcją dostępności interfejsu użytkownika (UIAccess lub UIA, User Interface Accessibility) mogą automatycznie wyłączać bezpieczny pulpit na potrzeby monitowania o podniesienie uprawnień przez użytkownika standardowego.	Wyłączone
Kontrola konta użytkownika: zachowanie monitu o podniesienie uprawnień dla administratorów w trybie zatwierdzania przez administratora	To ustawienie zabezpieczeń określa zachowanie monitu o podniesienie uprawnień dla administratorów.	Monituj o zgodę na pliki binarne niepochodzące z systemu Windows

Kontrola konta użytkownika: zachowanie monitu o podniesienie uprawnień dla użytkowników standardowych	To ustawienie zabezpieczeń określa zachowanie monitu o podniesienie uprawnień dla użytkowników standardowych.	Monituj o poświadczenia
Kontrola konta użytkownika: wykrywanie instalacji aplikacji i monitowanie o podniesienie uprawnień	To ustawienie zabezpieczeń steruje procesem wykrywania instalacji aplikacji dla komputera.	Włączone
Kontrola konta użytkownika: podnoszenie uprawnień tylko tych plików wykonywalnych, które są podpisane i mają sprawdzoną poprawność	To ustawienie zabezpieczeń wymusza sprawdzanie podpisów infrastruktury kluczy publicznych (PKI) dla każdej aplikacji interakcyjnej, która żąda podniesienia uprawnień. Administratorzy przedsiębiorstwa mogą kontrolować listę dozwolonych aplikacji administratora poprzez dodanie certyfikatów znajdujących się w magazynie zaufanych wydawców na komputerach lokalnych.	Wyłączone
Kontrola konta użytkownika: Podnieś uprawnienia tylko tych aplikacji z poziomem UIAccess, które są zainstalowane w bezpiecznych lokalizacjach	To ustawienie zabezpieczeń kontroluje, czy aplikacje żądające wykonywania działań z poziomem integralności UIAccess muszą znajdować się w bezpiecznej lokalizacji systemu plików. Bezpieczne lokalizacje ograniczają się do następujących katalogów: - …\Program Files\ wraz z podkatalogami - …\Windows\system32 - …\Program Files (x86)\ wraz z podkatalogami dla 64-bitowych wersji systemu Windows Uwaga: system Windows wymusza sprawdzanie podpisu infrastruktury kluczy publicznych (PKI) w każdej aplikacji interaktywnej, która żąda wykonywania działań z poziomem	Włączone

	integralności UIAccess, niezależnie od stanu tego ustawienia zabezpieczeń.	
Kontrola konta użytkownika: uruchamianie wszystkich administratorów w trybie zatwierdzania przez administratora	To ustawienie zabezpieczeń kontroluje zachowanie wszystkich zasad funkcji Kontrola konta użytkownika dla komputera.	Włączone
Kontrola konta użytkownika: przełącz na bezpieczny pulpit przy monitowaniu o podniesienie uprawnień	To ustawienie zabezpieczeń kontroluje zachowanie wszystkich zasad funkcji Kontrola konta użytkownika dla komputera.	Włączone
Kontrola konta użytkownika: wirtualizuj błędy zapisu plików i rejestru w lokalizacjach poszczególnych użytkowników	To ustawienie zabezpieczeń kontroluje przekierowywanie błędów zapisu starszych aplikacji do zdefiniowanych lokalizacji – zarówno w rejestrze, jak i w systemie plików. Funkcja ta ogranicza aplikacje, które wcześniej były uruchamiane z uprawnieniami administratora i w czasie działania zapisywały dane aplikacji, do katalogów %ProgramFiles%, %Windir%, %Windir%\system32 lub HKLM\Software\.	Włączone

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnego ustawienia można znaleźć w zakładce **POMOC** w ustawieniach Edytora obiektów zasad grupy.

3.4. Zabezpieczenia biometryczne

Windows 7 SP1 zawiera strukturę biometryczną systemu Windows (ang. Windows Biometric Framework), obsługującą czytniki linii papilarnych oraz inne urządzenia biometryczne przez aplikacje wyższego poziomu. Wbudowane komponenty systemu Windows zapewniają wsparcie tej czynności z poziomu systemu operacyjnego i ułatwiają obsługę rozpoznawania linii papilarnych przez aplikacje korzystające z rozwiązań biometrycznych. W poprzednich wersjach systemu Windows do prawidłowej obsługi i logowania do systemu z zastosowaniem linii papilarnych potrzebne były sterowniki i aplikacje firm trzecich. System Windows 7 obsługuje natywnie rozwiązania biometryczne, wymagając jedynie instalacji sterownika do urządzenia czytnika biometrycznego.

Ocena ryzyka

Standardowe metody weryfikacji użytkownika, z zastosowaniem hasła, posiadają liczne wady, które mogą stwarzać zagrożenie dla bezpieczeństwa zarządzanego środowiska informatycznego. Gdy hasła są jedynym mechanizmem uwierzytelniającym użytkowników, istnieje ryzyko, że zostaną one przez

użytkowników zapomniane lub zapisane na kartkach bądź staną się łatwym celem ataku siłowego, przeprowadzanego na systemie w celu ujawnienia i pozyskania haseł. Aby zwiększyć poziom ochrony kont użytkowników, należy stosować wieloczynnikowe metody uwierzytelniania przy użyciu takich urządzeń jak karty inteligentne. Mechanizm ten wymaga od użytkownika wprowadzenia informacji, którą zna (PIN), oraz zastosowania czegoś, co posiada fizycznie (karta inteligenta). Metoda ta zwiększa poziom bezpieczeństwa uwierzytelnienia, ale nadal podatna jest na utratę i – w niewielkim stopniu – na modyfikację.

Minimalizacja ryzyka

Zastosowane wsparcie dla urządzeń biometrycznych w systemie Windows 7 SP1 pozwala organizacjom na wprowadzenie dodatkowego sposobu weryfikacji tożsamości, realizowanego poprzez wymaganie informacji będącej integralną częścią weryfikowanej osoby. Wbudowany mechanizm obsługi czytników biometrycznych w Windows 7 SP1 może współpracować z wieloma różnymi typami uwierzytelnienia biometrycznego. Coraz większa dostępność czytników linii papilarnych oraz ich niska cena sprawiły, że forma uwierzytelnienia biometrycznego może zostać skutecznie wdrożona w wielu organizacjach.

Identyfikacja na podstawie linii papilarnych oferuje następujące zalety:

- odcisk palca pozostaje w normalnych okolicznościach niezmienny przez całe życie
- nie występują dwa identyczne odciski palca (nawet w przypadku bliźniąt)
- czytniki linii papilarnych stały się tańsze i przez to ogólnie dostępne
- proces skanowania linii papilarnych jest prosty i szybki
- stopień niezawodności skanowanych próbek jest wysoki; system ten cechuje się małą liczbą błędnych próbek biometrycznych (ang. false acceptance rate [FAR]) w porównaniu z innymi formami biometrycznego skanowania, takimi jak rozpoznawanie twarzy lub analiza głosu

Identyfikacja na podstawie linii papilarnych posiada również wady:

- użytkownicy z uszkodzonymi (poprzez obrażenia fizyczne naskórka) odciskami palców nie będą mogli się uwierzytelnić w sposób poprawny
- zostało udowodnione naukowo, iż możliwe jest uzyskanie dostępu do komputerów poprzez przedstawienie systemowi spreparowanych odcisków palców. Aby uzyskać dodatkowe informacje na ten temat, należy odwiedzić witrynę: Impact of Artificial "Gummy" Fingers on Fingerprint Systems[19]
- wiek użytkownika oraz zakres wykonywanej przez niego pracy fizycznej mogą wpłynąć na poziom niezawodności procesu skanowania linii papilarnych

Zagadnienia minimalizacji ryzyka wymagające rozważenia

[19] http://cryptome.org/gummy.htm

Mechanizm weryfikacji biometrycznej, takiej jak odciski linii papilarnych, jest częścią procesu wdrażania systemu Windows 7 SP1. Przed wdrożeniem takiego rozwiązania należy zastanowić się nad przedstawionymi poniżej kwestiami:

- Systemy biometryczne zwykle wymagają odpowiedniego przetwarzania wrażliwych danych biometrycznych użytkowników, które przechowywane są na komputerach, by umożliwić dokonanie uwierzytelnienia. Może to stanowić naruszenie prywatności, konieczny jest więc właściwy sposób przetwarzania wrażliwych danych osobowych w organizacji.

- Większość nowoczesnych komputerów przenośnych posiada wbudowany czytnik linii papilarnych, co ułatwia proces wdrażania urządzeń biometrycznych. Jednak – w porównaniu z dedykowanymi rozwiązaniami biometrycznymi – wbudowane czytniki mogą cechować się różną precyzją skanowania, nie zawsze najwyższej jakości. Zaleca się oszacowanie jakości czytników na podstawie przeprowadzonych testów w zakresie biometrii: false rejection rate (FRR), false acceptance rate (FAR), crossover error rate (CER), failure to enroll rate (FTE/FER) oraz wskaźnika wydajności.

- Jeśli środowisko pracy zawiera obszary, w których z uwagi na rodzaj wykonywanej pracy nie jest możliwe utrzymanie czystych rąk, czytniki linii papilarnych nie mogą być stosowane. W tej sytuacji zaleca się rozważyć wykorzystanie w tym celu innych indywidualnych cech fizycznych (np. rozpoznanie na podstawie siatkówki oka, twarzy lub geometrii dłoni).

- Zaleca się, aby podczas uwierzytelnienia użytkownik wprowadzał dodatkowy czynnik, taki jak: fraza kodująca, kod PIN lub karta inteligentna. Rozwiązanie takie jest rekomendowane z uwagi na fakt, iż znane są sposoby oszukania czytników linii papilarnych, np. poprzez podstawienie sztucznego odcisku palca, wykonanego z żelu, w celu ominięcia zabezpieczeń. Aby uzyskać dodatkowe informacje na ten temat, należy odwiedzić witrynę: Impact of Artificial "Gummy" Fingers on Fingerprint Systems[20].

Proces minimalizacji ryzyka

Każda organizacja ze względu na unikalne środowisko, w którym funkcjonuje, posiada własną specyfikę pracy. Przed wdrożeniem rozwiązania należy dokładnie przeanalizować jego potencjalne skutki i upewnić się, czy spełni ono wymaganie zwiększenia poziomu bezpieczeństwa procesu uwierzytelnienia.

W celu efektywnego wdrożenia zabezpieczeń biometrycznych oraz minimalizacji ryzyka zaleca się:

1. Sprawdzenie – przy pomocy szeregu testów – różnorodnych rozwiązań weryfikacji biometrycznych; pomoże to wybrać najlepsze dostępne rozwiązania, które spełnią wymagania i potrzeby organizacji.

2. Zapoznanie się z polityka prywatności obowiązującą w danej organizacji, ze szczególnym uwzględnieniem zasad przetwarzania wrażliwych danych osobowych.

[20] http://cryptome.org/gummy.htm

3. Określenie wymagań technicznych stawianych urządzeniom biometrycznym oraz zaplanowanie fazy testowej, która sprawdzi zgodność urządzeń z wymaganiami.

4. Określenie dodatkowych wymagań technicznych niezbędnych do wdrożenia rozwiązania biometrycznego; np. infrastruktura klucza publicznego lub instalacja oprogramowania klienckiego do obsługi biometrii.

5. Oszacowanie liczby pracowników, którzy mogą mieć trudności podczas korzystania z rozwiązania biometrycznego z uwagi na ich cechy fizyczne, wraz z przygotowaniem alternatywnego rozwiązania dla tej grupy osób. Należy rozważyć alternatywny sposób uwierzytelnienia, obejmujący korzystanie z haseł lub kart inteligentnych wymagających wprowadzenia kodu PIN.

6. Uświadomienie pracowników w zakresie stosowania uwierzytelnienia biometrycznego oraz poprawnego wykorzystania tego rozwiązania, a w przypadku braku możliwości użytkowania tego systemu – wskazanie alternatywnego procesu uwierzytelnienia.

7. Przeprowadzenie wdrożenia pilotażowego, obejmującego dużą grupę osób, w celu identyfikacji potencjalnych problemów, a następnie ich rozwiązania przed właściwym wdrożeniem rozwiązania w środowisku produkcyjnym.

8. Zapisanie indywidualnych cech fizycznych pracowników w bazie rozwiązania biometrycznego, stosując się do instrukcji przekazanych przez dostawcę urządzenia. Proces obejmuje skanowanie i weryfikację pobranych danych.

9. Przeszkolenie pracowników w zakresie korzystania z systemu biometrycznego oraz zapewnienie wsparcia w przypadku napotkanych trudności.

10. Zaplanowanie wdrożenia alternatywnego sposobu uwierzytelnienia dla osób, które odmówią korzystania z systemu biometrycznego, nie wyrażając zgody na przetwarzanie wrażliwych danych osobowych lub kierując się innymi przesłankami.

Zastosowanie ustawień zasad grup w celu minimalizacji ryzyka dla rozwiązań biometrycznych

Konfiguracja tych ustawień dostępna jest w gałęzi:

Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Biometria

(Computer Configuration\Administrative Templates\Windows Components\Biometrics)

Poniższa tabela przedstawia szczegółowe ustawienia zabezpieczeń dostępne w systemie Windows 7 SP1 dla omawianej technologii:

Ustawienie zasad	***Opis***	***Domyślne ustawienie w systemie Windows 7 SP1***
Zezwalaj na używanie biometrii	Jeżeli to ustawienie zasad zostanie włączone (lub nie zostanie skonfigurowane),	Nie skonfigurowano

	usługa biometryczna systemu Windows będzie dostępna, a użytkownicy systemu Windows będą mogli uruchamiać aplikacje używające biometrii.	
Zezwalaj użytkownikom na logowanie przy użyciu biometrii	To ustawienie zasad określa, czy użytkownicy domeny mogą logować się lub podwyższać poziom uprawnień Kontroli konta użytkownika przy użyciu biometrii. Domyślnie użytkownicy domeny nie mogą używać biometrii w celu logowania. Jeżeli to ustawienie zasad zostanie włączone, użytkownicy domeny będą mogli logować się do komputera z systemem Windows przy użyciu biometrii. W zależności od rodzaju używanej biometrii, włączenie prezentowanego ustawienia zasad może osłabić zabezpieczenia użytkowników logujących się przy użyciu tej technologii.	Nie skonfigurowano
Zezwalaj użytkownikom	To ustawienie zasad określa, czy	Nie skonfigurowano

domeny na logowanie przy użyciu biometrii	użytkownicy domeny mogą logować się lub podwyższać poziom uprawnień Kontroli konta użytkownika przy użyciu biometrii. Domyślnie użytkownicy domeny nie mogą używać biometrii w celu logowania. Jeżeli to ustawienie zasad zostanie włączone, użytkownicy domeny będą mogli logować się do komputera z systemem Windows przy użyciu biometrii. W zależności od rodzaju używanej biometrii, włączenie prezentowanego ustawienia zasad może osłabić zabezpieczenia użytkowników logujących się przy użyciu tej technologii.	
Limit czasu zdarzeń szybkiego przełączania użytkowników	To ustawienie zasad określa liczbę sekund, przez którą oczekujące zdarzenie szybkiego przełączania użytkowników pozostanie aktywne przed zainicjowaniem przełączenia. Domyślnie zdarzenie	Nie skonfigurowano

	szybkiego przełączania użytkowników jest aktywne przez 10 sekund; potem staje się nieaktywne.	

Tabela 3.4.1. Ustawienia zasad grupowych dla rozwiązań biometrycznych

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnego ustawienia można znaleźć w zakładce **POMOC** w ustawieniach Edytora obiektów zasad grupy.

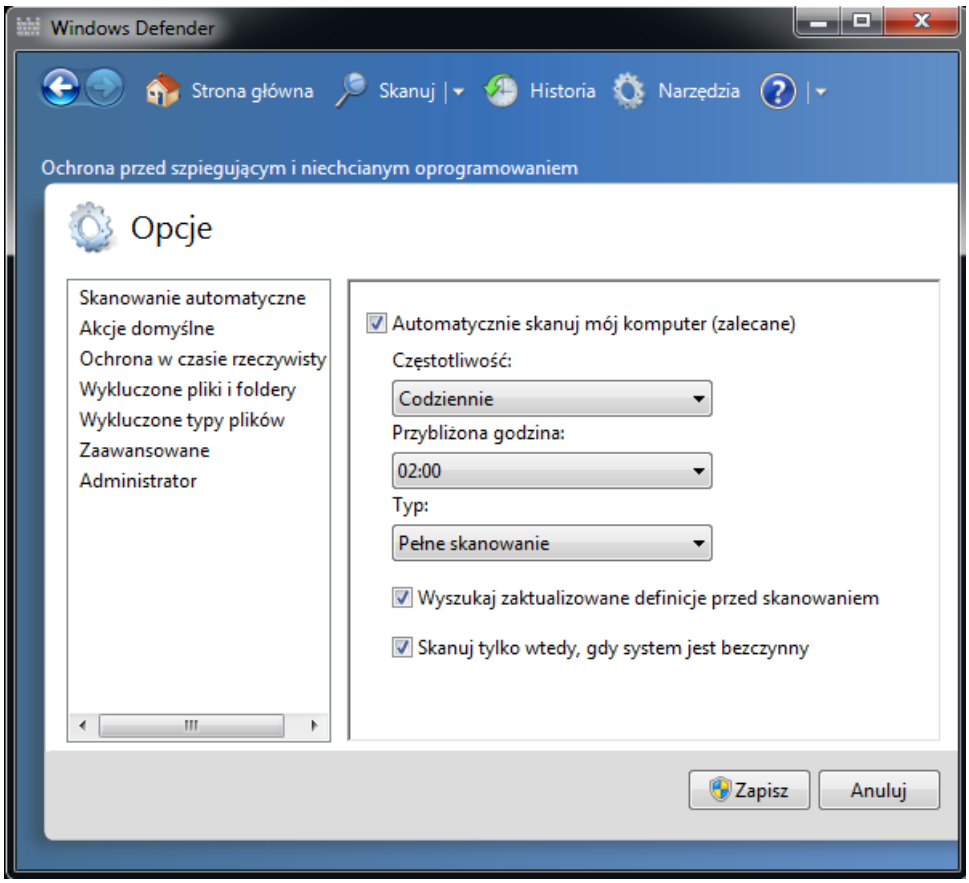
3.5. Oprogramowanie Windows Defender

Usługa Windows Defender jest oprogramowaniem antyszpiegowskim dołączonym do systemu Windows 7 SP1 i uruchamianym automatycznie po włączeniu systemu. W systemie Windows XP usługa była opcjonalna; można było ją pobrać i zainstalować. Używanie oprogramowania antyszpiegowskiego może pomóc w zapewnieniu ochrony komputera przed programami szpiegującymi i innym potencjalnie niechcianym oprogramowaniem. Program szpiegujący może zostać zainstalowany na komputerze bez wiedzy użytkownika podczas każdego połączenia z Internetem. 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. 3.5.1 przedstawiono rekomendowane ustawienia dla usługi Windows Defender dla komputerów pracujących w systemie Windows 7 SP1.



Rys. 3.5.1. Widok okna ustawień rekomendowanych dla usługi Windows Defender

Społeczność Microsoft SpyNet

Microsoft SpyNet to społeczność online, pomagająca wybrać odpowiednie reakcje na potencjalnie zagrożenia programami szpiegującymi. Społeczność ta pomaga również zatrzymać infekcje rozprzestrzeniające się poprzez nowe programy szpiegujące. SpyNet do prawidłowego działania wymaga dostępu do Internetu dla stacji klienckiej.

Gdy Windows Defender wykryje takie oprogramowanie lub próbę zmiany ważnych ustawień systemu Windows dokonywaną przez wykryte programy, które nie zostały jeszcze sklasyfikowane jako zagrożenie, użytkownik może zasięgnąć informacji, jakie rozwiązania w analizowanej sytuacji wdrożyli członkowie społeczności SpyNet. Natomiast akcje, które po wykryciu zagrożenia zostaną podjęte przez użytkownika, mogą pomóc innym członkom wspólnoty w doborze czynności naprawczych. Informacje dodatkowe ułatwiają firmie Microsoft sprawdzenie potencjalnych zagrożeń oraz tworzenie nowych definicji, umożliwiających lepszą ochronę komputera. Danymi takimi mogą być na przykład informacje o lokalizacji szkodliwego oprogramowania, które zostało wykryte i usunięte. W tych przypadkach program Windows Defender będzie automatycznie zbierał i wysyłał dane do społeczności Microsoft SpyNet. Administratorzy – poprzez konfigurację usługi Windows Defender – mogą zdecydować o przyłączeniu się do społeczności Microsoft SpyNet lub rezygnacji z tego kroku. Dodatkowe informacje

na temat zasad zachowania poufności danych można znaleźć w dokumencie: Zasady zachowania poufności informacji w systemie Windows 7[21].

Ocena ryzyka

Oprogramowanie szpiegujące wiąże się z poważnym ryzykiem dla organizacji. W celu zapewnienia jej bezpieczeństwa ryzyko to musi być minimalizowane poprzez zapobieganie ujawnieniu danych przechowywanych na komputerach. Oto najważniejsze zagrożenia, które stwarza oprogramowanie szpiegujące:

- wrażliwe dane organizacji mogą zostać narażone na ryzyko ujawnienia przez osoby nieupoważnione
- dane osobiste pracowników mogą zostać narażone na ryzyko ujawnienia przez osoby nieupoważnione
- na skutek działań zewnętrznej osoby atakującej komputery mogą zostać narażone na utratę kontroli nad systemem
- ryzyko przestojów z powodu oprogramowania szpiegującego, wynikające z obniżenia wydajności i stabilności systemów komputerowych
- ryzyko dotyczące wzrostu kosztów utrzymania i zapewnienia ochrony z powodu oprogramowania szpiegującego
- potencjalne ryzyko szantażu organizacji w przypadku, kiedy zainfekowany system ujawni wrażliwe dane

Minimalizacja ryzyka

Usługa Windows Defender została zaprojektowana w celu minimalizacji ryzyka związanego z oprogramowaniem szpiegującym. Należy regularne i automatycznie pobierać aktualizacje definicji, korzystając z usług Windows Update lub Windows Server Update Services (WSUS).

Oprócz ochrony antyszpiegowskiej, zapewnianej przez Windows Defender, wysoce rekomendowana jest instalacja oprogramowania antywirusowego, które dodatkowo rozszerzy ochronę antyszpiegowską i zapewni ochronę przed wirusami, trojanami, robakami oraz innymi zagrożeniami ze strony oprogramowania złośliwego. Uniwersalną ochronę przed oprogramowaniem złośliwym, stosowaną na komputerach przenośnych, stacjonarnych oraz serwerach, zapewnia np. program Microsoft System Center 2012 Endpoint Protection.

Zagadnienia minimalizacji ryzyka wymagające rozważenia

Usługa Windows Defender domyślnie jest włączona i uruchamiana automatycznie po włączeniu komputera z systemem Windows 7 SP1. Rozwiązanie to zostało zaprojektowane tak, aby nie przeszkadzało zwykłym użytkownikom w ich codziennej pracy. W celu efektywnego wdrożenia Windows 7 SP1 w organizacji, należy rozważyć następujące rekomendowane działania:

- Przeprowadzenie testów interoperacyjności przed wdrożeniem oprogramowania firm trzecich zapewniającego ochronę antywirusową i antyszpiegowską w czasie rzeczywistym.

[21] http://windows.microsoft.com/pl-PL/windows7/windows-7-privacy-statement

- Zaprojektowanie systemu, który wspomaga zarządzanie aktualizacją sygnatur i definicji, w przypadku, gdy nadzorujemy dużą liczbę komputerów.

- Zapewnienie użytkownikom wiedzy w zakresie możliwych ataków dokonywanych przez oprogramowanie złośliwe oraz metod ataków socjotechnicznych.

- Dostosowanie zaplanowanego czasu wykonywania automatycznego skanowania do potrzeb danej organizacji. Domyślny czas uruchomienia skanowania codziennego to godzina 2:00 w nocy. Jeśli komputer nie będzie mógł przeprowadzić skanowania w zaplanowanym czasie, użytkownik zostanie o tym fakcie poinformowany i zapytany o zgodę na uruchomienie skanowania w innym terminie. Jeśli jednak skanowanie nie odbędzie się w ciągu 2 następnych dni, przeprowadzone zostanie ono o tym czasie automatycznie po upływie 10 minut od startu komputera. W systemie Windows 7 SP1 proces skanowania uruchamiany jest z niskim priorytetem w sposób minimalizujący obciążenie pracującego komputera.

- Windows Defender nie został zaprojektowany jako aplikacja klasy Enterpise, skierowana do dużych organizacji. Rozwiązanie to nie zapewnia pełnego centralnego raportowania, monitorowania i mechanizmów kontroli konfiguracji. W przypadku potrzeby wykorzystania dodatkowego elementu zapewniającego te funkcje należy rozważyć wdrożenie produktów zaawansowanych, takich jak Microsoft System Center 2012 Endpoint Protection.

- Określenie polityki poufności dla organizacji w zakresie wysyłania i raportowania wykrytego oprogramowania spyware oraz możliwości przyłączenia się do programu społeczności Microsoft SpyNet.

Proces minimalizacji ryzyka

Windows Defender jest domyślnym składnikiem systemu Windows 7 SP1 i nie wymaga dodatkowych czynności aktywacyjnych. Należy jednak rozważyć wykonanie kilku dodatkowych rekomendowanych kroków, które zapewnią organizacji stałą ochronę:

1. Przeprowadzenie testów możliwości usługi Windows Defender działającej pod kontrolą systemu Windows 7 SP1.
2. Przeprowadzenie testów konfiguracji Windows Defender poprzez zastosowanie zasad grup.
3. Oszacowanie i przetestowanie dodatkowej ochrony antywirusowej, wraz z określeniem, czy oferowana ochrona zapewnia zabezpieczenie przed oprogramowaniem szpiegującym i ochronę antywirusową.
4. Zaplanowanie optymalnych regularnych aktualizacji sygnatur i definicji dla wszystkich komputerów (należy pamiętać, iż komputery przenośne mogą wymagać innej konfiguracji niż komputery stacjonarne).
5. Przeprowadzenie szkoleń wśród użytkowników, które pozwolą im uzyskać wiedzę w zakresie samodzielnego identyfikowania podejrzanych działań komputera i możliwych infekcji dokonanych przez oprogramowanie złośliwe.
6. Przeprowadzenie szkoleń wśród pracowników działu technicznego, które zapewnią użytkownikom wsparcie z zakresu działania usługi Windows Defender i jej narzędzi.

Zastosowanie ustawień zasad grupowych w celu minimalizacji ryzyka dla Widnows Defender

Konfiguracja tych ustawień dostępna jest w następującej lokalizacji w narzędziu Edytor obiektów zasad grupowych:

Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Program Windows Defender

(Computer Configuration\Administrative Templates\Windows Components\Windows Defender)

Poniższa tabela przedstawia szczegółowe ustawienia zabezpieczeń dostępne w systemie Windows 7 SP1 dla omawianego rozwiązania:

Ustawienie zasad	***Opis***	***Domyślne ustawienie w systemie Windows 7 SP1***
Włącz aktualizowanie definicji za pomocą usług WSUS i Windows Update	To ustawienie zasad umożliwia skonfigurowanie Windows Defender w taki sposób, aby w przypadku niedostępności lokalnie zarządzanego serwera usług WSUS (Windows Server Update Services) program sprawdzał dostępność definicji wirusów i instalował je z witryny Windows Update .	Nie skonfigurowano
Włącz przeprowadzanie aktualizacji definicji za pośrednictwem zarówno usług WSUS, jak i Centrum firmy Microsoft ds. ochrony przed złośliwym oprogramowaniem	To ustawienie zasad umożliwia skonfigurowanie programu Windows Defender w taki sposób, aby w przypadku niedostępności lokalnie zarządzanego serwera usług WSUS (Windows Server Update Services) sprawdzał dostępność definicji wirusów i instalował je z witryny Windows Update Centrum firmy Microsoft ds. ochrony przed złośliwym oprogramowaniem.	Nie skonfigurowano
Sprawdzaj przed zaplanowanym skanowaniem, czy są nowe sygnatury	Włączenie tego ustawienia zasad spowoduje sprawdzanie dostępności nowych sygnatur przed rozpoczęciem każdego zaplanowanego skanowania. Jeśli to ustawienie zasad zostanie **wyłączone** lub **nie zostanie skonfigurowane**, zaplanowane skanowania będą inicjowanie bez	Nie skonfigurowano

	pobierania nowych sygnatur.	
Wyłącz program Windows Defender	Powoduje wyłączenie dostępnego w ramach programu Windows Defender mechanizmu ochrony w czasie rzeczywistym i anulowanie zaplanowanych skanowań.	Nie skonfigurowano
Wyłącz program Windows Defender	Umożliwia wyłączenie monitów ochrony w czasie rzeczywistym dotyczących wykrywania znanego złośliwego oprogramowania.	Nie skonfigurowano
Wyłącz rutynowo podejmowaną akcję	Wyłącza rutynowo podejmowaną akcję. To ustawienie zasad umożliwia określenie, czy program Windows Defender ma automatycznie podejmować daną akcję dla wszystkich wykrytych zagrożeń. Akcja podejmowana w przypadku określonego zagrożenia będzie ustalana na podstawie kombinacji: akcji zdefiniowanej przez zasady, akcji zdefiniowanej przez użytkownika i akcji zdefiniowanej przez sygnaturę. Jeśli to ustawienie zasad zostanie włączone, program Windows Defender nie będzie automatycznie podejmował akcji dla wykrytych zagrożeń. Zamiast tego wyświetli monit o wybranie jednej z akcji dostępnych dla danego zagrożenia. Jeśli to ustawienie zasad zostanie wyłączone lub pozostanie nieskonfigurowane, program Windows Defender będzie automatycznie	Nie skonfigurowano

	podejmował akcję dla wszystkich wykrytych zagrożeń po upływie około 10 minut (czasu tego nie można zmienić).	
Konfigurowanie raportowania programu Microsoft SpyNet	Określa zasady członkostwa we wspólnocie Microsoft SpyNet.	Nie skonfigurowano

Tabela 4.5.1. Ustawienia zasad grupowych dla programu Windows Defender

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnego ustawienia można znaleźć w zakładce **POMOC** w ustawieniach Edytora obiektów zasad grupy.

3.6. Narzędzie do usuwania złośliwego oprogramowania

Narzędzie do usuwania złośliwego oprogramowania (ang. MSRT – Malicious Software Removal Tool) jest programem wykonywalnym niewielkich rozmiarów, który ułatwia usuwanie najbardziej rozpowszechnionych rodzajów złośliwego oprogramowania (w tym wirusy: Blaster, Sasser i Mydoom) z komputerów z systemami Windows.

Firma Microsoft co miesiąc dostarcza nową wersję programu MSRT poprzez usługi aktualizacji: Microsoft Update, Windows Updates, WSUS oraz Centrum pobierania Microsoft. Narzędzie do usuwania złośliwego oprogramowania jest uruchamiane w trybie cichym; po zakończeniu pracy wyświetli raport, gdy wykryte zostanie oprogramowanie złośliwe. Narzędzie to nie jest instalowane w systemie operacyjnym i nie posiada ustawień zasad grupowych. Domyślnie plik z raportem z przeprowadzonego skanowania umieszczony jest w lokalizacji: **%SystemRoot%\Debug\mrt.log**.

Program MSRT nie został zaprojektowany jako program antywirusowy klasy Enterprise, skierowany do dużych organizacji. Rozwiązanie to nie zapewnia pełnego centralnego raportowania, monitorowania i mechanizmów kontroli konfiguracji. W przypadku potrzeby dodatkowego elementu oferującego te funkcje należy rozważyć wdrożenie produktów zaawansowanych, takich jak Microsoft System Center 2012 Endpoint Protection[22].

Ocena ryzyka

Zaleca się, aby dostępne w systemach Windows 7 SP1 usługi zapewniające bezpieczeństwo uzupełnione zostały o instalację zewnętrznego programu antywirusowego na każdym komputerze w organizacji. Należy jednak pamiętać, iż istnieją dodatkowe czynniki ryzyka, które mogą mieć wpływ na bezpieczeństwo organizacji:

- Program antywirusowy może nie wykryć specyficznego oprogramowania złośliwego.
- Oprogramowanie złośliwe wyłączy lub zablokuje ochronę antywirusową na atakowanym komputerze.

W przedstawionej powyżej sytuacji oprogramowanie MSRT dostarczy dodatkową ochronę w celu wykrycia i usunięcia najbardziej rozpowszechnionych rodzajów złośliwego oprogramowania. Pełna lista złośliwego oprogramowania, które jest wykrywane i usuwane przez MSRT, podlega bieżącej

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

aktualizacji. Lista dostępna jest na stronie internetowej: Rodziny programów usuwane przez narzędzie do usuwania złośliwego oprogramowania[23].

Minimalizacja ryzyka

Aby zminimalizować ryzyko ataku, rekomenduje się włączenie na komputerach klienckich funkcji „Aktualizacje automatyczne". Gwarantuje ona regularne otrzymywanie nowej wersji narzędzia MSRT (co miesiąc) i możliwość jego błyskawicznego użycia. MSRT został zaprojektowany w celu minimalizacji ryzyka związanego z oprogramowaniem złośliwym, które firma Microsoft zidentyfikowała i zakwalifikowała jako zagrożenie wysokie i rozpowszechniające się na szeroką skalę, co powoduje zagrożenie dla bezpieczeństwa użytkowników systemu Windows.

Zagadnienia dotyczące minimalizacji ryzyka, które wymagają rozważenia

Jeśli rozważamy zastosowanie omawianego narzędzia MSRT we własnym środowisku, warto zapoznać się z listą najważniejszych czynników ułatwiających jego prawidłowe wdrożenie:

- Program MSRT zajmuje około 9 MB; równoczesne pobieranie tego programu przez dużą liczbę użytkowników może wpłynąć niekorzystnie na wydajność połączenia internetowego.
- Narzędzie MSRT zostało pierwotnie zaprojektowane z myślą o użytkownikach niekorporacyjnych, którzy nie posiadają zainstalowanych aktualnych rozwiązań antywirusowych. Może ono jednak stanowić uzupełnienie użytkowanego już rozwiązania ochrony antywirusowej, stanowiąc dodatkowy element strategii defense-in-depth. Aby wdrożyć narzędzie MSRT w środowisku organizacji, można wykorzystać następujące sposoby instalacji:
  - Windows Server Update Services
  - Pakiet instalacyjny SMS / SCCM
  - Skrypt startowy komputera uruchamiany przez zasady grupowe
  - Skrypt startowy użytkownika uruchamiany przez zasady grupowe

  W przypadku dużych środowisk rekomendowane jest zastosowanie się do wytycznych zawartych w dokumencie: Wdrażanie Narzędzia Microsoft Windows do usuwania złośliwego oprogramowania w środowisku przedsiębiorstwa[24]; numer ID artykułu w bazy wiedzy Microsoft Knowledge Base: 891716.

- Program MSRT nie zapewnia ochrony w czasie rzeczywistym, dlatego wysoce rekomendowane jest zainstalowanie programu antywirusowego, który oferuje tę funkcjonalność. Przykładem takiego rozwiązania jest Microsoft System Center 2012 Endpoint Protection, zapewniający uniwersalną ochronę przed oprogramowaniem złośliwym, stosowaną na komputerach przenośnych, stacjonarnych oraz serwerach.

- Program MSRT w trakcie uruchamiania tworzy tymczasowy katalog o losowej nazwie, który lokalizowany jest wewnątrz dysku posiadającego największą możliwą przestrzeń do zapisu (przeważnie jest to główny dysk z systemem operacyjnym). Katalog ten zawiera kilka

[23] http://www.microsoft.com/pl-pl/security/pc-security/malware-families.aspx
[24] http://support.microsoft.com/Default.aspx?kbid=891716

plików, m.in. Mrtstub.exe. W większości przypadków katalog zostaje usunięty automatycznie po zakończeniu procesu skanowania lub ponownym uruchomieniu komputera. Może jednak zdarzyć się, że proces ten nie zostanie wykonany automatycznie; w takim przypadku należy usunąć folder ręcznie, bez obawy o szkodę dla komputera.

Proces minimalizacji ryzyka

Aby efektywnie wykorzystać narzędzie MSRT i zminimalizować ryzyko ataków, zaleca się zastosować poniższe kroki:

3.7 Przeprowadzenie testów możliwości narzędzia MSRT; w celu uzyskania dodatkowych informacji należy odwiedzić witrynę: Narzędzie do usuwania złośliwego oprogramowania- Malicious Software Removal Tool[25]

3.7 Oszacowanie potrzeby wdrożenia narzędzia MSRT we własnym środowisku

3.7 Określenie najbardziej odpowiedniego sposobu wdrożenia narzędzia MSRT w organizacji.

3.7 Dokonanie identyfikacji systemów, na których wdrożenie narzędzia MSRT zapewni dodatkowy stopień ochrony w organizacji.

3.7 Zastosowanie właściwej metody wdrożenia narzędzia

3.7 Zapora systemu Windows 7 SP1

Zapora osobista jest krytycznym komponentem systemu obrony przed wieloma rodzajami oprogramowania złośliwego. Zapora osobista jest domyślnie włączona w systemach Windows od czasu wydania Windows XP SP2, a więc także w Windows 7 SP1. Jej celem jest zapewnienie komputerowi ochrony, która realizowana jest od momentu, gdy system operacyjny uzyskuje gotowość do pracy.

Zapora osobista w systemie Windows 7 SP1 wykorzystuje ten sam mechanizm ochrony, który dostępny był w Windows Vista, włączając w to filtrowanie ruchu wchodzącego i wychodzącego dla zapewnienia ochrony poprzez ograniczenie dostępu sieciowego do zasobów systemu operacyjnego. W rozwiązaniu tym została zastosowana ta sama konsola interfejsu użytkownika zapory systemu Windows z zabezpieczeniami zaawansowanymi, która jest znana z systemu Windows Vista. Konsola ta stanowi centralny punkt zarządzania, upraszczający związane z nim procedury. Z jej poziomu możemy zarządzać filtrowaniem ruchu sieciowego przychodzącego i wychodzącego z interfejsów sieciowych oraz ustawieniami protokołu Ipsec, zapewniającymi bezpieczeństwo połączenia dzięki zastosowaniu: wymiany kluczy, uwierzytelniania, integralności danych i – opcjonalnie – szyfrowania danych.

W systemie Windows 7 SP1 istnieją trzy profile aplikacji Zapora systemu Windows z zabezpieczeniami zaawansowanymi:

Profil domenowy

Profil stosowany jest wtedy, gdy komputer został podłączony do sieci oraz nastąpiło uwierzytelnienie do kontrolera domeny, do którego należy komputer.

Profil publiczny

Jest to domyślny profil, stosowany wtedy, gdy komputer nie jest dołączony do domeny. Ustawienia

[25] http://www.microsoft.com/pl-pl/security/pc-security/malware-removal.aspx

profilu publicznego powinny być restrykcyjne w najwyższym stopniu, ponieważ komputer jest połączony z siecią publiczną, w której nie można kontrolować bezpieczeństwa.

Profil prywatny

Profil stosowany jest, gdy użytkownik posiadający poświadczenia lokalnego administratora przypisze go – w ramach bieżącego połączenia sieciowego – do sieci zdefiniowanej wcześniej jako sieć publiczna. Zaleca się, aby używać profilu prywatnego w sieciach zaufanych.

W systemie Windows Vista w danej chwili na komputerze może być aktywny tylko jeden profil. System Windows 7 SP1 zapewnia wsparcie wielu aktywnych profili na poziomie kart sieciowych. Jeśli istnieje wiele kart sieciowych połączonych z różnymi sieciami, dla wszystkich kart na komputerze stosowany jest profil o ustawieniach najlepiej dostosowanych do typu sieci, do której został on przyłączony. Jeśli np. znajdujemy się w kawiarence i korzystamy z darmowego punktu dostępowego sieci bezprzewodowej, aby połączyć się z siecią naszej organizacji przy wykorzystaniu VPN, to profil publiczny w dalszym ciągu zapewnia nam ochronę ruchu sieciowego, który nie jest transmitowany przez zestawiony tunel połączenia VPN. To samo odnosi się do karty sieciowej niepodłączonej do sieci lub podłączonej do sieci nierozpoznanej; w takim przypadku przypisany zostanie profil publiczny, a pozostałe karty sieciowe będą używały profili odpowiednich dla typu sieci, do której zostały przyłączone.

Ocena ryzyka

Połączenie sieciowe i możliwa przy jego użyciu łączność z całym światem są obecnie niezbędne w prowadzeniu nowoczesnego biznesu. Z drugiej jednak strony, połączenie takie może stać się głównym celem przeprowadzenia ataku. Aby zapewnić organizacji bezpieczeństwo i nie dopuścić do ujawnienia ważnych danych oraz do infekcji komputerów, zagrożenie towarzyszące nawiązywanym połączeniom musi być minimalizowane. Pomóc w tym może znajomość najczęściej identyfikowanych zagrożeń związanych z atakami z sieci:

- Zainfekowanie komputera oraz przejęcie kontroli nad komputerem – łącznie z uzyskaniem uprawnień administracyjnych – przez nieupoważnioną osobę atakującą.
- Zastosowanie przez osobę atakującą skanerów sieciowych w celu zdalnego ustalenia otwartych portów (niezbędnych do działania usług w sieci Internet), które mogą zostać wykorzystane do przeprowadzenia ataku z zewnątrz.
- Wrażliwe dane organizacji mogą zostać narażone na ryzyko ujawnienia przez osoby nieupoważnione w przypadku, kiedy złośliwe oprogramowanie, takie jak koń trojański, zainicjuje i nawiąże połączenie wewnątrz sieci – bezpośrednio ze stacji roboczej do komputera atakującego.
- Komputery przenośne mogą zostać narażone na zewnętrzne ataki sieciowe, pracując z sieci niezaufanych, poza kontrolą firmowej zapory sieciowej.
- Komputery pracujące w sieci wewnętrznej mogą zostać narażone na ataki sieciowej pochodzące z zainfekowanych komputerów podłączonych do tej samej sieci wewnętrznej.

- Istnieje ryzyko szantażu organizacji w przypadku, kiedy atakujący zainfekuje komputery pracujące w sieci wewnętrznej.

Minimalizacja ryzyka

Zapora sieciowa Windows 7 SP1 zapewnia ochronę komputera i jest dostępna od razu po instalacji systemu. Blokuje ona niechciane połączenia przychodzące do czasu, kiedy stosowne zmiany zostaną dokonane przez administratora lub odpowiednią zasadę grupową.

Zapora sieciowa zawiera również funkcjonalność filtrowania ruchu wychodzącego z komputera. Reguła ta domyślnie zezwala na cały ruch wychodzący; zastosowanie odpowiednich ustawień zasad grupowych pozwala na konfigurację reguł dostępnych w zaporze sieciowej – tak, aby pozostawić ustawienia zabezpieczeń komputera klienckiego w stanie niezmiennym.

Zagadnienia dotyczące minimalizacji ryzyka, które wymagają rozważenia

Poniżej przedstawiono listę najważniejszych zadań ułatwiających prawidłowe wykonanie procesu wdrożenia zapory sieciowej:

3.8 Przeprowadzenie testów interoperacyjności aplikacji niezbędnych w pracy na komputerach organizacji. Dla każdej z tych aplikacji należy zanotować porty, które umożliwiają ich prawidłową pracę, aby zapora sieciowa umożliwiła ich otwarcie.

3.8 Tak jak w przypadku Windows Vista, zapora sieciowa systemu Windows 7 SP1 obsługuje trzy profile: domenowy, publiczny i prywatny. Zapewnia to odpowiedni poziom ochrony komputerów klienckich, które pracują w sieciach niezaufanych – poza siecią wewnętrzną organizacji.

3.8 Określenie odpowiedniego poziomu ochrony na podstawie monitoringu logów generowanych przez zaporę sieciową. Pozwoli to na wzajemne dopasowanie istniejących rozwiązań raportowania i kontroli w organizacji.

3.8 Domyślnie zapora sieciowa blokuje połączenia zdalnego sterowania oraz zdalnego zarządzania komputerami opartymi na systemie Windows 7 SP1. Jednak dostępne w ramach zapory wbudowane, zdefiniowane reguły umożliwiają użytkownikom wykonywanie zadań zdalnych. W przypadku potrzeby takiego działania wystarczy te reguły włączyć w odpowiednich profilach zapory. Istnieje np. możliwość włączenia reguły „Pulpit zdalny” dla profilu domenowego, aby zezwolić pracownikom działu wsparcia na zdalne połączenia z komputerami w celu świadczenia usług pomocy zdalnej. W przypadku profili publicznego i prywatnego reguły te można pozostawić wyłączone, aby zminimalizować ryzyko ataku sieciowego na komputery znajdujące się poza siecią wewnętrzną.

Proces minimalizacji ryzyka

System Windows 7 SP1 zawiera ustawienia zasad grupowych oraz odpowiednie narzędzia graficzne, które wspomagają administratorów w przeprowadzaniu odpowiedniej konfiguracji funkcjonalności zapory sieciowej. Zaawansowane ustawienia zabezpieczeń dostępne dla systemu Windows 7 SP1 można zastosować również na komputerach pracujących pod kontrolą systemu Windows Vista. Nie można jednak skorzystać z nich w przypadku komputerów klienckich lub obrazów systemów wirtualnych trybu XP Mode pracujących pod kontrolą systemu Windows XP.

Jeśli planujemy modyfikację domyślnej konfiguracji zapory sieciowej w celu zarządzania komputerami pracującymi po kontrolą systemów Windows Vista oraz Windows 7 SP1, rekomendowane jest

wykorzystanie ustawień zasad grupowych dla Zapory systemu Windows z zabezpieczeniami zaawansowanymi.

Zasady dotyczące Zapory systemu Windows z zabezpieczeniami zaawansowanymi dostępne są w ramach gałęzi:

Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zapora systemu Windows z zabezpieczeniami zaawansowanymi

(Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security)

Użytkownikom zaleca się włączenie Zapory systemu Windows z zabezpieczeniami zaawansowanymi dla wszystkich trzech profili. Ponadto zapora systemu Windows z zabezpieczeniami zaawansowanymi wspiera i obsługuje Reguły zabezpieczeń połączeń (ang. Connection security rules). Zabezpieczenia połączeń obejmują uwierzytelnianie dwóch komputerów przed rozpoczęciem komunikacji między nimi i zabezpieczanie wysyłanych przez nie informacji. Aplikacja Zapora systemu Windows z zabezpieczeniami zaawansowanymi używa zabezpieczeń protokołu internetowego (IPsec), aby uzyskać bezpieczeństwo połączenia dzięki zastosowaniu: wymiany kluczy, uwierzytelniania, integralności danych i – opcjonalnie – szyfrowania danych.

Więcej informacji na temat IPSec[26] można uzyskać w witrynie Microsoft Technet.

Zbiór ustawień bazowych, opisujący zalecane ustawienia Zapory systemu Windows z zabezpieczeniami zaawansowanymi dla systemu Windows 7 SP1, wraz ze wskazaniem zalecanych ustawień, dostępny jest w narzędziu Security Compliance Manager[27] (SCM). Narzędzie SCM zostanie opisane w dodatku do niniejszego dokumentu.

3.8 Ograniczanie dostępu do aplikacji – AppLocker

Windows 7 SP1 zawiera uaktualnioną i ulepszoną wersję zasad ograniczeń oprogramowania (ang. Software Restriction Policies). Narzędzie to nosi nazwę AppLocker i zastępuje funkcję Zasady ograniczania oprogramowania. Funkcja AppLocker udostępnia nowe możliwości i rozszerzenia, które zmniejszają liczbę obowiązków związanych z administracją i ułatwiają administratorom kontrolowanie sposobu, w jaki użytkownicy uzyskują dostęp do plików i możliwość ich użytkowania. Chodzi tu o pliki wykonywalne, skrypty, pliki Instalatora Windows i pliki DLL. Konfiguracja funkcji AppLocker może zostać przeprowadzona z zastosowaniem zasad grupowych w obrębie domeny Active Directory lub lokalnie, na komputerze, z zastosowaniem konsoli Zasady zabezpieczeń lokalnych.

Ocena ryzyka

Każdorazowa próba instalacji nieautoryzowanej aplikacji stwarza zagrożenie dokonania nieuprawnionych zmian w systemie. Proces instalacyjny modyfikuje komponenty systemu operacyjnego komputera; w efekcie tego działania powstaje ryzyko uruchomienia dodatkowych usług lub otworzenia dodatkowych portów Zapory systemu Windows. Nawet jeśli obawy te nie potwierdzą się, to w systemie pozostanie zainstalowana aplikacja, która wymaga sprawdzenia pod kątem

[26] http://go.microsoft.com/fwlink/?LinkId=69843
[27] http://go.microsoft.com/fwlink/?LinkId=156033

możliwego celu ataku oraz podatności na atak. Nieautoryzowana aplikacja w zamierzeniu twórców może być szkodliwa (niebezpieczna). Jej instalacja mogła zostać przeprowadzona przez użytkownika omyłkowo lub celowo. Stwarza ona jednak niebezpieczeństwo przeprowadzenia ataku na systemy wewnętrzne po podłączeniu komputera do sieci organizacji.

Minimalizacja ryzyka

AppLocker umożliwia administratorom wprowadzenie zestawu zasad sterowania aplikacjami, które znacznie zmniejszą ryzyko ataku będącego efektem instalacji nieautoryzowanego oprogramowania na komputerach organizacji. AppLocker pozwala na minimalizację ryzyka związanego z instalacją oprogramowania dzięki poniższym działaniom:

1. Definiowanie reguł na podstawie atrybutów plików uzyskanych z podpisu cyfrowego, w tym: wydawcy, nazwy produktu, nazwy pliku i wersji pliku. Reguły można np. utworzyć na podstawie atrybutu wydawcy, który zachowa trwałość po dokonaniu aktualizacji, lub określonej wersji pliku.
2. Przypisywanie reguły do grupy zabezpieczeń lub do użytkownika.
3. Tworzenie wyjątków od reguł. Można np. utworzyć regułę zezwalającą na uruchamianie wszystkich procesów systemu Windows z wyjątkiem Edytora rejestru (Regedit.exe).
4. Użycie trybu Tylko inspekcja, aby wdrożyć zasady i poznać ich wpływ przed zastosowaniem.
5. Importowanie i eksportowanie reguł. Działanie to wpływa na całą zasadę; jeśli np. zasada zostanie wyeksportowana, razem z nią wyeksportowane zostaną wszystkie reguły, ze wszystkich kolekcji reguł, w tym ustawienia wymuszania dla kolekcji reguł. Zaimportowanie zasady spowoduje zastąpienie istniejącej zasady.
6. Prostsze tworzenie i zarządzanie regułami zasad ograniczeń oprogramowania dzięki zastosowaniu apletów poleceń programu PowerShell dla zasad ograniczeń oprogramowania.

Zagadnienia dotyczące minimalizacji ryzyka, które wymagają rozważenia

Jeśli rozważamy zastosowanie funkcji AppLocker we własnym środowisku, warto zapoznać się z zasadami umożliwiającymi prawidłowe przeprowadzenie tego procesu. Poniżej zaprezentowano listę działań, które ułatwią wdrożenie omawianego narzędzia:

3.9. Przeprowadzenie dokładnych testów zasad sterowania aplikacjami przed wdrożeniem ich w środowisku produkcyjnym. Wszelkie błędy popełnione podczas procesu planowania i wprowadzania tej funkcjonalności mogą spowodować poważne utrudnienia i wpłynąć znacząco na wydajność pracy użytkownika.

3.9. Zaplanowanie czasu na proces szacowania użytkowanych aplikacji w organizacji poprzez użycie trybu **„Tylko inspekcja”** funkcji AppLocker. Ma on na celu zapoznanie się – przed wdrożeniem ograniczeń – z zakresem działania aplikacji wykorzystywanych przez użytkowników.

3.9. Rozważenie stopniowego wdrażania ograniczeń, rozpoczynając od zastosowania ich wśród użytkowników. W ich przypadku instalacja oprogramowania stanowi duże zagrożenie dla bezpieczeństwa organizacji lub komputerów zawierających wrażliwe dane.

Proces minimalizacji ryzyka

Aby wyświetlić interfejs konfiguracji funkcji AppLocker, należy przejść do gałęzi Zasady sterowania aplikacjami w zasadach grupowych. System Windows 7 SP1 nadal wspiera zasady ograniczeń oprogramowania (SRP).

Uwaga: Funkcja AppLocker jest dostępna w systemach Windows 7 Ultimate oraz Windows 7 Enterprise. System Windows 7 Professional umożliwia tworzenie reguł funkcji AppLocker. Reguły funkcji AppLocker nie mogą być jednak wymuszane na komputerach z systemem Windows 7 Professional.

Zastosowanie zasad grupowych w celu minimalizacji ryzyka stosując funkcję AppLocker

Interfejs konfiguracji funkcji AppLocker dostępny jest w gałęzi:

Konfiguracja komputera\Ustawienia systemu Windows\Ustawienie zabezpieczeń\Zasady sterowania aplikacjami

(Computer Configuration\Windows Settings\Security Settings\Application Control Policies)

Z uwagi na specyficzne wymagania każdej organizacji przewodnik ten nie zawiera rekomendacji, jakie aplikacje warto zablokować na stacjach klienckich. Aby uzyskać dodatkowe informacje na temat planowania i wdrażania zasad AppLocker, należy zapoznać się z dokumentami: Zasady ograniczeń oprogramowania

Zasady ograniczeń oprogramowania (ang. Software Restriction Policies (SRP)), wprowadzone w systemach Windows Vista, Windows XP, Windows Server 2003 oraz Windows Server 2008, są dostępne i wspierane także w systemie Windows 7 SP1. Dzięki nim administratorzy mogą określić, jakie aplikacje pracują na lokalnych komputerach, oraz sterować ich działaniem. Firma Microsoft rekomenduje jednak zastąpienie zasad ograniczeń oprogramowania nowymi zasadami sterowania aplikacjami; oferują one nowe możliwości i rozszerzenia działania funkcji AppLocker dla systemu Windows 7 SP1.

3.9. Dodatkowe informacje i wskazówki

Poniżej przedstawiono dodatkowe źródła informacji na temat bezpieczeństwa systemu Windows 7 SP1, opublikowane na stronach Microsoft.com:

- AppLocker Technical Documentation for Windows 7 and Windows Server 2008 R2[28]
- "Deployment of the Microsoft Windows Malicious Software Removal Tool in an enterprise environment[29], artykuł nr 891716 w bazy wiedzy Microsoft Knowledge Base
- Impact of Artificial "Gummy" Fingers on Fingerprint Systems[30]
- Install the latest Windows Defender definition updates[31]
- Internet Explorer 8 Security Baseline[32]
- IPsec[33]

[28] http://go.microsoft.com/fwlink/?LinkId=154902
[29] http://support.microsoft.com/Default.aspx?kbid=891716
[30] http://cryptome.org/gummy.htm
[31] http://www.microsoft.com/security/portal/Definitions/HowToWD.aspx
[32] http://go.microsoft.com/fwlink/?LinkId=160809
[33] http://go.microsoft.com/fwlink/?LinkId=69843

- System Center 2012 Endpoint Protection[34]
- Getting Started with User Account Control on Windows Vista[35]
- Malicious Software Removal Tool[36]
- Malware Families Cleaned by the Malicious Software Removal Tool[37]
- Microsoft Security Compliance Manager[38]
- Privacy Statement for the Microsoft Error Reporting Service[39]
- "The Microsoft Windows Malicious Software Removal Tool helps remove specific, prevalent malicious software from computers that are running Windows Vista, Windows Server 2003, Windows Server 2008, Windows XP, or Windows 2000"; artykuł nr 890830 w bazy wiedzy Microsoft Knowledge Base
- Windows Defender Privacy Policy
- Windows Firewall
- Windows Server Group Policy
- Windows Server Update Services (WSUS)
- artykuł "Windows Vista Application Development Requirements for User Account Control Compatibility"
- Understanding and Configuring User Account Control in Windows Vista
- User Account Control
- Using Software Restriction Policies to Protect Against Unauthorized Software

[34] http://www.microsoft.com/en-us/server-cloud/system-center/endpoint-protection-2012.aspx
[35] http://go.microsoft.com/fwlink/?linkid=84129
[36] http://go.microsoft.com/fwlink/?LinkId=51307
[37] http://www.microsoft.com/security/malwareremove/families.aspx
[38] http://go.microsoft.com/fwlink/?LinkId=113940
[39] http://go.microsoft.com/fwlink/?linkid=62936

5. Ochrona wrażliwych danych

Firma Microsoft dostarczyła nowe i rozszerzone funkcje oraz usługi zapewniające organizacjom ochronę danych przechowywanych na komputerach klienckich. Rozwiązania te uwzględniają także mechanizmy zabezpieczające przed ryzykiem kradzieży oraz ujawnienia danych.

W rozdziale tym zostaną omówione rekomendowane ustawienia, których wdrożenie pozwoli podwyższyć poziom ochrony danych przechowywanych na komputerach klienckich pracujących pod kontrolą systemu Windows 7 SP1. Konfiguracja, którą wybierzemy dla poszczególnych funkcji ochrony, zależna jest od wymagań, jakie stawiamy własnemu środowisku informatycznemu, i poziomu jego zabezpieczeń. Informacje zawarte w tym rozdziale pomogą w identyfikacji, projektowaniu oraz dostosowywaniu konfiguracji następujących funkcji i usług:

- szyfrowanie dysków funkcją BitLocker
  - ochrona plików przechowywanych na woluminie, na którym zainstalowany jest system Windows (dysk systemu operacyjnego), oraz na stałych dyskach z danymi
  - ochrona danych znajdujących się na dyskach wymiennych (zewnętrzne dyski danych lub dyski flash USB) z zastosowaniem funkcji BitLocker To Go
- system szyfrowania plików (EFS)
- usługi zarządzania prawami dostępu (RMS)
- mechanizm instalacji i zarządzania urządzeniami w systemie Windows

Aby zapewnić ochronę wrażliwych danych, możemy skorzystać z funkcji: Bitlocker, EFS, RMS oraz mechanizmu instalacji urządzeń i zarządzania nimi. Każde z tych rozwiązań oferuje organizacji inny rodzaj zabezpieczenia informacji. Stosowanie dostępnych w systemie Windows 7 mechanizmów ochrony danych jest wysoce rekomendowane i powinno stać się częścią realizowanej przez organizację strategii bezpieczeństwa. Przedstawione w tabeli przykłady, odnoszące się do najczęściej spotykanych konfiguracji, pokazują, w jakich scenariuszach poszczególne funkcje mogą zostać wykorzystane w organizacjach.

Scenariusz	BitLocker	EFS	RMS	Zarządzanie urządzeniami
Ochrona danych komputerów przenośnych	☑	☑		☑
Ochrona danych serwera biura oddziału	☑			☑
Ochrona lokalnych plików i folderów użytkownika		☑		
Ochrona komputerów stacjonarnych	☑	☑		☑

Ochrona danych dysków wymiennych	☑			☑
Ochrona plików i folderów współużytkowanych komputerów		☑		
Ochrona plików i folderów zdalnych		☑		
Ochrona administratora pracującego w niezaufanej sieci		☑		
Egzekwowanie zasad ochrony dokumentów zdalnych			☑	
Ochrona treści podczas przesyłania przez sieć			☑	
Ochrona treści podczas współpracy grupowej			☑	
Ochrona danych przed kradzieżą	☑			☑

Tabela 4.1. Porównanie mechanizmów ochrony danych stosowanych w systemie Windows 7 SP1

Ustawienia bazowe konfiguracji zaprezentowano w dołączonych do narzędzia **Security Compliance Manager (SCM)** arkuszach programu Excel. Wykazano w nich sposoby ograniczania powierzchni ataków dla wybranych produktów Microsoft. Skoroszyty zawierające ustawienia wybranych produktów dostępne będą w sekcji **Attachments\Guides** po wybraniu i wskazaniu właściwego produktu w narzędziu SCM.

Uwaga: Podstawowe ustawienia dla każdego z obszarów wskazanych w tym rozdziale są – wraz z ustawieniami dla zasad grupowych – uwydatnione w domyślnej konfiguracji dla nowych instalacji systemu Windows 7 SP1. Zalecane lub rekomendowane ustawienia zasad grupowych oznaczono za pomocą symbolu „‡”. Więcej informacji na temat podstawowych ustawień bazowych i ich wartości zawarto w tabelach dokumentu „Windows 7 SP1 Security Baseline settings”, dostępnych w narzędziu Security Compliance Manager[40] (SCM).

4.1. Szyfrowanie i ochrona dysków przy zastosowaniu funkcji BitLocker

Szyfrowanie dysków funkcją BitLocker to mechanizm pozwalający na szyfrowanie całych woluminów, a nie tylko poszczególnych plików systemu. Rozwiązanie to zapewnia ochronę wszystkich danych przechowywanych na dyskach pracujących pod kontrolą systemu Windows 7 SP1. Mechanizm zapewnia bezpieczeństwo danych również w przypadku, gdy dysk zostanie wymontowany i zainstalowany na innym komputerze. Funkcja BitLocker, dostępna tylko w edycjach Enterprise i Ultimate systemów Windows 7 SP, zapewnia ochronę danych znajdujących się na dyskach twardych

[40] http://go.microsoft.com/fwlink/?LinkId=156033

komputerów użytkowników, włączając w to ochronę dysków wymiennych, pamięci przenośnych USB oraz dysków podłączonych poprzez interfejs IEEE 1394.

Gdy za pomocą omawianego narzędzia włączymy ochronę dysków systemu operacyjnego, BitLocker chronić będzie sekwencję rozruchu aż do momentu wprowadzenia przez użytkownika właściwych i uprawnionych danych uwierzytelniających. Funkcja BitLocker zezwala na zastosowanie pamięci flash USB do przechowywania kluczy deszyfrujących, ale najwyższy stopień bezpieczeństwa uzyskuje się przy wykorzystaniu modułu TPM 1.2 (ang. Trusted Platform Module), który zapewnia sprzętową ochronę kluczy szyfrujących i zapobiega atakom programowym na bezpieczeństwo i integralność danych przechowywanych na dyskach. Funkcja BitLocker może korzystać z modułu TPM do weryfikowania integralności składników biorących udział we wczesnej fazie uruchamiania oraz do weryfikowania danych konfiguracji rozruchu. Umożliwia to uzyskanie dostępu do zaszyfrowanego dysku tylko wtedy, gdy składniki te nie zostały naruszone, a zaszyfrowany dysk znajduje się w oryginalnym komputerze.

4.2. Tryby pracy BitLocker oraz zarządzanie układem TPM

Funkcja BitLocker oferuje kilka trybów pracy, które można konfigurować i dostosowywać do własnych wymagań. Tryb pracy, który zostanie wybrany i zastosowany, w dużej mierze zależy od dostępności modułu TPM na chronionych komputerach oraz stopnia ochrony, który ma zostać wyegzekwowany. Tryb pracy obejmuje zastosowanie modułu TPM, numeru PIN oraz klucza uruchomienia (ang. startup key). Klucz uruchomienia jest plikiem wygenerowanym w sposób kryptograficzny i umieszczonym na oddzielnym nośniku pamięci flash USB.

Tryby pracy funkcji BitLocker:

- **Tylko moduł TPM**. Używanie weryfikacji Tylko moduł TPM nie wymaga żadnej interakcji z użytkownikiem w celu odszyfrowania i udostępnienia dysku. Do startu systemu nie są potrzebne hasło, numer PIN ani klucz uruchomienia. Jeśli weryfikacja przy użyciu modułu TPM powiedzie się, przebieg logowania jest z punktu widzenia użytkownika taki sam, jak podczas logowania standardowego. W przypadku, gdy modułu TPM brakuje, został on zmieniony, wykryto zmiany o znaczeniu krytycznym w plikach startowych systemu operacyjnego lub nastąpi próba uruchomienia dysku na innym komputerze, funkcja BitLocker przejdzie do trybu odzyskiwania dostępu do danych. Wówczas konieczne będzie podanie hasła odzyskiwania. Tryb ten zapewnia ochronę środowiska rozruchowego systemu Windows 7 SP1 poprzez moduł TPM i – z uwagi na brak dodatkowego uwierzytelnienia do uruchomienia systemu Windows – oferuje najsłabszy poziom zabezpieczenia dostępny w ramach funkcji BitLocker .

- **Moduł TPM z kluczem uruchomienia**. Oprócz ochrony zapewnianej przez moduł TPM część klucza szyfrowania przechowywana jest na dysku flash USB. Dostępu do danych na zaszyfrowanym woluminie nie można uzyskać bez wpisania poprawnego klucza uruchomienia. Tryb ten wymaga, by urządzenie USB zawierające klucz uruchomienia podłączone było do komputera w czasie uruchamiania systemu Windows. Jeśli system nie odczyta poprawnie klucza uruchomienia, komputer przejdzie w tryb odzyskiwania (ang.

Recovery mode). Tryb ten zapewnia ochronę środowiska rozruchowego dla systemu Windows 7 SP1 poprzez moduł TPM.

- **Moduł TPM z kodem PIN**. W tym trybie oprócz ochrony zapewnianej przez moduł TPM funkcja BitLocker oferuje dodatkowe zabezpieczenie – wymaga od użytkownika wprowadzenia osobistego numeru identyfikacyjnego (PIN). Dostępu do danych na zaszyfrowanym woluminie nie można uzyskać bez podania kodu PIN. Dodatkowo za pomocą zasad grup można wymusić konieczność użycia hasła złożonego zamiast prostego numeru PIN. Jeśli w czasie uruchamiania systemu użytkownik nie wprowadzi prawidłowego kodu PIN, komputer przejdzie w tryb odzyskiwania. Tryb ten zapewnia ochronę środowiska rozruchowego dla systemu Windows 7 SP1 poprzez moduł TPM.

- **Moduł TPM z kluczem uruchomienia i kodem PIN**. Opcję tę można skonfigurować wyłącznie przy użyciu narzędzia wiersza polecenia **Manage-bde.exe** oraz za pomocą zasad grupowych. Oprócz ochrony podstawowych składników, którą zapewnia sprzętowy moduł TPM, część klucza szyfrowania przechowywana jest na dysku flash USB, a uwierzytelnienie użytkownika w module TPM wymaga podania kodu PIN. Uzyskane w ten sposób uwierzytelnianie wieloczynnikowe gwarantuje najwyższy poziom bezpieczeństwa; nawet jeśli klucz USB zostanie zgubiony lub skradziony, nie będzie można go użyć w celu uzyskania dostępu do dysku, ponieważ do tego celu konieczne jest również podanie poprawnego numeru PIN. Tryb ten zapewnia ochronę środowiska rozruchowego dla systemu Windows 7 SP1 poprzez moduł TPM. Ustawienie tego trybu zalecane jest w środowiskach wymagających zapewnienia bardzo wysokiego poziomu bezpieczeństwa.

- **Tryb pracy funkcji BitLocker bez modułu TPM.** Tryb ten zapewnia pełne szyfrowanie całego dysku, ale nie oferuje ochrony środowiska rozruchowego systemu Windows 7 SP1. To ustawienie zalecane jest dla komputerów nieposiadających sprzętowego modułu TPM. Aby zastosować ten tryb, niezbędna jest konfiguracja ustawień zasad grupowych: **Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Szyfrowanie dysków funkcją BitLocker\Dyski z systemem operacyjnym\Wymagaj dodatkowego uwierzytelniania przy uruchamianiu**.

  (Computer Configuration\Administrative Templates\WindowsComponents\BitLocker Drive Encryption\Operating System Drives\Require Additional Authentication At Startup)

  Tryb pracy bez modułu TPM wymaga urządzenia pamięci flash USB zawierającego klucz uruchomienia systemu Windows.

Funkcja BitLocker w większości przypadków generuje klucze szyfrujące, które zostaną zapisane w pamięci (bezpieczny magazyn danych) modułu TPM. W momencie włączania i konfiguracji modułu TPM system Windows 7 SP1 będzie korzystał z niewielkiej informacji (ziarna – ang. seed) dostarczanej do generatora liczb losowych systemu Windows (RNG- ang. Random Number Generator). System RNG odpowiada za generowanie kluczy kryptograficznych dla różnych aplikacji w systemie Windows. Stopień przypadkowości kluczy kryptograficznych będzie znacznie wyższy, gdy zastosujemy TPM, niż przy użyciu do tego celu wyłącznie oprogramowania. Rekomendowane jest więc włączenie i skonfigurowanie sprzętowego modułu TPM w ustawieniach BIOS komputera.

Domyślnie w systemach Windows 7 SP1 generator liczb losowych (RNG) pobiera wartość z modułu TPM podczas startu systemu i powtarza tę czynność cyklicznie – co 40 minut. W systemie dostępne są trzy konfiguracje, które pozwalają kontrolować to ustawienie. Parametry domyślne są optymalne dla większości zastosowań.

Ustawienie TPMBOOTENTROPY można modyfikować poprzez mechanizm danych konfiguracji rozruchu (ang. Boot Configuration Data – BCD). Jeśli w konfiguracji ustawiono opcję „fałsz" (ang. false), mechanizm wyłączy pobieranie entropii z modułu TPM dla komputerów z włączonym układem TPM. Podczas normalnego startu systemu parametr ten ma domyślnie ustawioną wartość: „prawda" (ang. true), a w trybach awaryjnym oraz awaryjnym z obsługą sieci – „fałsz". Więcej informacji na temat zarządzania ustawieniami przechowywanymi w BCD można znaleźć w dokumentach: Boot Configuration Data in Windows Vista[41] oraz BCDEdit Commands for Boot Environment[42].

Parametr dotyczący częstotliwości odświeżania (ang. refresh interval) określa, jak często (w minutach) entropia danych jest pobierana z układu TPM. Gdy wartość tego ustawienia wynosi zero, entropia nie jest pobierana – wartość nie wpływa więc na ilość danych pobieranych podczas startu systemu. Podczas modyfikacji tego parametru należy zachować szczególną uwagę; nawet najmniejsza zmiana może wpłynąć na ustawienie „Mean Time To Failure" w poszczególnych implementacjach różnych dostawców układu TPM. Wartość tego parametru przechowywana jest w gałęzi rejestru **Hkey_Local_Machine** (wartość DWORD o nazwie **TpmRefreshEntropyIntervalInMinutes**) i umieszczona w lokalizacji **\Software\Policies\Microsoft\Cryptography\RNG**. Domyślna wartość tego ustawienia wynosi 40 i można ją konfigurować w zakresie od 0 do 40. Dodatkowo możemy zmodyfikować liczbę milibitów (ang. millibits) danych na każdy bajt wychodzący z generatora liczb losowych układu TPM. Wartość tego parametru przechowywana jest w gałęzi rejestru **Hkey_Local_Machine** (wartość DWORD o nazwie **TpmEntropyDensityInMillibitsPerByte**) i zlokalizowana w **\System\CurrentControlSet\Control\Cryptography\RNG**. Domyślna wartość tego ustawienia wynosi 8000 i można ją konfigurować w zakresie od 1 do 8000. Więcej informacji na temat technologii TPM oraz jej specyfikacji można znaleźć na stronie Trusted Computing Group[43].
Należy podkreślić, iż w przypadku niedostępności modułu TPM funkcja BitLocker może nadal zabezpieczać dane, ale nie oferuje wówczas ochrony integralności systemu oraz ochrony środowiska rozruchowego. Użytkownik może jednak skorzystać z takich rozwiązań jak:

- ochrona danych znajdujących się dyskach systemowych oraz dyskach stałych
- ochrona danych przechowywanych na wymiennych dyskach przy zastosowaniu funkcji BitLocker To Go

Szczegóły wskazanych rozwiązań omówione są w dalszej części niniejszego rozdziału.

Uwaga: Funkcja BitLocker umożliwia zabezpieczenie danych w systemie Windows Server 2008, ale scenariusz ten nie został opisany w niniejszym przewodniku.

[41] http://go.microsoft.com/fwlink/?LinkId=93005
[42] http://go.microsoft.com/fwlink/?LinkId=113151
[43] http://www.trustedcomputinggroup.org/

Uwaga: Mimo że dane w programie Windows Virtual PC można zapisać w formie wirtualnych dysków (VHD) wewnątrz systemu plików chronionego przez mechanizm BitLocker, to nie ma możliwości wykorzystania chronionych przez funkcję BitLocker wirtualnych dysków (VHD) do uruchomienia systemu Windows z pliku VHD (native VHD boot). Nie można także uruchomić funkcji BitLocker na wolumenach, które zawarte są wewnątrz plików VHD.

4.3. Ochrona danych znajdujących się na dyskach systemowych oraz dyskach stałych

Zastosowanie funkcji BitLocker umożliwi w takim przypadku ochronę wszystkich stałych dysków z danymi (wewnętrzne dyski twarde), które zawierają pliki systemu operacyjnego a także inne dane. Jest to zalecana konfiguracja, która gwarantuje, że wszystkie dane w systemie są chronione przez funkcję BitLocker.

Ocena ryzyka

Głównym zagrożeniem bezpieczeństwa dla organizacji jest utrata danych z komputerów przenośnych, które zostały utracone lub skradzione. Osoba nieupoważniona uzyskuje wówczas fizyczny dostęp do niezabezpieczonego komputer. To zaś wiąże się z potencjalnymi niebezpieczeństwami:

- Atakujący może zalogować się do komputera z systemem Windows 7 SP1 i skopiować dane
- Atakujący może uruchomić komputer z alternatywnego systemu operacyjnego, aby:
    - przejrzeć listę plików
    - skopiować pliki
    - odczytać dane z plików hibernacji lub pliku stronicowania w celu pozyskania informacji przechowywanych jawnie lub dokumentów związane z uruchomionym procesem
    - odczytać dane z plików hibernacji w celu ujawnienia i pozyskania kopii kluczy prywatnych przechowywanych w postaci tekstowej

Nawet jeśli pliki zostały zaszyfrowane przy wykorzystaniu systemu szyfrowania plików EFS, istnieje zagrożenie, iż nieostrożny użytkownik systemu przeniesie je lub skopiuje do katalogu, na którym funkcja EFS nie jest włączona (np. katalogi tymczasowe lub ukryte). To zaś może skutkować pozostawieniem kopii plików w postaci niezaszyfrowanej i dostępnej dla atakującego. Nieświadomi pracownicy działów IT mogą dopuścić się zaniedbania, nie szyfrując katalogów ukrytych, w których mogą być przechowywane kopie plików wykonywane przez aplikacje podczas normalnej pracy systemu i aplikacji. Istnieje również ryzyko operacyjne; nieupoważnione osoby mogą dokonać modyfikacji plików systemowych lub rozruchowych, które uniemożliwią normalną pracę systemu operacyjnego.

Minimalizacja ryzyka

Funkcja BitLocker została zaprojektowana m.in. po to, by zmniejszyć ryzyko, które wiąże się z przedstawionymi sytuacjami. Przy odpowiedniej konfiguracji systemu narzędzie BitLocker wykryje

zmiany o znaczeniu krytycznym w plikach startowych systemu operacyjnego oraz zapewni ochronę środowiska rozruchowego dla systemu Windows 7 SP1 wraz z wymuszeniem dodatkowego procesu uwierzytelnienia przed uruchomieniem systemu i uzyskaniem dostępu do w pełni zaszyfrowanego dysku. Pomoże to utrzymać wysoki poziom zabezpieczenia systemu operacyjnego oraz chronić dane przed nieautoryzowanym dostępem.

Zagadnienia dotyczące minimalizacji ryzyka, które wymagają rozważenia

Funkcja BitLocker stosowana na dyskach, na których zainstalowany jest system Windows (dysk systemu operacyjnego), oraz stałych dyskach z danymi (wewnętrzne dyski twarde) może zmniejszyć zagrożenie zdefiniowane w poprzedniej sekcji („Ocena ryzyka”,). Jednak przed zastosowaniem tego narzędzia należy wziąć pod uwagę związane z nim wymagania i najlepsze praktyki:

- Aby zastosować konfigurację optymalną, płyta główna komputera powinna posiadać moduł TPM 1.2 lub nowszy oraz obsługiwać system BIOS zgodny z wytycznymi Trusted Computing Group. Zaleca się także stosowanie kodu PIN, który zostanie nadany przez użytkownika w celu umożliwienia startu systemu operacyjnego. Opcjonalnie można zastosować klucz uruchomienia umieszczony na nośniku pamięci flash USB.

- Dysk twardy chronionego komputera powinien zawierać minimum 2 partycje: partycję z systemem operacyjnym i aktywną partycję systemową. Partycja systemowa to miejsce, gdzie zostaną zainstalowane pliki systemu operacyjnego w postaci zaszyfrowanej, które pozwolą na uruchomienie systemu. Aktywna partycja systemowa w postaci niezaszyfrowanej musi posiadać minimalną wielkość 100 MB. Domyślnie podczas instalacji systemu Windows 7 SP1, instalator systemu Windows automatycznie tworzy partycję systemową, do której nie jest przypisana żadna litera dysku i która jest ukryta przed użytkownikami. Jeśli system nie posiada oddzielnej aktywnej partycji systemowej, układ partycji zostanie zmodyfikowany w sposób automatyczny podczas włączenie i zastosowanie funkcji BitLocker.

- Jeśli konfiguracja BitLockera uwzględni żądanie pamięci USB lub kodu PIN, konieczne jest ustalenie i wprowadzenie procedury, która przewiduje sytuacje awaryjne związane z utratą kluczy uruchomienia lub zapomnieniem kodów PIN i jednocześnie pozwala na ich odzyskanie przez użytkowników.

- Funkcja BitLocker ma niewielki wpływ na wydajność komputera. Niedogodności związane z jej stosowaniem pozostają niezauważalne dla większości użytkowników. Jeśli jednak wydajność systemu ma bardzo duże znaczenie, warto w fazie testów przedwdrożeniowych sprawdzić, czy narzędzie to nie wpływa negatywnie na wydajność pracy użytkownika.

- W zależności od rozwiązań zastosowanych przez producenta komputerów, narzędzia służące do zarządzania modułem TPM mogą wymagać ręcznej konfiguracji komputera lub ustawień BIOS. Należy wziąć to pod uwagę, planując wdrożenie funkcjonalności BitLocker w organizacji(w sposób pełni zautomatyzowany lub wykorzystując skrypty) – zarówno w przypadku nowych instalacji, jak i aktualizacji poprzednich systemów Windows.

- Aby zastosować dysk USB z kluczem uruchomienia w celu odblokowania procedury startu i rozruchu systemu, BIOS komputera musi umożliwiać odczyt danych z dysku USB w środowisku przed zainicjowaniem systemu operacyjnego.

- BitLocker może mieć wpływ na proces dystrybucji oprogramowania, który został zautomatyzowany i przewiduje zdalne instalacje lub aktualizacje aplikacji, zaplanowane w nocy lub poza godzinami pracy, i który wymaga ponownego rozruchu komputera bez obecności użytkownika. Opisaną sytuację ilustrują poniższe przykłady:

  - Konfiguracja komputera przewiduje ochronę wykorzystującą zastosowanie modułu TPM wraz z kodem PIN lub modułu TPM wraz z kluczem uruchomienia znajdującym się na nośniku USB, a w ustawieniach jednej z aplikacji zaplanowano czynność na godzinę 2.00 w nocy. Jeśli proces wdrożenia aplikacji będzie wymagał restartu komputera, komputer nie zostanie poprawnie zrestartowany z uwagi na wymaganie wprowadzenia kodu PIN lub obecności klucza uruchomienia na nośniku pamięci USB.

  - Jeśli w organizacji wykorzystywana jest technologia Wake-on-LAN lub funkcja automatycznego uruchomienia komputera poprzez BIOS w celu wykonania czynności serwisowych, to takie komputery również nie zostaną automatycznie uruchomione z powodu zastosowania modułu TPM z dodatkowym elementem uwierzytelniającym.

- Wszelkie aktualizacje oprogramowania układowego (ang. firmware) mogą wpłynąć niekorzystnie na komputery z włączoną funkcją BitLocker. Aktualizacja oprogramowania BIOS może zostać rozpoznana przez BitLocker jako modyfikacja środowiska, co spowoduje, że komputer przejdzie w tryb odzyskiwania (ang. Recovery mode). Jeśli funkcja BitLocker jest już włączona i zachodzi konieczność zaktualizowania systemu BIOS, należy wstrzymać jej działanie na czas przeprowadzenia aktualizacji, a następnie, po zakończeniu tego procesu, wznowić funkcjonowanie narzędzia BitLocker.

- Choć istnieje małe prawdopodobieństwo, że aktualizacje aplikacji mogą mieć wpływ na działanie komputerów z włączoną funkcją BitLocker, to należy zwrócić szczególna uwagę na zmiany wprowadzane do systemu przez aktualizacje, szczególnie zaś na zmiany wprowadzane do menadżera rozruchu (ang. boot manager). Mogą one powodować błędy podczas rozruchu systemu i przejście komputera w tryb odzyskiwania. Przed przystąpieniem do instalacji lub aktualizacji aplikacji zaleca się przetestowanie tych czynności na komputerze z włączoną funkcją BitLocker.

- Wszystkie kontrolery domenowe muszą pracować pod kontrolą systemu Windows Server 2003 z dodatkiem Service Pack 2 (SP2) lub wyższym.

Uwaga: Windows Server 2003 wymaga rozszerzenia schematu usługi katalogowej (Active Directory), aby umożliwić poprawną obsługę i przechowywanie kopii zapasowej informacji odzyskiwania funkcji BitLocker w usługach domenowych usługi Active Directory (AD DS).

Proces minimalizacji ryzyka

Poniżej przedstawiono proces minimalizacji ryzyka, który pozwoli oszacować i wdrożyć najlepsze praktyki w konfiguracji funkcji BitLocker, aby zapewnić ochronę wrażliwych danych znajdujących się na komputerach klienckich zarządzanych w organizacji.

W celu minimalizacji ryzyka zaleca się zastosowanie następujących czynności:

1. Sprawdzenie i przeprowadzenie testów funkcji BitLocker.

Uwaga: Aby uzyskać dodatkowe informacje na temat funkcji BitLocker, należy zapoznać się z dokumentami: BitLocker Drive Encryption Deployment Guide for Windows 7[44] i Windows BitLocker Drive Encryption Design and Deployment Guides[45], dostępnymi na stronach witryny Microsoft TechNet.

2. Oszacowanie potrzeby wdrożenia funkcji BitLocker w organizacji.

3. Ustalenie wymagań dotyczących sprzętu, oprogramowania oraz oprogramowania firmware, które należy spełnić, by zastosować ochronę BitLocker.

4. Dokonanie identyfikacji komputerów, które wymagają zapewnienia ochrony przez funkcję BitLocker.

5. Określenie pożądanego poziomu ochrony z uwzględnieniem możliwości zastosowania zabezpieczeń dodatkowych (kodów PIN lub nośników pamięci USB z kluczem uruchomienia), mając na uwadze fakt, iż system nie uruchomi się poprawnie bez wprowadzenia wymaganych danych.

6. Instalacja niezbędnych sterowników w systemie testowym.

7. Wykorzystanie obiektów zasad grup (GPO) w celu skonfigurowania funkcji BitLocker w systemach testowych.

8. Wdrożenie funkcji BitLocker – po uprzednim przeprowadzeniu testów – w środowisku produkcyjnym.

9. Stosowanie zasad grup w celu kontrolowania opcji włączania funkcji BitLocker i prawidłowego zarządzania jej konfiguracją.

4.4. Zastosowanie ustawień zasad grup do wdrożenia BitLocker w celu minimalizacji ryzyka

Poniżej przedstawione zostaną dwa szablony ustawień zasad grup, które zaleca się stosować w zarządzaniu konfiguracją funkcji BitLocker. Szablony te umożliwiają zarządzanie konfiguracją modułu TPM niezależnie od reszty funkcji BitLocker. Poniższa tabela przedstawia ustawienia zasad grup dostępne dla funkcji BitLocker w szablonie **VolumeEncryption.admx**. Konfiguracji tych ustawień można dokonać w narzędziu Edytor obiektów zasad grupy, w następującej lokalizacji:

Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Szyfrowanie dysków funkcją BitLocker
(Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption)

[44] http://go.microsoft.com/fwlink/?LinkId=140286
[45] http://go.microsoft.com/fwlink/?LinkId=134201

W systemie Windows 7 SP1 dostępne są trzy poziomy ustawień zasad grupowych, udostępnione w poniższym porządku:

- Dyski z systemem operacyjnym
- Stałe dyski danych
- Wymienne dyski danych

Na poziomie globalnym ustawień dostępne są następujące ustawienia zasad grupowych:

§ – Oznacza ustawienia zasad grupowych, które są nowością w Windows 7 SP1.

Zasada	***Poziom ważności***	***Opis***	***Domyślne ustawienie w systemie Windows 7 SP1***	***Ustawienie zalecane przez Microsoft***
Przechowuj informacje odzyskiwania funkcji BitLocker w usługach domenowych w usłudze Active Directory (systemy Windows Server 2008 i Windows Vista)		To ustawienie zasad umożliwia zarządzanie kopią zapasową informacji odzyskiwania szyfrowania dysków funkcją BitLocker w usługach domenowych w usłudze Active Directory (AD DS, Active Directory Domain Services) Ta zasada dotyczy tylko komputerów z systemami Windows Server 2008 lub Windows Vista.	Nie skonfigurowano	
Wybierz folder domyślny dla hasła odzyskiwania	Opcjonalny	To ustawienie zasad umożliwia określenie domyślnej ścieżki wyświetlanej w monicie Kreatora instalacji szyfrowania dysków funkcją BitLocker o wprowadzenie lokalizacji folderu, w którym ma zostać zapisane hasło	Nie skonfigurowano	Nie skonfigurowano

		odzyskiwania.		
Określ, jak użytkownicy mogą odzyskiwać dyski chronione funkcją BitLocker (systemy Windows Server 2008 i Windows Vista)		To ustawienie zasad umożliwia określenie, czy w Kreatorze instalacji szyfrowania dysków funkcją BitLocker będzie można wyświetlić i określić opcje odzyskiwania funkcji BitLocker.	Nie skonfigurowano	
Wybierz metodę szyfrowania dysków i siłę szyfrowania	Istotny	To ustawienie zasad umożliwia skonfigurowanie algorytmu i siły szyfrowania, używanych przez funkcjonalność szyfrowania dysków funkcją BitLocker. Funkcja BitLocker będzie używać domyślnej metody szyfrowania — AES 128 bitów z rozpraszaniem.	Nie skonfigurowano	Włączone AES 256 bitów z rozpraszaniem
§ Podaj unikatowe identyfikatory dla organizacji	Opcjonalny	To ustawienie zasad umożliwia skojarzenie unikatowych identyfikatorów organizacyjnych z nowym dyskiem, dla którego włączono funkcję BitLocker.	Nie skonfigurowano	Nie skonfigurowano
Zapobiegaj zastępowaniu pamięci podczas ponownego uruchamiania komputera	Opcjonalny	To ustawienie zasad steruje wydajnością pracy podczas ponownego uruchamiania komputera przy narażeniu na ryzyko ujawnienia tajnych	Nie skonfigurowano	Nie skonfigurowano

		kluczy funkcji BitLocker.		
§ Sprawdzaj zgodność użycia certyfikatu karty inteligentnej z regułami	Opcjonalny	To ustawienie zasad umożliwia skojarzenie identyfikatora obiektu pochodzącego z certyfikatu karty inteligentnej z dyskiem chronionym funkcją BitLocker.	Nie skonfigurowano	Nie skonfigurowano

Tabela 4.4.1. Ustawienia globalne szyfrowania dysków funkcją BitLocker

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnego ustawienia można znaleźć w zakładce **POMOC** w ustawieniach Edytora obiektów zasad grupy.

Tabela poniżej przedstawia ustawienia zasad grupowych dostępne dla modułu TPM w szablonie **TPM.admx**. To ustawienie można skonfigurować w narzędziu Edytor obiektów zasad grupy, w następującej lokalizacji:

Konfiguracja komputera\Szablony administracyjne System\Usługi modułu TPM
(Computer Configuration\Administrative Templates\System\Trusted Platform Module Services)

Ustawienie zasad	***Opis***	***Domyślne ustawienie w systemie Windows 7 SP1***
Włącz tworzenie kopii zapasowej modułu TPM w usługach domenowych Active Directory	*To ustawienie zasad umożliwia zarządzanie kopiami zapasowymi informacji o właścicielu zgodnego sprzętowego modułu zabezpieczającego TPM (Trusted Platform Module) w usługach domenowych usługi Active Directory (AD DS).*	Nie skonfigurowano
Konfigurowanie listy blokowanych poleceń modułu TPM	*To ustawienie zasad umożliwia zarządzanie listą zasad grupy poleceń modułu TPM (Trusted Platform Module) blokowanych w systemie Windows.*	Nie skonfigurowano
Ignorowanie listy domyślnej blokowanych poleceń modułu TPM	*To ustawienie zasad umożliwia wymuszanie lub ignorowanie domyślnej listy poleceń modułu TPM (Trusted Platform Module) zablokowanych na komputerze.*	Nie skonfigurowano
Ignorowanie listy lokalnej blokowanych poleceń modułu	*To ustawienie zasad umożliwia wymuszanie lub ignorowanie lokalnej*	Nie skonfigurowano

TPM	*listy poleceń modułu TPM (Trusted Platform Module) zablokowanych na komputerze.*	

Tabela 4.4.2. Ustawienia modułu Trusted Platform Module

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnej konfiguracji można znaleźć w zakładce **POMOC** w ustawieniach Edytora obiektów zasad grupy.

Dostępne opcje dla ustawień: Stałe dyski danych

Ustawienia charakterystyczne dla dysków stałych (wewnętrzne dyski twarde), zawierających dane użytkownika lub aplikacji (ale nie są to dyski, na których zainstalowany jest system Windows), dostępne są w Edytorze obiektów zasad grupy, w następującej lokalizacji:

Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Szyfrowanie dysków funkcją BitLocker\Stałe dyski danych

(Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives)

Poniższa tabela przedstawia ustawienia zasad grupowych, które są dostępne dla funkcji BitLocker w szablonie **VolumeEncryption.admx**. Na poziomie **Stałe dyski danych** dostępne są następujące ustawienia zasad grupowych:

§ – Oznacza ustawienia zasad grupowych, które są nowością w Windows 7 SP1.

Zasada	***Poziom ważności***	***Opis***	***Domyślne ustawienie w systemie Windows 7 SP1***	***Ustawienie zalecane przez Microsoft***
§ Konfiguruj użycie kart inteligentnych na stałych dyskach danych	Krytyczny	To ustawienie zasad umożliwia określenie, czy można używać kart inteligentnych do uwierzytelniania dostępu użytkownika do dysków stałych na komputerze, które są chronione funkcją BitLocker.	Nie skonfigurowano	Włączone Wymagaj użycia kart inteligentnych na stałych dyskach twardych
§ Odmawiaj dostępu do zapisu do dysków stałych niechronionych funkcją BitLocker	Opcjonalny	To ustawienie zasad określa, czy ochrona funkcją BitLocker jest wymagana, aby komputer umożliwiał zapisywanie danych na dyskach stałych. Takie	Nie skonfigurowano	Nie skonfigurowano

		ustawienie zasad jest stosowane po włączeniu funkcji BitLocker.		
§ Zezwalaj na dostęp do stałych dysków danych chronionych funkcją BitLocker ze starszych wersji systemu Windows	Krytyczny	To ustawienie zasad określa, czy stałe dyski sformatowane za pomocą systemu plików FAT można odblokowywać i przeglądać na komputerach z systemami operacyjnymi: Windows Server 2008, Windows Vista, Windows XP z dodatkiem Service Pack 3 (SP3) lub Windows XP z dodatkiem Service Pack 2 (SP2).	Nie skonfigurowano	Wyłączone
§ Konfiguruj używanie haseł dla stałych dysków danych	Istotny	To ustawienie zasad określa, czy do odblokowania stałych dysków chronionych funkcją BitLocker wymagane jest hasło. Jeśli wybrana zostanie opcja zezwalania na używanie hasła, można będzie zażądać użycia hasła, wymusić przestrzeganie wymagań dotyczących złożoności hasła oraz skonfigurować minimalną długość hasła.	Nie skonfigurowano	Wyłączone
§ Określ, jak mogą być odzyskiwane dyski stałe chronione funkcją	Krytyczny	To ustawienie zasad umożliwia określenie, w jaki sposób odzyskiwane będą	Nie skonfigurowano	Włączone

BitLocker		stałe dyski chronione funkcją BitLocker w przypadku braku wymaganych poświadczeń.		Zezwalaj na używanie agenta odzyskiwania danych Nie zezwalaj na używanie 48-cyfrowego hasła odzyskiwania Nie zezwalaj na używanie 256-bitowego klucza odzyskiwania Usuń opcje odzyskiwania z Kreatora instalacji funkcji bitlocker Wykonaj kopie zapasowe haseł odzyskiwania i pakietów kluczy

Tabela 4.4.3. Ustawienia Stałe dyski danych

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat konkretnego ustawienia można znaleźć w zakładce **POMOC** w ustawieniach Edytora obiektów zasad grupy.

Dostępne opcje dla ustawień: Dyski z systemem operacyjnym

Ustawienia charakterystyczne dla woluminów, na których zainstalowany jest system Windows (dysk systemu operacyjnego), dostępne są w Edytorze obiektów zasad grupy, w następującej lokalizacji:

Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Szyfrowanie dysków funkcją BitLocker\Dyski z systemem operacyjnym

(Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives)

Poniższa tabela przedstawia ustawienia zasad grupowych, które są dostępne dla funkcji BitLocker w szablonie **VolumeEncryption.admx**. Na poziomie **Dyski z systemem operacyjnym** dostępne są następujące ustawienia zasad grupowych:

§ – Oznacza ustawienia zasad grupowych, które są nowością w Windows 7 SP1.

Zasada	***Poziom ważności***	***Opis***	***Domyślne ustawienie w systemie Windows 7 SP1***	***Ustawienie zalecane przez Microsoft***
§ Wymagaj dodatkowego uwierzytelniania przy uruchamianiu	Krytyczny	To ustawienie zasad umożliwia określenie, czy funkcja BitLocker będzie wymagać dodatkowego uwierzytelniania przy każdym uruchomieniu komputera i czy ma być ona używana wraz z modułem TPM, czy bez niego.	Nie skonfigurowano	Włączone **Nie** zezwalaj na używanie funkcji BitLocker bez zgodnego modułu TPM Konfiguruj uruchomienia modułu TPM: Nie zezwalaj na używanie modułu TPM Konfiguruj numer PIN uruchomienia modułu TPM: Wymagaj startowego kodu PIN z modułem TPM Nie zezwalaj na używanie klucza

				uruchomienia z modułem TPM Nie zezwalaj na używanie klucza i numeru PIN uruchomienia z modułem TPM
Wymagaj dodatkowego uwierzytelniania przy uruchamianiu (systemy Windows Server 2008 i Windows Vista)		To ustawienie zasad umożliwia określenie, czy Kreator instalacji szyfrowania dysków funkcją BitLocker uwzględni opcję konfiguracji dodatkowej metody uwierzytelniania, której użycie będzie wymagane przy każdym uruchomieniu komputera.	Nie skonfigurowano	
§ Zezwalaj na używanie rozszerzonych numerów PIN przy uruchamianiu	Istotny	To ustawienie zasad umożliwia określenie, czy rozszerzone numery PIN uruchomienia będą używane z funkcją BitLocker.	Nie skonfigurowano	Włączone
§ Konfiguruj minimalną długość numeru PIN uruchomienia	Krytyczny	To ustawienie zasad umożliwia skonfigurowanie minimalnej długości numeru PIN uruchomienia modułu TPM. Takie ustawienie zasad jest stosowane po włączeniu funkcji BitLocker. Minimalna długość numeru PIN uruchomienia to 4	Nie skonfigurowano	Włączone Minimalna liczba znaków: 7 Włączone

		cyfry, a maksymalna – 20 cyfr.		
§ Określ, jak mogą być odzyskiwane dyski z systemem operacyjnym chronione funkcją BitLocker	Krytyczny	To ustawienie zasad umożliwia określenie, w jaki sposób odzyskiwane będą dyski z systemem operacyjnym, które są chronione funkcją BitLocker, w przypadku braku wymaganych informacji o kluczu uruchomienia.	Nie skonfigurowano	Włączone Wymagaj używania 48-cyfrowego hasła odzyskiwania Nie zezwalaj na używanie 256-bitowego klucza odzyskiwania Usuń opcje odzyskiwania z Kreatora instalacji funkcji BitLocker Zapisz informacje odzyskiwania funkcji BitLocker w usługach AD DS dla dysków z systemem operacyjnym Nie włączaj funkcji BitLocker, dopóki informacje odzyskowania dla dysków z

				systemem operacyjnym nie będą przechowywane w usługach AD DS.
Konfiguruj profil sprawdzania poprawności platformy modułu TPM	Opcjonalny	To ustawienie zasad umożliwia skonfigurowanie sposobu zabezpieczenia klucza szyfrowania funkcji BitLocker przez zabezpieczenia sprzętowe modułu TPM. Takie ustawienie zasad nie jest stosowane, gdy komputer nie ma zgodnego modułu TPM oraz wtedy, gdy funkcja BitLocker została już włączona z ochroną za pomocą modułu TPM.	Nie skonfigurowano	Nie skonfigurowano

Tabela 4.4.4. Ustawienia Stałe dyski danych

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat danej konfiguracji można znaleźć w zakładce **POMOC** w ustawieniach Edytora obiektów zasad grupy.

Polityka bezpieczeństwa powinna skutecznie wspierać stosowane dla funkcji BitLocker procedury dotyczące haseł i zarządzania kluczami. Polityka ta powinna uwzględniać wiele aspektów, aby wystarczająco zabezpieczyć dane, a jednocześnie nie utrudniać normalnej pracy funkcji BitLocker. Poniższa lista zawiera przykłady takich zasad:

- Zalecane jest wymaganie stosowania kopii zapasowej informacji odzyskiwania szyfrowania dysków funkcją BitLocker w usługach domenowych Active Directory.
- Zalecane jest wymaganie stosowania kopii zapasowej informacji o właścicielu zgodnego sprzętowego modułu zabezpieczającego TPM (Trusted Platform Module) w usługach domenowych Active Directory (AD DS).
- Zalecane jest stosowanie kluczy odzyskiwania danych oraz haseł odzyskiwania jako metody dostępu do zaszyfrowanych danych na wypadek awarii.

- W przypadku korzystania z modułu TPM w połączeniu z dodatkowymi zabezpieczeniami – numerem PIN lub nośnikiem USB zawierającym klucz uruchomienia – uwzględnione w nich hasła dostępu należy zmieniać w regularnych odstępach czasu.
- W przypadku komputerów z włączonym i skonfigurowanym modułem TPM zalecane się założenie hasła administratora dla BIOS, aby zapobiec modyfikacji ustawień BIOS przez nieupoważnione osoby.
- Zalecane jest stosowanie procedur, które zabraniają przechowywania wraz komputerem nośników pamięci USB zawierających klucz uruchomienia (np. jedna torba na komputer i nośnik pamięci czy pozostawienie klucza USB w pobliżu komputera).
- Zalecane jest stosowanie bezpiecznej lokalizacji centralnej do przechowywania kluczy odzyskiwania funkcji BitLocker w przypadku odzyskiwania danych po awarii.
- Zalecane jest przechowywanie w bezpiecznym miejscu – poza główną lokalizacją organizacji – kopii materiałów zawierających informacje niezbędne do odzyskiwania zaszyfrowanych danych.

Dodatkowym narzędziem, które wspomaga funkcję BitLocker, jest MBAM (ang. BitLocker Administration and Monitoring). Narzędzie to pozwala na łatwiejsze wdrażanie i odzyskiwanie kluczy, centralizację zapewniania dostępu, monitorowanie i raportowanie stanu szyfrowania dysków stałych i wymiennych oraz minimalizację kosztów obsługi. MBAM jest częścią pakietu Microsoft Desktop Optimization Pack dla Software Assurance[46]. Więcej informacji na temat MBAM można uzyskać na stronie dokumentacji produktu MBAM[47].

4.5. Ochrona danych przechowywanych na wymiennych dyskach danych z zastosowaniem funkcji BitLocker To Go

Funkcja BitLocker To Go dostępna jest tylko w edycjach Enterprise i Ultimate systemu Windows 7 SP1. Na komputerach pracujących pod kontrolą systemu operacyjnego Windows 7 SP1 możliwe jest skonfigurowanie urządzeń USB tak, aby wspierały funkcję BitLocker To Go. Pozostałe edycje systemu Windows 7 SP1 mogą odczytać dane z zaszyfrowanego dysku USB i zapisać dane w innej lokalizacji, ale nie mogą skonfigurować nowych urządzeń USB do obsługi funkcji BitLocker To Go. Funkcja BitLocker To Go pozwala na szyfrowanie dysków przenośnych i umożliwia korzystanie z tych urządzeń na innych komputerach – pod warunkiem posiadania odpowiedniego hasła. W tym scenariuszu możliwe jest zastosowanie BitLocker To Go w celu ochrony danych na wymiennych dyskach, takich jak zewnętrzne dyski IEEE 1394, karty pamięci lub pamięci flash USB. Funkcja BitLocker To Go pozwala organizacjom na zabezpieczenie danych przechowywanych na tych nośnikach przed nieautoryzowanym dostępem; nawet gdy nośnik zostanie zgubiony lub skradziony.

Ocena ryzyka

Przenośne nośniki danych stanowią istotne zagrożenie dla ważnych i wrażliwych danych w organizacji. Urządzenia te szybko stały się powszechne z uwagi na niską cenę, prostotę stosowania oraz funkcjonalność, umożliwiającą kopiowanie i przenoszenie bardzo dużych ilości danych w bardzo krótkim czasie. Jednak komputery przenośne i urządzenia pamięci flash USB są często narażone na

[46] http://www.microsoft.com/pl-pl/windows/enterprise/products-and-technologies/mdop/mbam.aspx
[47] http://onlinehelp.microsoft.com/en-us/mdop/gg703313.aspx

zagrożenia związane z ich utratą lub kradzieżą podczas przewożenia. Stwarza to ryzyko, że dane wrażliwe trafią do niepowołanych osób, co narazi organizację na ogromne straty.

Minimalizacja ryzyka

Aby zmniejszyć zagrożenie związane z powyższymi kwestiami, organizacje stosują różne ograniczenia: zakazują stosowania urządzeń, wyłączają porty i urządzenia USB oraz IEEE 1394, a także wdrażają konfiguracje chroniące sekwencję startową poprzez zezwolenie na uruchomienie systemu tylko wtedy, gdy spełnione zostanie wymaganie w zakresie dodatkowego uwierzytelnienia. Ponadto często podejmowane są kroki w celu zapewnienia ochrony plików systemu operacyjnego i plików danych. BitLocker To Go zapewnia skuteczną warstwę ochronną, co oznacza, że nawet jeśli atakujący uzyska fizyczny dostęp do dysku, to taka sytuacja nie musi wiązać się z dostępem do zapisanych na nim danych. Korzystając z zasad grupowych, organizacje mogą wymusić, aby dyski wymienne korzystały z funkcji BitLocker To Go zanim dane zostaną skopiowane na urządzenie; wszystko po to, aby chronić dysk przed nieautoryzowanym dostępem.

Zagadnienia dotyczące minimalizacji ryzyka, które wymagają rozważenia

BitLocker To Go może zmniejszyć zagrożenie zdefiniowane w poprzedniej sekcji („Ocena ryzyka"). Jednak przed zastosowaniem tego narzędzia należy wziąć pod uwagę związane z nim wymagania i najlepsze praktyki:

- Funkcja BitLocker To Go nie wymaga modułu TPM.
- Dyski wymienne zaszyfrowane przy pomocy BitLocker To Go można skonfigurować tak, aby wymagały podania hasła lub zastosowania karty inteligentnej z odpowiednim certyfikatem w celu umożliwienia dostępu do danych. W przypadku zastosowania kart inteligentnych należy pamiętać o wyposażeniu komputerów w odpowiednie czytniki, które umożliwią odczyt danych z nośników wymiennych.
- Funkcja BitLocker ma niewielki wpływ na wydajność komputera. Niedogodność z tym związana jest niezauważalna dla większości użytkowników. Jeśli jednak wydajność systemu ma bardzo duże znaczenie, warto w fazie testów przedwdrożeniowych sprawdzić, czy narzędzie to nie wpływa negatywnie na wydajność pracy użytkownika.
- Należy pamiętać, że na komputerach z systemami Windows XP lub Windows Vista dyski mogą być dostępne jako urządzenia tylko do odczytu. Użytkownicy starszych wersji systemu Windows będą widzieć drugą partycję na urządzeniu, która zazwyczaj jest ukryta w systemie Windows 7 SP1. Funkcjonalność ta nazywana jest dyskiem odnajdywalnym (ang. discovery drive). Dysk ten zawiera aplikację BitLocker To Go Reader. Dzięki niej użytkownicy mogą odblokować zaszyfrowany dysk, podając prawidłowe hasła lub hasła odzyskiwania. Możliwe jest również skonfigurowanie zasad grupowych **Zezwalaj na dostęp do wymiennych dysków danych chronionych funkcją BitLocker ze starszych wersji systemu Windows.** Mają one na celu przeprowadzanie kontroli, czy utworzono dysk odnajdywalny i czy zostanie na nim umieszczona aplikacja BitLocker To Go podczas włączania obsługi ochrony BitLocker dla dysku wymiennego. Więcej informacji na ten temat można znaleźć w dokumencie: Best Practices for BitLocker in Windows 7[48].

[48]http://technet.microsoft.com/en-us/library/dd875532(WS.10).aspx

- Wszystkie kontrolery domenowe w domenie muszą pracować pod kontrolą systemu Windows Server 2003 SP2 lub wyższego.

Uwaga: Windows Server 2003 wymaga rozszerzenia schematu usługi katalogowej (Active Directory) w celu umożliwienia poprawnej obsługi i przechowywania kopii zapasowej informacji odzyskiwania funkcji BitLocker w usługach domenowych w Active Directory (AD DS).

Proces minimalizacji ryzyka

Poniżej przedstawiono proces minimalizacji ryzyka, który ma pomóc oszacować i wdrożyć najlepsze praktyki w konfiguracji funkcji BitLocker. Zapewni to ochronę wrażliwych danych przechowywanych na wymiennych dyskach w komputerach klienckich zarządzanych w organizacji.

W celu minimalizacji ryzyka zaleca się wykonanie poniższych czynności:

1. Sprawdzenie i przeprowadzenie testów technologii BitLocker To Go.

Uwaga: Aby uzyskać dodatkowe informacje na temat funkcji BitLocker, należy zapoznać się z dokumentami: BitLocker Drive Encryption Deployment Guide for Windows 7[49] i Windows BitLocker Drive Encryption Design and Deployment Guides[50], dostępnymi w witrynie Microsoft TechNet.

2. Oszacowanie potrzeby wdrożenia funkcji BitLocker To Go na wymiennych dyskach danych w organizacji.

3. Określenie wymagań dotyczących sprzętu i oprogramowania, które należy spełnić, by zastosować ochronę BitLocker To Go na wymiennych dyskach danych.

4. Dokonanie identyfikacji komputerów, które wymagają zapewnienia przez funkcję BitLocker To Go ochrony na wymiennych dyskach danych.

5. Przeprowadzenie niezbędnych testów urządzeń z wymiennymi dyskami, włączając w to wszelkie nośniki pamięci flash USB.

6. Wykorzystanie obiektów zasad grupowych (GPO) w celu skonfigurowania funkcji BitLocker na wymiennych dyskach w systemach testowych.

7. Przeszkolenie użytkowników w zakresie prawidłowego użytkowania funkcji BitLocker To Go na dyskach wymiennych w ich własnym środowisku.

8. Wdrożenie funkcjonalności BitLocker – po uprzednim przeprowadzeniu testów – na wymiennych dyskach danych w środowisku produkcyjnym.

Aby wyłączyć ochronę BitLocker na dyskach wymiennych, należy skorzystać z opcji **Szyfrowanie dysków funkcją BitLocker** dostępnej w **Panelu Sterowania**.

[49] http://go.microsoft.com/fwlink/?LinkId=140286
[50] http://go.microsoft.com/fwlink/?LinkId=134201

4.6. Zastosowanie ustawień zasad grup do wdrożenia BitLocker To Go w celu minimalizacji ryzyka

Poniższa tabela przedstawia ustawienia zasad grup dostępne dla funkcji BitLocker To Go w szablonie **VolumeEncryption.admx**. Konfiguracja tych ustawień dostępna jest w narzędziu Edytor obiektów zasad grupy, w następującej lokalizacji:

Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Szyfrowanie dysków funkcją BitLocker\Wymienne dyski danych

(Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives)

Na poziomie globalnym ustawień dostępne są następujące ustawienia zasad grupowych:

§ – Oznacza ustawienia zasad grupowych, które są nowością w Windows 7 SP1.

Zasada	*Poziom ważności*	*Opis*	*Domyślne ustawienie w systemie Windows 7 SP1*	*Ustawienie zalecane przez Microsoft*
§ Kontroluj użycie funkcji BitLocker na dyskach wymiennych	Opcjonalny	To ustawienie zasad kontroluje użycie funkcji BitLocker na wymiennych dyskach danych.	Nie skonfigurowano	Nie skonfigurowano
§ Konfiguruj użycie kart inteligentnych na wymiennych dyskach danych	Krytyczny	To ustawienie zasad umożliwia określenie, czy można używać kart inteligentnych do uwierzytelniania dostępu użytkownika do wymiennych dysków danych w komputerze, które są chronione funkcją BitLocker.	Nie skonfigurowano	Włączone Wymagaj użycia kart inteligentnych na wymiennych dyskach danych
§ Odmawiaj dostępu do zapisu do dysków wymiennych niechronionych funkcją BitLocker	Istotny	To ustawienie zasad umożliwia określenie, czy można używać kart inteligentnych do uwierzytelniania dostępu użytkownika do wymiennych dysków w komputerze, które są	Nie skonfigurowano	Włączone Nie zezwalaj na dostęp do zapisu do urządzeń skonfigurowanych w innej

		chronione funkcją BitLocker.		organizacji
§ Zezwalaj na dostęp do wymiennych dysków danych chronionych funkcją BitLocker ze starszych wersji systemu Windows	Istotny	To ustawienie zasad określa, czy wymienne dyski danych sformatowane za pomocą systemu plików FAT można odblokowywać i przeglądać na komputerach z systemami operacyjnymi: Windows Server 2008, Windows Vista, Windows XP z dodatkiem Service Pack 3 (SP3) lub Windows XP z dodatkiem Service Pack 2 (SP2).	Nie skonfigurowano	Wyłączone
§ Konfiguruj użycie haseł dla wymiennych dysków danych	Istotny	To ustawienie zasad określa, czy do odblokowania wymiennych dysków chronionych funkcją BitLocker wymagane jest hasło. Jeśli wybrana zostanie opcja zezwalania na używanie hasła, można będzie zażądać użycia hasła, wymusić przestrzeganie wymagań dotyczących złożoności hasła oraz skonfigurować jego minimalną długość.	Nie skonfigurowano	Wyłączone
§ Określ, jak mogą być odzyskiwane dyski wymienne chronione	Krytyczny	To ustawienie zasad umożliwia określenie, w jaki sposób, w przypadku braku	Nie skonfigurowano	Włączone Zezwalaj na

funkcją BitLocker		wymaganych poświadczeń, będą odzyskiwane wymienne dyski danych chronione funkcją BitLocker.		używanie agenta odzyskiwania danych Nie zezwalaj na używanie 48-cyfrowego hasła odzyskiwania Nie zezwalaj na używanie 256-bitowego klucza odzyskiwania Usuń opcje odzyskiwania z Kreatora instalacji funkcji BitLocker Wykonaj kopie zapasowe haseł odzyskiwania i pakietów kluczy

Tabela 4.6.1. Ustawienia funkcji BitLocker dla wymiennych dysków danych

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat danej konfiguracji można znaleźć w zakładce **POMOC** w ustawieniach Edytora obiektów zasad grupy.

4.7. System szyfrowania plików EFS

System szyfrowania plików (EFS) pozwala na zaszyfrowanie plików i folderów w celu zabezpieczenia ich przed nieautoryzowanym dostępem. Funkcjonalność ta, będąca jednym z komponentów systemu plików NTFS, nie ingeruje w działania użytkownika i aplikacji. Podczas normalnej pracy, kiedy użytkownik lub aplikacja próbują uzyskać dostęp do zaszyfrowanego pliku, system operacyjny automatycznie uzyskuje dostęp do klucza deszyfrującego zawartość pliku; operacje szyfrowania i deszyfrowania odbywają się w tle, a system wykonuje te działania w imieniu użytkownika. Użytkownicy, którzy posiadają dostęp do właściwych kluczy szyfrujących, pracują z plikami zaszyfrowanymi tak samo jak z plikami zwykłymi; inni użytkownicy otrzymują odmowę dostępu do zaszyfrowanych plików.

W systemie Windows 7 SP1 wprowadzono zmiany w architekturze. Obecnie system wspiera kryptografię opartą na krzywych eliptycznych (ECC – ang. Eliptic Curve Cryptography). Funkcjonalność ta jest zgodna z wymaganiami Suite B – zestawem algorytmów kryptograficznych zdefiniowanych przez NSA (National Security Agency) na potrzeby amerykańskich agencji rządowych w celu zapewnienia ochrony informacji niejawnych. Zdefiniowany zestaw Suite B wymaga zastosowania kryptograficznych algorytmów AES, SHA oraz ECC, aby zapewnić najwyższy stopień ochrony, i nie zezwala na stosowanie algorytmów kryptografii RSA. Jednak system szyfrowania plików (EFS) w systemie Windows 7 SP1 wspiera i obsługuje nowy „tryb mieszany", obsługujący algorytmy ECC i RSA. Tryb ten zapewnia zgodność plików zaszyfrowanych, które utworzono przy zastosowaniu algorytmów dostępnych w poprzednich wersjach systemów Windows. Funkcjonalność ta może być bardzo użyteczna dla organizacji, które stosują kryptograficzne algorytmy RSA i jednocześnie planują wykorzystywanie algorytmów ECC, aby przygotować własne środowisko do zapewnienia zgodności z zestawem Suite B.

Uwaga: Zaleca się stosowanie równoczesne mechanizmów BitLocker oraz EFS w celu zapewnienia najwyższego stopnia ochrony danych.

Ocena ryzyka

Nieautoryzowany dostęp do danych może wpłynąć negatywnie na procesy w organizacji; zwłaszcza tam, gdzie wielu użytkowników ma dostęp do tego samego systemu lub korzysta z przenośnych systemów komputerowych, co stwarza duże ryzyko ujawnienia danych. EFS został zaprojektowany, by zminimalizować ryzyko kradzieży danych oraz ujawnienia danych wrażliwych w przypadku zgubienia lub kradzieży komputerów przenośnych. W szczególności chodzi o ryzyko ujawnienia danych wrażliwych przez pracowników wewnętrznych, którzy posiadają do tych informacji dostęp. Na powyższe ryzyko narażone są również komputery ogólnodostępne i współdzielone.

Jeśli atakujący uzyska fizyczny dostęp do niezabezpieczonego komputera, konsekwencje takiego czynu mogą objąć następujące działania:

- Atakujący może uruchomić ponownie komputer i podwyższyć swoje uprawnienia do poziomu lokalnego administratora w celu uzyskania dostępu do danych użytkownika. Atakujący może również pobrać programy narzędziowe i wykonać atak siłowy, aby uzyskać hasła użytkownika. Po dokonaniu skutecznego ataku możliwe będzie zalogowanie się do systemu przy wykorzystaniu konta użytkownika i ujawnionego hasła, a w konsekwencji – uzyskanie dostępu do danych użytkownika.
- Atakujący może zalogować się do komputera z systemem Windows 7 SP1, aby przekopiować dostępne dane na nośniki przenośne, przesłać je poprzez wiadomość pocztową (e-mail) lub przekopiować za pomocą sieci komputerowej. Może także dokonać transferu danych do zdalnego serwera z wykorzystaniem protokołu FTP.
- Atakujący może ponownie uruchomić komputer z alternatywnego systemu operacyjnego i przekopiować dane bezpośrednio z lokalnego dysku twardego.
- Atakujący może połączyć komputer do innej sieci komputerowej, uruchomić skradziony komputer i następnie zalogować się do niego zdalnie.

- Jeśli użytkownik buforuje swoje pliki sieciowe w trybie offline, atakujący może wykorzystać je do podwyższenia swoich uprawnień do poziomu administratora systemu lokalnego, a następnie sprawdzić zawartość plików buforowanych w trybie offline.
- Atakujący może ponownie uruchomić komputer z alternatywnego systemu operacyjnego i dokonać odczytu zawartości pliku stronicowania. Pozwoli mu to na przechwycenie informacji przechowywanych jawnie lub kopii dokumentów w postaci otwartego tekstu, które zintegrowane są z uruchomionym procesem.
- Ciekawski współpracownik może zdobyć wrażliwe dane należące do innych użytkowników ogólnodostępnego i współdzielonego komputera.

Minimalizacja ryzyka

W celu zmniejszenia powyższego ryzyka zaleca się zaszyfrowanie danych przechowywanych na dyskach twardych. Ulepszenia w technologii EFS zastosowane w systemie Windows 7 SP1 pozwolą na zmniejszenie zagrożenia i podwyższą poziom bezpieczeństwa. By wykorzystać możliwości oferowanych rozwiązań, warto podjąć rekomendowane kroki:

- Należy stosować szyfrowanie (EFS) plików i folderów. Uniemożliwi to atakującemu odczyt plików za pośrednictwem innego systemu operacyjnego, jeśli nie posiada on klucza deszyfrującego do odszyfrowania zawartości pliku. W celu zwiększenia bezpieczeństwa klucz taki może zostać umieszczony na karcie inteligentnej.
- Należy wymuszać silne mechanizmy szyfrowania stosowane w EFS poprzez zastosowanie zasad grup.
- Należy udaremnić działania atakującej osoby, która przeprowadzając atak siłowy na hasło użytkownika, próbuje uzyskać dostęp do jego danych. Możemy uniemożliwić skuteczność takiego ataku, stosując karty inteligentne – jako magazyn dla kluczy szyfrujących EFS – lub połączenie obu technologii szyfrowania: BitLocker i EFS.
- Należy uniemożliwić atakującemu dostęp do wrażliwych danych użytkowników poprzez wymuszenie szyfrowania folderu „Moje dokumenty”, stosując zasady grupowe. Alternatywnie można wymusić szyfrowanie innych lokalizacji zawierających dane użytkownika lub zaszyfrować całą partycję z danymi użytkownika poprzez skrypty logowania.
- Należy stosować system szyfrowania plików EFS, aby zapewnić szyfrowanie na wielu dyskach i udziałach sieciowych.
- Należy stosować system szyfrowania plików EFS, aby zapewnić ochronę pliku stronicowania i buforowanych podręcznych plików sieciowych trybu offline.

Zagadnienia dotyczące minimalizacji ryzyka, które wymagają rozważenia

Szyfrowany system plików (EFS) może zmniejszyć zagrożenie zdefiniowane w poprzedniej sekcji („Ocena ryzyka”). Ważne jest jednak, aby przed zastosowaniem funkcji EFS wziąć pod uwagę następujące wymagania:

- Należy wdrożyć sprawdzone procedury zarządzania kluczami stosowanymi do odzyskiwania danych oraz procedur odzyskiwania danych. W przypadku braku niezawodnych i

poprawnie zdefiniowanych procedur, krytyczne dane organizacji mogą być niedostępne i nie możliwe do odszyfrowania w momencie utraty kluczy deszyfrujących.

- Funkcjonalność EFS ma niewielki wpływ na wydajność komputera. Niedogodność ta dla większości użytkowników jest niezauważalna podczas normalnej pracy. Jeśli jednak wydajność systemu ma bardzo duże znaczenie, warto w fazie testów przedwdrożeniowych sprawdzić, czy EFS nie wpływa negatywnie na wydajność pracy użytkownika.
- W przypadku gdy konieczne jest zapewnienie zgodności z zestawem Suite B, należy wdrożyć algorytm ECC w celu przygotowania systemu komputerowego do spełnienia wymagań wprowadzenia tego poziomu standardu szyfrowania.
- Gdy szyfrowanie plików EFS jest włączone, nie ma możliwości równoczesnego kompresowania plików na tym samym wolumenie; funkcja kompresji wbudowana jest w system plików NTFS.
- Użytkownicy i pracownicy działu IT muszą być odpowiednio przeszkoleni, aby uniknąć popełniania takich błędów jak:
  - kopiowanie oraz przenoszenie plików z miejsc zaszyfrowanych do miejsc niezaszyfrowanych, które może pozostawić pliki w postaci jawnej
  - niestosowanie szyfrowania plików w folderach ukrytych, w których aplikacje przechowują swoje kopie zapasowe
- Należy bardzo dokładnie przetestować konfigurację EFS w celu sprawdzenia, czy szyfrowanie EFS zostało wdrożone na wszystkich lokalizacjach plików z danymi wrażliwymi, wliczając w to folder „Moje dokumenty”, Pulpit oraz foldery z plikami tymczasowymi.

Proces minimalizacji ryzyka

Poniżej przedstawiono proces minimalizacji ryzyka, który pozwoli na określenie i wdrożenie najlepszych praktyk konfiguracji funkcji EFS. Zapewni to ochronę wrażliwych danych znajdujących się na komputerach klienckich zarządzanych w organizacji.

W celu minimalizacji ryzyka zaleca się zastosowanie następujących czynności:

1. Sprawdzenie i przeprowadzenie testów technologii szyfrowania EFS.
   Uwaga: W celu uzyskania dodatkowych informacji na temat EFS, należy zapoznać się z artykułem: „Best practices for the Encrypting File System"[51], umieszczonym w witrynie firmy Microsoft.
2. Oszacowanie potrzeby wdrożenia funkcji szyfrowania EFS.
3. Przeprowadzenie testów konfiguracji EFS poprzez zastosowanie zasad grup.
4. Dokonanie identyfikacji komputerów, które wymagają ochrony przez szyfrowanie EFS.
5. Określenie pożądanego poziomu ochrony (wymaga to m.in. rozważenia, czy organizacja wymaga stosowania kart inteligentnych w połączeniu z systemem EFS).
6. Ustawienie szyfrowania EFS w sposób odpowiedni dla środowiska przy wykorzystaniu zasad grupowych.

[51] http://support.microsoft.com/default.aspx?scid=kb;en-us;223316

4.8. Szczegółowe ustawienia systemu EFS zapewniające ochronę wrażliwych danych

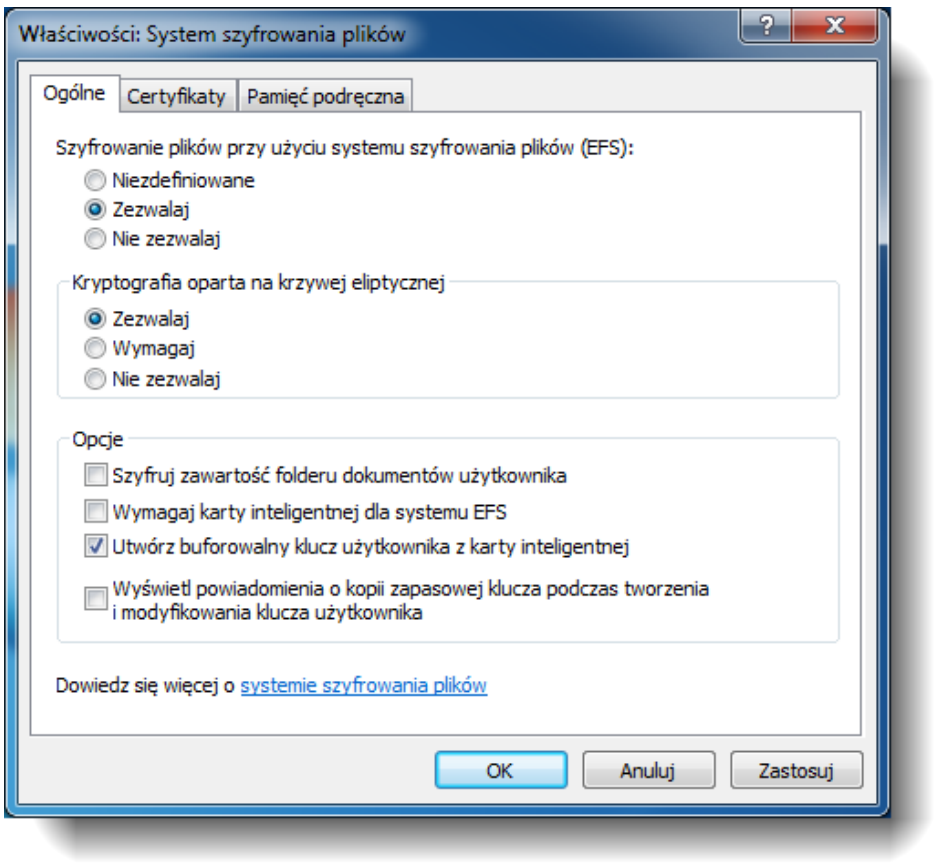
System szyfrowania plików EFS – poprzez mechanizm zasad grup – udostępnia kilka ustawień konfiguracyjnych. Są one dostępne w następującej lokalizacji:

Konfiguracja Komputera\Ustawienia systemu Windows\Ustawienie zabezpieczeń\Zasady kluczy publicznych\System szyfrowania plików

(Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypting File System)

Aby dodać lub utworzyć agenta odzyskiwania danych (DRA – ang. Data Recovery Agent), należy kliknąć prawym przyciskiem myszki na **System szyfrowania plików,** a następnie wybrać **Dodaj agenta odzyskiwania danych.**

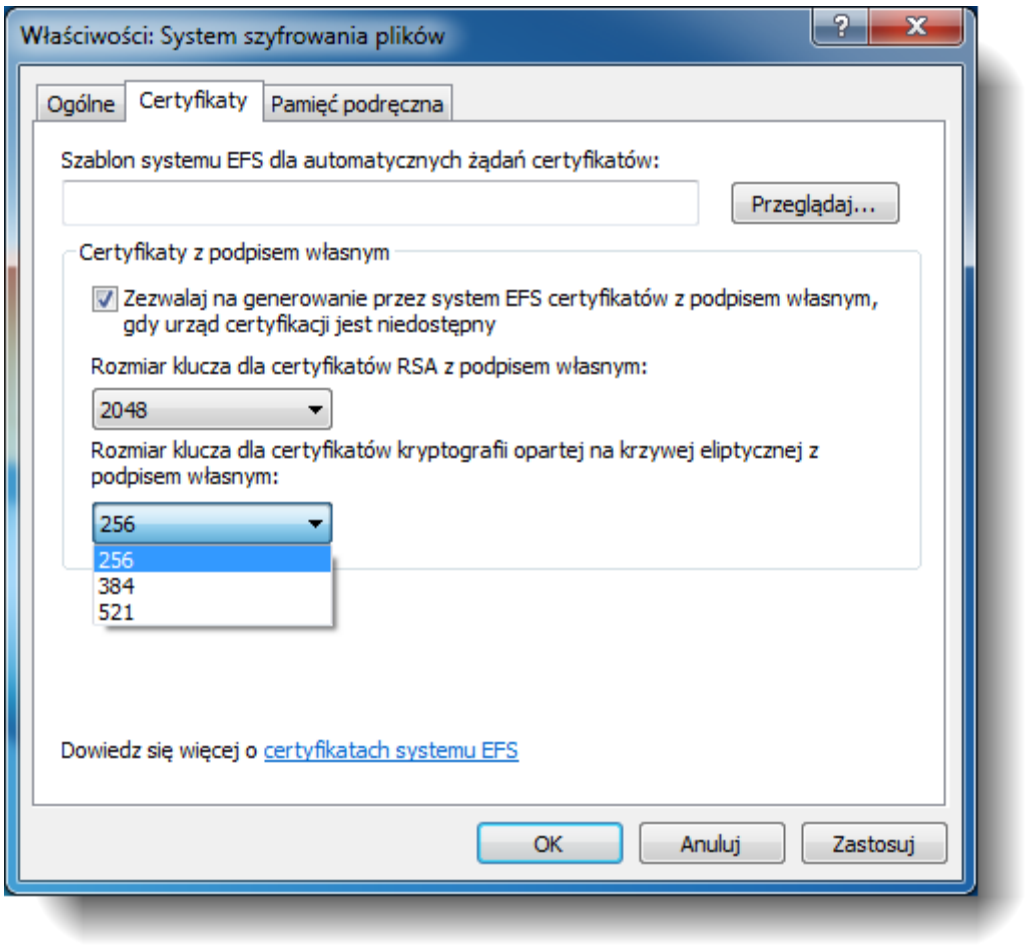
W celu wyświetlenia ustawień dotyczących EFS należy kliknąć prawym przyciskiem myszki na **System szyfrowania plików,** a następnie wybrać opcję **Właściwości.** Otworzy się wówczas okno **Właściwości: System szyfrowania plików.**



Rys. 4.8.1. Właściwości systemu szyfrowania plików; widok zakładki „Ogólne”

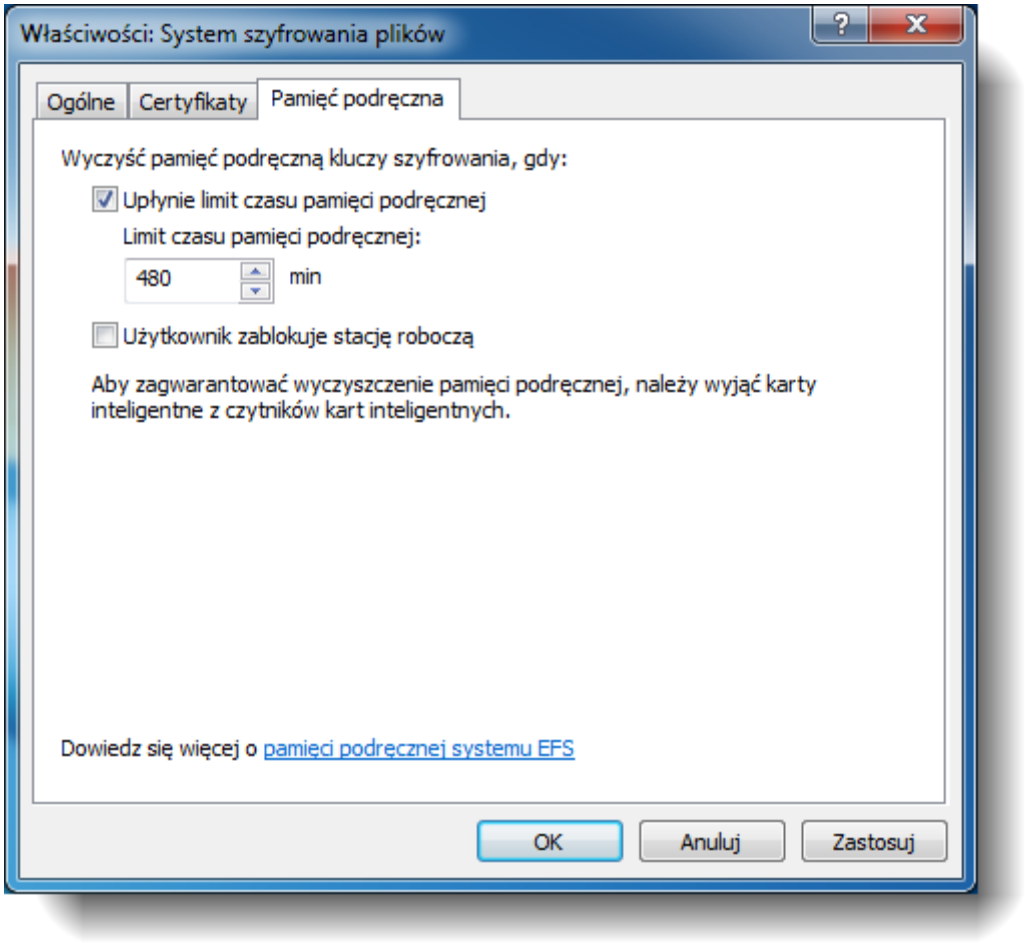
Ustawienie pokazanej na rysunku 4.8.1 opcji „**Kryptografia oparta na krzywej eliptycznej” (ECC)** w tryb: **Zezwalaj** ustawia system szyfrowania plików (EFS) w „tryb mieszany”, który pozwoli komputerom na stosowanie algorytmów RSA lub ECC. W przypadku gdy środowisko wymaga zgodności z wymaganiami zestawu Suite B, przy ustawieniu „**Kryptografia oparta na krzywej eliptycznej” (ECC)**

należy ustawić opcję: **Wymagaj**, a następnie wybrać odpowiedni **rozmiar klucza dla certyfikatów kryptografii opartej na krzywej eliptycznej z podpisem własnym** (rys. 4.8.2).



Rys. 4.8.2. Właściwości systemu szyfrowania plików; widok zakładki „Certyfikaty”

Ważna uwaga: Należy pamiętać, że przedstawione ustawienie zasad grupowych zostanie zastosowane tylko wtedy, kiedy plik lub folder będą zaszyfrowane po włączeniu tej opcji. W przypadku gdy plik lub folder zostały zaszyfrowane zanim przedstawiona opcja została skonfigurowana, użytkownik będzie korzystał z algorytmu, który został wybrany przy szyfrowaniu. Opcja: **Wymagaj** w ustawieniu „**Kryptografia oparta na krzywej eliptycznej” (ECC)** nie wiąże się ze stosowaniem algorytmu AES dla tworzonych kluczy szyfrujących; wymusza jedynie zastosowanie algorytmu ECC.



Rys.4.8.3. Właściwości system szyfrowania plików; widok zakładki „Pamięć podręczna”

Poniższa tabela przedstawia 4 szablony ustawień zasad grup dla funkcji systemu szyfrowania plików EFS.

Szablon oraz ustawienia	**Ścieżka oraz opis**	**Domyślne ustawienie w systemie Windows 7 SP1**
GroupPolicy.admx *Przetwarzanie ustawień dotyczących zasad odtwarzania EFS*	*Konfiguracja komputera\Szablony administracyjne\System\Zasady grupy* *Ustawienia te określają, kiedy zasady dotyczące szyfrowania są aktualizowane.*	*Nie skonfigurowano*
EncryptFilesonMove.admx *Nie wykonuj automatycznie szyfrowania plików przenoszonych do zaszyfrowanych folderów*	*Konfiguracja komputera\Szablony administracyjne\System* *Zapobiega automatycznemu szyfrowaniu pliku po przeniesieniu go do zaszyfrowanego folderu.*	*Nie skonfigurowano*
OfflineFiles.admx *Encrypt the Offline Files cache*	*Computer Configuration\ Administrative Templates\ Network\Offline Files*	*Nie skonfigurowano*

	This setting determines whether offline files are encrypted. *Note On Windows XP SP3, these files are encrypted with the system key whereas on Windows Vista SP1 or later, they are encrypted with the user's key.*	
Search.admx *Allow indexing of encrypted files*	*Computer Configuration\ Administrative Templates\ Windows Components\ Search* *This setting allows encrypted items to be indexed by Windows Search.* *Note There may be data security issues if encrypted files are indexed and the index is not adequately protected by EFS or another means.*	*Nie skonfigurowano*

Tabela 4.8.1. Ustawienia systemu szyfrowania plików EFS

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat danej konfiguracji można znaleźć w zakładce **POMOC** w ustawieniach Edytora obiektów zasad grupy.

4.9. Usługi zarządzania prawami do informacji (RMS)

Usługi zarządzania prawami do informacji (RMS – ang. Rights Management Services) zostały zaprojektowane w celu zapewnienia ochrony i egzekwowania zasad użytkowania zawartości: wrażliwych treści informacji przechowywanych w wiadomościach poczty elektronicznej, dokumentów, zawartości stron internetowych oraz innych rodzajów informacji. RMS zapewnia bezpieczeństwo zawartości dokumentów przez trwały mechanizm szyfrowania informacji i przypisywania praw użytkowania zawartości. Zawartość każdej wiadomości pocztowej oraz pliku, które przesyłane są przez sieć w organizacji lub sieć Internet z zastosowaniem rozwiązania RMS, dostępna jest tylko i wyłącznie dla użytkowników uwierzytelnionych i upoważnionych do tego w wyniku przyznania uprawnień. Każda nieuprawniona osoba pomimo dostępu do pliku nie będzie w stanie odczytać jego treści; informacja jest chroniona poprzez odpowiednie uprawnienia i mechanizm szyfrowania.

RMS składa się trzech głównych komponentów:

- **serwer RMS** – system Windows 7 SP1 wymaga Usługi zarządzania prawami dostępu w systemie Windows dla systemu Windows Server 2003 lub nowszego
- **oprogramowanie klienta RMS** – oprogramowanie to wbudowane jest w system Windows 7 SP1 i nie wymaga dodatkowej instalacji
- **platforma lub aplikacja RMS** – jest to platforma lub aplikacja zaprojektowana w celu obsługi RMS poprzez mechanizm szyfrowania i kontroli dostępu do treści informacji zarządzanych przez ten mechanizm

Uwaga: Mimo że oprogramowanie klienta usług zarządzania prawami (RMS) wbudowane jest w system Windows 7 SP1, wymaga ono zakupu oddzielnej licencji dostępowej RMS CAL, która umożliwi wykorzystanie tego rozwiązania.

Ocena ryzyka

Usługi zarządzania prawami (RMS) pozwalają na zmniejszenie ryzyka w organizacjach, w których nieuprawnione osoby mogą zapoznać się z treścią wrażliwych danych. Informacje wrażliwe mogą zostać rozpowszechnione lub udostępnione osobom nieuprawnionym w wyniku pomyłki lub zaplanowanych działań złośliwych. Poniżej opisano kilka przykładów możliwych scenariuszy ryzyka:

- Nieuprawnieni użytkownicy mogą pozyskać informacje poprzez: podsłuchanie ruchu sieciowego, uzyskanie fizycznego dostępu do przenośnych urządzeń pamięci flash bądź dysków twardych lub w wyniku niewłaściwego zabezpieczenia udziałów sieciowych serwerów lub magazynów danych.
- Uprawnieni użytkownicy mogą wysłać informacje wrażliwe do nieuprawnionych odbiorców wewnątrz lub na zewnątrz organizacji.
- Uprawnieni użytkownicy mogą skopiować lub przenieść dane wrażliwe do nieautoryzowanych lokalizacji lub aplikacji, a także wykonać kopie danych z autoryzowanego miejsca przechowywania danych do nieautoryzowanych pamięci przenośnych flash lub dysków twardych (nośniki zewnętrzne).
- Uprawnieni użytkownicy przypadkowo udzielili dostępu do wrażliwych informacji użytkownikom nieuprawnionym poprzez sieci P2P (peer-to-peer) lub komunikatory internetowe.
- Uprawnieni użytkownicy wydrukowali informacje wrażliwe i nie zabezpieczyli ich w sposób właściwy, przez co narazili organizację na ryzyko pozyskania wydruków przez nieuprawnione osoby, które mogą te informacje skopiować, przefaksować lub przesłać poprzez wiadomości poczty elektronicznej (e-mail).

Minimalizacja ryzyka

W celu skutecznej ochrony danych współdzielonych poprzez zasoby sieciowe – niezależnie od mechanizmu ich wykorzystania – zaleca się zabezpieczenie zawartości informacji przy wykorzystaniu usługi zarządzania prawami do informacji (RMS). Mechanizm RMS doskonale chroni treść informacji, które są przesyłane pomiędzy serwerami, urządzeniami oraz współdzielonymi zasobami sieciowymi. Informacja, która została pozyskana w sposób nieautoryzowany, pozostaje w postaci zabezpieczonej i zaszyfrowanej przez mechanizm RMS.

Zagadnienia dotyczące minimalizacji ryzyka, które wymagają rozważenia

Usługi zarządzania prawami do informacji (RMS) mogą zmniejszyć zagrożenie zdefiniowane w poprzedniej sekcji („Ocena ryzyka”). Jednak przed zastosowaniem i wdrożeniem tego rozwiązania należy wziąć pod uwagę następujące wymagania i najlepsze praktyki:

- RMS wymaga zainstalowanej usługi zarządzania prawami dostępu na serwerze RMS w systemie Windows dla systemu Windows Server 2003 lub nowszego, a także aplikacji obsługujących technologię RMS zainstalowanych na stacjach klienckich użytkowników.
- Microsoft® Office SharePoint® Server lub nowszy wymagany jest w przypadku zastosowania komponentu SharePoint-RMS Integration (mechanizm RMS chroni

przechowywane w witrynach programu SharePoint dokumenty i informacje przed nieupoważnionym dostępem do nich).

- Jeśli planujemy zastosowanie opcjonalnej integracji kart inteligentnych (SMART CARD), należy sprawdzić, czy każda stacja kliencka, która będzie korzystała z chronionej zawartości informacji, jest w pełni kompatybilna ze stosowanymi kartami inteligentnymi.

- W przypadku zastosowania aplikacji internetowych (ang. web based), takich jak Microsoft Outlook® Web Access (OWA) z komponentem RMS, należy pamiętać, iż wymagany jest dodatek do programu Internet Explorer, który umożliwi korzystanie z RMS.

- Zalecane jest przeszkolenie osób działu IT z zakresu wdrażania technologii RMS oraz związanych z nią wsparciem technicznym oraz rozwiązywaniem problemów.

Proces minimalizacji ryzyka

Poniżej przedstawiono proces minimalizacji ryzyka poprzez określenie i wdrożenie najlepszych praktyk konfiguracji usługi zarządzania prawami (RMS). Zapewni on ochronę wrażliwych danych przechowywanych na komputerach klienckich zarządzanych w organizacji.

- przeprowadzenie testów technologii usługi zarządzania prawami (RMS)

Uwaga: W celu uzyskania dodatkowych informacji na temat RMS należy zapoznać się z artykułem: „Active Directory Rights Management Services"[52], dostępnym w witrynie firmy Microsoft.

- oszacowanie potrzeby wdrożenia usługi zarządzania prawami (RMS)
- przeprowadzenie identyfikacji aplikacji i usług wspieranych przez RMS
- określenie scenariuszy wdrożenia usługi zarządzania prawami (RMS), tj:
  - pojedynczy serwer RMS (lub pojedynczy klaster) – Single server (or single cluster)
  - single certification, single license
  - Single certification, multiple license
  - multiple certification, single license
  - multiple certification, multiple license
- dokonanie identyfikacji i oszacowania zakresu chronionych informacji, korzystając z technologii RMS
- dokonanie identyfikacji i oszacowania grup użytkowników, którzy wymagają dostępu do określonych i chronionych informacji
- konfiguracja usługi zarządzania prawami (RMS) w sposób, który zezwala na dostęp do określonych informacji tylko osobom uprawnionym

4.10. Zastosowanie ustawień zasad grup do wdrożenia usługi RMS

Ustawienia zasad grup do konfigurowania usługi zarządzania prawami (RMS) nie są integralnym elementem instalacji systemu Windows 7 SP1. RMS to przede wszystkim rozwiązanie oparte na

[52] w języku polskim – http://technet.microsoft.com/pl-pl/library/cc771234(v=ws.10).aspx ,
w języku angielskim http://go.microsoft.com/fwlink/?LinkId=153465

konfiguracji serwera, w związku z czym konfiguracja usługi zarządzania prawami (RMS) powinna być wykonana na serwerze pełniącym rolę serwera RMS. Ponadto aplikacje współpracujące z usługą zarządzania prawami (RMS) mogą posiadać indywidulane ustawienia, które określają, w jaki sposób zarządzać chronioną zawartością informacji.

4.11. Instalacja i zarządzanie urządzeniami w systemie Windows 7 SP1

Technologia urządzeń Plug and Play (PnP) daje użytkownikom dużą swobodę w użytkowaniu urządzeń, w tym również przenośnych, na ich stacjach roboczych. Z drugiej strony urządzenia takie jak pamięci przenośne USB lub przenośne dyski twarde stwarzają istotne wyzwanie w utrzymaniu właściwego poziomu bezpieczeństwa dla administratorów i pracowników IT. Zagrożenie to wynika nie tylko z trudności w utrzymaniu niekompatybilnego i nieautoryzowanego sprzętu na stacjach klienckich i zarządzaniu nim, ale również ze względu na bezpieczeństwo przetwarzanych danych. W systemie Windows 7 SP1 wprowadzono szereg zmian w zasadach grup, które mają pomóc administratorom IT w zarządzaniu i kontroli każdej próby instalacji nieobsługiwanych i nieautoryzowanych urządzeń. Ważne jest jednak, aby mieć świadomość, iż każde urządzenie zainstalowane w systemie dostępne jest dla każdego użytkownika tego systemu; nie tylko dla konkretnego użytkownika. Systemy Windows 7 SP1 oraz Windows Vista zapewniają wsparcie na poziomie użytkownika w zapewnieniu kontroli dostępu w trybie do odczytu lub zapisu dla urządzenia zainstalowanego w systemie. Można np. zapewnić pełny dostęp do zapisu i odczytu danych na zainstalowanym urządzeniu, takim jak przenośna pamięć USB, dla specyficznego użytkownika, a dla innych użytkowników – tylko dostęp do odczytu danych z tego urządzenia na tym samym komputerze. Więcej informacji na temat zarządzania urządzeniami, ich instalacji oraz sposobu, w jaki ustawienia zasad grupowych mogą pomóc w utrzymaniu i zarządzaniu urządzeń, można znaleźć w artykule: „Step-By-Step Guide to Controlling Device Installation Using Group Policy[53]”.

Ocena ryzyka

Nieautoryzowane dodawanie urządzeń do komputerów lub usuwanie tego sprzętu stanowi bardzo wysokie zagrożenie dla bezpieczeństwa organizacji, ponieważ działania te mogą pozwolić atakującemu na uruchomienie szkodliwego oprogramowania, usunięcie danych oraz zainstalowanie oprogramowania lub innych danych. Urządzenia te stanowią główne źródło wycieku danych. Kilka przykładów zawierających możliwe scenariusze ryzyka przedstawiono poniżej:

- Uprawnieni użytkownicy mogą skopiować lub przenieść dane wrażliwe zawarte na autoryzowanych nośnikach lub urządzeniach do nieautoryzowanych pamięci masowych lub dysków twardych (nośniki zewnętrzne). Czynności te mogą zostać wykonane przez użytkowników w sposób świadomy lub nieświadomy. Sytuacja taka może obejmować kopiowanie danych z zaszyfrowanych nośników danych lub lokalizacji do nieautoryzowanych i nieszyfrowanych, ogólnodostępnych pamięci przenośnych.

- Atakujący może zalogować się do komputerów autoryzowanych użytkowników, a następnie skopiować dane na nośniki pamięci przenośnych.

- Atakujący może wykorzystać nośniki pamięci przenośnych lub udziały sieciowe zawierające oprogramowanie szkodliwe w celu automatycznego uruchomienia skryptu,

[53] http://go.microsoft.com/fwlink/?LinkId=130390

wykorzystując mechanizm autouruchomienia (ang. AutoRun) w celu instalacji oprogramowania złośliwego na nienadzorowanych komputerach klienckich.

- Atakujący może zainstalować nieautoryzowane oprogramowanie lub urządzenie przechwytujące wszystkie wprowadzane dane z klawiatury (ang. Keyloger), które mogą zostać wykorzystane do przechwycenia nazwy konta, hasła lub innych danych wrażliwych w celu przeprowadzenia późniejszego ataku.

Minimalizacja ryzyka

W celu zmniejszenia zagrożenia, zaleca się ochronę systemów komputerowych – ze szczególnym uwzględnieniem kontroli i nadzoru instalacji oraz użytkowania nieautoryzowanych urządzeń podłączanych do komputerów. Do kontroli i nadzoru urządzeń PnP, takich jak pamięci przenośne USB lub przenośne dyski twarde, można wykorzystać ustawienia zasad grup.

Zagadnienia dotyczące minimalizacji ryzyka, które wymagają rozważenia

Zastosowanie ustawień zasad grup dotyczących instalacji urządzeń w systemie Windows 7 SP1 może zmniejszyć zagrożenie zdefiniowane w poprzedniej sekcji („Ocena ryzyka”.) Jednak przed wdrożeniem ustawień dotyczących instalacji i zarządzania urządzeń w komputerach klienckich należy wziąć pod uwagę następujące kwestie:

- Ograniczenie korzystania z urządzeń może zablokować możliwość korzystania z udostępniania danych uprawnionym użytkownikom lub zmniejszyć efektywność użytkowników mobilnych poprzez zablokowanie dostępu do urządzeń przenośnych.

- Ograniczenie korzystania z urządzeń przenośnych może uniemożliwić zastosowanie klucza USB, będącego częścią procesu wdrożenia szyfrowania dysków przy wykorzystaniu technologii BitLocker. Jeśli np. zastosujemy ustawienie zasad grupowych „**Dyski wymienne: Odmowa prawa do zapisu**” – mimo że ustawienie to przeznaczone jest dla użytkowników – to będzie obowiązywało ono również w przypadku użytkownika z prawami administratora. Spowoduje to, że program instalacyjny BitLocker nie będzie mógł zapisać klucza uruchomienia na dysku przenośnym USB.

- Pewna cześć urządzeń identyfikowana jest w systemie podwójnie: jako urządzenie magazynu wymiennego (ang. removable storage ID) oraz jako urządzenie magazynu lokalnego (ang. local storage ID). Takiej identyfikacji dokonują np. niektóre typy dysków przenośnych USB, uruchamianych: podczas startu systemu, w zależności od momentu podłączenia urządzenia, przed startem systemu lub w czasie, kiedy system jest już uruchomiony. Dlatego ważne jest, aby dokładnie przetestować ustawienia zasad grupowych (GPO), aby zapewnić właściwą ochronę dla odpowiednich typów urządzeń i określić, czy wykorzystanie tych urządzeń jest zabronione czy zezwolone w środowisku organizacji.

Proces minimalizacji ryzyka

Poniżej przedstawiono proces minimalizacji ryzyka, pozwalający na wdrożenie najlepszych praktyk dla instalacji urządzeń i zarządzania nimi w systemie Windows 7 SP1. Zapewni to ochronę wrażliwych danych znajdujących się na zarządzanych komputerach:

W celu minimalizacji ryzyka zaleca się zastosowanie następujących czynności:

1. Sprawdzenie i przeprowadzenie testów dotyczących zagadnienia instalacji i zarządzania urządzeniami w systemie Windows 7 SP1.

Uwaga: W celu uzyskania dodatkowych informacji na ten temat, należy zapoznać się z dokumentem: Step-By-Step Guide to Controlling Device Installation Using Group Policy[54], dostępnym na stronach witryny Microsoft.

2. Oszacowanie potrzeby wdrożenia mechanizmu instalacji urządzeń i zarządzania nimi w systemie Windows 7 SP1.

3. Sprawdzenie i przeprowadzenie testów dotyczących ustawień zasad grup dla mechanizmu instalacja i zarządzanie urządzeniami w systemie Windows 7 SP1.

4. Dokonanie identyfikacji niezbędnych urządzeń przenośnych pracujących w środowisku organizacji, i przygotowanie listy ustawień dla tych urządzeń ze szczególnym uwzględnieniem identyfikatorów sprzętu (ang. Hardware ID) oraz identyfikatorów zgodnych(ang. Compatible ID).

5. Dokonanie identyfikacji i wskazanie komputerów oraz użytkowników, którzy wymagają codziennej pracy z urządzeniami przenośnymi.

6. Wdrożenie i zastosowanie ustawień zasad grupowych w celu włączenia możliwości instalacji niezbędnych i odpowiednich klas urządzeń.

7. Wdrożenie i zastosowanie ustawień zasad grupowych w celu włączenia możliwości instalacji na wybranych komputerach, na których jest to niezbędne do codziennej pracy.

4.12. Zastosowanie ustawień zasad grupowych do nadzorowania instalacji urządzeń

W celu nadzorowania instalacji i zarządzania urządzeń rekomendowane jest zastosowanie ustawień zasad grupowych dostępnych w szablonie zasad grupowych **Deviceinstallation.admx**. Tabela poniżej przedstawia zasady grupowe dostępne w tym szablonie**.** Konfiguracja tych ustawień możliwa jest w gałęzi:

Konfiguracja komputera\Szablony administracyjne\System\Instalacja urządzenia\Ograniczenia dotyczące instalacji urządzeń

(Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions)

Ustawienie zasad	***Opis***	***Domyślne ustawienie w systemie Windows 7 SP1***
Zezwalaj administratorom na zastępowanie zasad ograniczających instalację urządzeń	*To ustawienie zasad umożliwia określenie, czy członkowie grupy Administratorzy mogą instalować i aktualizować sterowniki dowolnego urządzenia, bez względu na inne ustawienia zasad.*	Nie skonfigurowano

[54]http://go.microsoft.com/fwlink/?LinkId=130390

Zezwalaj na instalację urządzeń za pomocą sterowników odpowiadających tym klasom konfiguracji urządzeń	*To ustawienie zasad umożliwia określenie, czy członkowie grupy Administratorzy mogą instalować i aktualizować sterowniki dowolnego urządzenia, bez względu na inne ustawienia zasad.*	Nie skonfigurowano
Nie zezwalaj na instalację urządzeń za pomocą sterowników odpowiadających tym klasom konfiguracji urządzeń	*To ustawienie zasad umożliwia określenie listy unikatowych identyfikatorów globalnych (GUID) klasy konfiguracji urządzeń dla sterowników urządzeń, których instalacja w systemie Windows ma być niedozwolona. To ustawienie zasad ma pierwszeństwo przed każdym innym ustawieniem zasad, które zezwala na instalację urządzenia w systemie Windows.*	Nie skonfigurowano
Wyświetl niestandardowy komunikat, jeśli ustawienie zasad uniemożliwia instalację	*To ustawienie zasad umożliwia wyświetlanie niestandardowego komunikatu w dymku powiadomienia w sytuacji, gdy podjęto próbę instalacji urządzenia, a jedno z ustawień zasad uniemożliwia instalację.*	Nie skonfigurowano
Wyświetl niestandardowy tytuł komunikatu, jeśli ustawienie zasad uniemożliwia instalację	*To ustawienie zasad umożliwia wyświetlanie niestandardowego komunikatu w dymku powiadomienia w sytuacji, gdy podjęto próbę instalacji urządzenia i jedno z ustawienień zasad uniemożliwia instalację.*	Nie skonfigurowano
Zezwalaj na instalację urządzeń o identyfikatorach odpowiadających tym identyfikatorom urządzeń	*To ustawienie zasad umożliwia określenie listy identyfikatorów sprzętu typu Plug and Play i zgodnych identyfikatorów urządzeń, których instalacja w systemie Windows ma być dozwolona. Tego ustawienia zasad należy używać tylko wtedy, gdy jest włączone ustawienie zasad „Zapobiegaj instalacji urządzeń nieopisanych w innych ustawieniach zasad". Inne ustawienia zasad, które zapobiegają instalacji urządzeń, mają przed tym ustawieniem pierwszeństwo.*	Nie skonfigurowano
Zapobiegaj instalacji urządzeń o identyfikatorach odpowiadających tym identyfikatorom urządzeń	*To ustawienie zasad umożliwia określenie listy identyfikatorów sprzętu typu Plug and Play oraz zgodnych identyfikatorów urządzeń, których instalacja w systemie Windows ma być niedozwolona. To ustawienie zasad ma*	Nie skonfigurowano

	pierwszeństwo przed każdym innym ustawieniem zasad, które zezwala na instalację urządzenia w systemie Windows.	
Czas (w sekundach), po jakim jest wymuszany ponowny rozruch, jeśli jest on wymagany do zastosowania zmian zasad	*Umożliwia ustawienie czasu (w sekundach), przez jaki system ma czekać zanim dokona ponownego rozruchu, by wymusić zmiany w zasadach ograniczających instalację urządzeń.* *W przypadku włączenia tego ustawienia należy określić czas w sekundach, przez jaki system ma czekać zanim dokona ponownego rozruchu.*	Nie skonfigurowano
Zapobiegaj instalacji urządzeń wymiennych	*Umożliwia ustawienie czasu (w sekundach), przez jaki system ma czekać zanim dokona ponownego rozruchu, by wymusić zmiany w zasadach ograniczających instalację urządzeń.* *W przypadku włączenia tego ustawienia należy określić czas w sekundach, przez jaki system ma czekać zanim dokona ponownego rozruchu.*	Nie skonfigurowano
Zapobiegaj instalacji urządzeń wymiennych	*To ustawienie zasad pozwala zapobiec instalacji urządzeń, które nie są w sposób precyzyjny opisane w żadnym innym ustawieniu zasad.* *Jeśli to ustawienie zostanie włączone, w systemie Windows nie będzie możliwe zainstalowanie ani zaktualizowanie sterownika żadnego urządzenia, które nie jest opisane w ustawieniu zasad: „Zezwalaj na instalację urządzeń o identyfikatorach odpowiadających tym identyfikatorom urządzeń" lub „Zezwalaj na instalację urządzeń tych klas".*	Nie skonfigurowano

Tabela 4.12.1. Ustawienia zasad grupowych do nadzorowania instalacji urządzeń

Powyższa tabela zawiera krótki opis dla każdego ustawienia. Więcej informacji na temat danej konfiguracji można znaleźć w zakładce **POMOC** w ustawieniach Edytora obiektów zasad grupy.

4.13. Zastosowanie ustawień zasad grupowych do kontroli obsługi urządzeń

Aby zapewnić nadzór instalacji urządzeń, system Windows 7 SP1 pozwala dodatkowo na kontrolowanie poziomu dostępu użytkowników do poszczególnych klas urządzeń, które uprzednio zostały zainstalowane. Szablon **RemovableStorage.admx** zawiera ustawienia dla urządzeń magazynu wymiennego. Konfiguracja tych ustawień dostępna jest w gałęzi:

Konfiguracja komputera\Szablony administracyjne\System\Dostęp do magazynu wymiennego

(Computer Configuration\Administrative Templates\System\Removable Storage Access)

Ustawienie zasad	***Opis***	***Domyślne ustawienie w systemie Windows 7 SP1***
Czas (w sekundach) do wymuszenia ponownego uruchomienia	*Należy ustawić czas (w sekundach) oczekiwania na ponowne uruchomienie systemu, aby wymusić zmiany w prawach dostępu do wymiennych urządzeń magazynowania.* *Jeśli to ustawienie zostanie włączone, należy podać czas (w sekundach), przez jaki system ma czekać zanim dokona ponownego uruchomienia.* *Jeśli to ustawienie zostanie wyłączone lub nie zostanie skonfigurowane, system nie będzie wymuszał ponownego uruchomienia.* *UWAGA: Prawa dostępu nie będą obowiązywały do momentu ponownego uruchomienia systemu.*	Nie skonfigurowano
Dysk CD i DVD: odmowa dostępu do wykonywania	*To ustawienie zasad powoduje odmowę dostępu do wykonywania zadań w przypadku klasy magazynów wymiennych CD i DVD.*	Nie skonfigurowano
Dysk CD i DVD: odmowa dostępu do odczytu	*To ustawienie zasad powoduje odmowę dostępu do odczytu danych w przypadku klasy magazynów wymiennych CD i DVD.*	Nie skonfigurowano
Dysk CD i DVD: odmowa prawa do zapisu	*To ustawienie zasad powoduje odmowę prawa do zapisu danych w przypadku klasy magazynów wymiennych CD i DVD.*	Nie skonfigurowano
Klasy niestandardowe: odmowa dostępu do odczytu	*To ustawienie zasad powoduje odmowę dostępu do odczytu danych w przypadku niestandardowych klas magazynów wymiennych.*	Nie skonfigurowano

Klasy niestandardowe: odmowa prawa do zapisu	*To ustawienie zasad powoduje odmowę prawa do zapisu danych w przypadku niestandardowych klas magazynów wymiennych.*	Nie skonfigurowano
Stacje dyskietek: odmowa dostępu do wykonywania	*To ustawienie zasad powoduje odmowę dostępu do wykonywania zadań w przypadku klasy magazynów wymiennych Stacje dyskietek, obejmującej też stacje dyskietek USB.*	Nie skonfigurowano
Stacje dyskietek: odmowa dostępu do odczytu	*To ustawienie zasad powoduje odmowę dostępu do odczytu danych w przypadku klasy magazynu wymiennego Stacje dyskietek, obejmującej też stacje dyskietek USB.*	Nie skonfigurowano
Stacje dyskietek: odmowa dostępu do odczytu	*To ustawienie zasad powoduje odmowę prawa do zapisu danych w przypadku klasy magazynu wymiennego Stacje dyskietek, obejmującej też stacje dyskietek USB.*	Nie skonfigurowano
Dyski wymienne: odmowa dostępu do wykonywania	*To ustawienie zasad powoduje odmowę dostępu do wykonywania zadań w odniesieniu do dysków wymiennych.*	Nie skonfigurowano
Dyski wymienne: odmowa dostępu do odczytu	*To ustawienie zasad powoduje odmowę dostępu do wykonywania zadań w odniesieniu do dysków wymiennych.*	Nie skonfigurowano
Dyski wymienne: odmowa prawa do zapisu	*To ustawienie zasad powoduje odmowę dostępu do zapisu danych na dyskach wymiennych.*	Nie skonfigurowano
Wszystkie klasy magazynów wymiennych: odmowa dostępu	*Konfiguruje dostęp do wszystkich klas magazynów wymiennych.* *To ustawienie zasad ma pierwszeństwo przed wszystkimi ustawieniami zasad dla poszczególnych magazynów wymiennych. Aby zarządzać poszczególnymi klasami, należy użyć ustawień zasad dla każdej klasy.*	Nie skonfigurowano
Wszystkie magazyny wymienne: Zezwalaj na dostęp bezpośredni w sesjach zdalnych	*To ustawienie zasad zapewnia zwykłym użytkownikom bezpośredni dostęp do wymiennych urządzeń pamięci masowej w sesjach zdalnych.*	Nie skonfigurowano
Stacje taśm: odmowa dostępu do wykonywania	*To ustawienie zasad powoduje odmowę dostępu do wykonywania*	Nie skonfigurowano

	zadań w przypadku klasy magazynu wymiennego Stacja taśm.	
Stacje taśm: odmowa dostępu do odczytu	*To ustawienie zasad powoduje odmowę dostępu do odczytu danych w przypadku klasy magazynu wymiennego Stacja taśm.*	Nie skonfigurowano
Stacje taśm: odmowa dostępu do odczytu	*To ustawienie zasad powoduje odmowę prawa do zapisu danych w przypadku klasy magazynu wymiennego Stacja taśm.*	Nie skonfigurowano
Stacje taśm: odmowa dostępu do odczytu	*To ustawienie zasad powoduje odmowę dostępu do odczytu danych z dysków wymiennych, które mogą obejmować: odtwarzacze multimedialne, telefony komórkowe, wyświetlacze pomocnicze i urządzenia z systemem Windows CE.*	Nie skonfigurowano
Urządzenia WPD: odmowa prawa do zapisu	*To ustawienie zasad powoduje odmowę prawa do zapisu danych na dyskach wymiennych, które mogą obejmować: odtwarzacze multimedialne, telefony komórkowe, wyświetlacze pomocnicze i urządzenia z systemem Windows CE.*	Nie skonfigurowano

4.14. Zastosowanie ustawień zasad grup do kontroli i blokowania funkcji autostartu i autoodtwarzania

Szablon **Autoplay.admx** zawiera ustawienia mające wpływ na zachowanie funkcji automatycznego odtwarzania i uruchamiania dla wymiennych urządzeń magazynujących oraz nośników wymiennych w systemie Windows 7 SP1. Konfiguracja tych ustawień dostępna jest w gałęzi:

Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Zasady autoodtwarzania

(Computer Configuration\Administrative Templates\Windows Components\AutoPlay Policies)

Ustawienie zasad	***Opis***	***Domyślne ustawienie w systemie Windows 7 SP1***
Wyłącz funkcję Autoodtwarzanie	*To ustawienie wyłącza funkcję Autoodtwarzanie dla stacji dysków CD/DVD-ROM i dysków wymiennych albo do wszystkich dysków. Wyłączenie funkcji Autoodtwarzanie pomaga zapobiec rozprzestrzenianiu się oprogramowania złośliwego korzystającego ze skryptów autoodtwarzania na dyskach*	Nie skonfigurowano

	wymiennych lub udziałach sieciowych.	
Nie zaznaczaj pola wyboru Zawsze wykonuj tę czynność	*Jeśli ta zasada zostanie włączona, pole wyboru „Zawsze wykonuj tę czynność...", znajdujące się w oknie dialogowym Autoodtwarzanie, będzie domyślnie odznaczone po otwarciu tego okna.*	Nie skonfigurowano
Wyłącz autoodtwarzanie dla urządzeń niezawierających woluminów	*Jeżeli ta zasada zostanie włączona, autoodtwarzanie nie będzie włączone dla urządzeń niezawierających woluminów, takich jak urządzenia MTP. Jeżeli ta zasada zostanie wyłączona lub nie zostanie skonfigurowana, autoodtwarzanie nadal będzie włączone dla urządzeń niezawierających woluminów.*	Nie skonfigurowano
Domyślne zachowanie autouruchamiania	*Określa domyślne działanie poleceń autouruchamiania.* *Jeśli ta zasada zostanie wyłączona lub nie zostanie skonfigurowana, użytkownik systemu Windows Vista będzie otrzymywał monit o wskazanie, czy polecenie autouruchamiania ma być inicjowane, czy nie.*	Nie skonfigurowano

Ustawienia powyższe dostępne są również w gałęzi:

Konfiguracja użytkownika\Szablony Administracyjne\Składniki systemu Windows\Zasady autoodtwarzania

(User Configuration\Administrative Templates\Windows Components\AutoPlay Policies)

Jeśli ustawienia dotyczące nadzorowania instalacji urządzeń powodują konflikt, to ustawienie dla konfiguracji komputera zastąpi ustawienie konfiguracji użytkownika.

4.15. Dodatkowe informacje i wskazówki

Poniżej przedstawiono dodatkowe źródła informacji na temat bezpieczeństwa systemu Windows 7 SP1:

- BCDEdit Commands for Boot Environment[55]
- Best Practices for BitLocker in Windows 7[56]
- Best practices for the Encrypting File System[57]
- BitLocker Drive Encryption Deployment Guide for Windows 7[58]

[55]http://go.microsoft.com/fwlink/?LinkId=113151
[56]http://technet.microsoft.com/en-us/library/dd875532(WS.10).aspx
[57]http://support.microsoft.com/default.aspx?scid=kb;en-us;223316
[58]http://go.microsoft.com/fwlink/?LinkId=140286

- BitLocker Drive Encryption Overview[59]
- Boot Configuration Data in Windows Vista[60]
- First Look: New Security Features in Windows Vista[61] for general information about security features in Windows Vista SP1
- How Setup Selects Drivers[62]
- Microsoft Security Compliance Manager[63]
- Office 2003 Policy Template Files and Deployment Planning Tools[64]
- Step-By-Step Guide to Controlling Device Installation Using Group Policy[65]
- The Encrypting File System[66]
- Trusted Computing Group[67]
- Windows BitLocker Drive Encryption Design and Deployment Guides[68]
- Active Directory Rights Management Services[69]
- Windows Vista Security and Data Protection Improvements[70]: "Data Protection"

[59] http://technet.microsoft.com/en-us/library/cc732774.aspx
[60] http://go.microsoft.com/fwlink/?LinkId=93005
[61] https://www.microsoft.com/technet/technetmag/issues/2006/05/FirstLook/default.aspx
[62] http://msdn.microsoft.com/en-us/library/ff546228.aspx
[63] http://go.microsoft.com/fwlink/?LinkId=113940
[64] http://office.microsoft.com/en-us/assistance/HA011513711033.aspx
[65] http://go.microsoft.com/fwlink/?LinkId=130390
[66] http://www.microsoft.com/technet/security/topics/cryptographyetc/efs.mspx

[67] http://www.trustedcomputinggroup.org/
[68] http://go.microsoft.com/fwlink/?LinkId=134201
[69] http://go.microsoft.com/fwlink/?LinkId=153465
[70] http://technet.microsoft.com/en-us/library/cc507844.aspx

5. Zapewnienie kompatybilności aplikacji w kontekście bezpieczeństwa stacji z Windows 7

Wraz z systemem Windows Vista wprowadzono wiele zmian w zakresie ochrony współpracy na linii aplikacja – jądro systemu. To z kolei spowodowało problemy z kompatybilnością aplikacji. Ponieważ model architektury w kolejnej wersji Windows jest taki sam, konieczne jest skupienie się na weryfikacji oprogramowania, które planujemy wdrożyć w organizacji, pod kątem możliwości pracy w środowisku Windows 7 SP1. Funkcjonalności takie jak Kontrola konta użytkownika UAC (z ang. User Account Control) czy Ochrona zasobów system Windows WRP (z ang. Windows Resource Protection) mogą powodować, że aplikacje zaprojektowane dla starszych systemów nie będą prawidłowo funkcjonowały w Windows 7 SP1.

5.1. Testowanie zgodności aplikacji z systemem Windows 7 SP1

Testowanie zgodności stanowi podstawową czynność, którą należy wykonać przed wdrożeniem oprogramowania w środowisku Windows 7 SP1.

Testowanie zgodności aplikacji z Windows 7 SP1 powinno obejmować następujące kroki:

1. Zalogowanie się na konto z uprawnieniami administracyjnymi.
2. Uruchomienie instalacji oprogramowania.
3. W przypadku błędów instalatora należy go uruchomić w trybie „Uruchom jako administrator”. Jeśli błędy nie są zgłaszane, kolejnym krokiem jest wykonanie czynności opisanej w punkcie 5.
4. Jeśli błędy wciąż występują, we właściwościach instalatora należy ustawić tryb kompatybilności na Windows XP Professional SP3 i powtórzyć czynność z punktu 2. W przypadku dalszych błędów należy wykonać czynność z punktu 7.
5. Zalogowanie się na konto bez uprawnień administracyjnych.
6. Uruchomienie aplikacji. Jeśli wyświetlane są błędy, należy włączyć tryb kompatybilności Windows XP Professional SP3 i ponownie uruchomić aplikację.
7. Jeśli aplikacja uruchomiła się prawidłowo, należy wykonać szereg testów związanych z jej czynnościami obsługowymi. Po zakończeniu tego procesu aplikacja jest gotowa do działania w systemie Windows 7 SP1.
8. Jeśli aplikacja nie zainstalowała się, nie uruchomiła prawidłowo, przestaje odpowiadać lub wyświetla błędy, oznacza to problemy z kompatybilnością. Należy przeprowadzić dodatkową analizę działania oprogramowania.

5.2. Znane problemy zgodności aplikacji w kontekście rozszerzonych mechanizmów ochrony

Istnieje kilka znanych powodów, dla których kompatybilność aplikacji nie jest zachowana. Mogą one wynikać z wbudowanych w Windows 7 SP1 mechanizmów ochrony, które opisane zostały poniżej.

Kontrola konta użytkownika

Funkcja ta, dostępna w Windows Vista i Windows 7 SP1, zapewnia separację standardowych uprawnień użytkownika i zadań od tych, które wymagają dostępu administracyjnego. Dzięki kontroli

konta użytkownika podnoszony jest poziom bezpieczeństwa, co pozwala standardowym użytkownikom wykonywać więcej czynności bez konieczności korzystania z kont posiadających uprawnienia administracyjne. Jedną z cech tego mechanizmu jest również możliwość wirtualizacji na poziomie rejestru i systemu plików. Dzięki temu można zapewnić kompatybilność aplikacji, które zaprojektowane zostały do korzystania z chronionych obecnie obszarów w rejestrze i systemie plików.

Ochrona zasobów systemu Windows

Mechanizm ochrony zasobów systemu Windows, dostępny od systemu Windows Vista, zapewnia ochronę kluczy rejestru i folderów na tych samych zasadach, na jakich zabezpieczane są kluczowe pliki systemowe. Aplikacje, które próbują uzyskać dostęp plików do chronionych przez mechanizm, mogą nieprawidłowo funkcjonować w środowisku Windows 7 SP1. W takim przypadku wymagana jest modyfikacja sposobu działania aplikacji.

Tryb chroniony

Funkcja Internet Explorer 7 ułatwia ochronę pracujących pod kontrolą Windows komputerów przed instalacją złośliwego oprogramowania i innych aplikacji powodujących niestabilność systemu. Jeśli Internet Explorer pracuje w trybie chronionym, przeglądarka współpracuje wyłącznie z określonymi obszarami systemu plików i rejestru. Domyślnie tryb chroniony jest włączony w Internet Explorer 8, kiedy odbywa się próba dostępu do witryn zlokalizowanych w strefie Intranet i/lub strefie witryn zaufanych.

5.3. Zmiany i ulepszenia systemu operacyjnego Windows 7 SP1

W Windows 7 SP1 wprowadzone zostały zmiany, które mogą powodować brak kompatybilności aplikacji firm trzecich. Należą do nich:

- Nowy interfejs programowania aplikacji API (z ang. Application Programming Interface). Dostępny od Windows Vista interfejs programowania aplikacji w odmienny sposób zapewnia komunikację między programami. Przykładami są tutaj oprogramowanie antywirusowe oraz zapora ogniowa, które opierając się na nowym API, zapewniają lepszą ochronę, ale wymuszają jednocześnie uwzględnienie ich istnienia dla działających w Windows 7 SP1 aplikacji.
- 64-bitowa wersja Windows

Aplikacje 16-bitowe oraz sterowniki 32-bitowe nie są wspierane w środowisku 64-bitowym Windows 7 SP1. Automatyczne przekierowanie rejestru i plików systemowych jest dostępne wyłącznie dla aplikacji 32-bitowych. Z tego powodu aplikacje 64-bitowe muszą być napisane w pełnej zgodzie ze standardami aplikacji Windows Vista oraz Windows 7 SP1.

- Wersje systemu operacyjnego

Zdarza się, że starsze aplikacje sprawdzają wersje Windows. W przypadku wykrycia innej wersji niż ta, której są dedykowane, ich działanie jest zatrzymywane. Jednym z dostępnych rozwiązań tej sytuacji jest uruchomienie aplikacji w trybie kompatybilności z wcześniejszymi systemami.

5.4. Omówienie stosowanych narzędzi w celu zapewnienia zgodności aplikacji z systemem Windows 7 SP1

W ramach Windows 7 SP1 dostępnych jest wiele narzędzi, które służą do zapewnienia kompatybilności aplikacji.

Asystent zgodności programów

Funkcja Asystent zgodności programów stworzona została w celu umożliwienia uruchamiania aplikacji zaprojektowanych dla wcześniejszych wersji Windows. W sytuacji, kiedy Windows 7 SP1 wykryje aplikację, która wymaga trybu kompatybilności dla Windows 2000, Windows XP Professional SP3 bądź innych systemów, Windows 7 SP1 automatycznie ustawia odpowiedni tryb działania aplikacji. Asystent zgodności programów uruchamia się automatycznie.

Kreator kompatybilności programów

Funkcja ta w ramach dostępnego kreatora umożliwia określenie problemów związanych z kompatybilnością wybranej aplikacji i wykrycie ich przyczyn – z jednoczesnym zaproponowaniem rozwiązania. Uruchomienie kreatora kompatybilności programów jest możliwe z poziomu **Panelu sterowania,** w sekcji **Programy** po kliknięciu opcji **Uruchom programy napisane dla starszych wersji systemu Windows**.

Application Compatibility Toolkit (ACT)

Pakiet ACT jest zbiorem narzędzi oraz dokumentacji umożliwiających zarządzanie aplikacjami w organizacji pod kątem zapewnienia ich kompatybilności w środowisku Windows 7 SP1. ACT umożliwia inwentaryzację oprogramowania, zarządzanie aplikacjami krytycznymi oraz wskazanie rozwiązań, które zapewnią prawidłowe wdrożenie Windows 7 SP1. Pakiet jest dostępny bezpłatnie na stronach Microsoft.

Tryb Windows XP Mode

Tryb Windows XP Mode jest funkcją zapewniającą uruchamianie aplikacji wewnątrz maszyny wirtualnej Windows XP, bezpośrednio z Windows 7 SP1. Aplikacja jest udostępniana tak, jak każda inna w systemie, ale dzięki przeniesieniu jej działania na platformę wirtualną Windows XP zapewniana jest pełna kompatybilność działania. Tryb Windows XP Mode dostępny jest w edycjach Windows 7 SP1 Professional, Ultimate oraz Enterprise i wymaga oddzielnej instalacji pakietów, które pobiera się ze stron firmy Microsoft. Tryb Windows XP Mode domyślnie skonfigurowany jest do pracy z funkcją translacji adresów sieciowych NAT (z ang. Network Address Translation), co zapewnia działanie w sieci, do której dołączony jest Windows 7 SP1, stanowiący podstawę dla działania pakietu.

5. Ład korporacyjny, zarządzanie ryzykiem oraz zgodność ze standardami w IT (IT GRC)

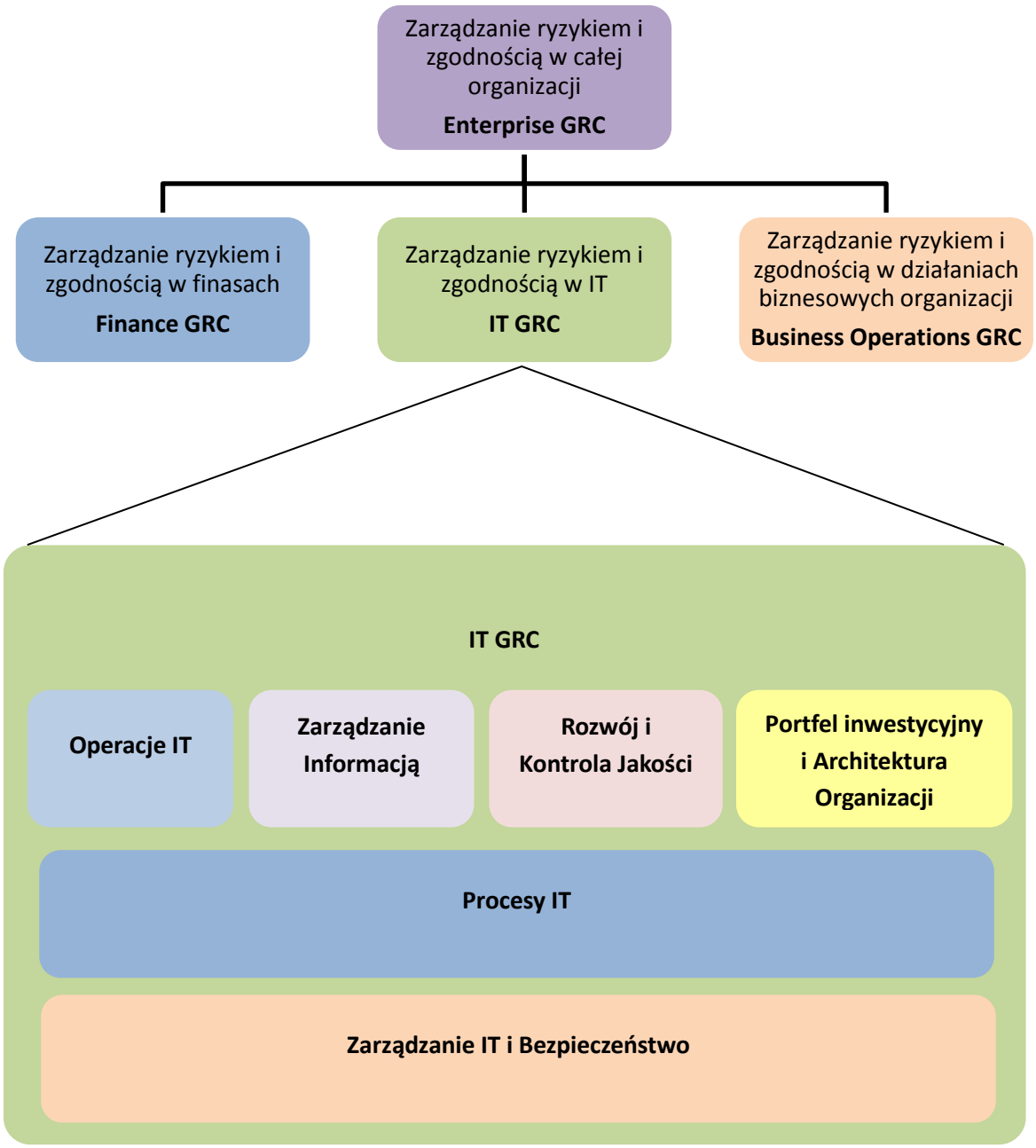
System ładu korporacyjnego, zarządzania ryzykiem i zgodności ze standardami – GRC (ang. Governance, Risk, and Compliance) – to system, na który składają się ludzie, procesy i technologie w ramach całej infrastruktury. Przynosi on danej organizacji następujące korzyści:

- ograniczenie ryzyka
- ujednolicenie procesów biznesowych
- poprawę efektywności
- uwolnienie zasobów
- usprawnienie zarządzania zmianami

W poniższym rozdziale przedstawione zostały przykłady zastosowania produktów Microsoft w kontekście bazowych ustawień systemu przy wykorzystaniu IT Governance, Risk, and Compliance (IT GRC) Process Management Pack (PMP) dla systemu Microsoft System Center Service Manager 2012 – w taki sposób, aby utrzymanie ładu korporacyjnego, zarządzania ryzykiem i zgodności ze standardami w IT przyniosło organizacji korzyści. Process Management Pack jest pakietem administracyjnym dla produktu System Center Service Manager, który wspomaga proces zarządzania IT, bazując na regulacjach, międzynarodowych standardach oraz najlepszych praktykach, takich jak: Microsoft Operations Framework (MOF) oraz Information Technology Infrastructure Library (ITIL). IT GRC Process Management Pack wraz z ustawieniami bazowymi systemu pomaga zapewnić automatyczny proces zgodności komputerom klienckim oraz serwerom. Aby uzyskać dodatkowe informacje na temat rozwiązań Microsoft wspierających system GRC, należy zapoznać się z przewodnikami Compliance Solution Accelerators[71], opisanymi na stronach przewodników Microsoft Solution Accelerators.

Poniższy rysunek przedstawia umiejscowienie IT GRC w strukturze zarządzania ryzykiem i zgodnością całej organizacji. IT GRC Process Management Pack skupia się wyłącznie na systemie IT GRC bez uwzględniania innych aspektów zarządzania ryzykiem i zgodnością całej organizacji.

[71] http://go.microsoft.com/fwlink/?LinkId=199861



Rys. 6.1. Umiejscowienie IT GRC w strukturze zarządzania ryzykiem i zgodnością całej organizacji

6.1. Wprowadzenie

W rozdziale tym zostały przedstawione procesy oraz wskazane dodatkowe zasoby opisujące wykorzystanie IT GRC Process Management Pack dla produktu System Center Service Manager. W celu uzyskania dodatkowych informacji należy zapoznać się z przewodnikami:

- IT GRC Process Management Pack Deployment Guide – przewodnik ten opisuje proces wdrożenia IT GRC Process Management Pack
- IT GRC Process Management Pack Operations Guide – przewodnik ten zawiera informacje na temat wykorzystania IT GRC Process Management Pack oraz budowania własnych pakietów

- IT GRC Process Management Pack Developers Guide – przewodnik ten opisuje proces dostosowania IT GRC Process Management Pack do własnych potrzeb

Wymienione przewodniki można pobrać ze strony IT GRC Process Management Pack SP1 for System Center Service Manager[72]; dostępne są w dziale Centrum Pobierania Microsoft. W celu uzyskania dodatkowych informacji należy zapoznać się z dodatkowymi zasobami:

- IT Compliance Management Library Deployment Guide, który zawarty jest w każdej bibliotece obejmującej zarządzanie zgodnością ze standardami IT. Przewodnik ten zawiera informacje na temat wdrożenia IT GRC Process Management Pack oraz pakietów konfiguracyjnych Microsoft System Center Configuration Manager
- Microsoft System Center Service Manager[73]
- Microsoft System Center Configuration Manager[74]

6.2. Omówienie i budowa IT GRC PMP

IT GRC Process Management Pack dostarcza informacji na temat możliwości i sposobu zarządzania procesem IT GRC w obrębie całej organizacji oraz określa możliwości automatyzacji tego procesu. IT GRC Process Management Pack umożliwia importowanie gotowych bibliotek zgodności ze standardami, które mogą być zastosowane w celu określenia punktów kontrolnych niezbędnych dla wymagań stawianych systemowi IT GRC w organizacjach.

Biblioteki zgodności przeznaczone dla IT GRC Process Management Pack określają punkty kontrolne wykorzystywane do zapewnienia zgodności z dokumentami organów nadrzędnych IT GRC, powołując się na wytyczne określone przez międzynarodowe, rządowe oraz branżowe instytucje opracowujące ogólne wytyczne IT GRC. Dokumenty te zawierają wytyczne oraz określają wymagania szczegółowe dotyczące procesów biznesowych oraz technologii różnych sektorów organizacji i instytucji.

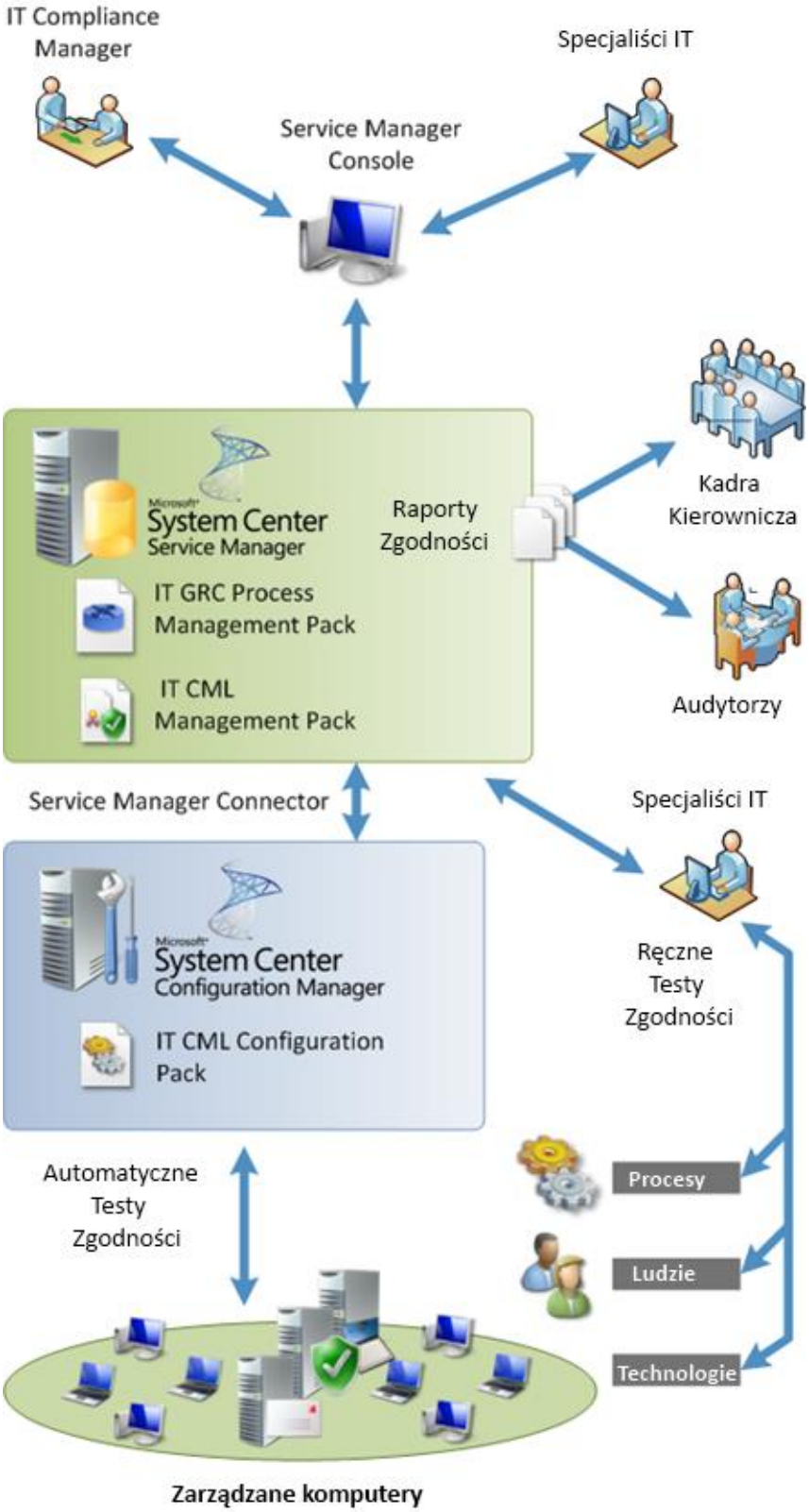
Dodatkowe pakiety administracyjne i informacje dla produktów System Center dostępne są w Microsoft System Center Marketplace[75]; oferują one zintegrowane rozwiązania i automatyzację, pomagając organizacjom w sprawnym spełnieniu wymagań GRC.

Korzyści wynikające ze stosowania integracji produktów System Center Service Manager, System Center Configuration Manager oraz System Center Operations Manager:

- efektywny sposób na monitorowanie, sprawdzanie oraz raportowanie stanu zgodności wdrożonych produktów Microsoft
- jednoczesne stosowanie wymienionych rozwiązań wspomaga zrozumienie i połączenie złożonych celów biznesowych, którym musi sprostać infrastruktura organizacji

[72] http://go.microsoft.com/fwlink/?LinkId=201578
[73] http://go.microsoft.com/fwlink/?LinkId=155958
[74] http://go.microsoft.com/fwlink/?LinkId=206193
[75] http://go.microsoft.com/fwlink/?LinkId=82105

Przedstawiony poniżej rysunek ilustruje rozwiązanie IT GRC Process Management Pack:



Rys.6.2.1. Ilustracja rozwiązania IT GRC Process Management Pack

Kadra kierownicza oraz audytorzy wykorzystują raporty IT GRC Process Management Pack w celu oceny procesów IT GRC organizacji i analizy ich zgodności. Ta grupa użytkowników przeważnie wymaga dostępu tylko do odczytu oraz możliwości wykonania raportów dotyczących informacji zarządzanych przez proces GRC Process Management Pack.

W przedstawionym rozwiązaniu IT compliance managerowie oraz specjaliści IT sterują scentralizowanym procesem zapewnienia zgodności IT GRC, korzystając z narzędzia Service Manager Console. Narzędzie to zapewnia osobie pełniącej rolę IT compliance managera możliwość zarządzania wieloma programami IT GRC oraz postawionymi celami kontrolnymi, które odnoszą się do wytycznych oraz wymagań szczegółowych przedstawionych w dokumentach wydanych przez organy nadrzędne.

Specjaliści IT, korzystając z centralnego narzędzia, mogą dokonać oszacowania wyników zgodności IT GRC dla wszystkich celów kontrolnych określonych w systemie IT GRC. Wyniki przeprowadzonych testów zgodności mogą być osiągnięte na kilka sposobów:

- **automatycznie –** funkcjonalność zarządzania docelową konfiguracją (ang. Desired Configuration Management (DCM)), zawarta w System Center Configuration Manager oraz IT CML Configuration Packs, pomaga osiągnąć rezultaty zgodności dla zautomatyzowanych celów kontrolnych. Automatyczne cele kontrolne w znacznym stopniu redukują nakład pracy wymagany do osiągnięcia zgodności IT GRC,

- **ręcznie** – specjaliści IT mogą samodzielnie ocenić wyniki zgodności:

- **technologia –** wyniki zawierają ustawienia zgodności IT GRC, które nie mogą być oszacowanie metodami automatycznymi

- **procesy –** raport uwzględnia procesy zgodności stosowane w organizacji i powiązane z IT GRC, takie jak właściwe i bezpieczne usuwanie danych z systemów wycofywanych z organizacji, a zawierających informacje wrażliwe,

- **ludzie –** raport zawiera aspekty ergonomii pracy w zakresie zgodności z IT GRC, takie jak dokładne sprawdzenie pracownika przed udzieleniem dostępu do informacji wrażliwych.

Zastosowanie integracji opartej na produktach System Center Service Manager oraz System Center Configuration Manager zapewnia następujące funkcjonalności i korzyści:

- System Center Configuration Manager analizuje oczekiwaną, docelową konfigurację z aktualną konfiguracją zarządzanych zasobów, wykorzystując pakiety DCM, umieszczone na poziomie konfiguracji elementu, aby zapewnić obsługę celów kontrolnych.

- Element konfiguracji znajdujący się w Service Manager CMDB (baza danych zarządzania konfiguracją) może być automatycznie wypełniony informacjami dostarczonymi przez System Center Configuration Manager.

- Przeprowadzone testy zgodności dla zautomatyzowanych celów kontrolnych mogą być aktualizowane w Service Manager CMDB.

Produkt System Center Service Manager umożliwia tworzenie i wykorzystanie własnych łączników (ang. connector), za pomocą których można zdefiniować połączenia z innymi systemami. Umożliwia to

zebranie informacji na temat zgodności z innymi systemami stosowanymi w organizacji. Funkcjonalność ta rozszerza proces automatyzacji testów i zbierania wyników z wcześniej zdefiniowanych celów kontrolnych.

6.3. Korzyści wynikające ze stosowania IT GRC PMP

Rozwiązanie zarządzania procesem zgodności oraz zarządzania ryzykiem oferowane przez IT GRC Process Management Pack, IT Compliance Management Libraries, System Center Service Manager, oraz System Center Configuration Manager oferuje następujące możliwości i korzyści:

- **Mapowanie celów biznesowych bezpośrednio na cele i działania IT GRC –** mechanizm ten w łatwy sposób odwzorowuje cele biznesowe określone przez kadrę zarządzającą w postaci celów i działań dla programu zgodności działu IT. Rozwiązanie to:

- zawiera bibliotekę tysięcy dokumentów zgodności pochodzących z setek dokumentów urzędowych, które zostały dostosowane w ujednolicony zestaw celów kontrolnych,

- tworzy bibliotekę zgodności, zawierającą cele kontrolne, działania i ustawienia dla kluczowych produktów Microsoft oraz nowych systemów Windows 7 SP1 i Windows Server 2008, przedstawione w postaci zbioru zaktualizowanych ustawień bazowych dla konfiguracji.

- **Zauważalne zwiększenie zgodności ze standardami –** użytkownicy w łatwy sposób mogą zidentyfikować niezgodności, korzystając z raportów IT GRC Process Management Pack.

- **Utworzenie pojedynczego punktu sterowania zarządzaniem programów IT GRC –** organizacje mogą zarządzać wieloma programami zgodności IT GRC, spełniając jednocześnie wymagania wielu złożonych dokumentów urzędowych. IT GRC Process Management Pack wprowadza kontrolę obejmującą wszystkie źródła dokumentów urzędowych, redukując problemy małej wydajności w przypadku regulacji wzajemnie się pokrywających.

- **Wykorzystanie najlepszych branżowych praktyk do zarządzania procesami** – procesy zaimplementowane w IT GRC PMP zostały utworzone w oparciu o najlepsze praktyki wykorzystywane do zarządzania incydentami i zarządzania zmianami, bazując na MOG oraz ITIL.

- **Redukcja nakładu pracy** – proces automatyzacji testów, uwzględniający integrację funkcjonalności DCM w System Center Configuration Manager, redukuje ręczny nakład pracy, który jest wymagany do przeprowadzanie testów sprawdzających zgodność ze standardami.

- **Obniżenie kosztów kontroli i raportowania** – redukcja nakładu pracy poświęconego na przygotowanie i wykonywania czynności kontrolujących stan zgodności ze standardami wpływa na obniżenie kosztów związanych z przygotowaniem audytów.

- **Minimalizacja ryzyka** – użytkownicy mogą w łatwy sposób zidentyfikować niezgodności, a co za tym idzie – na bieżąco kontrolować występujące ryzyko. Prowadzi to do zmniejszenia ryzyka związanego z zapewnieniem zgodności.

- **Ułatwienie zmian zachodzących w biznesie** – biznes wymaga ciągłych zmian, w związku z tym opisywane rozwiązanie zarządzania zgodnością wykrywa zachodzące zmiany w zarządzanej infrastrukturze i stosuje odpowiednie mechanizmy kontroli zgodności.

- **Przygotowanie do audytów zewnętrznych –** przygotowane predefiniowane raporty IT Compliance Management Pack odzwierciedlają większość informacji na temat zgodności ze standardami wymaganych przez audytorów. Wykorzystując te raporty, organizacje mogą – na prośbę audytorów, konsultantów lub zarządu organizacji – w szybki i łatwy sposób przedstawić stan zgodności ze standardami.

- **Podejmowanie czynności korygujących w celu wyeliminowania niezgodności – o**soby pełniące funkcje IT GRC managerów mogą zidentyfikować niezgodne ze standardami ustawienia konfiguracji i korzystając z procesu zarządzania incydentami, w łatwy sposób zlecić specjalistom IT zadanie przywrócenia ustawień konfiguracji do stanu zapewniającego zgodność ze standardami.

6.4. Terminy i definicje

W poniższej tabeli przedstawiono podstawowe terminy i pojęcia związane z wykorzystaniem IT GRC Process Management Pack.

Termin lub pojęcie	***Opis***
Regulacje dotyczące ładu korporacyjnego, zarządzania ryzykiem oraz zgodności ze standardami (GRC) (ang. GRC authority document)	Dokumenty obejmujące regulacje w zakresie GRC zawierają wymagania opublikowane przez organy urzędowe w postaci rozporządzeń lub wytycznych, opisanych standardów lub polityki organizacji. Regulacje GRC mogą obejmować wymagania dotyczące procesów minimalizacji ryzyka, które określają specyficzne bądź ogólne opisy konfiguracji i użytkowania lub inne parametry obsługi, które dotyczą organizacji, personelu, procesów biznesowych oraz technologii. Różnorodne regulacje zwracają uwagę na te same aspekty ryzyka zgodności; pomimo to, dokumenty te pozwalają na spojrzenie z różnych perspektyw na kwestie strategii minimalizacji ryzyka oraz stawianych wymagań. Wymagania wskazane przez regulacje GRC przekształcone na cele kontrolne i odnoszą się do czynności kontrolnych zaprojektowanych w celu zapewnienia, iż towarzyszące ryzyka są minimalizowane w odpowiedni i uzasadniony sposób. IT GRC Process Management Pack zawiera cele kontrolne, przytoczone z odpowiednich regulacji i spełniające stawiane im wymagania. Regulacje obejmują swoim zakresem ustawy dotyczące finansów, polityki prywatności oraz ochrony zdrowia, takie jak: Sarbanes–Oxley (SOX), European Union Data Protection Directive (EUDPD) oraz Health Insurance Portability and Accountability Act

	(HIPAA). Pełna lista regulacji, zawarta w produkcie IT GRC Process Management Pack, znajduje się w sekcji **Library,** w konsoli Service Manager – Library **| Authority Documents** .
Program	Definiuje zbiór ryzyk, celów kontrolnych, działań oraz wyników zgodności. Programy definiują również role użytkownika i towarzyszące mu prawa w określonym zakresie poprzez zdefiniowanie odpowiednich uprawień. Zdefiniowane zakresy zezwalają osobie pełniącej rolę menedżera programu na zarządzanie ryzykiem i kontrolę w obrębie tego programu. Programy zostały utworzone w celu określenia zgodności z jednym lub wieloma dokumentami regulacji oraz ryzyk towarzyszących strategii zarządzania IT GRC.
Cele kontrolne (ang. Control objectives)	Sprecyzowane określenie wymagań i wytycznych zawartych w regulacjach GRC. Cele kontrolne mogą być wymagane przez jeden lub wiele zbiorów regulacji w celu wykonania jednej lub wielu czynności kontrolnych.
Powoływanie się na dokumenty organów w zakresie regulacji (ang. Authority document citation)	Odniesienie w obrębie celów kontrolnych do jednego lub wielu szczegółowych wymagań dotyczących obowiązujących przepisów i regulacji.
Czynności kontrolne (ang. Control Activities)	Szczegółowe, podlegające zaskarżeniu stopnie konfigurowania i obsługi produktu poprzez określenie zgodności z wymaganiami celów kontrolnych. Działania kontrolne mogą obejmować jeden lub wiele celów kontrolnych.
Ryzyko (ang. Risk)	Możliwość wystąpienia szansy lub zagrożenia, mających wpływ na osiągnięcie wyznaczonych celów biznesowych lub celów IT danej organizacji. Ryzyko jest mierzone z wykorzystaniem określeń: wpływ lub prawdopodobieństwo. Pojęcie ryzyka związane jest z celami kontrolnymi, czynnościami kontrolnymi lub innymi ryzykami.
Próg (ang. Threshold)	Minimalny udział procentowy obowiązujący dla zarządzanych jednostek w zakresie programu, który musi być zgodny dla czynności kontrolnych, aby został uznany za zgodny.
Zatwierdzanie przepływu pracy (ang. Approval workflow)	Proces, w którym wszystkie zmiany zachodzące dla jednostek zarządzanych przez IT GRC PMP są zatwierdzone. Zazwyczaj zmiany wykonuje ten sam proces zatwierdzania, jak w przypadku żądania

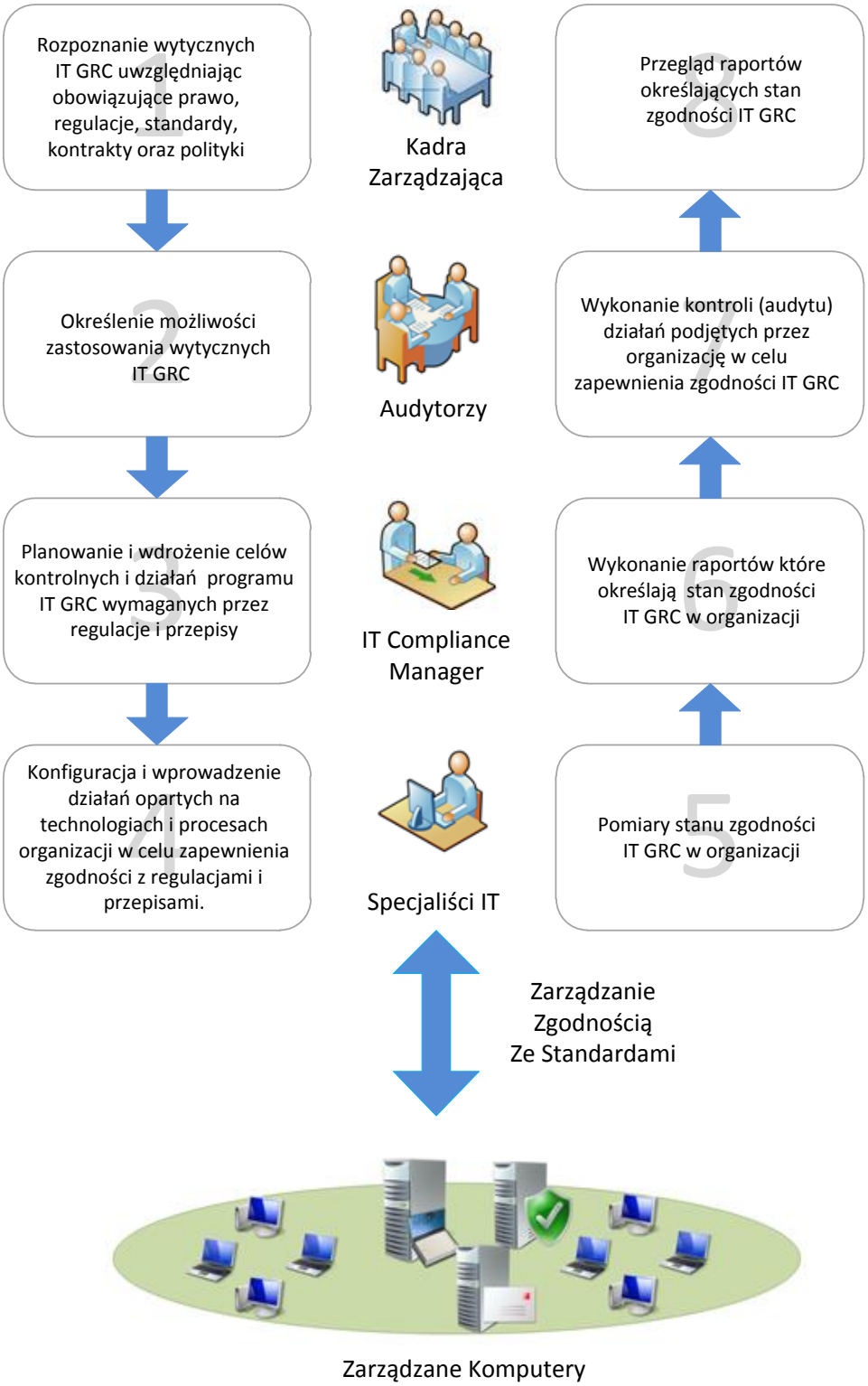
	zmiany przez System Center Service Manager.
Automatyzacja (ang. Automation)	Zastosowanie komponentów IT w celu wykonania zadań lub kroków wymaganych do rozwiązania jednego lub wielu celów kontrolnych, które zawierają automatycznie zgromadzone wyniki zgodności IT GRC.
Rezultaty testów kontroli (ang. Managed entity result)	Rezultaty testów zgodności, które zostały wykonane na zarządzanej jednostce, takiej jak pojedynczy komputer.

Tabela 6.4.1. Terminy i definicje związane z IT GRC

6.5. Cykl życia procesu zgodności w oparciu o IT GRC PMP

Narzędzia IT GRC Process Management Pack, System Center Service Manager oraz System Center Configuration Manager dostarczają zamknięty i pełny cykl zarządzania dla procesu zgodności IT. Cykl życia zgodności integruje procesy oraz wiedzę poprzez mechanizm mapowania szczegółowych wymagań w obrębie obowiązujących przepisów i regulacji na konfigurację i działania dla określonych produktów, a następnie śledzenie zachodzących tam zmian poprzez dokonywanie raportów kontrolnych.

Poniższy rysunek ilustruje główne zadania i obowiązki osób zaangażowanych w cykl życia zgodności IT w obrębie każdego kroku procesu.



Rys. 6.5.1. Główne zadania i obowiązki osób zaangażowanych w cykl życia procesu zgodności IT

Należy zwrócić uwagę, że przepływ cyklu życia zgodności IT zaprezentowany na rysunku 2.5.1 jest ściśle określony na wysokim szczeblu kadry zarządzającej oraz wskazuje precyzyjny przepływ procesów pomiędzy rolami, ale został celowo uproszczony. Każdy osoba wykonująca swoją pracę musi komunikować się z innymi na temat następujących cech wymagań stawianych przez IT GRC:

Zastosowanie – cecha ta zawiera proces rozpoznania wymagań w obrębie obowiązujących przepisów i regulacji, które są znaczące i pełnią istotną rolę dla organizacji. Na przykład Payment Card Industry Data Security Standard (PCI DSS) będzie dotyczyło organizacji prowadzących działalność biznesową z użytkownikami kart kredytowych przetwarzających ich dane zawarte na kartach kredytowych w ramach utrzymywanej infrastruktury IT.

Wystarczalność – cecha ta zawiera proces rozpoznania wymagań w obrębie obowiązujących regulacji i rozpoznanie, czy przedstawione regulacje są wystarczające i pozwolą na zapewnienie zgodności. Na przykład: ustawienie minimalnej długości hasła na wartość 8-znakową dla wszystkich użytkowników jest elementem wystarczającym dla wszystkich obowiązujących i stosowanych regulacji.

Zasadność – cecha ta zawiera proces rozpoznania wymagań w obrębie obowiązujących regulacji i określenia, czy przedstawione regulacje są rozsądne, racjonalne i praktyczne. Na przykład decyzja o wymaganiu minimalnej długości hasła o wartości 16 znaków może być technicznie wykonalna, ale niepraktyczna we wdrożeniu z uwagi na fakt, iż użytkownicy mogą nie zapamiętać swoich haseł.

Dodatkowe informacje na temat stosowania IT GRC w kontekście cyklu życia usług IT oraz innych ról użytkowników działu IT dostępne są w dokumencie: Governance, Risk, and Compliance Service Management Function[76] w kontekście MOF 4.0.

6.6. Dodatkowe informacje i wskazówki

Poniżej przedstawiono dodatkowe źródła informacji na temat bezpieczeństwa systemu Windows 7 SP1, opublikowanych na stronach Microsoft.com:

- Compliance Solution Accelerators[77]
- Governance, Risk, and Compliance Service Management Function[78] w oparciu o MOF 4.0
- IT GRC Process Management Pack SP1 for System Center Service Manager[79]
- Microsoft System Center Marketplac.[80]
- System Center Configuration Manager[81]
- System Center Service Manager[82]
- System Center Service Manager team blog[83]

[76] http://go.microsoft.com/fwlink/?LinkId=115630
[77] http://go.microsoft.com/fwlink/?LinkId=199861
[78] http://go.microsoft.com/fwlink/?LinkId=115630
[79] http://go.microsoft.com/fwlink/?LinkId=201578
[80] http://go.microsoft.com/fwlink/?LinkId=82105
[81] http://go.microsoft.com/fwlink/?LinkId=206193
[82] http://go.microsoft.com/fwlink/?LinkId=155958
[83] http://blogs.technet.com/servicemanager/

7. Narzędzie Security Compliance Manager (SCM) w praktyce

Rozdział dostępny jest w formie Załącznika do niniejszego opracowania.