Microsoft Business Solutions

Navision Security Hardening Guide

Data publikacji: październik 2004 r.

Microsoft

Spis treści

Wprowadzenie

W systemie Microsoft® Windows® są dostępne zaawansowane zabezpieczenia sieciowe zgodne z powszechnymi standardami. W najszerszym znaczeniu zabezpieczenia obejmują planowanie i uwzględnianie kompromisów. Komputer można na przykład zamknąć z sejfie i udostępnić tylko jednemu administratorowi systemu. Będzie on wówczas bezpieczny, ale niezbyt przydatny z powodu braku możliwości połączenia z innym komputerem. Musisz rozważyć, w jaki sposób maksymalnie zabezpieczyć sieć z minimalnym wpływem na funkcjonalność.

Większość organizacji zabezpiecza się przed atakami z zewnątrz, stawiając zapory, ale wiele firm nie zastanawia się nad sposobem zmniejszenia szkód powstałych po sforsowaniu zapory przez użytkownika o złych zamiarach. Środki bezpieczeństwa w środowisku klienta będą skuteczne, gdy bezpieczne prowadzenie działalności nie będzie wymagało od użytkowników wykonywania zbyt wielu procedur i kroków. Implementowanie zasad bezpieczeństwa powinno być jak najłatwiejsze, w przeciwnym razie użytkownicy będą dążyli do znalezienia mniej bezpiecznych metod realizacji zadań.

Ponieważ wielkość instalacji systemu Navision może się znacznie różnić, ważne jest, aby dokładnie przemyśleć potrzeby poszczególnych klientów i rozważyć stosunek skuteczności zabezpieczeń do kosztów ich wprowadzenia. Będąc zaufanym doradcą klienta, należy jak najlepiej ocenić sytuację i zalecić klientowi wprowadzenie zasad, które zaspokoją jego potrzeby w zakresie zabezpieczeń i nie będą stanowić zbyt wielkiego obciążenia.

Najważniejsze wskazówki dotyczące zabezpieczeń systemu Navision

Opisane poniżej ogólne reguły mogą ułatwić zwiększenie bezpieczeństwa w środowisku systemu Navision:

- Aby uruchomić serwer bazy danych systemu Navision jako usługę lub podczas uruchamiania serwera użyć parametru wiersza polecenia *installasservice*, należy upewnić się, że usługa jest uruchamiana na odpowiednim koncie usługi sieciowej (Zarządzanie NT\Usługa sieciowa). Konto Zarządzanie NT\Usługa sieciowa istnieje tylko w systemach Windows™ XP i Windows Server™ 2003. W przypadku systemu Windows 2000 Server należy utworzyć dla tej usługi konto o najmniejszych uprawnieniach, w przeciwnym przypadku usługa zostanie przypisana do konta systemu lokalnego. W najgorszym razie to konto powinno mieć takie same uprawnienia jak zwykłe konto Użytkownicy lub powinno być kontem domeny, które nie będzie kontem administratora ani w domenie, ani na którymkolwiek komputerze lokalnym.

  Należy pamiętać o tym, aby dla konta Zarządzanie NT\Usługa sieciowa lub konta użytkownika, na którym został uruchomiony serwer, przyznać dostęp do plików bazy danych z możliwością odczytu i zapisu, co pozwoli użytkownikom na łączenie się z bazą danych.

  Aby przyznać kontu Zarządzanie NT\Usługa sieciowa dostęp do pliku bazy danych z możliwością odczytu i zapisu w systemie Windows XP:

  1. W Eksploratorze Windows przejdź do folderu zawierającego plik bazy danych.
  2. Zaznacz plik bazy danych, kliknij go prawym przyciskiem myszy, a następnie kliknij polecenie Właściwości.
  3. W oknie ***Właściwości*** kliknij kartę ***Zabezpieczenia*** i w obszarze **Nazwy grupy lub użytkownika** kliknij przycisk Dodaj.
  4. W oknie ***Wybieranie: Użytkownicy, Komputery lub Grupy*** wpisz *Usługa sieciowa* i kliknij przycisk OK.
  5. W oknie ***Właściwości***, w polu **Nazwy grupy lub użytkownika** zostanie dodana pozycja USŁUGA SIECIOWA.
  6. Zaznacz pozycję USŁUGA SIECIOWA i **Uprawnienia** nadaj jej uprawnienia *Odczyt* i *Zapis*.
- Usługa Serwer aplikacji systemu Navision jest uruchamiana domyślnie na koncie Zarządzanie NT\Usługa sieciowa, co zapewnia jej dostęp lokalny do serwera bazy danych systemu Navision. Jednak aby mieć dostęp do serwera bazy danych, należy upewnić się w sieci, że usługa Serwer aplikacji systemu Navision została uruchomiona na koncie domeny systemu Windows rozpoznawanym przez serwer bazy danych systemu Navision. To konto nie powinno być kontem administratora ani w domenie, ani na którymkolwiek komputerze lokalnym.
- Jeśli uruchamiana jest opcja programu SQL Server dla systemu Navision, program Microsoft SQL Server™ działa jako usługa. Opcja programu SQL Server dla systemu Navision wymaga, aby program SQL Server mógł tworzyć listy grup użytkowników systemu Windows dla celów uwierzytelniania, przeszukując usługę Active Directory. Dlatego należy upewnić się, że usługa SQL Server została uruchomiona na koncie Zarządzanie NT\Usługa sieciowa.

Aby upewnić się, że usługa została uruchomiona na koncie Zarządzanie NT\Usługa sieciowa:

1. Na komputerze z programem SQL Server znajdź usługę MSSQLSERVER, kliknij ją prawym przyciskiem myszy, a następnie kliknij polecenie Właściwości.
2. W oknie ***Właściwości*** kliknij kartę ***Logowanie***.
3. Na karcie ***Logowanie*** w polu Logowanie jako kliknij opcję To konto i wpisz *Zarządzanie NT\Usługa sieciowa*, a następnie kliknij przycisk OK.

Więcej informacji na temat zabezpieczeń programu SQL Server można znaleźć pod adresem:

http://www.microsoft.com/security/guidance/prodtech/SQLServer.mspx

i

http://www.microsoft.com/technet/security/prodtech/dbsql/default.mspx

- W przypadku korzystania z produktu z rodziny Navision E-business, takiego jak Commerce Gateway, należy upewnić się, że serwer żądań modułu Commerce Gateway został prawidłowo zainstalowany z domyślnym ustawieniem konta usług. Domyślne ustawienie konta nosi nazwę *CGRSUser*. Przyznaje ono serwerowi modułu Commerce Gateway odstęp do minimalnego zestawu innych wymaganych przez niego usług, takich jak *MSSQLSERVER* czy usługa *Grupa BizTalk: BizTalkServerApplication*. W odróżnieniu od konta *System lokalny* nie zawiera ono żadnych globalnych ustawień kont.
- Zawsze należy używać silnych haseł. Więcej informacji na temat silnych haseł można znaleźć w sekcji Silne hasła.
- Należy używać identyfikatorów logowania systemu Windows. System Navision umożliwia tworzenie dwóch rodzajów identyfikatorów logowania — do bazy danych i do systemu Windows. Zalecane jest stosowanie identyfikatorów logowania do systemu Windows, ponieważ wykorzystują one uwierzytelnianie systemu Windows i umożliwiają wymuszanie odpowiednich zasad stosowania haseł.
- Haseł nie należy używać ponownie. Często stosowaną praktyką jest używanie tych samych haseł w systemach i domenach. Administrator odpowiedzialny za dwie domeny może na przykład utworzyć w każdej z nich konta Administrator domeny korzystające z tych samych haseł, a nawet określić takie same lokalne hasła administratora na komputerach w całej domenie. W takim przypadku sforsowanie zabezpieczeń jednego konta lub komputera może spowodować zagrożenie dla całej domeny.
- Po zainstalowaniu systemu Navision i utworzeniu lub zaktualizowaniu baz danych należy utworzyć identyfikator logowania systemu Windows, a następnie przypisać mu w systemie Navision rolę administratora nadrzędnego (SUPER). Administrator ten będzie mógł administrować bazą danych, zarządzać zabezpieczeniami itd. Do tego identyfikatora należy przypisać silne hasło. Należy zadbać o zachowanie poufności tego hasła. Powinno ono gwarantować taki sam poziom ochrony, jaki zapewnia hasło administratora systemu w programie SQL Server. Rola administratora nadrzędnego (SUPER) umożliwia zarządzanie dostępem do wszystkich baz danych, dlatego wymaga najwyższego poziomu ochrony. Hasło tego administratora powinno być znane tylko administratorom systemu.
- Wszyscy pozostali użytkownicy, którzy mają dostęp do bazy danych systemu Navision, powinni logować się do kont z najmniejszymi uprawnieniami. Oznacza to przypisanie im w systemie Navision ról zapewniających dostęp jedynie do funkcji, których potrzebują do wykonywania swoich zadań w przedsiębiorstwie.
- Możliwość importowania plików FOB, zmiany konstrukcji obiektów, a także tworzenia i przywracania kopii zapasowych baz danych należy udostępnić tylko tym użytkownikom, których role w przedsiębiorstwie tego wymagają.

- Należy regularnie wykonywać kopie zapasowe bazy danych systemu Navision oraz pamiętać o sprawdzaniu kopii zapasowych, aby upewnić się, że można je pomyślnie przywrócić.
- Kopie zapasowe należy przechowywać w bezpiecznym miejscu, aby ograniczyć możliwość zniszczenia ich przez ogień, dym, pył, wysoką temperaturę, pioruny i katastrofy naturalne (na przykład trzęsienia ziemi).
- System Navision można uruchomić w kilku wersjach systemu Windows, jednak zalecane jest korzystanie z najnowszych systemów operacyjnych, które zawierają najnowocześniejsze funkcje zabezpieczeń. Obecnie są to systemy Windows XP z dodatkiem Service Pack 2 oraz Windows Server 2003.
- Najnowsze aktualizacje zabezpieczeń można zastosować przy użyciu usługi Windows Update dostępnej w systemach Windows 2000, Windows XP i Windows Server 2003. Dzięki najnowszym poprawkom zabezpieczeń, dodatkom Service Pack i aktualizacjom dostarczanym przez funkcję Aktualizacje automatyczne systemu Windows ochrona komputerów klienckich jest zawsze aktualna.
- Do komunikacji między klientami i serwerem bazy danych systemu Navision zalecane jest stosowanie protokołu zabezpieczeń TCPS. TCPS to bezpieczna wersja protokołu TCP/IP, w której zastosowano interfejs SSPI (Security Support Provider Interface) z włączonym szyfrowaniem oraz uwierzytelnianie Kerberos. TCPS jest domyślnym protokołem serwera bazy danych systemu Navision.
- Klient powinien mieć plan odzyskiwania danych na wypadek awarii, który zapewni szybkie wznowienie usług po wystąpieniu problemów. Plan odzyskiwania danych powinien obejmować następujące zagadnienia:
  - Nabycie nowego/tymczasowego sprzętu.
  - Przywrócenie kopii zapasowych w nowych systemach.
  - Sprawdzenie, czy plan odzyskiwania danych rzeczywiście działa.

Zabezpieczenia fizyczne

Zabezpieczenia fizyczne są absolutnie niezbędne, ponieważ nie ma możliwości zastąpienia ich zabezpieczeniami programowymi. Na przykład kradzież dysku twardego oznacza także utratę zapisanych na nim danych. Podczas opracowywania zasad należy omówić z klientem następujące kwestie związane z zabezpieczeniami fizycznymi:

- W przypadku dużych instalacji ze specjalnymi działami informatycznymi należy upewnić się, że pomieszczenia serwerów oraz miejsca przechowywania oprogramowania są zamykane.
- Do komputerów z tej kategorii należą:
  - Serwer programu Microsoft SQL Server 2000
  - Serwer plików, na którym znajdują się pliki wykonywalne systemu Navision.
- Do komputerów nie powinni mieć dostępu nieupoważnieni użytkownicy.
- Bez względu na ważność danych należy zainstalować alarmy antywłamaniowe.
- Kopie zapasowe ważnych danych powinny znajdować się w ognioodpornych pojemnikach przechowywanych w innym miejscu.

Pracownicy

Dobrym pomysłem jest ograniczenie praw do administrowania wszystkimi produktami I funkcjami. Domyślnie pracownicy korzystający z komputerów klienckich powinni mieć jedynie prawa do odczytu funkcji systemowych, chyba że ich praca wymaga większych uprawnień dostępu. Firma Microsoft sugeruje stosowanie zasady najmniejszych uprawnień: użytkownikom należy przyznać tylko minimalne uprawnienia wymagane do korzystania z danych i funkcji.
Niezadowoleni i byli pracownicy stanowią zagrożenie dla zabezpieczeń sieciowych. Podczas omawiania z klientami kwestii zabezpieczeń należy zaproponować następujące zasady dotyczące pracowników:

- Przed zatrudnieniem pracownika należy sprawdzić jego przeszłość.
- Ze strony niezadowolonych i byłych pracowników można spodziewać się „odwetu”.
- Po odejściu pracownika należy zablokować wszystkie związane z nim konta i hasła systemu Windows. Dla celów raportowania nie należy usuwać użytkowników. Nie należy używać ponownie tych samych kont.
- Użytkowników należy przeszkolić, aby zwracali uwagę na podejrzaną działalność i zgłaszali takie przypadki.
- Nie należy przyznawać uprawnień automatycznie. Jeśli użytkownicy nie muszą korzystać z określonych komputerów, pomieszczeń lub zestawów plików, nie powinni mieć do nich dostępu.
- Kadrę kierowniczą należy przeszkolić w zakresie identyfikowania potencjalnych problemów pracowniczych i reagowania na tego rodzaju przypadki.
- Pracownicy powinni zdawać sobie sprawę z ról, jakie pełnią w procesie obsługi zabezpieczeń sieciowych.
- Każdy pracownik powinien otrzymać kopię dokumentu zawierającego zasady obowiązujące w przedsiębiorstwie.
- Użytkownicy nie powinni instalować oprogramowania, które nie zostało zatwierdzone przez ich pracodawców.

Administrator

Zalecane jest, aby administratorzy systemów w przedsiębiorstwach klientów stosowali najnowsze poprawki zabezpieczeń udostępniane przez firmę Microsoft. Osoby o złych zamiarach potrafią znakomicie wykorzystać drobne usterki w celu spowodowania wielkich włamań do sieci. Administratorzy powinni przede wszystkim upewnić się, że poszczególne komputery są w maksymalnym stopniu zabezpieczone, a następnie dodać aktualizacje zabezpieczeń i użyć oprogramowania antywirusowego. W niniejszym podręczniku podano liczne łącza i zasoby ułatwiające znalezienie cennych informacji i najważniejszych wskazówek.

Złożoność systemu wymusza kompromis w zakresie zabezpieczenia sieci. Im bardziej złożona jest sieć, tym trudniejsze jest jej zabezpieczenie lub usunięcie skutków udanego włamania. Administrator powinien starannie dokumentować topografię sieci, aby zachować jej maksymalną prostotę.

Bezpieczeństwo jest podstawową kwestią związaną z zarządzaniem ryzykiem. Ponieważ sama technologia nie jest panaceum na wszystko, bezpieczeństwo wymaga połączenia technologii z zasadami. Innymi słowy, nigdy nie uda się stworzyć produktu, który po rozpakowaniu i zainstalowaniu w sieci pozwoli uzyskać doskonałe zabezpieczenie. Bezpieczeństwo to połączenie technologii i zasad, co oznacza, że poziom zabezpieczeń w sieci jest ostatecznie określony przez sposób wykorzystania technologii. Firma Microsoft oferuje technologie i funkcje umożliwiające zapewnienie bezpieczeństwa, ale tylko administrator z pomocą doradcy może określić odpowiednie zasady dla konkretnej organizacji. Zabezpieczenia należy planować na wczesnych etapach procesu implementowania I wdrażania systemu. Doradca musi wiedzieć, co i w jaki sposób chce chronić jego klient.

Na koniec należy opracować plany na wypadek nieprzewidzianych sytuacji awaryjnych, zanim takie sytuacje wystąpią. Połączenie starannego planowania z solidną technologią zapewni klientowi znakomite zabezpieczenia.

Więcej ogólnych informacji na temat zabezpieczeń można znaleźć w dokumencie „The Ten Immutable Laws of Security Administration" (Dziesięć niezmiennych praw administrowania zabezpieczeniami) pod adresem:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx

oraz w artykułach poświęconych zarządzaniu zabezpieczeniami pod adresem:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Zabezpieczanie systemu operacyjnego serwera

Chociaż wielu drobnych klientów może nie mieć serwerowych systemów operacyjnych, doradca powinien znać najważniejsze wskazówki dotyczące zabezpieczeń oraz przekazać je większym klientom, których środowiska sieciowe są bardziej złożone. Należy także pamiętać o tym, że wiele zasad i wskazówek opisanych w tym dokumencie można z łatwością zastosować w przypadku kontrahentów dysponujących jedynie klienckimi systemami operacyjnymi.

Pojęcia opisane w tej sekcji dotyczą zarówno systemu Microsoft Windows 2000 Server, jak I Microsoft Windows Server 2003, chociaż przedstawione informacje pochodzą głównie z Pomocy online systemu Windows Server 2003. System Windows Server 2003 oferuje solidny zestaw funkcji zabezpieczeń. Pełne informacje na temat wszystkich funkcji i procedur związanych z zabezpieczeniami znajdują się w Pomocy online systemu Windows Server 2003.

Dodatkowe informacje na temat systemu Windows 2000 Server można znaleźć w witrynie Centrum zabezpieczeń systemu Windows 2000 pod adresem:
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx

Można również przeczytać podręcznik wzmacniania zabezpieczeń systemu Windows 2000 znajdujący się pod adresem:
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Dodatkowe informacje na temat systemu Windows Server 2003 można znaleźć w *podręczniku zabezpieczeń systemu Windows Server 2003* pod adresem:
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

Podstawowe funkcje modelu zabezpieczeń serwera systemu Windows to uwierzytelnianie, kontrola dostępu i rejestracja pojedyncza.

- Uwierzytelnianie to proces potwierdzania przez system tożsamości użytkownika za pomocą poświadczeń logowania. Nazwa użytkownika i hasło są porównywane z autoryzowaną listą. Jeśli podczas uwierzytelniania system stwierdzi, że nazwa i hasło użytkownika są zgodne, użytkownik otrzyma dostęp do systemu w zakresie określonym na liście uprawnień.
- Kontrola dostępu ogranicza dostęp do informacji i zasobów komputerowych na podstawie tożsamości użytkownika i jego członkostwa w różnych wstępnie zdefiniowanych grupach. Zazwyczaj kontrola dostępu jest używana przez administratorów systemu w celu sterowania dostępem użytkowników do zasobów sieciowych, takich jak serwery, katalogi i pliki. Zwykle jest ona realizowana przez przyznawanie użytkownikom i grupom praw dostępu do określonych obiektów.
- Rejestracja pojedyncza umożliwia użytkownikowi jednokrotne zalogowanie się do domeny systemu Windows przy użyciu jednego hasła oraz uwierzytelnienie się na dowolnym komputerze w domenie systemu Windows. Rejestracja pojedyncza pozwala administratorom zaimplementować uwierzytelnianie za pomocą haseł w sieci systemu Windows, zapewniając jednocześnie użytkownikom końcowym łatwy dostęp do systemu.

Bardziej szczegółowy opis tych trzech głównych funkcji znajduje się w poniższych sekcjach.

Uwierzytelnianie

Uwierzytelnianie to podstawowy aspekt zabezpieczeń systemu. Służy do potwierdzania tożsamości każdego użytkownika podejmującego próbę zalogowania się do domeny lub uzyskania dostępu do zasobów sieciowych. Najsłabszym ogniwem w większości systemów uwierzytelniania jest hasło użytkownika.

Hasła stanowią pierwszą linię obrony przed dostępem osób nieupoważnionych do domeny I komputerów lokalnych. Doradca powinien przekazać klientowi następujące wskazówki:

- Zawsze należy używać silnych haseł.
- Jeśli hasła wymagają zapisania na papierze, notatki należy przechowywać w bezpiecznym miejscu i zniszczyć je, gdy tylko staną się niepotrzebne.
- Nie należy udostępniać haseł innym osobom.
- Dla wszystkich kont użytkowników należy używać różnych haseł.
- Hasła należy zmieniać w regularnych odstępach czasu.
- Należy uważać, w którym miejscu hasła są zapisywane na komputerze.

Silne hasła

Rola haseł w zabezpieczaniu sieci organizacji jest często niedoceniana i pomijana. Jak wspomniano wcześniej, hasła stanowią pierwszą linię obrony przed dostępem do sieci osób nieupoważnionych. Dlatego należy upewnić się, że klienci poinformowali swoich pracowników o konieczności stosowania silnych haseł.

Jednak narzędzia umożliwiające łamanie haseł są wciąż ulepszane, a komputery służące do tego celu są wydajniejsze niż kiedykolwiek. Mając wystarczająco dużo czasu, automatyczne narzędzie do łamania haseł może złamać każde hasło. Niemniej silne hasła jest dużo trudniej złamać niż słabe.

Wskazówki dotyczące tworzenia silnych haseł łatwych do zapamiętania przez użytkownika można znaleźć pod adresem:
http://www.microsoft.com/athome/security/privacy/password.mspx
i
http://www.microsoft.com/ntworkstation/technicalresources/PWDguidelines.asp

Określanie zasad stosowania haseł

Pomagając klientowi w określeniu zasad stosowania haseł, należy utworzyć zasadę wymagającą od wszystkich kont użytkowników stosowania silnych haseł. W przypadku większości systemów wystarczające są następujące zalecenia zawarte w podręczniku zabezpieczeń systemu Windows Server 2003:

- Należy określić ustawienie zasad **Wymuszaj tworzenie historii haseł**, aby system pamiętał kilka wcześniejszych haseł. Ustawienie to spowoduje, że po wygaśnięciu haseł użytkownicy nie będą mogli użyć ich ponownie.

  Zalecane ustawienie: 24

- Należy określić ustawienie zasad **Maksymalny okres ważności hasła**, aby hasła wygasały tak często, jak to potrzebne w środowisku klienta.

  Zalecane ustawienie: między 42 (domyślnie) a 90.

- Należy określić ustawienie zasad **Minimalny okres ważności hasła**, aby nie można było zmieniać haseł przed upływem określonej liczby dni. Ustawienie to działa w połączeniu z ustawieniem zasad **Wymuszaj tworzenie historii haseł**. Po określeniu minimalnego okresu ważności haseł użytkownicy nie mogą obejść ustawienia zasad **Wymuszaj tworzenie historii haseł** przez kilkakrotną zmianę hasła, aby używać poprzednich haseł. Przed zmianą haseł musi upłynąć określona liczba dni.

  Zalecane ustawienie: 2.

- Należy określić ustawienie zasad **Minimalna długość hasła**, aby hasła zawierały co najmniej określoną liczbę znaków. Długie hasła (co najmniej siedem znaków) są zazwyczaj silniejsze od krótkich. Ustawienie to powoduje, że użytkownicy nie mogą używać pustych haseł i muszą tworzyć hasła o określonej długości lub dłuższe.

  Zalecane ustawienie: 8.

- Należy włączyć ustawienie zasad **Hasło musi spełniać wymagania co do złożoności**. Ustawienie to powoduje sprawdzanie wszystkich nowych haseł, aby zapewnić ich zgodność z podstawowymi wymaganiami dotyczącymi silnych haseł. Dzięki temu ustawieniu hasła zawierają co najmniej trzy symbole z czterech kategorii (wielkie litery, małe litery, cyfry i symbole inne niż alfanumeryczne) i nie zawierają żadnego fragmentu nazwy użytkownika ani jego imienia i nazwiska.

Uwaga
Hasła spełniające te wymagania nie muszą być bardzo silne. Na przykład hasło „Hasło1” spełnia te wymagania.

Zalecane ustawienie: Tak

- Pełną listę tych wymagań można znaleźć w temacie „Hasło musi spełniać wymagania co do złożoności” Pomocy online systemu Windows Server.
- Hasła należy przechowywać, korzystając z szyfrowania odwracalnego. Szyfrowanie odwracalne jest stosowane w systemach, w których aplikacja wymaga dostępu do haseł zapisanych zwykłym tekstem. W większości wdrożeń nie jest potrzebne.

  Zalecane ustawienie: Nie.

Więcej informacji można znaleźć w podręczniku zabezpieczeń systemu Windows Server 2003 pod adresem:

http://www.microsoft.com/technet/security/prodtech/Win2003/W2003HG/SGCH00.mspx

Określanie zasad blokady konta

Podczas określania zasad blokady konta należy zachować ostrożność. Zasad blokady konta nie należy stosować w małych firmach, ponieważ wysoce prawdopodobne jest także zablokowanie autoryzowanych użytkowników, co może być bardzo kosztowne dla klienta.

Jeśli klient zdecyduje się na stosowanie zasad blokady konta, ustawienie **Próg blokady konta** powinno mieć wystarczająco dużą wartość, aby kilkakrotne nieprawidłowe wpisanie hasła nie powodowało blokowania kont autoryzowanych użytkowników.

Więcej informacji na temat zasad blokowania kont można znaleźć w temacie „Omówienie zasad blokady konta” w Pomocy online systemu Windows Server.

Informacje na temat stosowania i modyfikowania zasad blokady konta można znaleźć w temacie „Aby zastosować lub zmodyfikować zasady blokady konta” w Pomocy online systemu Windows Server.

Kontrola dostępu

Sieć systemu Windows i jej zasoby (w tym także system Navision) można zabezpieczyć, uwzględniając uprawnienia użytkowników, grup użytkowników i innych komputerów w sieci. Komputer lub wiele komputerów można zabezpieczyć, przyznając użytkownikom lub grupom określone uprawnienia. Obiekt, na przykład plik lub folder, można zabezpieczyć, przypisując mu uprawnienia umożliwiające użytkownikom lub grupom wykonywanie określonych czynności związanych z tym obiektem. Najważniejsze pojęcia związane z kontrolą dostępu:

- Uprawnienia
- Własność obiektów
- Dziedziczenie uprawnień
- Prawa użytkowników
- Inspekcja obiektów

Uprawnienia

Uprawnienia określają typ dostępu przyznanego użytkownikowi lub grupie do obiektu lub właściwości obiektu, na przykład do plików, folderów i obiektów rejestru. Uprawnienia dotyczą wszystkich zabezpieczonych obiektów, takich jak pliki lub obiekty rejestru. Można przyznawać je dowolnym użytkownikom, grupom lub komputerom. Dobrą praktyką jest przypisywanie uprawnień do grup.

Własność obiektów

Właściciel obiektu jest przypisywany podczas tworzenia tego obiektu. Domyślnie w systemie Windows 2000 Server właścicielem jest twórca obiektu. W przypadku obiektów tworzonych przez członków grupy Administratorzy w systemie Windows Server 2003 jest inaczej.

Po utworzeniu obiektu przez członka grupy administratorów w systemie Windows Server 2003 właścicielem staje się ta grupa (Administratorzy), a nie pojedyncze konto, na którym został utworzony obiekt. Można to zmienić za pomocą przystawki Ustawienia zabezpieczeń lokalnych konsoli MMC (Microsoft Management Console), korzystając z ustawienia **Obiekty systemu: domyślny właściciel dla obiektów utworzonych przez członków grupy Administratorzy**. Bez względu na rodzaj uprawnień określonych dla obiektu, właściciel obiektu zawsze może zmienić te uprawnienia.

Więcej informacji można znaleźć w temacie „Własność” w Pomocy online systemu Windows Server.

Dziedziczenie uprawnień

Dziedziczenie umożliwia administratorom łatwe przypisywanie uprawnień i zarządzanie nimi. Funkcja ta powoduje automatyczne dziedziczenie przez obiekty znajdujące się w kontenerze wszystkich podlegających dziedziczeniu uprawnień tego kontenera. Na przykład pliki utworzone w folderze dziedziczą uprawnienia folderu. Dziedziczone są tylko uprawnienia oznaczone jako podlegające dziedziczeniu.

Prawa użytkowników

Prawa użytkowników przyznają użytkownikom i grupom znajdującym się w określonym systemie komputerowym specjalne uprawnienia logowania.

Informacje na temat praw użytkowników można znaleźć w temacie „Prawa użytkowników” w Pomocy online systemu Windows Server.

Inspekcja obiektów

Dostęp użytkowników do obiektów można kontrolować. Korzystając z apletu Podgląd zdarzeń, można następnie przeglądać zdarzenia związane z zabezpieczeniami, zapisane w dzienniku zabezpieczeń.

Więcej informacji można znaleźć w temacie „Inspekcje” w Pomocy online systemu Windows Server.

Najważniejsze wskazówki dotyczące kontroli dostępu

- Uprawnienia należy przypisywać do grup, a nie do użytkowników. Ponieważ bezpośrednie zarządzanie kontami użytkowników jest nieefektywne, przypisywanie uprawnień do pojedynczych użytkowników powinno stanowić wyjątek.
- W specjalnych przypadkach należy stosować odmowę przyznania uprawnień. Odmowę przyznania uprawnień można na przykład zastosować w celu wykluczenia określonego podzbioru użytkowników należących do grupy mającej przyznane uprawnienia.
- Nie należy odmawiać dostępu do obiektu grupie Wszyscy. Odmowa uprawnień dostępu do obiektu wszystkim użytkownikom obejmie także administratorów. Gdy użytkownikom, grupom lub komputerom nadawane są uprawnienia do obiektu, najlepszym rozwiązaniem jest usunięcie grupy Wszyscy. Należy pamiętać, że przy braku zdefiniowanych uprawnień dostęp będzie niemożliwy.
- Uprawnienia należy przypisać do obiektu w jak najwyższej części drzewa, a następnie zastosować funkcję dziedziczenia, aby przenieść ustawienia zabezpieczeń na inne gałęzie drzewa. Ustawienia kontroli dostępu można szybko i skutecznie zastosować do wszystkich elementów podrzędnych obiektu nadrzędnego. W ten sposób można uzyskać najlepszy efekt najmniejszym wysiłkiem. Określane ustawienia uprawnień powinny być odpowiednie dla większości użytkowników, grup i komputerów.
- Uprawnienia odziedziczone można czasami zastąpić wyraźnie określonymi. Odziedziczona odmowa uprawnień nie zapobiega dostępowi do obiektu, jeśli dla tego obiektu wyraźnie określono zgodę na uprawnienia dostępu. Wyraźnie określone uprawnienia mają priorytet nad uprawnieniami odziedziczonymi (nawet w przypadku odziedziczonej odmowy uprawnień).
- W przypadku uprawnień dotyczących obiektów usługi Active Directory® należy poznać najważniejsze wskazówki dla tych obiektów.

Więcej informacji można znaleźć w temacie „Najważniejsze wskazówki dotyczące przypisywania uprawnień do obiektów usługi Active Directory" w Pomocy online systemu Windows Server 2003.

Zapora zewnętrzna

Zapora to sieciowe zabezpieczenie programowe lub sprzętowe uniemożliwiające ruch przychodzący lub wychodzący pakietów danych. Kontrolę przepływu danych w sieci zapewniają porty zapory, które są otwierane lub zamykane dla określonych pakietów informacji. W każdym pakiecie danych zapora sprawdza kilka informacji: protokół, za pomocą którego pakiet jest dostarczany, informacje o odbiorcy lub nadawcy pakietu, typ danych znajdujących się w pakiecie oraz numer portu, do którego pakiet jest wysyłany. Jeśli konfiguracja zapory pozwala na przejście określonego protokołu przez port docelowy, pakiet jest przepuszczany. System Microsoft Windows Small Business Server 2003 Premium Edition jest dostarczany z oprogramowaniem Microsoft Internet Security and Acceleration (ISA) Server 2000, które pełni rolę zapory. Także w systemie Small Business Server Standard Edition znajduje się zapora.

ISA Server 2004

Program Internet Security and Acceleration (ISA) Server 2000 umożliwia bezpieczne kierowanie żądań i odpowiedzi między Internetem a komputerami klienckimi w sieci wewnętrznej.

Program ISA Server pełni rolę bezpiecznej bramki do Internetu dla klientów znajdujących się w sieci lokalnej. Komputer z programem ISA Server jest niewidoczny dla pozostałych uczestników komunikacji. Użytkownik Internetu nie powinien zdawać sobie sprawy z istnienia serwera zapory, dopóki nie podejmie próby uzyskania dostępu do usługi lub witryny, do której dostęp jest zabroniony przez komputer z oprogramowaniem ISA Server. Sewer internetowy, do którego użytkownik chce uzyskać dostęp, traktuje żądania z komputera z oprogramowaniem ISA Server jak pochodzące z aplikacji klienta.

Wybranie funkcji filtrowania fragmentów protokołu IP umożliwia usługom serwera proxy w sieci Web i zapory filtrowanie fragmentów pakietów. Filtrowanie fragmentów pakietów pozwala odrzucić wszystkie pofragmentowane pakiety IP. Wysyłanie pofragmentowanych pakietów, a następnie składanie ich w sposób mogący spowodować uszkodzenie systemu, jest dobrze znaną metodą ataku.

Program ISA Server zawiera mechanizm wykrywania włamań do sieci, który określa czas podjęcia ataku na sieć, a w przypadku ataku wykonuje zestaw skonfigurowanych czynności (lub alertów).

Jeśli na serwerze programu ISA jest zainstalowany program IIS, należy skonfigurować go w taki sposób, aby nie korzystał z portów używanych przez serwer dla wychodzących (domyślnie 8080) i przychodzących (domyślnie 80) żądań sieci Web. Ustawienia programu IIS można na przykład zmienić w taki sposób, aby monitorowany był port 81, a następnie skonfigurować program ISA Server, aby kierował przychodzące żądania sieci Web do portu 81 na komputerze lokalnym z uruchomionym programem IIS.

Jeśli istnieje konflikt między portami używanymi przez programy ISA Server i IIS, program instalacyjny powoduje zatrzymanie usługi publikowania programu IIS. Następnie można zmienić ustawienia programu IIS w celu monitorowania innego portu i uruchomić usługę publikowania.

Zasady programu ISA Server

Istnieje możliwość zdefiniowania zasad serwera programu ISA rządzących przychodzącymi I wychodzącymi żądaniami dostępu. Dostęp do witryn i zawartości jest określany przez reguły dotyczące witryn i zawartości. Reguły dotyczące protokołów wskazują, czy określony protokół jest dostępny dla komunikacji przychodzącej i wychodzącej.

Użytkownik może utworzyć reguły dotyczące witryn i zawartości, reguły dotyczące protokołów, reguły dotyczące publikowania w sieci Web oraz filtry pakietów IP. Zasady te pozwalają określić sposób komunikacji klientów serwera programu ISA z Internetem oraz dozwolone metody komunikacji.

Ochrona antywirusowa

Wirus komputerowy to plik wykonywalny, którego zadaniem jest samodzielne powielanie się, wymazywanie lub uszkadzanie plików danych i programów oraz unikanie wykrywania. Wirusy często są modyfikowane i dostosowywane,

aby uniemożliwić ich wykrycie. Są również wysyłane jako załączniki do poczty e-mail. Wyszukiwanie nowych i zmodyfikowanych wirusów wymaga ciągłej aktualizacji programów antywirusowych. Wirusy to główna metoda stosowana przez komputerowych wandali.

Zadaniem oprogramowania antywirusowego jest wykrywanie wirusów i ochrona przed ich działaniem. Ponieważ cały czas tworzone są nowe wirusy, wielu producentów programów antywirusowych oferuje klientom okresowe aktualizacje swojego oprogramowania. Firma Microsoft zdecydowanie zaleca implementowanie oprogramowania antywirusowego w środowisku klienta.

Oprogramowanie antywirusowe zazwyczaj jest instalowane w każdym z następujących trzech miejsc: na stacjach roboczych użytkowników, na serwerach i w sieciach, przez które do organizacji przychodzi (a w niektórych przypadkach wychodzi) poczta e-mail.

Typy wirusów

Istnieją trzy główne typy wirusów infekujących systemy komputerowe: wirusy sektora rozruchowego dysku, wirusy infekujące pliki i wirusy typu „koń trojański".

Wirusy sektora rozruchowego

Podczas uruchamiania komputera skanują sektor rozruchowy dysku twardego przed załadowaniem systemu operacyjnego lub jakichkolwiek plików uruchamiania. Zadaniem wirusa sektora rozruchowego jest zastąpienie informacji znajdujących się w sektorach rozruchowych dysku twardego jego własnym kodem. Po zainfekowaniu komputera wirusem sektora rozruchowego kod wirusa jest wczytywany do pamięci przed wszystkimi innymi danymi. Wirus, który znajduje się w pamięci, może powielać się na wszystkie pozostałe dyski używane w zainfekowanym komputerze.

Wirusy infekujące pliki

Najpopularniejszy typ wirusa — wirus infekujący pliki — dołącza się do pliku wykonywalnego programu, dodając do niego własny kod. Kod wirusa jest zazwyczaj dodawany w taki sposób, aby uniknąć wykrycia. Po uruchomieniu zainfekowanego pliku wirus może dołączać się do innych plików wykonywalnych. Pliki zainfekowane przez tego typu wirusa zwykle mają rozszerzenie com, exe lub sys.

Niektóre wirusy infekujące pliki są przeznaczone dla konkretnych programów. Najczęściej atakowane typy programów to pliki nakładek (ovl) i pliki bibliotek dynamicznych (dll). Chociaż pliki te nie są uruchamiane, pliki wykonywalne odwołują się do nich. Wirus jest przesyłany po wywołaniu takiego pliku.

Wyzwolenie wirusa powoduje uszkodzenie danych. Wirusa można wyzwolić po uruchomieniu zainfekowanego pliku lub po spełnieniu określonego warunku w środowisku (na przykład konkretnej daty systemowej).

Konie trojańskie

Koń trojański w rzeczywistości nie jest wirusem. Najważniejsza różnica między wirusem a koniem trojańskim polega na tym, że koń trojański nie powiela się,

a jedynie niszczy informacje na dysku twardym. Program tego typu ukrywa się pod postacią zwykłego programu, takiego jak gra lub program narzędziowy. Jednak po uruchomieniu może zniszczyć lub poprzestawiać dane.

Najważniejsze wskazówki dotyczące ochrony antywirusowej

Rozprzestrzeniania się wirusów makr można uniknąć. Oto kilka wskazówek pozwalających uniknąć infekcji, które doradca powinien przekazać klientom:

- Należy instalować rozwiązania antywirusowe, które umożliwiają skanowanie wiadomości przychodzących z Internetu w poszukiwaniu wirusów, zanim wiadomości te przejdą przez router. Dzięki temu wiadomości e-mail będą skanowane pod kątem znanych wirusów.
- Należy znać źródło odbieranych dokumentów. Nie należy otwierać dokumentów, jeśli nie pochodzą od nadawców uważanych przez klienta za zaufanych.
- Należy porozmawiać z twórcą dokumentu. Jeśli użytkownicy nie mają pewności co do bezpieczeństwa dokumentu, powinni skontaktować się z twórcą tego dokumentu.
- Należy stosować ochronę przed wirusami makr dostępną w pakiecie Microsoft Office. Aplikacje pakietu Office ostrzegają użytkownika, jeśli dokument zawiera makra. Funkcja ta umożliwia użytkownikowi włączanie lub wyłączanie makr podczas otwierania dokumentu.
- Wirusy makr należy wykrywać i usuwać przy użyciu oprogramowania skanującego. Oprogramowanie skanujące umożliwia wykrywanie, a często usuwanie, wirusów makr zawartych w dokumentach. Firma Microsoft zaleca używanie oprogramowania certyfikowanego przez organizację International Computer Security Association (ICSA).

Więcej informacji na temat wirusów i zabezpieczeń komputerów można znaleźć w następujących witrynach firmy Microsoft w sieci Web:

- Microsoft Security: http://www.microsoft.com/security/default.asp
- Dokumentacja dotycząca zabezpieczeń w witrynie Microsoft TechNet: http://www.microsoft.com/technet/security/Default.mspx

Strategie dotyczące zabezpieczeń sieciowych

Ponieważ projektowanie i wdrażanie środowisk korzystających z protokołu IP wymaga znalezienia kompromisu między problemami związanymi z sieciami prywatnymi i publicznymi, kluczowym składnikiem bezpiecznej sieci stała się zapora. Zapora nie jest pojedynczym składnikiem. Stowarzyszenie National Computer Security Association (NCSA) określa zaporę jako „system (lub kombinację systemów) stanowiący granicę między co najmniej dwiema sieciami”. Chociaż stosowane są różne terminy, granica ta najczęściej nosi nazwę sieci granicznej (peryferyjnej). Sieć graniczna chroni intranet lub korporacyjną sieć lokalną (LAN) przed włamaniami, kontrolując dostęp z Internetu lub z innych dużych sieci.

Na poniższym diagramie przedstawiono sieć graniczną ograniczoną przez zapory I umieszczoną między siecią prywatną a Internetem w celu zabezpieczenia sieci prywatnej:

Podstawowa sieć graniczna

Istnieją różne metody stosowania zapór zapewniających bezpieczeństwo w organizacjach. Filtrowanie pakietów IP oferuje słabe zabezpieczenia, jest trudne do zarządzania i łatwe do pokonania. Bramki aplikacji są bezpieczniejsze niż filtry pakietów i łatwiejsze do zarządzania, ponieważ dotyczą tylko kilku konkretnych aplikacji, takich jak określony system poczty e-mail. Bramki obwodów są najskuteczniejsze, gdy użytkownik aplikacji jest ważniejszy niż dane przechodzące przez tę aplikację. Serwer proxy to kompleksowe narzędzie zabezpieczające, które obejmuje bramkę aplikacji, bezpieczny dostęp dla użytkowników anonimowych i inne usługi. Oto kilka informacji na temat tych różnych opcji:

- **Filtrowanie pakietów IP**
  Filtrowanie pakietów IP było najstarszą implementacją technologii zapory. W metodzie tej nagłówki pakietów są sprawdzane pod kątem adresów źródłowych i docelowych, numerów portów TCP (Transmission Control Protocol) i UCP (User Datagram Protocol) oraz innych informacji. Filtrowanie pakietów to technologia o ograniczonych możliwościach, działająca najlepiej w czystych środowiskach zabezpieczeń, w których na przykład wszystko, co znajduje się poza siecią graniczną, nie jest zaufane, a wszystko, co znajduje się wewnątrz — jest. W ciągu ostatnich kilku lat różni producenci ulepszyli metodę filtrowania pakietów, uzupełniając filtrowanie pakietów o funkcje inteligentnego podejmowania decyzji i tworząc w ten sposób nowy format filtrowania pakietów nazywany *inspekcją protokołów na podstawie stanów*. Filtrowanie pakietów można skonfigurować w taki sposób, aby akceptowane były określone typy pakietów i odrzucane wszystkie pozostałe lub aby odrzucane były określone typy pakietów i akceptowane wszystkie pozostałe.
- **Bramki aplikacji**
  Bramki aplikacji są stosowane, gdy najważniejsza jest rzeczywista zawartość aplikacji. Fakt, że są one specyficzne dla aplikacji, stanowi zarówno ich siłę, jak i ograniczenie, ponieważ nie przystosowują się one łatwo do zmian technologicznych.
- **Bramki obwodów**
  Bramki obwodów to tunele w zaporze umożliwiające łączenie określonych procesów lub systemów po jednej stronie zapory z określonymi procesami lub systemami po drugiej stronie. Najlepszym zastosowaniem bramek obwodów są sytuacje, w których osoba korzystająca z aplikacji może stanowić większe zagrożenie niż informacje przetwarzane przez aplikację. Bramka obwodu różni się od filtru pakietu możliwością łączenia ze schematem aplikacji spoza zakresu, który może zawierać dodatkowe informacje.
- **Serwery proxy**
  Serwery proxy to kompleksowe narzędzia zabezpieczające, które składają się z zapór i bramek aplikacji zarządzających przesyłaniem danych internetowych do i z sieci LAN. Serwery proxy umożliwiają również buforowanie dokumentów i kontrolę dostępu. Serwer proxy zapewnia także poprawę wydajności przez buforowanie i bezpośrednie dostarczanie najczęściej żądanych danych, takich jak popularne strony sieci Web. Pozwala również

filtrować i odrzucać żądania uważane przez właściciela za nieodpowiednie, na przykład żądania nieautoryzowanego dostępu do zastrzeżonych plików.

Doradca powinien upewnić się, że klient korzysta z zalet tych funkcji zabezpieczeń zapory, które są dla niego pomocne. Sieć graniczną należy umieścić w topologii w miejscu, w którym wszystkie dane spoza sieci korporacyjnej muszą przejść przez obwód zapory zewnętrznej. Kontrolę dostępu do zapory można precyzyjnie dostosować, aby spełniała potrzeby klienta. Można również skonfigurować zapory w taki sposób, aby zgłaszały wszystkie próby nieautoryzowanego dostępu.

W celu zmniejszenia liczby portów potrzebnych do otwarcia zapory wewnętrznej można użyć zapory w warstwie aplikacji, na przykład programu ISA Server 2000.

Więcej informacji na temat protokołu TCP/IP można znaleźć w dokumencie „Designing a TCP/IP Network" (Projektowanie sieci TCP/IP) pod adresem: http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp

Sieci bezprzewodowe

Domyślnie sieci bezprzewodowe są zazwyczaj skonfigurowane w sposób umożliwiający podsłuchiwanie sygnałów bezprzewodowych. Ze względu na domyślne ustawienia niektórych urządzeń bezprzewodowych, dostępność oferowaną przez sieci bezprzewodowe oraz zastosowane metody szyfrowania, mogą być one podatne na niepożądane ingerencje z zewnątrz. Istnieją opcje konfiguracji i narzędzia umożliwiające ochronę przed podsłuchiwaniem, należy jednak pamiętać, że nie chronią one komputerów przed hakerami I wirusami przedostającymi się przez połączenie internetowe. Dlatego niezwykle ważna jest ochrona komputerów przez intruzami z Internetu przy użyciu zapory.

Więcej informacji na temat ochrony sieci bezprzewodowej można znaleźć w dokumencie „How to Make Your 802.11b Wireless Home Network More Secure" (Jak lepiej zabezpieczyć domową sieć bezprzewodową 802.11b) pod adresem: http://support.microsoft.com/default.aspx?scid=kb;en-us;309369

Scenariusze zabezpieczeń sieciowych

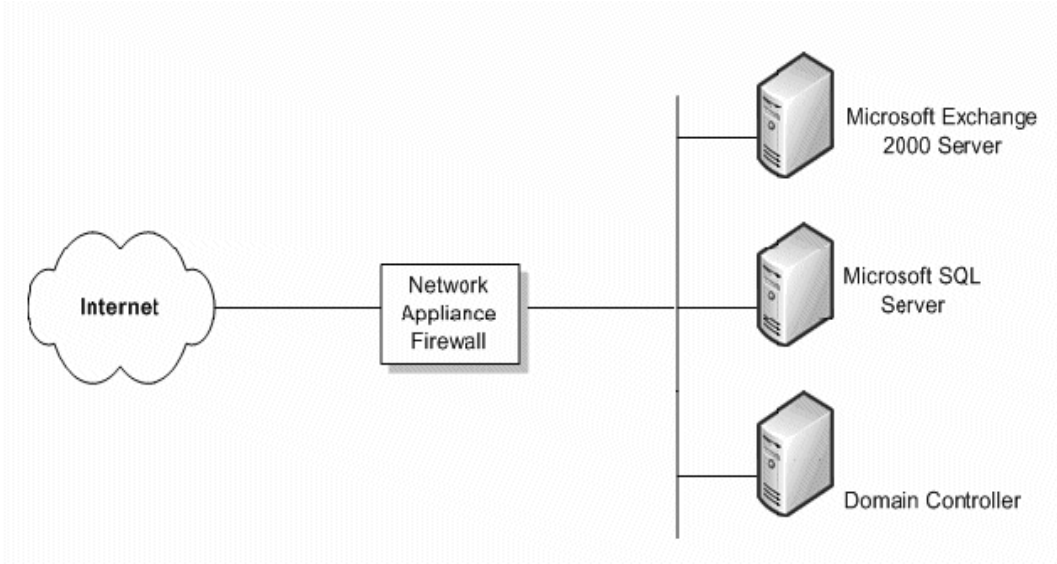
Poziom zabezpieczeń sieciowych wymaganych przez organizację klienta zależy od kilku czynników. Zazwyczaj sprowadza się do kompromisu między budżetem a potrzebą zapewnienia bezpieczeństwa danych korporacyjnych. W małych firmach można zastosować bardzo złożoną strukturę zabezpieczeń, która zapewnia najwyższy możliwy poziom zabezpieczeń sieciowych, ale taki poziom może okazać się zbyt drogi. W niniejszej sekcji omówiono cztery scenariusze i dla każdego z nich podano zalecenia dotyczące różnych poziomów zabezpieczeń.

Brak zapory

Jeśli klient ma połączenie z Internetem, ale nie ma zapory, należy zaimplementować pewne środki bezpieczeństwa w sieci. Istnieje kilka prostych sprzętowych zapór sieciowych, które stanowią wystarczające zabezpieczenie, aby powstrzymać potencjalnych hakerów.

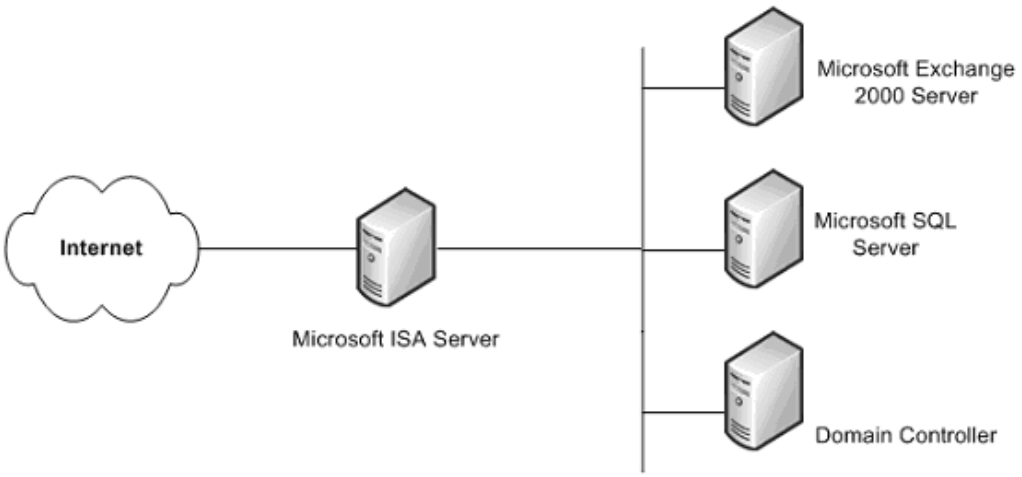
Jedna prosta zapora

Minimalnym zalecanym poziomem zabezpieczeń jest jedna zapora między Internetem a danymi klienta. Zapora ta może nie zapewniać wszystkich poziomów zabezpieczeń zaawansowanych i nie powinna być uznawana za bardzo bezpieczną. Ale jest lepsza niż brak zapory.



Zapora prosta

Pozostaje mieć nadzieję, że budżet klienta pozwoli na zastosowanie bezpieczniejszego rozwiązania zapewniającego ochronę danych korporacyjnych. Jednym z takich rozwiązań jest program ISA Server. Większy koszt związany z zakupem dodatkowego serwera jest rekompensowany znacznie większym bezpieczeństwem niż w przypadku przeciętnej zapory, która zazwyczaj zapewnia tylko translację adresów sieciowych (NAT) i filtrowanie pakietów.



Zapora z serwerem programu ISA

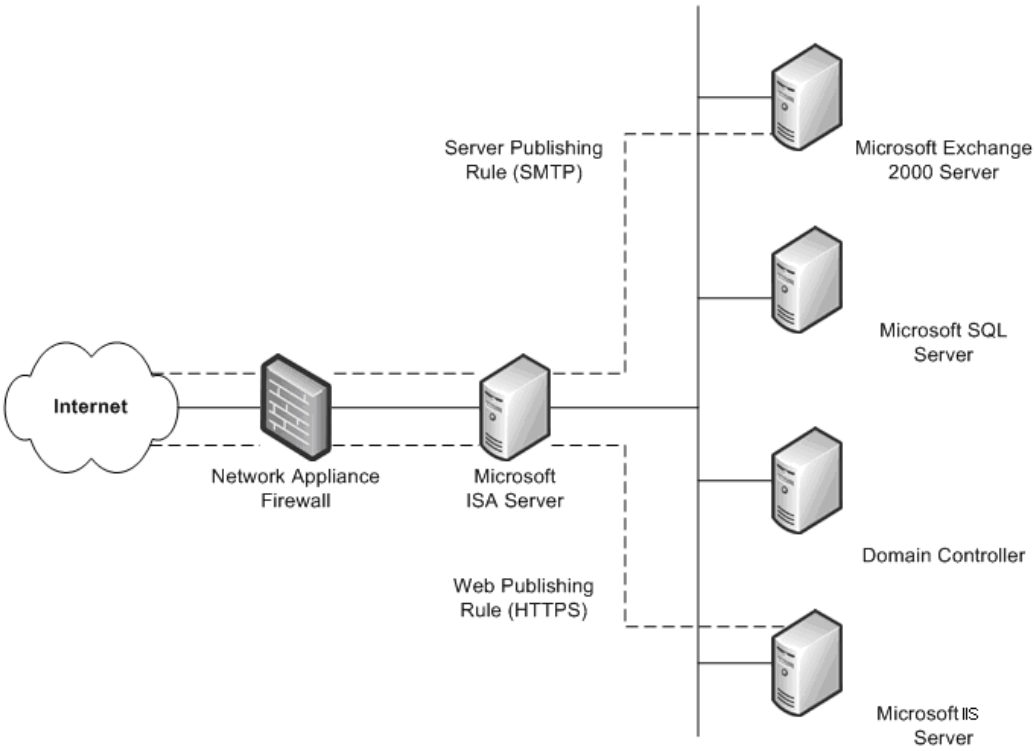
Tego rodzaju rozwiązanie z jedną zaporą jest bezpieczniejsze niż podstawowa zapora sprzętowa i zapewnia dodatkowe usługi zabezpieczeń w systemie Windows.

Jedna istniejąca zapora

Jeśli klient ma zaporę oddzielającą jego sieć intranet od Internetu, można rozważyć zakup dodatkowej zapory oferującej różne metody konfigurowania zasobów wewnętrznych do Internetu.

Jedną z takich metod jest publikowanie w sieci Web. Metoda ta jest stosowana, gdy program ISA Server został wdrożony przed serwerem sieci Web organizacji zapewniającym dostęp dla użytkowników Internetu. Po nadejściu żądań sieci Web program ISA Server może reprezentować serwer sieci Web na zewnątrz, realizując żądania klientów dotyczące zawartości sieci Web ze swojej pamięci podręcznej. Program ISA Server przekazuje żądania do serwera sieci Web tylko w przypadku, gdy nie może obsłużyć ich przy użyciu swojej pamięci podręcznej.

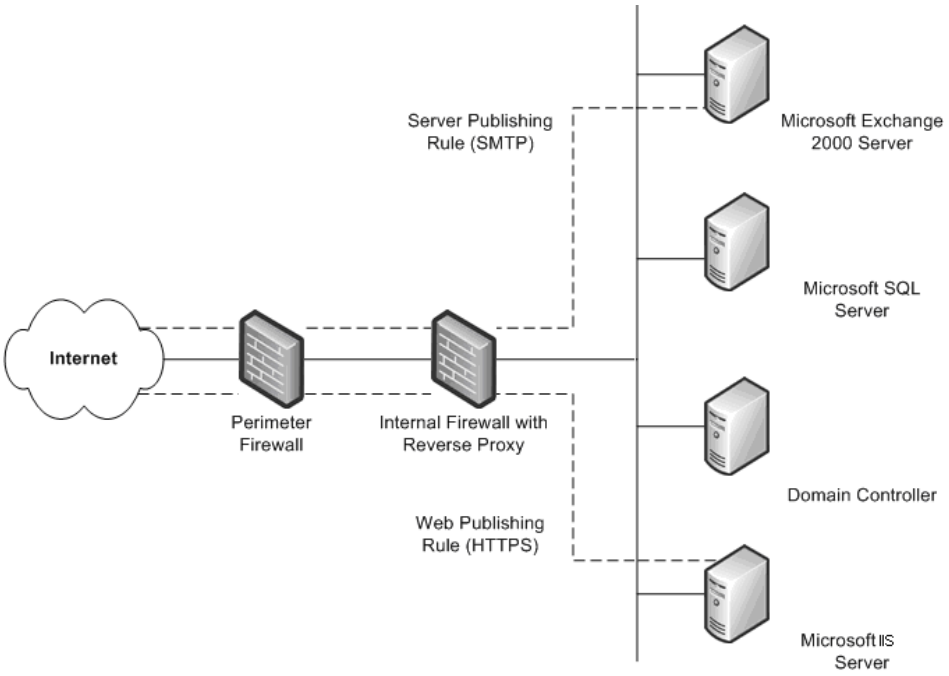
Inną metodą jest publikowanie serwerów. Program ISA Server umożliwia publikowanie serwerów wewnętrznych w Internecie bez pogorszenia bezpieczeństwa sieci wewnętrznej. Istnieje możliwość skonfigurowania reguł dotyczących publikowania w sieci Web i publikowania serwerów, które pozwolą określić, które żądania powinny być wysyłane do serwera w sieci lokalnej, zapewniając większe bezpieczeństwo serwerów wewnętrznych.



Istniejąca zapora z dodatkowym serwerem programu ISA

Dwie istniejące zapory

Czwarty scenariusz dotyczy sytuacji, w której organizacja ma dwie zapory oraz sieć graniczną (DMZ). Co najmniej jeden z tych serwerów pełni rolę zwrotnego serwera proxy, dzięki czemu klienci z Internetu nie mają bezpośredniego dostępu do serwerów w intranecie. Zamiast tego jedna z zapór, najlepiej zapora wewnętrzna, przechwytuje żądania z serwerów wewnętrznych, sprawdza te pakiety, a następnie przesyła je w imieniu hosta internetowego.



Dwie istniejące zapory

Scenariusz ten jest podobny do poprzedniego z dodaną drugą zaporą. Jedyną różnicą jest to, że zapora wewnętrzna obsługująca zwrotny serwer proxy nie jest serwerem programu ISA. Scenariusz ten zakłada ścisłą współpracę z menedżerami poszczególnych zapór w celu zdefiniowania reguł publikowania serwerów, które będą zgodne z zasadami zabezpieczeń.

Zarządzanie poprawkami zabezpieczeń

Systemy operacyjne i aplikacje są często bardzo złożone. Mogą składać się z milionów wierszy kodu napisanych przez wielu różnych programistów. Niezwykle ważne jest, aby oprogramowanie działało niezawodnie i nie pogarszało bezpieczeństwa ani stabilności środowiska informatycznego. W celu zminimalizowania liczby problemów programy są starannie testowane przed opublikowaniem. Jednak osoby przeprowadzające ataki wciąż próbują znaleźć luki w oprogramowaniu, co powoduje, że nie da się przewidzieć wszystkich przyszłych ataków.

W wielu organizacjach zarządzanie poprawkami stanowi część ogólnej strategii zmian I zarządzania konfiguracją. Jednak niezależnie od rodzaju i wielkości organizacji warto opracować dobrą strategię zarządzania poprawkami, nawet jeśli w danej organizacji nie istnieją jeszcze skuteczne procedury zarządzania zmianami i konfiguracją. Ogromna większość skutecznych ataków na systemy komputerowe występuje w systemach, w których nie zainstalowano poprawek zabezpieczeń.

Poprawki zabezpieczeń stanowią szczególne wyzwanie dla większości organizacji. Po wykryciu luki w oprogramowaniu osoby atakujące na ogół szybko rozprzestrzeniają informacje o niej w środowisku hakerów. Jeśli luka wystąpi w oprogramowaniu firmy Microsoft, firma stara się jak najszybciej opublikować poprawkę zabezpieczeń. Dopóki poprawka nie zostanie wdrożona, bezpieczeństwo klienta jest poważnie ograniczone.

W środowisku systemu Navision należy instalować w systemach klientów najnowsze poprawki zabezpieczeń. Doradca powinien upewnić się, że klient korzysta z jednej z technologii udostępnionych przez firmę Microsoft. Są to następujące technologie:

- **Usługa powiadamiania o zabezpieczeniach firmy Microsoft**
  Usługa powiadamiania o zabezpieczeniach to lista dystrybucyjna umożliwiająca wysyłanie pocztą e-mail powiadomień o udostępnieniu nowych aktualizacji. Powiadomienia te stanowią cenny element profilaktycznej strategii zabezpieczeń. Są one także dostępne w witrynie sieci Web TechNet Product Security Notification pod adresem: http://www.microsoft.com/technet/security/bulletin/notify.mspx
- **Usługa Aktualizacje automatyczne firmy Microsoft**
  System Windows umożliwia automatyczne stosowanie aktualizacji zabezpieczeń na komputerach.
- **Narzędzie do wyszukiwania biuletynów zabezpieczeń firmy Microsoft**
  Narzędzie do wyszukiwania biuletynów zabezpieczeń jest dostępne w witrynie sieci Web biuletynów zabezpieczeń pod adresem: http://www.microsoft.com/technet/security/current.aspx. W zależności od systemu operacyjnego, aplikacji i dodatków Service Pack klient może określić, których aktualizacji potrzebuje.
- **Narzędzie Microsoft Baseline Security Analyzer (MBSA)**
  To narzędzie graficzne jest dostępne w witrynie sieci Web Microsoft Baseline Security Analyzer pod adresem: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Działanie tego narzędzia polega na porównywaniu bieżącego stanu komputera z listą aktualizacji udostępnianą przez firmę Microsoft. Narzędzie MBSA przeprowadza także pewne podstawowe testy zabezpieczeń sprawdzające siłę haseł i ustawienia ich wygasania, zasady dotyczące kont gości oraz kilka innych dziedzin. Narzędzie MBSA wyszukuje także luki w programach Internetowe usługi informacyjne (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000 i Exchange Server 2003.
- **Usługi aktualizacji oprogramowania firmy Microsoft**
  Narzędzie to, znane wcześniej pod nazwą Windows Update Corporate Edition, umożliwia przedsiębiorstwom przechowywanie na komputerach lokalnych wszystkich aktualizacji krytycznych oraz skumulowanych pakietów zabezpieczeń (SRP) dostępnych w publicznej witrynie Windows Update. Współpracuje ono z nową wersją klientów aktualizacji automatycznych, tworząc podstawę skutecznej strategii automatycznego pobierania i instalowania. Nowy zestaw klientów aktualizacji automatycznych obejmuje klientów dla systemów operacyjnych Windows 2000 i Windows Server 2003, umożliwia także automatyczne instalowanie pobranych aktualizacji. Więcej informacji na temat usług aktualizacji oprogramowania firmy Microsoft można znaleźć pod adresem: http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp
- **Dodatek Microsoft Systems Management Server (SMS) Software Update Services Feature Pack**
  Dodatek SMS Software Update Services Feature Pack zawiera kilka narzędzi ułatwiających proces wydawania aktualizacji oprogramowania w przedsiębiorstwie. Wśród tych narzędzi znajdują się: Security Update Inventory Tool, Microsoft Office Inventory Tool for Updates, Distribute Software Updates Wizard i SMS Web Reporting Tool z dodatkiem Web Reports. Więcej informacji na temat poszczególnych narzędzi można znaleźć pod adresem: http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/

Doradca powinien porozmawiać z klientami na temat każdego z tych narzędzi i zachęcić do ich stosowania. Niezwykle ważne jest, aby problemy dotyczące zabezpieczeń były jak najszybciej rozwiązywane z zachowaniem stabilności środowiska.

Ustawienia zabezpieczeń programu SQL Server 2000

Ponieważ system Navision można także uruchomić na serwerze programu SQL Server 2000, ważne jest, aby zastosować środki zwiększające bezpieczeństwo instalacji programu SQL Server 2000 u klienta. Bezpieczeństwo serwera programu SQL Server można zwiększyć, wykonując następujące kroki:

- Należy upewnić się, że zostały zainstalowane najnowsze dodatki Service Pack i aktualizacje systemu operacyjnego oraz programu SQL Server 2000. Najnowsze informacje na ten temat można znaleźć w witrynie zabezpieczeń firmy Microsoft w sieci Web pod adresem: http://www.microsoft.com/security/default.asp
- W celu zapewnienia bezpieczeństwa na poziomie systemu plików należy upewnić się, że wszystkie dane programu SQL Server 2000 i pliki systemowe zostały zainstalowane na partycjach NTFS. Pliki powinny być dostępne tylko dla administratorów lub użytkowników na poziomie systemu za pośrednictwem uprawnień NTFS. Pozwoli to zabezpieczyć się przed użytkownikami korzystającymi z tych plików, gdy usługa MSSQLSERVER nie jest uruchomiona.
- W przypadku usługi programu SQL Server 2000 (MSSQLSERVER) należy używać konta domeny o niskich uprawnieniach, takiego jak Zarządzanie NT\Usługa sieciowa lub konto System lokalny (zalecane). Konto to powinno mieć minimalne uprawnienia w domenie i powinno ułatwić przyjęcie (ale nie zatrzymanie) ataku na serwer w przypadku włamania. Innymi słowy, konto powinno mieć tylko uprawnienia na poziomie użytkownika lokalnego w domenie. Jeśli usługi na serwerze programu SQL Server 2000 są uruchamiane przy użyciu konta Administrator domeny, pogorszenie bezpieczeństwa serwera doprowadzi do pogorszenia bezpieczeństwa całej domeny. Ustawienie to można zmienić przy użyciu programu SQL Server Enterprise Manager. Listy kontroli dostępu (ACL) do plików, rejestru i praw użytkowników zostaną zmienione automatycznie.
- Większość wersji programu SQL Server 2000 jest instalowanych z dwiema domyślnymi bazami danych: **Northwind** i **pubs**. Obie bazy danych są przykładowymi bazami używanymi do testowania, szkolenia i jako ogólne przykłady. Nie należy wdrażać ich w systemie produkcyjnym. Świadomość istnienia tych baz danych może zachęcić napastnika do podejmowania prób wykorzystania luk w domyślnych ustawieniach i domyślnej konfiguracji. Jeśli bazy **Northwind** i **pubs** znajdują się na komputerze produkcyjnym z programem SQL Server 2000, należy je usunąć.
- Inspekcja programu SQL Server 2000 jest domyślnie wyłączona, dlatego nie są kontrolowane żadne warunki. Utrudnia to wykrywanie włamań i ułatwia osobom atakującym ukrywanie śladów ich działalności. Należy włączyć przynajmniej inspekcję nieudanego logowania.

Najbardziej aktualne informacje dotyczące zabezpieczeń programu SQL Server 2000 można znaleźć pod adresem:
http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp

Microsoft Business Solutions — informacje

Firma Microsoft Business Solutions, będąca oddziałem firmy Microsoft, oferuje szeroki zakres zintegrowanych, całościowych aplikacji i usług biznesowych, które zostały zaprojektowane jako rozwiązania wspomagające małe i średnie firmy w dążeniu do nawiązania bliższych relacji z klientami, pracownikami, partnerami i dostawcami. Aplikacje firmy Microsoft Business Solutions optymalizują strategiczne procesy biznesowe w ramach przeprowadzania analiz, a także zarządzania finansami, zasobami ludzkimi, projektami, relacjami z klientami, serwisem u klienta, łańcuchem zaopatrzenia, handlem elektronicznym, produkcją i handlem detalicznym. Dzięki swojej konstrukcji aplikacje te zapewniają użytkownikom dostęp do informacji niezbędnych do osiągnięcia sukcesu w biznesie. Więcej informacji o produktach firmy Microsoft Business Solutions można znaleźć pod adresem:
http://www.microsoft.com/BusinessSolutions/