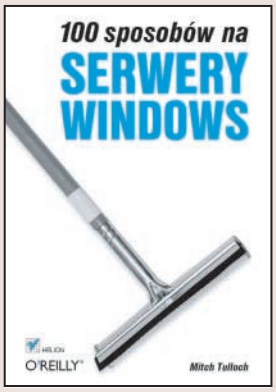
# 100 sposobów na serwery Windows




Autor: Mitch Tulloch
Tłumaczenie: Radosław Meryk
ISBN: 83-7361-811-2
Tytuł oryginału: Windows Server Hacks
Format: B5, stron: 376

**Niezawodne rozwiązania dla administratorów serwerów Windows**

- Wykorzystaj skrypty i narzędzia tekstowe
- Zoptymalizuj wydajność serwerów
- Popraw bezpieczeństwo i szybkość działania sieci

Popularność systemów z rodziny Windows Server to efekt połączenia olbrzymich możliwości z łatwością administracji i użytkowania. Dzięki wygodnemu interfejsowi graficznemu, spójnemu zestawowi narzędzi oraz kreatorom przeprowadzającym przez większość zadań, można szybko poznać podstawowe zasady instalacji, konfiguracji i administrowania serwerami opartymi na systemach Windows Server.
Z czasem jednak, po opanowaniu podstawowych możliwości pojawia się pytanie – czy nie można wycisnąć z nich więcej. Można – wystarczy zajrzeć „pod maskę", aby odkryć dodatkowe własności i możliwości.

Książka „100 sposobów na serwery Windows" to zestawienie sztuczek i metod, które zmienią Twoje podejście do administrowania serwerami Windows. Nauczysz się korzystać z trybu tekstowego i narzędzi skryptowych, optymalizować działanie serwerów i wykonywać standardowe zadania w szybszy i wygodniejszy sposób. Dowiesz się, jak wykorzystać niewidoczne na pierwszy rzut oka możliwości narzędzi i elementów systemu i sprawisz, że sieć oparta o serwer Windows będzie wydajniejsza, bezpieczniejsza i łatwiejsza do administracji.

- Administrowanie systemem
- Konfigurowanie usługi Active Directory
- Zarządzanie kontami użytkowników
- Usługi sieciowe
- Serwer DHCP
- Optymalizowanie działania IIS
- Zabezpieczenia antywirusowe
- Instalowanie aktualizacji
- Tworzenie kopii zapasowych

Jeśli nie poświęcasz zbyt wiele czasu na korzystanie z wiersza poleceń serwera Windows to nie wiesz, co tracisz. Po przeczytaniu tej książki przekonasz się, jak wiele możesz zmienić stosując to, pozornie przestarzałe, narzędzie.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

# Spis treści

ROZDZIAŁ ÓSMY

# Bezpieczeństwo

## Sposoby 69. – 78.

Prawdopodobnie nie ma dziś ważniejszego obszaru zadań administratora systemu od bezpieczeństwa, a szczególnie dotyczy to komputerów z systemem Windows. Ciągle rosnące ryzyko infekcji wirusowych, robaków, Trojanów i innych eksploitów oznacza, że administratorzy muszą poświęcać czas i energię na uczenie się sposobów ochrony sieci swoich firm przed zakusami złośliwych hakerów z internetu.

W tym rozdziale przeanalizowano sposoby ochrony sieci przed tymi zagrożeniami. Opisano też najlepsze praktyki ochrony antywirusowej, sposoby zabezpieczeń konta administratora, kopii zapasowych, kontrolerów domen, a także wyszukiwania komputerów z włączoną funkcją automatycznego logowania. Wiedzę zawartą w niniejszym rozdziale można uzupełnić, zapoznając się z odpowiedziami na najczęściej zadawane pytania oraz przeglądając narzędzia zabezpieczeń dostępne w witrynie WWW firmy Microsoft. W ten sposób zbudujemy arsenał najlepszych praktyk i narzędzi, które pozwolą na utrzymanie bezpieczeństwa sieci na odpowiednim poziomie. Opisy dodatkowych sposobów zabezpieczeń — mówiąc dokładniej, instalacji i zarządzania poprawkami bezpieczeństwa w sieci, można znaleźć w rozdziale 9.

SPOSÓB 69.

## Podstawowe zasady obowiązujące w sieci wolnej od wirusów

W tym punkcie opisano podstawowe zasady, które należy zachować, aby zabezpieczyć się przed wirusami w sieci.

Opisane w tym punkcie reguły sformułowałem metodą prób, błędów i obserwacji przez prawie trzy lata pracy w podwójnej roli administratora serwera SMS oraz specjalisty w dziedzinie ochrony antywirusowej. Zastosowanie tych reguł w mojej pracy umożliwiło osiągnięcie zerowego czasu przestojów w sieci z powodu infekcji wirusowych w okresie od stycznia 2000 roku do chwili obecnej (grudzień 2003).

### Świadomość zagrożeń

Pierwsza zasada to *świadomość zagrożeń*. Mówiąc prosto: nie można zabezpieczyć sieci przed zagrożeniami, jeśli się nie wie, że takie zagrożenia istnieją. Administratorzy muszą na bieżąco śledzić zagadnienia dotyczące wirusów, bieżących trendów w tej dziedzinie, a także

słabych punktów aplikacji i systemów operacyjnych. Poziom wiedzy administratora w zakresie tych tematów ma bardzo istotne znaczenie, ponieważ zależą od tego wszystkie jego decyzje podejmowane w celu zabezpieczenia sieci przed wirusami.

Jest kilka sposobów zdobywania wiedzy na temat zagrożeń w sieci. Informacje na temat wirusów oraz panujących trendów w tej dziedzinie można uzyskać w witrynach WWW producentów technologii antywirusowych (oprogramowanie wirusowe omówię wkrótce). W witrynach wszystkich producentów technologii antywirusowych można znaleźć sekcje zawierające informacje o wirusach.

Osobiście polecam, aby witrynę producenta swojego systemu antywirusowego odwiedzać kilka razy dziennie (najlepiej co kilka godzin). Autorzy wirusów są coraz sprytniejsi i stosują coraz bardziej wyrafinowane metody. W dogodnych warunkach, w ciągu kilku godzin, a nawet minut, może dojść do globalnej infekcji wirusowej, równie groźnej, jak te spowodowane przez wirusy Nimda czy Blaster. Im częściej odwiedzamy witrynę producenta oprogramowania antywirusowego, tym większe szanse, że nie poddamy się globalnej infekcji wirusowej.

Ponieważ producenci rozwiązań antywirusowych poziom zagrożenia wirusami oceniają, między innymi, na podstawie liczby próbek wirusów dostarczanych im przez klientów, informacji o wirusach dobrze poszukiwać w więcej niż jednej witrynie. Polecam odwiedzanie dwóch lub trzech witryn producentów technologii — to powinno wystarczyć, aby dobrze orientować się w temacie.

Oto kilka przykładów witryn producentów technologii antywirusowych:

- Symantec (*http://securityresponse.symantec.com*);
- Network Associates (*http://vil.nai.com/vil/newly-discovered-viruses.asp*);
- Trend Micro (*http://www.trendmicro.com/vinfo*);
- Computer Associates (*http://www3.ca.com/virusinfo*);
- F-Secure (*http://www3. ca. com/virusinfo*).

Osobiście najwyżej cenię witryny WWW firm Symantec, Network Associates oraz Trend Micro. Zgodnie z badaniami przeprowadzonymi przez ICSA Labs w 2002 roku (*http://www.icsalabs.com/2002avpsurvey/index.shtml*), sprzedaż produktów tych trzech firm stanowi około 89% rynku programów antywirusowych. Jeśli zdarzy się nowa światowa epidemia wirusowa, istnieje duże prawdopodobieństwo, że jedna z tych firm uzyska na ten temat informacje jako pierwsza.

Ostatnio również firma Microsoft uruchomiła witrynę zawierającą informacje na temat wirusów (*http://www.microsoft.com/security/antivirus/*). Witryna ta ma stanowić centralne źródło informacji o wirusach wykorzystujących wrażliwe punkty aplikacji i systemów operacyjnych firmy Microsoft. Jest to również doskonałe źródło informacji na temat wykorzystania produktów firmy Microsoft w sposób, który zabezpiecza przed infekcjami wirusowymi. Dostępny jest także artykuł bazy wiedzy firmy Microsoft na temat rozwiązań antywirusowych (*http://support.microsoft.com/default.aspx?scid=kb;pl:Q49500*).

W celu uzyskania informacji na temat słabych punktów aplikacji oraz systemów operacyjnych, można zapisać się do grupy mailingowej *NTBugtraq* (*http://www.ntbugtraq.com*). Jeśli ktoś znajdzie słaby punkt oprogramowania lub systemu, z reguły można przeczytać o tym na liście wcześniej niż gdziekolwiek indziej. Do innych dobrych witryn WWW należą SecurityFocus (*http://www.securityfocus.com*), CERT Coordination Center (*http://www.cert.org*) oraz *ICSA Labs* firmy TruSecure (*http://www.icsalabs.com*).

Polecam także zapisanie się do usługi *Security Notification* firmy Microsoft (*http://www.microsoft.com/technet/security/bulletin/notify.asp*). Dzięki temu otrzymamy wiadomość email za każdym razem, kiedy firma Microsoft ogłosi lukę bezpieczeństwa lub udostępni poprawkę.

Wirusy z dnia na dzień są coraz bardziej skomplikowane (przekonaliśmy się o tym przy okazji infekcji wirusów Nimda i Blaster). Kiedy nastąpiła epidemia wirusem Nimda, słabe punkty, które w nim wykorzystano, były znane od kilku miesięcy. Wirus Blaster rozprzestrzenił się masowo w niecały miesiąc po ogłoszeniu wykorzystywanych przez niego słabych punktów. Gdyby większa liczba administratorów wiedziała o tych słabych punktach, epidemie wirusów Nimda i Blaster nie miałyby tak dużego zasięgu. Wynika stąd następująca zasada: w wojnie przeciwko wirusom wiedza na ich temat jest pierwszą bronią, którą trzeba posiadać w swoim arsenale.

## Oprogramowanie antywirusowe

Drugą podstawą sieci bez wirusów jest zainstalowanie w niej oprogramowania antywirusowego. Dziś jest to dość oczywiste. Każdy, kto pracuje w branży informatycznej wystarczająco długo, wie, że oprogramowanie antywirusowe ma kluczowe znaczenie, szczególnie jeśli weźmie się pod uwagę fakt, iż wirusy są dzisiaj coraz bardziej skomplikowane. Jednak cechy, jakimi powinno się charakteryzować to oprogramowanie, nie są już tak oczywiste.

Poniżej zamieściłem listę cech, które według mojej wiedzy i doświadczenia są najbardziej pożądane w oprogramowaniu antywirusowym wykorzystywanym w firmie:

*Certyfikaty*
: Należy poszukiwać produktów, które uzyskały certyfikaty do wykorzystywania z wybranym systemem operacyjnym. Informacje na temat certyfikatów można uzyskać w witrynie ICSA Labs (*http://www.icsalabs.com*).

*Łatwa aktualizacja*
: Jedną z najbardziej poszukiwanych cech oprogramowania antywirusowego jest łatwość aktualizacji definicji wirusów. Oprogramowanie antywirusowe, w którym jest konieczność aktualizacji za pomocą oprogramowania zewnętrznego lub innych mechanizmów zewnętrznych, stwarza problemy logistyczne z instalacją uaktualnień, występujące szczególnie w dużych sieciach. Znacznie lepiej sprawdza się oprogramowanie antywirusowe z wbudowanymi mechanizmami aktualizacji. Wykorzystanie oprogramowania antywirusowego, którego aktualizacja wymaga interwencji użytkownika lub ponownego uruchamiania komputera, może prowadzić do podobnych problemów

logistycznych. Zastosowanie wbudowanego systemu automatycznych aktualizacji umożliwia uzyskanie znacznie lepszych wyników i daje pewność, że aktualizacja baz wirusów przebiega właściwie.

*Częstotliwość aktualizacji*
Podejmując decyzję dotyczącą oprogramowania antywirusowego, warto zajrzeć na stronę WWW jego producenta i dowiedzieć się, jak często pojawiają się uaktualnienia oraz w jaki sposób firma reaguje na sytuacje kryzysowe. Trzeba się upewnić, czy strategia producenta odpowiada wymaganiom naszego środowiska.

*Centralna konfiguracja*
Oprogramowanie antywirusowe, które ma możliwości konfiguracji wszystkich klientów w sieci z jednej centralnej konsoli, jest znacznie łatwiejsze do zarządzania i zapewnia spójność konfiguracji w sieci.

*Skanowanie w tle w czasie rzeczywistym*
Kluczową cechą nowoczesnego oprogramowania antywirusowego jest możliwość skanowania plików w tle, bez udziału użytkownika. Istotna jest także możliwość konfiguracji plików, które mają być skanowane w tle.

*Wyszukiwanie heurystyczne*
Oprogramowanie antywirusowe, które potrafi wykrywać działania przypominające działania wirusów, umożliwia identyfikację nowych wirusów bądź nowych odmian wirusów odkrytych wcześniej.

*Zdalne skanowanie*
W przypadku infekcji wirusowej możliwość zdalnego zainicjowania skanowania na serwerze, stacji roboczej lub w całej sieci ma istotne znaczenie w przeciwdziałaniu uszkodzeniom w sieci.

*Alarmowanie*
Biorąc pod uwagę szybkość, z jaką rozprzestrzeniają się dziś wirusy, kluczową cechą oprogramowania antywirusowego jest możliwość wysyłania ostrzeżeń w przypadku znalezienia wirusa. Bez tej cechy może się zdarzyć, że wirusy zainfekują wszystkie stacje robocze i serwery w sieci, a administrator nie będzie o tym nic wiedział.

*Obsługa komputerów przenośnych*
W dzisiejszych czasach trudno obyć się bez laptopów. Z tego powodu należy zaopatrzyć się w oprogramowanie antywirusowe, które umożliwia aktualizację komputerów przenośnych.

*Tworzenie raportów*
Każdy szef lubi otrzymywać co jakiś czas raporty. W związku z tym, aby ułatwić sobie pracę przy tworzeniu raportów dotyczących aktywności wirusów, zadbajmy o zakup oprogramowania antywirusowego wyposażonego w mechanizm tworzenia raportów.

Powyższa lista cech w żadnym razie nie jest „jedynie słuszna". Niektóre wymienione przeze mnie właściwości w pewnych warunkach są zupełnie nieważne, a być może są bardzo istotne cechy, których na tej liście nie umieściłem. Lista istotnych cech oprogramowania zależy od środowiska sieciowego, w którym pracujemy, oraz obsługiwanych systemów operacyjnych. Mam nadzieję, że powyższa lista nakreśliła właściwy kierunek, jaki należy obrać podczas analizowania własnych potrzeb dotyczących oprogramowania antywirusowego.

## Przechwytywanie

Trzecią zasadą, jaką musi spełnić sieć wolna od wirusów, jest zdolność przechwytywania pojawiających się infekcji. Mówiąc prosto: użytkownik nie wykona kodu wirusa, jeśli nie dopuścimy do zainfekowania sieci.

W świecie wirusów zmiany zachodzą bardzo szybko. Ponieważ duża część wirusów rozprzestrzenia się za pomocą poczty elektronicznej, w korzystnych warunkach infekcje wirusowe mogą w ciągu kilku godzin osiągnąć światowy zasięg. W zależności od wirusa, firma produkująca oprogramowanie antywirusowe potrzebuje zazwyczaj kilku godzin na opracowanie baz sygnatur zawierających definicję nowego wirusa. Najlepszym sposobem zabezpieczenia sieci przed infekcjami wirusowymi jest zablokowanie dostępu plikom określonych typów — tych, które są najczęściej używane do rozpowszechniania wirusów — do systemu poczty elektronicznej firmy.

Wydawałoby się, że wystarczy zablokować kilka specyficznych plików oraz kilka określonych tematów wiadomości — wszak zbyt restrykcyjne blokowanie poczty sprawia masę problemów. W czasach wirusa *I Love you* takie rozwiązanie było wystarczające. Niestety, teraz jest inaczej. Wirusy są dziś bardziej zaawansowane. Niemal wszystko, co generują, jest losowe (dobrym przykładem jest wirus *W32.Klez.H@mm*; więcej informacji na jego temat można znaleźć pod adresem *http://securityresponse.Symantec.com/avcenter/venc/data/w32.klez.h@mm.html*). Jedyne, czym można posługiwać się obecnie w blokowaniu dostępu wirusów do systemu poczty, są typy plików wykorzystywane przez wirusy.

Czy w ten sposób zablokujemy również pliki, które nie powinny być zablokowane? Niestety tak, jednak korzyści wynikające z zastosowania tej metody rekompensują niewielkie niedogodności użytkowników. W ciągu prawie trzech lat pracy u mojego poprzedniego pracodawcy w ten sposób udało nam się zatrzymać ponad 7 300 wirusów. Oceniam, że około 90% tej liczby stanowiły załączniki wiadomości e-mail. Kilkakrotnie, dzięki zastosowaniu tej metody, udało się nam uchronić przed infekcjami wirusowymi o światowym zasięgu, pomimo tego, że producenci oprogramowania antywirusowego jeszcze nie opracowali nowych baz sygnatur.

A zatem, trzeba dokładnie przeanalizować typy plików, które należałoby zablokować. Dobrym punktem startowym jest lista plików blokowanych przez system Outlook 98/2000 po wgraniu poprawki dostępnej pod adresem *http://office.microsoft.com/assistance/preview.aspx? AssetID=HA010550011033&CTT=6* (poprawka jest domyślnie instalowana w systemie Office XP):

*.ade*
Rozszerzenie plików projektów systemu Microsoft Access.

*.adp*
Projekty systemu Microsoft Access.

*.bas*
Moduły klas języka Visual Basic.

*.bat*
Pliki wsadowe.

*.chm*
Skompilowane pliki pomocy HTML.

*.cmd*
Skrypty systemu Windows NT.

*.com*
Aplikacje MS-DOS.

*.cpl*
Rozszerzenia Panelu sterowania.

*.crt*
Certyfikaty bezpieczeństwa.

*.exe*
Aplikacje.

*.hlp*
Pliki pomocy Windows.

*.hta*
Aplikacje HTML.

*.inf*
Pliki konfiguracyjne.

*.ins*
Pliki z parametrami komunikacji internetowej.

*.isp*
Pliki z parametrami komunikacji internetowej.

*.js*
Skrypty w języku JScript.

*.jse*
Kodowane skrypty w języku JScript.

*.lnk*
Skróty

*.mdb*
Aplikacje systemu Microsoft Access.

*.mde*
Skompilowane bazy danych Microsoft Access.

*.msc*
Dokumenty Microsoft Common Console.

*.msi*
Pakiety Instalatora Windows.

*.msp*
Uaktualnienia Instalatora Windows.

*.mst*
Pliki źródłowe pakietu Visual test.

*.pcd*
Obrazy programu Photo CD.

*.pif*
Skróty do programów MS-DOS.

*.reg*
Zapisy Rejestru.

*.scr*
Wygaszacze ekranu.

*.sct*
Skrypty *Windows Script Component*.

*.shs*
Obiekty Shell Scrap.

*.url*
Skróty internetowe.

*.vb*
Skrypty VBScript.

*.vbe*
Kodowane skrypty w języku VBScript.

*.vbs*
Skrypty VBScript.

*.wsc*
Skrypty *Windows Script Component*.

*.wsf*
Skrypty Windows.

*.wsh*
Pliki konfiguracyjne hosta skryptów Windows.

W firmie, w której pracuję, blokujemy większość z wymienionych powyżej typów plików, a także inne pliki, które w naszej ocenie, z powodu swojej natury, stwarzają potencjalne zagrożenie bezpieczeństwa. Na przykład, blokujemy także następujące pliki:

*.ocx*
Kontrolki Active X.

*.swf*
Obiekty *Shockwave Flash*.

*.wmv*
Pliki audio i wideo Odtwarzacza multimedialnego.

Sposób zastosowania powyższej strategii zależy od konfiguracji sieci oraz stosowanych mechanizmów zabezpieczeń. Dodatkowe wskazówki dotyczące rodzaju blokowanych typów plików można znaleźć w następnym podpunkcie.

Blokowanie potencjalnie niebezpiecznych załączników pocztowych w żadnym razie nie powinno być jedynym mechanizmem zabezpieczeń, który należy stosować w celu zabezpieczenia sieci przed wirusami. Jeśli jednak opisane tu zabezpieczenie zastosujemy jako dodatkowe, stworzymy solidne podstawy ochrony przed zagrożeniami wirusowymi. Więcej informacji dotyczących zabezpieczeń sieci przed wirusami można znaleźć w mojej rubryce, w witrynie myITforum.com (*http://www.myitforum.com*).

## Blokowanie plików — dalsze wskazówki

W niniejszym podpunkcie zaprezentowałem inne spojrzenie (moje — Briana Rogersa ) na ochronę sieci przed wirusami poprzez blokowanie plików określonych typów.

Chciałbym podzielić się moimi radami dotyczącymi typów plików, które należy zablokować, aby zabezpieczyć sieć przed zagrożeniami infekcji wirusowych. Listę tę jakiś czas temu opublikowałem na forum dyskusyjnym poświęconym tematyce zabezpieczeń przed

wirusami w witrynie myITforum.com (*http://www.myitforum.com*). Stworzyłem ją na podstawie informacji uzyskanych w kilku witrynach WWW oraz dodałem kilka własnych pozycji:

*.bas*
Moduły klas języka Visual Basic.

*.bat*
Pliki wsadowe.

*.cab*
Pliki instalacyjne Windows.

*.chm*
Skompilowane pliki pomocy HTML.

*.cmd*
Skrypty systemu Windows NT.

*.com*
Programy MS-DOS.

*.cpl*
Rozszerzenia Panelu sterowania.

*.crt*
Certyfikaty bezpieczeństwa.

*.exe*
Programy

*.hlp*
Pliki pomocy.

*.hta*
Programy HTML.

*.inf*
Pliki konfiguracyjne.

*.ins*
Pliki usługi WINS.

*.isp*
Pliki z parametrami komunikacji internetowej.

*.js*
Skrypty JScript.

*.jse*
Kodowane skrypty w języku Jscript.

*.lnk*
Skróty.

*.mde*
Skompilowane bazy danych Microsoft Access.

*.msc*
Dokumenty Microsoft Common Console.

*.msi*
Pakiety Instalatora Windows.

*.msp*
Uaktualnienia Instalatora Windows.

*.wst*
Pliki źródłowe systemu Microsoft Visual Test.

*.pcd*
Obrazy Photo CD, skompilowane skrypty Microsoft Visual.

*.pif*
Skróty do programów MS-DOS.

*.reg*
Zapisy Rejestru.

*.scr*
Wygaszacze ekranu.

*.sct*
Skrypty Windows.

*.shs*
Obiekty typu wycinek (Shell Scrap).

*.shb*
Obiekty typu wycinek (Shell Scrap).

*.uri*
Skróty internetowe.

*.vb*
Skrypty VBScript.

*.vbe*
Kodowane skrypty w języku VBScript.

*.vbs*
Skrypty VBScript.

*.wsc*
Skrypty Windows.

*.wsf*
Skrypty Windows.

*.wsh*
Pliki konfiguracyjne hosta skryptów Windows.

Od kiedy zablokowaliśmy załączniki z tymi rozszerzeniami, nie mieliśmy ani jednego przypadku infekcji wirusowej przez pocztę elektroniczną.

*— Chris Mosby i Brian Rogers*

SPOSÓB 70.

# Najczęściej zadawane pytania dotyczące ochrony antywirusowej

Rod Trent z witryny myITforum.com dzieli się swoimi odpowiedziami na niektóre często zadawane pytania dotyczące ochrony przed wirusami.

Jako prowadzący witrynę myITforum.com (*http://www.myitforum.com*) oraz autor kilku artykułów poświęconych bezpieczeństwu systemów, często otrzymuję pytania dotyczące sposobów zabezpieczania platform Microsoft przed wirusami, robakami i innymi zagrożeniami. W niniejszym punkcie zamieściłem wybrane pytania wraz z odpowiedziami, których na nie udzieliłem. Przy okazji dodam, że w witrynie myITforum.com można znaleźć mnóstwo dodatkowych informacji dotyczących zabezpieczania sieci.

## Czy zagrożenie jest prawdziwe, czy to fałszywy alarm?

**P**: W jaki sposób można stwierdzić, że zagrożenie infekcją wirusową jest prawdziwe i odróżnić je od fałszywych alarmów?

**O**: Warto mieć pod ręką kilka wymienionych poniżej odsyłaczy. Kiedy otrzymamy e-mail od użytkownika informujący o tym, że jego kumpel powiadomił go o grożącej infekcji wirusowej, można z nich skorzystać i sprawdzić, czy uzyskane informacje są prawdziwe:

Instytut CERT (*http://www.cert.org*);
McAfee — fałszywe alarmy (*http://vil.mcafee.com/hoax.asp*);
Symantec — fałszywe alarmy (*http://www.symantec.com/avcenter/hoax.html*);
TrendMicro — fałszywe alarmy (*http://www.antivirus.com/vinfo/hoaxes/hoax.asp*);
Sophos — fałszywe alarmy (*http://www.sophos.com/virusinfo/hoaxes/*);
Virus Busters (*http://www.itd.umich.edu/virusbusters/*);
Virus Myths (*http://www.stiller.com/myths.htm*);
Hoax Warnings (*http://www.europe.datafellows.com/news/hoax.htm*).

## Zablokowanie programów antywirusowych nie wystarczy

**P**: W jaki sposób można czasowo zablokować oprogramowanie antywirusowe, aby zdiagnozować problemy w systemie?

**O**: Czasami trzeba czasowo zablokować oprogramowanie antywirusowe w celu rozwiązania problemów z aplikacjami, drukowaniem lub samym systemem operacyjnym. W komputerach z systemem Windows 2000 samo wyłączenie usługi mechanizmu antywirusowego nie wystarcza do jego czasowego zablokowania. Trzeba także wyłączyć powiązane sterowniki urządzeń.

Oto, jak można dezaktywować popularne programy antywirusowe w systemie Windows 2000: kliknąć prawym przyciskiem myszy ikonę *Mój komputer* i wybrać pozycję *Właściwości*. Kliknąć zakładkę *Sprzęt*, a następnie przycisk *Menedżer urządzeń*. Kliknąć menu *Widok*, a w nim pozycję *Pokaż ukryte urządzenia*. Rozwinąć gałąź *Sterowniki niezgodne z Plug and Play* i znaleźć sterowniki związane z oprogramowaniem antywirusowym. Kliknąć prawym przyciskiem myszy określony sterownik i wybrać pozycję *Wyłącz*.

Nazwy sterowników urządzeń odpowiadających produktom popularnych pakietów antywirusowych zestawiono w tabeli 8.1. Trzeba jednak pamiętać, że sterowniki urządzeń dla każdej z tych aplikacji zmieniają się, a zatem zweryfikujmy poniższe informacje w witrynach WWW producentów oprogramowania.

*Tabela 8.1. Sterowniki urządzeń wykorzystywane przez oprogramowanie antywirusowe*

| Producent | Sterowniki |
|---|---|
| Symantec | *symevent.sys* |
| McAfee | *NaiFiltr* oraz *NaiFsRec* |
| Norton | *NAVAP*, *NAVENG* oraz *NAVEX15* |
| Inoculan | *INO_FLP* oraz *INO_Fltr* |

## Wystąpił błąd w programie Kernel32.exe

**P**: Uzyskałem komunikat o błędzie informujący mnie o tym, że wystąpił błąd w programie Kernel32.exe. Czy to błąd systemu, czy wirus?

**O**: W przypadku uzyskania komunikatu o błędzie programu Kernel32.exe należy uaktualnić program antywirusowy. *Kernel32.exe* nie jest bowiem plikiem Microsoft (w odróżnieniu od pliku *Kernel32.DLL*). A zatem w przypadku uzyskania tego błędu należy uaktualnić oprogramowanie antywirusowe i podjąć próbę usunięcia wirusa z komputera.

Taki problem może wystąpić w przypadku zainfekowania komputera przez jeden z następujących wirusów: *Worm_Badtrans.b*, *Backdoor.G_Door, Glacier Backdoor*, *Win32.Badtrans.29020*, *W32.Badtrans.B@mm* oraz *Win32/PWS.Badtrans.B.Worm*.

## Program Stinger

**P**: Czy istnieje program, który ma możliwość usuwania wielu typów wirusów, w odróżnieniu od narzędzi oferowanych przez producentów oprogramowania antywirusowego, usuwających pojedyncze wirusy?

**O**: Na forum dyskusyjnym w witrynie firmy McAfee można znaleźć informacje o narzędziu do usuwania wirusów o nazwie *Stinger*. Program ten jest ciągle aktualizowany i zapewnia możliwość usuwania coraz to nowych wirusów. Więcej informacji na temat programu Stinger można znaleźć pod adresem *http://forums.mcafeehelp.com/viewtopic.php?t=764*. Narzędzie można pobrać ze strony *http://vil.nai.com/vil/stinger/*.

*— Rod Trent*

SPOSÓB 71.

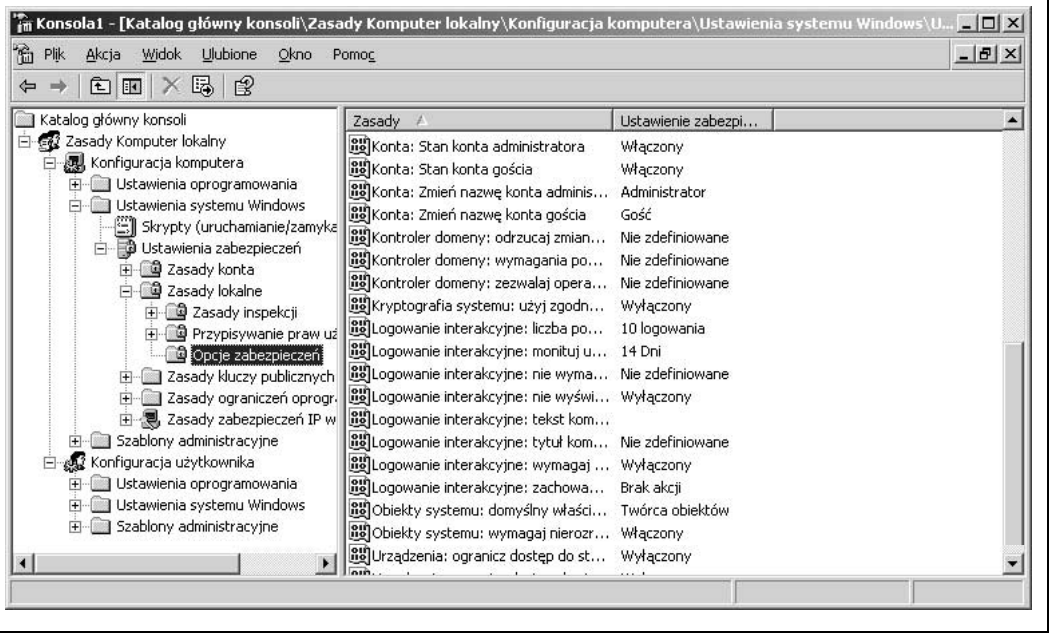
## Zmiana nazw kont Administrator i Gość

Zmiana nazw domyślnych kont administratora i gościa jest prostym i skutecznym sposobem poprawy bezpieczeństwa komputerów.

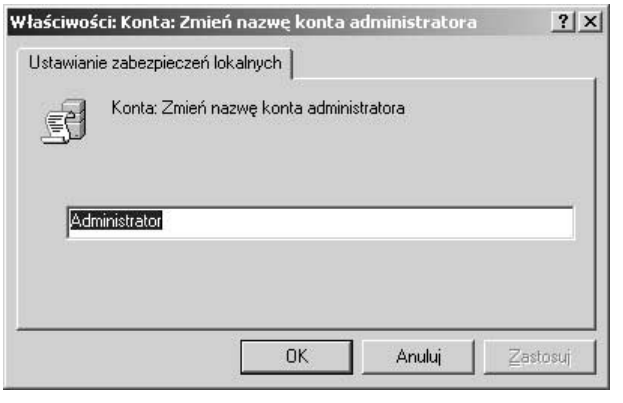
W celu poprawy bezpieczeństwa sieci z serwerami Windows należy zmienić nazwę konta administratora. Najlepiej wybrać taką nazwę, która nie kojarzy się z uprzywilejowaną rolą. Ten prosty zabieg znacznie utrudnia włamanie się do komputera lub sieci przez nieuprawnione osoby. Jedno z ustawień w systemach Windows 2000/2003 umożliwia wprowadzenie nazw, które zostaną użyte do automatycznej zmiany nazwy kont administratora i gościa za pomocą zasad zabezpieczeń lokalnych (w przypadku komputerów działających w grupie roboczej) lub zasad grupy (w środowisku Active Directory).

Aby uzyskać dostęp do ustawień zasad lokalnych, należy kliknąć *Start/Uruchom*, wpisać `mmc` i wcisnąć *Enter*. Wybrać polecenie *Plik/Dodaj/Usuń przystawkę*. Kliknąć przycisk *Dodaj*, przewinąć listę do pozycji *Zasady grupy* (w systemie Windows 2000) lub *Edytor obiektów zasad grupy* (w systemie Windows Server 2003). Kliknąć *Dodaj*, a następnie *Zakończ* (w ten sposób zostanie utworzony obiekt zasad grupy dla komputera lokalnego). Rozwinąć gałąź *Zasady Komputer lokalny*, *Konfiguracja komputera*, *Ustawienia systemu Windows*, *Ustawienia zabezpieczeń*, *Zasady lokalne*, *Opcje zabezpieczeń*. Konsolę tę można zapisać pod znaną nazwą, co pozwoli na szybki dostęp do przystawki w przyszłości. Po wybraniu gałęzi *Opcje zabezpieczeń* powinien wyświetlić się ekran podobny do tego, który zaprezentowano na rysunku 8.1 (jeśli korzystamy z systemów Windows Server 2003 lub Windows XP).

W panelu po prawej stronie można znaleźć pięć pozycji dotyczących zasad dla kont. Ostatnie dwie opcje w sekcji *Konta* służą do zmiany nazwy kont administratora i gościa. Kliknięcie pozycji *Konta: zmień nazwę konta administratora* spowoduje wyświetlenie ekranu pokazanego na rysunku 8.2. Podobny ekran wyświetli się, jeśli wybierzemy pozycję *Konta: Zmień nazwę konta gościa*. Wystarczy wpisać dowolną nazwę i kliknąć *OK*. Powyższe działanie spowoduje automatyczną zmianę nazw kont administratora lub gościa.




*Rysunek 8.1. Ustawienia zasad lokalnych dla domyślnych kont administratora i gościa w systemach Windows Server 2003 oraz Windows XP*




*Rysunek 8.2. Zmiana nazwy domyślnego konta Administrator*

## Uwagi

Należy pamiętać, że jeśli nasz komputer należy do domeny, skonfigurowane ustawienia zasad lokalnych za pomocą metody zaprezentowanej w powyższym punkcie mogą być przesłonięte przez ustawienia zasad grupy zdefiniowane na poziomie domeny, jednostki organizacyjnej bądź lokacji.

W systemie Windows 2000 są dostępne tylko dwa ustawienia zasad w sekcji *Konta* i mają one inne nazwy niż te, które pokazano na rysunku 8.1. Ustawienie systemu Windows Server 2003 *Konta: Zmień nazwę konta administratora* w systemie Windows 2000 ma nazwę *Zmień nazwę administratora*. Podobnie jest w przypadku konta gościa. Natomiast w systemie Windows XP nazwy opcji są identyczne jak w systemie Windows Server 2003.

Dodatkowym zabezpieczeniem po zmianie nazwy kont administratora i gościa jest dodanie kont *Administrator* i *Gość* (w sposób, w jaki tworzy się zwykłe konta użytkowników). Po utworzeniu tych kont należy nadać im bezpieczne hasła, ale odebrać wszelkie prawa w systemie. Nawet jeśli intruz przejmie te konta, nie będzie mógł nic zrobić w naszym komputerze.

*— John Gormly*

SPOSÓB 72.

## Pobranie listy lokalnych administratorów

Lokalni administratorzy mogą w swoich komputerach zrobić wszystko. W tym punkcie opisano, w jaki sposób dowiedzieć się, kto ma takie prawa.

Kiedy intruzowi uda się pokonać zabezpieczenia sieci, zazwyczaj próbuje uzyskać prawa lokalnego administratora komputera. Jeśli mu się to uda, może robić w przejętym systemie wszystko, na co ma ochotę.

Jeśli zatem mamy podejrzenia, że intruz włamał się do sieci, warto sprawdzić, kto posiada prawa lokalnych administratorów w naszych komputerach. Za pomocą interfejsu GUI można to zrobić, przeglądając gałąź *Użytkownicy i grupy lokalne* konsoli *Zarządzanie komputerem*, ale to rozwiązanie jest niewygodne.

Szybszym sposobem znalezienia użytkowników posiadających uprawnienia lokalnych administratorów w komputerach naszej sieci jest skorzystanie z poniższego skryptu VBScript. W miarę potrzeb można go odpowiednio dostosować.

### Kod

Wystarczy uruchomić edytor tekstowy, na przykład Notatnik (z wyłączonym zawijaniem wierszy), wpisać poniższy skrypt i zapisać z rozszerzeniem *.vbs*, jako *GetAdmins.vbs*.

```
computername = createobject("wscript.network").computername
set group = getobject("WinNT://" & computername & "/administratorzy,group")
s = ""
for each account in group.members
s = s & account.name & vbcrlf
next
msgbox s
```

### Wykorzystanie sposobu

Skorzystanie ze sposobu jest proste. Należy utworzyć skrót do skryptu na pulpicie i dwukrotnie go kliknąć. Wyświetli się okno dialogowe zawierające informacje o użytkownikach posiadających w komputerze uprawnienia lokalnego administratora, takie jak na

rysunku 8.3. Na podstawie tej listy można z łatwością odnaleźć konta administracyjne, które uzyskały te uprawnienia w sposób nielegalny (np. *backdOOr*). Istnienie takich kont może być sygnałem przejęcia systemu przez złośliwego hakera.


*Rysunek 8.3. Lista lokalnych administratorów na serwerze członkowskim domeny*

W komputerach, z których uruchamiamy zaprezentowany skrypt, powinny być zainstalowane najnowsze wersje mechanizmów obsługi skryptów. Można je pobrać ze strony *Microsoft Scripting* (*http://msdn.microsoft.com/scripting.asp?url=/nhp/default.asp?contentid=28001169*). Należy także zwrócić uwagę, że pracując z interfejsem ADSI (*Active Directory Services Interface*), trzeba mieć te same prawa, jakie są potrzebne do uruchamiania wbudowanych narzędzi administracyjnych.

## Modyfikacja sposobu

Skrypt pobiera informacje dotyczące zawartości grupy administratorów lokalnych, ale z łatwością można go zmodyfikować w taki sposób, aby pobierał informacje dotyczące dowolnej grupy w lokalnym komputerze. Na przykład, aby wyświetlić użytkowników należących do grupy *Użytkownicy*, wystarczy zmienić poniższy wiersz:

```
set group = getobject("WinNT://" & computername & "/administratorzy,group")
```

na następujący:

```
set group = getobject("WinNT://" & computername & "/użytkownicy,group")
```

i jeszcze raz uruchomić skrypt.

*— Rod Trent*

SPOSÓB 73.

# Wyszukiwanie wszystkich komputerów, w których działa określona usługa

Skryptu zaprezentowanego w niniejszym punkcie można użyć do wyszukania nieuprawnionych serwerów WWW, niewłaściwie skonfigurowanych klientów oraz innych systemów, które stwarzają potencjalne zagrożenie w sieci.

Narzędzie sprawdzające stan usługi w wielu komputerach jednocześnie może ułatwić życie administratorowi. Za jego pomocą można sprawdzić stan usługi klienta SMS, usługi antywirusowej, a nawet wirusów i Trojanów zainstalowanych jako usługi. W przypadku większości interfejsów takich jak WMI lub ADSI, sprawdzenie stanu usług wymaga

zalogowania się w docelowym komputerze z wykorzystaniem konta z uprawnieniami administratora. W wielu firmach w sieci działają komputery, w których pracownicy działu informatyki nie mają uprawnień administracyjnych. Takie niezarządzane komputery stanowią realne zagrożenie dla bezpieczeństwa sieci.

Kiedyś przy próbie sprawdzania zdalnego komputera za pomocą przystawki *Usługi systemu Windows 2000* zauważyłem, że do przeglądania usług uruchomionych w zdalnym komputerze nie są potrzebne uprawnienia administratora. Wystarczyło konto w zaufanej domenie z uprawnieniami użytkownika. Przy dokładniejszym zbadaniu sytuacji okazało się, że w tym przypadku wykonywane jest bezpośrednie zapytanie do *Menedżera sterowania usługami* (SCM) i nie są wykorzystywane wywołania API za pośrednictwem interfejsów WMI lub ADSI. Jednym z najlepszych narzędzi, w którym wykorzystano zapytania do menedżera SCM, jest program *Psservice* firmy *Sysinternals* (*http://www.sysinternals.com*). Chociaż jest to narzędzie działające wyłącznie w wierszu polecenia, można wprowadzić kilka odpowiednio przygotowanych parametrów i wykorzystać je z poziomu skryptu.

Na podstawie odpowiedzi na polecenie `ping` skrypt wyszukuje adresy IP według podsieci. W ten sposób, dzięki analizie wywołania NetBIOS, odnajduje komputery windowsowe. Następnie skrypt sprawdza, czy w komputerze działa określona usługa, poprzez wysłanie zapytania za pomocą programu *Psservice* i zarejestrowanie wyników w pliku rozdzielanym tabulatorami. W pliku wynikowym są następujące informacje: adres IP, nazwa komputera, zalogowany użytkownik, domena lub grupa robocza, do której jest dołączony komputer, oraz stan usługi. Adres IP jest umieszczony w wyniku nawet wtedy, kiedy nie odpowiada na polecenie `ping`. Można go uważać za identyfikator komputera. Następnie, w wyniku wyszukiwania DNS według adresu IP, skrypt znajduje nazwę komputera. Po jej znalezieniu szuka nazwy NetBIOS, a jeśli ją znajdzie, zastępuje nią nazwę DNS. Jeśli zarówno wyszukiwanie DNS, jak NetBIOS nie powiedzie się, do pliku wynikowego jest zapisywana pusta nazwa. W polu z informacjami o zalogowanym użytkowniku będą dane tylko wtedy, jeśli komputer jest zgodny z NetBIOS i ktoś jest na nim zalogowany. Jeśli jednak nikt nie jest zalogowany, pole jest puste. Zwróćmy uwagę, że pole nazwy może zawierać nazwę konta domeny lub konta lokalnego i nie ma sposobu, aby je od siebie odróżnić. Domena (grupa robocza), do której komputer jest podłączony, dotyczy konta komputera, a nie użytkownika.

Stan usługi może przyjąć jedną z siedmiu wartości, tak jak pokazano w tabeli 8.2.

*Tabela 8.2. Dopuszczalne wartości opisujące stan serwera*

| Stan | Opis |
|---|---|
| UnPingable | Adres IP nie odpowiada |
| RUNNING | Usługa jest uruchomiona |
| STOPPED | Usługa jest zatrzymana |
| PENDING | Usługa jest w trakcie uruchamiania bądź zatrzymywania |
| Brak wartości | Usługa nie istnieje |
| Access is Denied | Konto użytkownika ma niewystarczające uprawnienia |
| The RPC server is unavailable | W komputerze działa system Win9x,Win3.x lub Samba |

Do uruchomienia skryptu potrzeba kilku elementów. Po pierwsze, potrzebny jest program *Psservice* wchodzący w skład zestawu *Pstools* firmy *Sysinternals*. Program *psservice.exe* należy umieścić w tym samym katalogu co skrypt. Trzeba także zarejestrować darmowy obiekt COM *System Scripting Runtime* firmy *Netal* (*http://www.netal.com/ssr.htm*). Obiekt COM rejestruje się za pomocą programu *regsvr32*. Wcześniej trzeba skopiować plik DLL do katalogu *system32*. Należy to zrobić dla wszystkich komputerów, z których chcemy uruchomić skrypt, ale nie trzeba tego robić w komputerach zdalnych. Swoją drogą, polecam szczegółowe zapoznanie się z dokumentacją obu tych doskonałych narzędzi.

## Kod

Pokazany poniżej skrypt należy wpisać w Notatniku (z wyłączonym zawijaniem wierszy) i zapisać z rozszerzeniem *.vbs*, jako *FindNTService.vbs*. Można go również pobrać z witryny *ftp://ftp.helion.pl/przyklady/100SER.ZIP*.

```
' Dennis Abbott - speckled_trout@hotmail.com
' W komputerze, z którego uruchamiamy skrypt, należy najpierw
' zarejestrować w katalogu System32 obiekt COM System Scripting Runtime.
'
' Potrzebne jest także narzędzie psservice.exe z witryny www.sysinternals.com
' należy je skopiować do tego samego katalogu co skrypt. Trzeba także
' utworzyć plik tekstowy zawierający informacje o podsieciach.
' Poszczególne podsieci muszą być rozdzielone znakiem końca wiersza.
'
' przykład listingu podsieci
'
' 192.168.0.0
' 192.168.1.0
' 34.54.78.0
'
' Działanie skryptu można zaobserwować poprzez otwarcie pliku dziennika
' za pomocą przeglądarki dzienników, np. SMS Trace firmy Microsoft.
'
'On Error Resume Next
Option Explicit
Dim Title                  'tytuł okien dialogowych, a także nazwa pliku
dziennika
Dim PathToScript  'ścieżka do katalogu, w którym działa skrypt
Dim PathToLogFile  'pełna ścieżka włącznie z nazwą pliku dziennika
Dim WshShell  'obiekt powłoki
Dim WshNet                  'obiekt sieci
Dim WshFso  'obiekt systemu plików
Dim WshSysEnv                  'obiekt zawierający zmienne środowiskowe
Dim ScriptNet                  'obiekt System Scripting Runtime z witryny
www.netal.com
Dim ComSpec           'ścieżka do programu cmd.exe
Dim DataFile  'plik z nazwami komputerów
Dim LogFile           'plik dziennika z informacjami o stanie
Dim CompName          'nazwa bieżącego zdalnego komputera
Dim User                  'użytkownik zalogowany w zdalnym komputerze
Dim Domain  'domena, do której jest dołączony zdalny komputer
Dim IP  'adres IP zdalnego komputera
Dim CurLine  'zmienna wykorzystywana do przetwarzania plików tekstowych
Dim NbtFile  'plik przetwarzany w celu wyszukania informacji NetBIOS
Dim SubnetFileName          'plik z informacjami o podsieciach
Dim I          'licznik
Dim SysFolder  'folder systemowy
Dim TimeOut  'limit czasu wykonania polecenia ping (w milisekundach)
```

```
Dim Go          'zmienna umożliwiająca zatrzymanie działania skryptu
Dim ServiceToCheck 'nazwa wyszukiwanej usługi--TO NIE JEST NAZWA WYŚWIETLANA
Dim EditSubnets  'zmienna opisująca możliwość edycji pliku podsieci
Dim File  'obiekt plikowy
Dim Subnet  'przeszukiwana podsieć
Dim Service  'stan usługi
Dim ServFile  'plik, w którym są wyszukiwane informacje o usłudze

Set WshShell = CreateObject("WScript.Shell")
Set WshFso = CreateObject("Scripting.FileSystemObject")
Set WshNet = CreateObject("WScript.Network")
Set ScriptNet = CreateObject("SScripting.IPNetwork")

SysFolder = WshFso.GetSpecialFolder(1)
PathToScript = Left(WScript.ScriptFullName,(Len(WScript.ScriptFullName) -
(Len(WScript.ScriptName) + 1)))
Title = "FindNTService"
Set WshSysEnv = WshShell.Environment("SYSTEM")
ComSpec = WshSysEnv("COMSPEC")
Timeout = 125

'pobranie danych wejściowych
Go = MsgBox("Program przeszukuje sieć według podsieci " &_
 "w poszukiwaniu komputerów, w których działa usługa." & vbcrlf & _
 "Aby program mógł działać, należy utworzyć plik tekstowy z informacjami o
podsieciach" & _
 "oraz podać nazwę usługi." & vbcrlf & vbcrlf & "Czy chcesz
kontynuować?",vbyesno,Title)
Select Case Go
        Case VbYes
        Case VbNo Wscript.Quit(0)
End Select
If WshFso.FileExists(PathToScript & "\psservice.exe") <> True Then
        MsgBox "Nie zainstalowano programu PSSERVICE..." & vbcrlf & _
        "Program PSSERVICE można pobrać ze strony www.sysinternals.com",vbok +
         vbcritical, Title
        Wscript.Quit(0)
End If
If WshFso.FileExists(SysFolder & "\sscrrun.dll") <> True Then
        MsgBox "Brak pliku sscrrun.dll..." & vbcrlf & "Można go pobrać ze
strony www.netal.com",vbok + vbcritical, Title
        Wscript.Quit(0)
End If
ServiceToCheck = InputBox("Wprowadź nazwę usługi (nie nazwę wyświetlaną),
której " & _
  "chcesz wyszukiwać.",Title,"w3svc")
If ServiceToCheck = "" Then
        MsgBox "Nie wprowadzono nazwy usługi...",vbok + vbcritical, Title
        Wscript.Quit(0)
End If
SubnetFileName = InputBox("Wprowadź ścieżkę do nazwy pliku zawierającego " & _
"informacje o podsieciach.",Title,PathToScript & "\subnets.txt")
If WshFso.FileExists(SubnetFileName) <> True Then
 MsgBox "Plik z informacjami o podsieciach nie istnieje...", _
 vbok + vbcritical, Title
        Wscript.Quit(0)
End If
EditSubnets = MsgBox("Czy chcesz zmodyfikować plik z informacjami o
podsieciach?",vbyesno,Title)
Select Case EditSubnets
        Case vbyes WshShell.Run "notepad " & SubnetFileName,1,True
        Case vbno
End Select
```

```
PathToLogFile = PathToScript & "\" & Title & "_" & Month(Now) & "_" &
Day(Now) & "_" & Year(Now) & "-" & Hour(Now) & "_" & Minute(Now) & ".log"
Set LogFile = WshFso.CreateTextFile(PathToLogFile)
Set File = WshFso.GetFile(SubnetFileName)
Set DataFile = File.OpenAsTextStream(1,0)
LogFile.WriteLine "Adres IP" & vbtab & "Nazwa komputera" & vbtab & _
"Nazwa logowania" & vbtab & "Domena" & vbtab & "Status"
Do  While Not DataFile.AtEndOfStream
        Subnet = DataFile.ReadLine
        LogFile.WriteLine subnet & vbtab & vbtab & vbtab & vbtab & _
          "rozpoczęto analizę podsieci " & Now
        Discover(subnet)

Loop
MsgBox "Skrypt" & Title & " zakończył działanie.  Plik dziennika zapisano w:" & _
vbcrlf & PathToLogFile

Function Discover(boundary)
        Subnet = Left(boundary,InstrRev(boundary,"."))
        For i = 1 to 254
                IP = subnet & i
                CompName = Null
                User = Null
                Domain = Null
                Curline = Null
                Service = Null
                If ScriptNet.Ping(ip,,,Timeout) <> 0 Then
                        LogFile.WriteLine IP & vbtab & vbtab & vbtab & vbtab _
          & "UnPingableClient"
                Else
                        CompName = ScriptNet.DNSlookup(IP)
                        If InStr(CompName,".") <> 0 Then
                                CompName = Left(CompName,InStr(CompName,".")-1)
                        End If
                        Call GetNBTstat(IP,User,Domain)
                                Call GetService(IP, Service)
                        Call WriteToLog(IP,CompName,User,Domain,Service)
                End If
        Next
End Function

Function GetNBTstat(IP,User,Domain)
       WshShell.Run ComSpec & " /c nbtstat -a " & IP & " >" & PathToScript & _
 "\nbt.txt",6,True
        Set NbtFile = WshFso.OpenTextFile(PathToScript & "\nbt.txt", 1, True)
        Do While NbtFile.AtEndOfStream <> True
                CurLine = NbtFile.ReadLine
                If InStr(CurLine,"---") <> 0 Then
                        CurLine = NbtFile.ReadLine
                        CompName = Trim(Left(CurLine,InStr(CurLine,"<")-1))
                End If
                If InStr(CurLine,"<03>") <> 0 Then
                    If Trim(Left(CurLine,InStr(CurLine,"<03>")-1)) <> _
          UCase(CompName) and Trim(Left(CurLine,InStr(CurLine,"<03>")-1)) <> _
          UCase(CompName) & "$" Then
                                User =
                                Trim(Left(CurLine,InStr(CurLine,"<03>")-1))
                        End If
                End If
                If InStr(CurLine,"<1E>") <> 0 Then
                        If Trim(Left(CurLine,InStr(CurLine,"<1E>")-1)) <> _
          UCase(CompName) and Trim(Left(CurLine,InStr(CurLine,"<1E>")-1)) <> _
```

```
          UCase(CompName) & "$" Then
                                Domain =
                                Trim(Left(CurLine,InStr(CurLine,"<1E>")-1))
                        End If
                End If
        Loop
        NbtFile.Close
End Function

Function GetService(IP,Service)
        If CompName <> "" and User <> "" or Domain <> "" Then
             WshShell.Run ComSpec & " /c " & PathToScript & "\psservice  \\" _
      & IP & " query " & Chr(34) & ServiceToCheck & Chr(34) & " >" _
      & PathToScript & "\service.txt",6,True
                Set ServFile = WshFso.OpenTextFile(PathToScript _
      & "\service.txt", 1, True)
                Do While ServFile.AtEndOfStream <> True
                        CurLine = ServFile.ReadLine
                        If InStr(CurLine,"STATE") <> 0 Then
                                Service = Trim(Right(CurLine,InStr(CurLine,"
                               ")-1))
                        End If
                        If InStr(CurLine,"RPC") <> 0 Then
                                Service = CurLine
                        End If
                        If InStr(CurLine,"Access") <> 0 Then
                                Service = CurLine
                        End If
                        If InStr(CurLine,"function") <> 0 Then
                                Service = CurLine
                        End If
                        If InStr(CurLine,"Unable") <> 0 Then
                                Service = CurLine
                        End If
                Loop
                If InStr(Service,vbcr) <> 0 Then
                        Service = Left(Service,InStr(Service,vbcr)-1)
                End If
        End If
End Function

Function WriteToLog(IP,CompName,User,Domain,Service)
        If IP <> "" Then
                LogFile.Write IP
        End If
        LogFile.Write vbtab
        If CompName <> "" Then
                LogFile.Write CompName
        End If
        LogFile.Write vbtab
        If User <> "" Then
                LogFile.Write User
        End If
        LogFile.Write vbtab
        If Domain <> "" Then
                LogFile.Write Domain
        End If
        LogFile.Write vbtab
        If Service <> "" Then
                LogFile.Write Service
        End If
        LogFile.WriteLine
End Function
```

## Wykorzystanie sposobu

Najpierw należy utworzyć plik tekstowy zawierający informacje o podsieciach, w których chcemy wyszukiwać uruchomione usługi. Adres każdej podsieci powinien kończyć się ciągiem *.0* i być wpisany jako osobny wiersz w pliku. Plikowi można nadać nazwę *subnets.txt* i zapisać w tym samym katalogu, w którym zapisano skrypt. Następnie należy uruchomić skrypt. Wyświetli się szereg okien dialogowych, w których należy podać dane wejściowe. Pierwsze okno dialogowe zawiera opis skryptu. Kliknięcie przycisku *Nie* spowoduje zakończenie jego działania.

W kolejnym oknie dialogowym należy podać nazwę usługi. Nie chodzi tu o nazwę wyświetlaną, a zatem trzeba na to zwrócić uwagę. W tabeli 8.3 zaprezentowano przykłady usług, których nazwa wyświetlana znacznie różni się od nazwy usługi. Skrypt umożliwia wykrycie nieuprawnionych serwerów WWW działających w sieci, komputerów klienckich, w których zablokowano oprogramowanie antywirusowe, a także komputerów z wyłączonym oprogramowaniem klienckim SMS. W przypadku tych ostatnich instalacja uaktualnień bezpieczeństwa oraz dodatków *Service pack* jest znacznie utrudniona.

*Tabela 8.3. Nazwy wyświetlane oraz odpowiadające im nazwy usług*

| Nazwa wyświetlana | Nazwa usługi |
|---|---|
| World Wide Web Publishing Service | w3svc |
| Horton Antivirus Client | Norton Antivirus Server |
| SMS Client Service | clisvc |

Następnie wyświetla się pytanie o pełną ścieżkę dostępu do pliku tekstowego z informacjami o podsieciach. Po podaniu nazwy wyświetla się pytanie o to, czy chcemy modyfikować plik z informacjami o podsieciach. Skanowanie rozpoczyna się po kliknięciu przycisku *Nie* lub zamknięciu Notatnika. Po zakończeniu działania skryptu wyświetli się komunikat informujący o położeniu pliku z wynikami. W czasie działania skryptu nie wyświetla się wskaźnik postępu zadania. Aby anulować skrypt należy przejść do *Menedżera zadań* i zniszczyć proces *wscript.exe*.

Osobiście wykorzystywałem skrypt do wyszukiwania komputerów, w których wyłączono usługę *SMS Client Service*. Dzięki niemu znalazłem także kilka serwerów IIS oraz ich właścicieli. Narzędzie pomogło mi również odnaleźć usługę FLC, lepiej znaną jako wirus *FunLove*. Dzięki skryptowi mogłem przesłać kierownictwu długą listę komputerów z wirusem FunLove, wyłączoną obsługą SMS oraz nieaktywną ochroną antywirusową.

Przed użyciem skryptu w realnych warunkach należy przetestować go w warunkach laboratoryjnych i oszacować czas jego działania.

*— Dennis Abbott*

SPOSÓB 74.

# Zapewnienie dostępu administracyjnego do kontrolera domeny

W tym punkcie opisano sposób zabezpieczenia kontrolerów domeny działających w zdalnej sieci.

Wprowadzenie usługi Active Directory znacznie skomplikowało zarządzanie serwerami i zabezpieczeniami. Na przykład, aby udzielić administratorowi zdalnego ośrodka uprawnień do instalacji oprogramowania bądź usług w kontrolerze domeny, należy mu nadać uprawnienia administratora domeny. Wiadomo, że administrator domeny ma uprawnienia do tworzenia nowych kont użytkowników z uprawnieniami administratora. Jest oczywiste, że taka sytuacja jest daleka od idealnej.

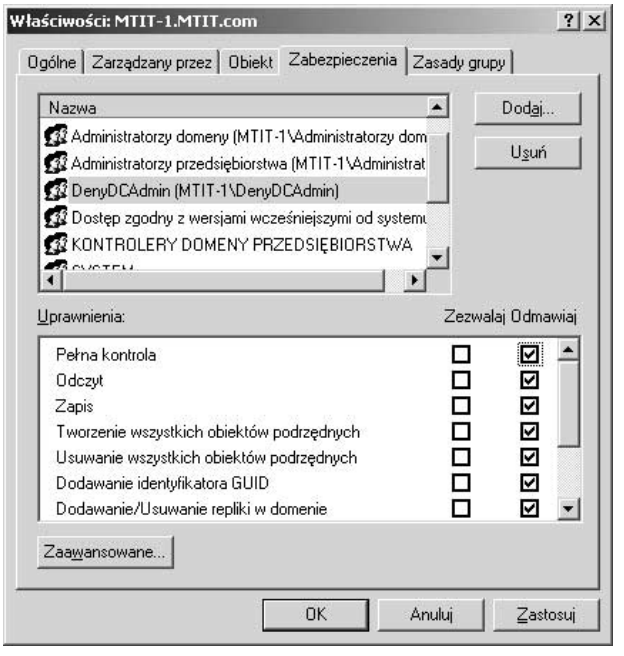
Poniżej zaprezentowano sposób udzielenia osobie uprawnień równych uprawnieniom administratora serwera członkowskiego bądź stacji roboczej w kontrolerze domeny, z jednoczesnym zablokowaniem dostępu do usługi Active Directory.

Należy pamiętać, że zastosowanie sposobu opisanego w tym punkcie nie eliminuje wszystkich możliwych zagrożeń bezpieczeństwa, a użytkownicy, którym udziela się opisanych uprawnień, muszą być zaufani.

1. Zalogować się w kontrolerze domeny z pełnymi uprawnieniami administratora. Należy się upewnić, czy domena Active Directory jest w trybie macierzystym.
2. W programie *Użytkownicy i komputery usługi Active Directory* utworzyć globalną grupę zabezpieczeń o nazwie *DCAdmins*. Dodać do niej użytkowników (grupy), którzy potrzebują dostępu do kontrolera domeny z uprawnieniami administratora.
3. Utworzyć inną globalną grupę zabezpieczeń o nazwie *DenyDCAdmins*.
4. Dodać grupę *DCAdmins* do grupy *DenyDCAdmins*.
5. W programie *Użytkownicy i komputery usługi Active Directory* kliknąć prawym przyciskiem myszy nazwę domeny i wybrać *Właściwości*. Kliknąć zakładkę *Zabezpieczenia* (jeśli nie jest dostępna, przejść do menu *Widok* i wybrać opcję *Zaawansowane*).
6. Kliknąć przycisk *Dodaj* i wybrać grupę *DenyDCAdmins*. Po wybraniu grupy, kliknąć pole wyboru *Odmawiaj* obok pozycji *Pełna kontrola* w obszarze *Uprawnienia* tak, jak pokazano na rysunku 8.4.

Od tej pory wszyscy użytkownicy (i grupy) należący do grupy *DCAdmins* będą mieli pełne prawa administracyjne do wszystkich kontrolerów domeny, ale nie będą mieć dostępu do usługi Active Directory.

Użytkownicy należący do grupy *DenyDCAdmins* nie będą nawet mieć uprawnień do przeglądania katalogu Active Directory i nadawania uprawnień do udziałów lub plików. Najlepiej, jeśli użytkownicy ci będą mieli dwa konta: jedno służące do administracji kontrolerów domen i drugie do codziennego użytku.




*Rysunek 8.4. Odbieranie uprawnień pełnej kontroli dla członków globalnej grupy zabezpieczeń DenyDCAdmins*

Jest to doskonały sposób ograniczenia praw zdalnym administratorom oraz grupom roboczym, które powinny mieć uprawnienia do wprowadzania zmian w kontrolerach domen. Polecam zastosowanie tego sposobu zamiast definiowania w usłudze Active Directory niepotrzebnych administratorów domen.

*— Tim Mintner*

SPOSÓB 75.

## Bezpieczne kopie zapasowe

Zabezpieczenie najważniejszych informacji poprzez ograniczenie liczby użytkowników posiadających uprawnienia do tworzenia kopii zapasowych i odtwarzania.

W małych firmach za tworzenie kopii zapasowych i odtwarzanie danych na serwerach jest odpowiedzialny jeden administrator, natomiast w dużych przedsiębiorstwach częściej uprawnienia administracyjne są podzielone na wiele grup. W systemach Windows 2000 oraz Windows Server 2003 są specjalne wbudowane grupy służące do tego celu. W tym punkcie pokażemy jednak, że utworzenie własnych grup pozwala na zapewnienie większej kontroli nad tym, kto może tworzyć kopie zapasowe i odtwarzać dane.

### Operatorzy kopii zapasowych

W systemach Windows 2000 oraz Windows Server 2003 są dwie grupy operatorów kopii zapasowych: grupa lokalna oraz grupa lokalna domeny. Jakie są różnice pomiędzy nimi?

Grupy lokalne są zdefiniowane w bazie danych SAM na serwerze członkowskim bądź stacji roboczej, natomiast lokalne grupy domeny w usłudze Active Directory w kontrolerach domen. W efekcie, na serwerach członkowskich i stacjach roboczych jest wbudowana grupa lokalna pod nazwą *Operatorzy kopii zapasowych*, a jej członków można dodawać za pomocą folderu *Użytkownicy i grupy lokalne* konsoli *Zarządzanie komputerem*.

W kontrolerach domen również jest wbudowana lokalna grupa domeny pod nazwą *Operatorzy kopii zapasowych*. Jej członków można dodawać bądź usuwać za pomocą konsoli *Użytkownicy i grupy usługi Active Directory* (grupa znajduje się wewnątrz wbudowanego kontenera dla każdej z domen).

W oknach dialogowych interfejsu GUI lokalna grupa domeny *Operatorzy kopii zapasowych* jest oznaczona jako wbudowana grupa lokalna, a nie jako wbudowana grupa lokalna domeny. Jest to błąd.

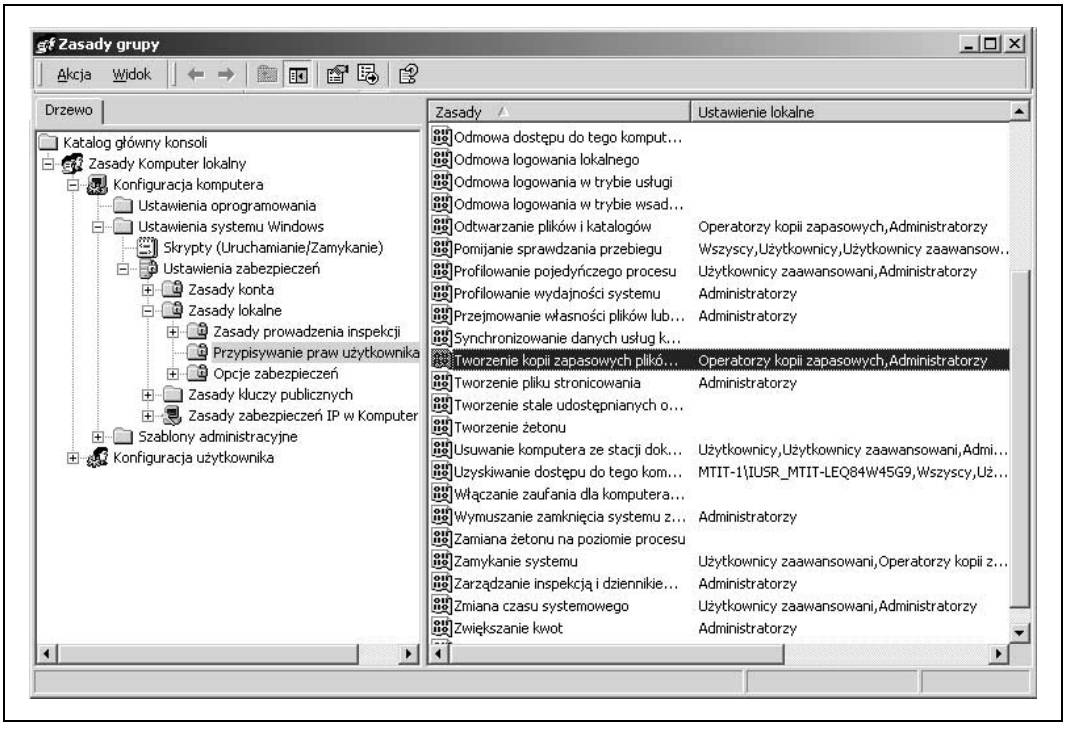
A zatem, jakie uprawnienia mają członkowie grupy *Operatorzy kopii zapasowych*? Przede wszystkim mogą tworzyć kopie zapasowe wszystkich plików i folderów na serwerze, na którym zdefiniowano grupę. Oznacza to, że użytkownik grupy *Operatorzy kopii zapasowych* na serwerze członkowskim może tworzyć kopie zapasowe i odtwarzać pliki wyłącznie na tym serwerze członkowskim. Jeśli zaś należy do grupy *Operatorzy kopii zapasowych* na kontrolerze domeny, może tworzyć kopie zapasowe i odtwarzać pliki na dowolnym serwerze domeny. Operatorzy kopii zapasowych mogą także wykonywać kilka innych zadań, takich jak interaktywne logowanie się na konsoli serwera oraz zamykanie serwera. Z kolei członkowie wbudowanej grupy *Operatorzy serwera* mogą wykonywać wszystkie czynności dozwolone dla grupy *Operatorzy kopii zapasowych* oraz dodatkowo tworzyć i zarządzać udostępnionymi folderami i drukarkami.

A zatem, kto należy do grupy *Operatorzy kopii zapasowych*? Domyślnie nikt. Jest tak dlatego, że uprawnienia użytkowników należących do tej grupy są bardzo duże — tworzenie kopii najważniejszych danych i odtwarzanie ich w innych komputerach. Trzeba zatem dwa razy pomyśleć, zanim nadamy komuś takie uprawnienia.

W jaki sposób operatorzy kopii zapasowych uzyskują tak duże możliwości? Poprzez nadane im uprawnienia. Uprawnienia oznaczają autoryzację lub przywilej do wykonywania pewnych działań. Przypisuje się je za pomocą *Zasad grupy* (w środowisku z usługą Active Directory) lub przystawki *Zasady zabezpieczeń lokalnych* (w samodzielnych serwerach grup roboczych). W obiekcie zasad grupy uprawnienia użytkowników definiuje się w następującej lokalizacji: *Konfiguracja komputera/Ustawienia systemu Windows/Ustawienia zabezpieczeń/Zasady lokalne/Uprawnienia użytkowników* (rysunek 8.5).

Domyślnie wbudowanym grupom *Operatorzy kopii zapasowych* oraz *Administratorzy* przypisuje się następujące uprawnienia:

- Wykonywanie kopii zapasowych plików i folderów;
- Odtwarzanie plików i folderów.




*Rysunek 8.5. Uprawnienia użytkowników wyświetlane w przystawce Zasady grupy*

W kontrolerach domen grupa *Operatorzy serwera* domyślnie także ma takie uprawnienia. Interesujące, że te dwa uprawnienia przesłaniają uprawnienia NTFS nadane plikom i katalogom. W związku z tym, nawet jeśli grupie *Operatorzy kopii zapasowych* jawnie odbierze się uprawnienia odczytu do folderu, członkowie tej grupy w dalszym ciągu będą mogli tworzyć kopie zapasowe folderu i jego zawartości. Mówiąc inaczej, uprawnienia użytkowników mają wyższy priorytet od uprawnień NTFS.

Istnieje sposób umożliwienia użytkownikom tworzenia kopii zapasowych plików i folderów w komputerze, bez nadawania im poprzednio wymienionych uprawnień. Należy tylko nadać im co najmniej poniższe uprawnienia NTFS:

- Przechodzenie przez folder/Wykonywanie pliku;
- Wyświetlanie zawartości folderu/Odczyt danych;
- Odczyt atrybutów;
- Odczyt atrybutów rozszerzonych;
- Odczyt uprawnień.

Metodę tę można zastosować w celu stworzenia użytkownikom możliwości tworzenia kopii zapasowych istotnych dokumentów w lokalnych folderach ich stacji roboczych. Dzięki nadaniu powyższych uprawnień, użytkownicy mogą tworzyć kopie zapasowe folderów,

choć nie mogą czytać plików, które są w nich zapisane. Sens tego rozwiązania polega na tym, że można w ten sposób, ze względów bezpieczeństwa, ograniczyć uprawnienia użytkowników do niezbędnego minimum. W ten sposób można ograniczyć potencjalne straty w przypadku przejęcia kont użytkowników przez intruza. Choć to dość skomplikowane podejście, pozwala zabezpieczyć się na wypadek ataku.

## Ograniczenie dostępu do kopii zapasowych

W planach awaryjnego odtwarzania stosowanych w firmach często nie dostrzega się faktu, że te osoby, które wykonują kopie zapasowe, niekoniecznie muszą być tymi, którzy odtwarzają z nich dane w przypadku awarii. Zadanie wykonywania kopii zapasowej jest rutynowe. Najlepiej wyznaczyć do niego jedną osobę odpowiedzialną za wykonywanie kopii zapasowej w regularnych odstępach czasu. Z kolei odtwarzanie danych daje użytkownikowi prawa dostępu do danych zapisanych w kopii zapasowej. W związku z tym, może dojść do sytuacji, że haker odtworzy kopię zapasową na przejętym serwerze i poprzez uruchomienie odpowiednich narzędzi ujawni kluczowe informacje osobom postronnym.

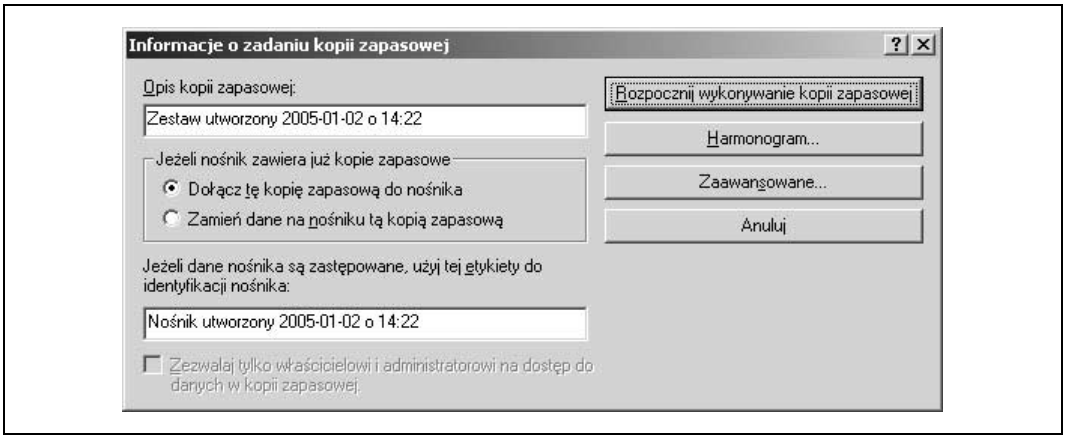
Rozdzielenie uprawnień tworzenia kopii zapasowych i odtwarzania jest możliwe dzięki zignorowaniu wbudowanej grupy *Operatorzy kopii zapasowych* i utworzeniu zamiast niej dwóch nowych grup zabezpieczeń. Można nadać im dowolne opisowe nazwy, na przykład *Kopie zapasowe* oraz *Odtwarzanie*. Następnie należy nadać uprawnienia *Tworzenie kopii zapasowych plików i katalogów* grupie *Kopie zapasowe* oraz uprawnienie *Odtwarzanie plików i katalogów* grupie *Odtwarzanie*. Tym dwóm grupom nie należy nadawać żadnych innych uprawnień.

Następnie należy do każdej z grup dodać użytkowników. Zazwyczaj grupa *Kopie zapasowe* powinna być obszerniejsza od grupy *Odtwarzanie*. Należy do niej przypisać zarówno młodszych administratorów (odpowiedzialnych za rutynowe wykonywanie kopii zapasowych), jak i starszych administratorów (którzy pełnią kluczowe role w sieci i zajmują się rozwiązywaniem problemów w przypadku awarii). Oczywiście młodsi administratorzy nie powinni należeć do domyślnej grupy *Administratorzy domeny*. Jeśli będą do niej należeć, automatycznie uzyskają uprawnienie *Odtwarzanie plików i katalogów*.

Do grupy *Odtwarzanie* powinni należeć wyłącznie starsi administratorzy — najbardziej zaufani pracownicy działu informatyki firmy. To, czy wszystkie te osoby powinny być administratorami domen, jest odrębną kwestią. Wiadomo jednak, że przynależność do grupy *Administratorzy domeny* powinna być ograniczona do jak najwęższej grupy osób, które powinny być starannie sprawdzone podczas procesu rekrutacji. Tak jak jedno zgniłe jabłko psuje zawartość całego koszyka, tak jeden skorumpowany administrator może spowodować katastrofę w naszej firmie.

Jeśli po przypisaniu grupie uprawnień *Tworzenie kopii zapasowej plików i katalogów* okaże się, że niektórzy użytkownicy należący do tej grupy nie mogą tworzyć kopii zapasowych wybranych woluminów, należy sprawdzić, czy przyczyną tych trudności nie są zdefiniowane limity dyskowe do tych woluminów.

Innym sposobem zabezpieczania kopii zapasowych jest skorzystanie z ustawienia dostępnego w oknie dialogowym *Informacje o zadaniu kopii zapasowej* (patrz rysunek 8.6), które wyświetla się po uruchomieniu narzędzia *Kopia zapasowa*. Należy wybrać w nim woluminy lub foldery, których kopię zapasową chcemy utworzyć, a następnie kliknąć przycisk *Rozpocznij wykonywanie kopii zapasowej*. Dzięki zaznaczeniu pola wyboru *Zezwalaj tylko właścicielowi i administratorowi na dostęp do danych kopii zapasowej*, tylko osoba, która utworzyła kopię zapasową, oraz domyślny administrator może odtworzyć z niej dane.




*Rysunek 8.6. Zezwolenie na odtwarzanie kopii zapasowej tylko jej właścicielowi i administratorowi*

Choć zastosowanie tego sposobu jest łatwiejsze od opisanego wcześniej, nie zapewnia tego samego poziomu bezpieczeństwa. Dodatkowo, sposób ten można wykorzystać tylko w przypadku tworzenia kopii zapasowej na nowej taśmie lub nadpisywania zawartości starej. Wspomniane ustawienie nie jest dostępne w przypadku dołączania kopii zapasowej na taśmie, na której poprzednio zapisano inne kopie zapasowe. Mówiąc inaczej, ograniczenie powodowane włączeniem tej opcji można stosować dla poszczególnych taśm, a nie zadań tworzenia kopii zapasowych. W związku z niższym poziomem bezpieczeństwa oraz niewygodą użytkowania, polecam stosowanie sposobu polegającego na zdefiniowaniu dwóch grup.

SPOSÓB 76.

## Wyszukiwanie komputerów z włączoną opcją automatycznego logowania

Włączenie opcji automatycznego logowania w komputerze stwarza zagrożenie dla jego bezpieczeństwa. W tym punkcie pokazano, w jaki sposób można dowiedzieć się, w których komputerach w sieci włączono tę opcję.

Choć włączenie opcji automatycznego logowania czasami się przydaje **[Sposób 4.]** — na przykład do testowania sieci — stwarza zagrożenie dla bezpieczeństwa. Jest tak szczególnie wtedy, kiedy opcję tę włączono bez wiedzy administratora sieci. W tym punkcie pokazano prosty sposób wyszukania wszystkich komputerów, w których w rejestrze Windows włączono opcję automatycznego logowania.

Należy przygotować następujące elementy:

- Program *regfind.exe*, dostępny w zestawach *resorce kit* systemów Windows NT/2000.
- Listę komputerów do sprawdzenia. Można ją utworzyć w dowolny sposób (za pomocą raportu serwera SMS, programu *Menedżer serwerów* itp.). Listę należy zapisać w postaci zwykłego tekstu w pliku o nazwie *serverlist.txt* o następującym formacie:

```
serwer1
serwer2
serwer3
serwer4
…
```

- Konto użytkownika z uprawnieniami administracyjnymi do Rejestru sprawdzanych komputerów. Może nim być, na przykład, konto administratora domeny.

Utworzymy plik wsadowy, który będzie przetwarzał listę i uruchamiał narzędzie *regfind.exe*. W pliku skorzystamy z polecenia DOS — `FOR` (całe polecenie w jednym wierszu — w tej książce z konieczności zostało przedstawione w kilku wierszach):

```
for /F %%A in (serverlist.txt) do (regfind.exe -m \\%%A -p "hkey_local_
machine\software\microsoft\windows nt\currentversion\winlogon" -n
"Autoadminlogon" >results.txt)
```

Jak łatwo zauważyć, działanie pliku wsadowego polega na przetwarzaniu pliku *serverlist.txt* — pobieraniu kolejno nazw serwerów i wywoływaniu polecenia *regfind.exe* w celu odnalezienia klucza Rejestru. Są jednak dwie uwagi. Po pierwsze, czytanie wyników wyświetlanych w czasie wykonywania wyszukiwania jest trudne. Najlepiej skierować wynik w formie potoku do pliku tekstowego (tak jak w powyższej instrukcji). Po drugie, program *regfind* odróżnia małe litery od wielkich. Z tego powodu wyszukiwanie trwa dłużej, choć odpowiednie przygotowanie pliku wsadowego nie jest trudne. Zamiast pojedynczego wiersza trzeba w nim zapisać kilka (prawie identycznych) wierszy. Oto przykład pliku wsadowego:

```
for /F %%A in (serverlist.txt) do (regfind.exe -m \\%%A -p
"hkey_local_machine\software\microsoft\windows nt\currentversion\winlogon" -n
"Autoadminlogon" >results.txt)
for /F %%A in (serverlist.txt) do (regfind.exe -m \\%%A -p
"hkey_local_machine\software\microsoft\windows nt\currentversion\winlogon" -n
"AutoadminLogon" >results.txt)
for /F %%A in (serverlist.txt) do (regfind.exe -m \\%%A -p
"hkey_local_machine\software\microsoft\windows nt\currentversion\winlogon" -n
"AutoAdminlogon" >results.txt)
for /F %%A in (serverlist.txt) do (regfind.exe -m \\%%A -p
"hkey_local_machine\software\microsoft\windows nt\currentversion\winlogon" -n
"AutoAdminLogon" >results.txt)
for /F %%A in (serverlist.txt) do (regfind.exe -m \\%%A -p
"hkey_local_machine\software\microsoft\windows nt\currentversion\winlogon" -n
"autoAdminlogon" >results.txt)
for /F %%A in (serverlist.txt) do (regfind.exe -m \\%%A -p
"hkey_local_machine\software\microsoft\windows nt\currentversion\winlogon" -n
"autoadminlogon" >results.txt)
```

```
for /F %%A in (serverlist.txt) do (regfind.exe -m \\%%A -p
"hkey_local_machine\software\microsoft\windows nt\currentversion\winlogon" -n
"autoAdminLogon" >results.txt)
for /F %%A in (serverlist.txt) do (regfind.exe -m \\%%A -p
"hkey_local_machine\software\microsoft\windows nt\currentversion\winlogon" -n
"autoadminLogon" >results.txt)
```

Za pomocą zaprezentowanej metody można stosunkowo szybko znaleźć stacje robocze i serwery, w których Rejestrach ustawiono opcję automatycznego logowania.

## Wykorzystanie sposobu

Procedurę opisaną w tym punkcie można z łatwością zmodyfikować w celu wyszukiwania innych kluczy Rejestru. Wystarczy zmienić nazwę wyszukiwanego klucza.

*— Donnie Taylor*

SPOSÓB 77.

# Najczęściej zadawane pytania dotyczące bezpieczeństwa

Rod Trent, dyrektor wykonawczy witryny myITforum.com prezentuje swoje odpowiedzi na często zadawane pytania dotyczące bezpieczeństwa.

W witrynie *myITforum.com* (*http://www.myitforum.com*) często pojawiają się pytania dotyczące ogólnych zagadnień związanych z bezpieczeństwem sieci. Odpowiedzi na te pytania publikuję w witrynie w formie listy FAQ. W tym punkcie zaprezentowałem kilka najczęstszych pytań wraz z moimi odpowiedziami. Więcej porad dotyczących bezpieczeństwa sieci można znaleźć w witrynie *myITforum.com*.

## Sposoby na komputerowe bezpieczeństwo

**P**: Co można zrobić, aby mieć pewność, że komputery są bezpieczne?

**O**: To zależy od skali. Inaczej jest w przypadku indywidualnych użytkowników, a inaczej w przypadku firm.

**Użytkownicy indywidualni.** Przede wszystkim, należy zainstalować zaporę firewall zabezpieczającą połączenia z internetem we wszystkich komputerach PC i laptopach. Taka zapora znacznie utrudnia intruzom dostanie się do komputerów w naszej sieci poprzez internet. W przypadku systemu Windows XP można wykorzystać wbudowaną zaporę firewall. Trzeba tylko włączyć tę własność. Należy także regularnie aktualizować system operacyjny. Można to robić za pomocą opcji Automatycznej aktualizacji lub poprzez regularne odwiedzanie witryny WWW Windows Update i pobieranie najnowszych uaktualnień bezpieczeństwa. Należy także dbać o aktualność baz sygnatur systemu antywirusowego. Zainstalowanie, właściwe skonfigurowanie i odpowiednia pielęgnacja oprogramowania antywirusowego ma znaczenie kluczowe.

**Firmy.** W firmach należy stosować podobne, choć nieco bardziej rozbudowane zabezpieczenia. Przede wszystkim, należy sprawdzić konfigurację zapór firewall zarówno w sieci internet, jak intranet. Dzięki audytowi konfiguracji zapór firewall można upewnić się,

czy konfiguracje te są zgodne z polityką bezpieczeństwa firmy. Zapory firewall są pierwszą linią obrony. W związku z tym, najlepiej zablokować wszystkie porty, które nie są wykorzystywane przez aplikacje. Należy także zadbać o to, aby pracownicy przestrzegali wskazówek firmy Microsoft (*http://www.microsoft.com/protect/*) zarówno w ich komputerach stacjonarnych, jak laptopach, w szczególności, jeśli używają tych komputerów do podłączania się do sieci firmowej. Komputery PC i laptopy, które łączą się z siecią firmy z wykorzystaniem technologii VPN bądź RAS, powinny być chronione przez odpowiednio skonfigurowane zapory firewall.

W firmach należy także zadbać o instalację najnowszych uaktualnień bezpieczeństwa, dostępnych w witrynie firmy Microsoft. W tym celu można zarejestrować się w darmowej usłudze powiadamiania firmy Microsoft (*Security notification service*) i skorzystać z usług aktualizacji umożliwiających automatyczne pobieranie uaktualnień sieciowych. Więcej informacji na ten temat można znaleźć w punkcie „Narzędzia zabezpieczeń firmy Microsoft" **[Sposób 78.]**. Firmy muszą także zainwestować w oprogramowanie antywirusowe. Programy te mają absolutnie kluczowe znaczenie dla zabezpieczenia danych przed napastnikami.

## Rodzaje słabych punktów

**P**: Jakie są typy słabych punktów, które należy monitorować?

**O**: Są trzy zasadnicze typy słabych punktów:

*Działania administratora*
: Brak stosowania właściwych praktyk — na przykład korzystanie z łatwych do odgadnięcia haseł lub logowanie się do kont, które mają większe uprawnienia, niż jest to potrzebne do wykonania określonego zadania.

*Słabe punkty programów*
: Błędy w programach stwarzające zagrożenia bezpieczeństwa. Listy takich błędów są publikowane w biuletynach dotyczących bezpieczeństwa. Błędy takie poprawia się poprzez instalację poprawek hotfix lub uaktualnień *Service pack*.

*Słabe punkty fizycznych zabezpieczeń*
: Brak właściwych zabezpieczeń fizycznych komputera — na przykład pozostawienie niezabezpieczonej stacji roboczej w miejscu, które jest dostępne dla nieuprawnionych osób, pozostawienie otwartego pokoju serwerów, zagubienie laptopa lub pozostawienie go u klienta.

## Polityka stosowania „silnych haseł"

**P**: Jakie należy stosować zasady podczas tworzenia haseł użytkowników?

**O**: Wymagany poziom zabezpieczeń w każdej firmie jest inny, ale ogólnie rzecz biorąc, „silne hasło" to takie, które składa się z co najmniej sześciu znaków, nie zawiera fragmentu (lub całości) nazwy konta użytkownika oraz zawiera co najmniej trzy z czterech następujących kategorii znaków: wielkich liter, małych liter, cyfr, symboli niealfanumerycznych dostępnych z klawiatury, np. !, @ oraz #.

## W jaki sposób firma Microsoft zapewnia bezpieczeństwo?

**P**: Czy istnieje dokumentacja opisująca sposoby zabezpieczeń przed wirusami i robakami stosowane przez firmę Microsoft?

**O**: Tak. Firma Microsoft opublikowała artykuł *Security At Microsoft* poświęcony zagadnieniom bezpieczeństwa (*http://www.microsoft.com/downloads/detail.aspx?FamilyID=73f1ba8e-a15c- 4c05-be87-8d21b1372485*). W dokumencie tym opisano działania grupy *Corporate Security Group* firmy Microsoft, mające na celu zabezpieczenie przed zniszczeniem lub nieuprawnionym dostępem do zasobów elektronicznych firmy Microsoft. Ochrona tych zasobów odbywa się w ramach formalnego schematu zarządzania ryzykiem, poprzez stosowanie procesów zarządzania ryzykiem, a także dzięki jasnemu sprecyzowaniu ról i zakresu odpowiedzialności określonych osób w firmie. Podstawą tego podejścia jest uznanie ryzyka za integralną część każdego środowiska oraz konieczności jego proaktywnego zarządzania. Zasady i techniki opisane w artykule można zastosować do zarządzania ryzykiem w każdej firmie.

## Zgłaszanie incydentów dotyczących bezpieczeństwa do firmy Microsoft

**P**: W jaki sposób można zgłosić incydent dotyczący bezpieczeństwa lub słaby punkt do firmy Microsoft?

**O**: Użytkownicy, którzy zakupili usługę pomocy technicznej w firmie Microsoft, powinni skontaktować się z Menedżerem TAM (*Technical Account Manager*). Do zgłoszenia incydentów i słabych punktów można także skorzystać z formularza dostępnego pod adresem *https://s.microsoft.com/technet/security/bulletin/alertus.asp*.

## Zgłaszanie incydentów dotyczących bezpieczeństwa do władz administracyjnych

**P:** Mieliśmy incydent dotyczący bezpieczeństwa. Gdzie go można zgłosić?

**O:** Federalne Biuro Śledcze (FBI) zachęca wszystkich do zgłaszania wszystkich przypadków naruszeń prawa federalnego USA. Nigdy nie należy uznawać problemu naruszenia bezpieczeństwa za nieistotny. Taki incydent może być częścią większego ataku lub początkiem ataku na szerszą skalę. Informacje dotyczące tego zagadnienia można znaleźć pod adresem *http://www.fbi.gov/contact/fo/fo.htm*.

## Uzyskanie poświadczenia bezpieczeństwa[1]

**P**: W jaki sposób ubiegać się o uzyskanie poświadczenia bezpieczeństwa wymaganego do objęcia stanowiska w administracji?

[1] Informacje zawarte w tym punkcie dotyczą USA. W Polsce wydawaniem poświadczeń bezpieczeństwa zajmuje się Urząd Ochrony Państwa oraz Wojskowe Służby Informacyjne — *przyp. tłum*.

**O**: W naszym codziennym biuletynie aktualności w witrynie myITforum.com (*http://www.myitforum.com/newsletter.asp*) czasami publikujemy informacje o wolnych stanowiskach w administracji, przy których jednym ze wstępnych wymagań jest uzyskanie poświadczenia bezpieczeństwa. O sposób uzyskania takiego poświadczenia pytało wiele osób, dlatego na forum Off-Topic (*http://www.topica.com/lists/myOTforum/*) pojawiło się na ten temat wiele interesujących informacji. Oto kilka dodatkowych miejsc, gdzie można znaleźć informacje dotyczące poświadczeń bezpieczeństwa:

FBI Information Sheet (*http://www.fbi.gov/clearance/securityclearance.htm*);

Security Clearance for IT Pros (*http://www.jobcircle.com/career/coach/if_2002_09.html*);

Security Clearances (*http://www.taonline.com/securityclearances/*).

SPOSÓB 78.

## Narzędzia zabezpieczeń firmy Microsoft

Oto przewodnik opisujący różne narzędzia firmy Microsoft ułatwiające zabezpieczenie komputerów przed atakami.

Na liście umieściłem kilka z szerokiego wachlarza narzędzi oferowanych przez firmę Microsoft. Są to programy służące do oceny i skanowania zabezpieczeń, aktualizacji systemów, blokowania, audytu, wykrywania intruzów, ochrony przed wirusami oraz usuwania złośliwego kodu. W punkcie umieściłem także krótką listę dokumentów RFC, z którymi powinien zapoznać się każdy profesjonalista zajmujący się zabezpieczeniami (także ci, którzy korzystają z systemów innych niż Windows).

Listę tę mam zamiar uaktualniać w witrynie myITforum.com (*http://www.myitforum.com*) w miarę pojawiania się nowych pozycji. Sugestie użytkowników dotyczące listy można przesyłać za pomocą poczty elektronicznej, pod adres *myITforum@cinci.rr.com*.

### Narzędzia i usługi do oceny zabezpieczeń, zarządzania uaktualnieniami i aktualizacji oprogramowania

Program *Microsoft Baseline Security Analyzer* (MBSA) — *http://www.microsoft.com/technet/security/tools/Tools/mbsahome.asp* — jest popularnym programem umożliwiającym skanowanie jednego lub kilku komputerów w sieci i wyszukiwanie w nich błędów konfiguracji oraz brakujących uaktualnień bezpieczeństwa.

Usługa aktualizacji oprogramowania (*Software Update Services* — SUS) — *http://www.microsoft.com/windowsserver/system/sus/default.mspx*) upraszcza proces instalacji najnowszych uaktualnień systemów windowsowych. Wskazówki dotyczące stosowania tego narzędzia można znaleźć w punkcie „Najczęściej zadawane na temat usługi aktualizacji oprogramowania" **[Sposób 89.]** w rozdziale 9.

Program *QChain* (*http://support.microsoft.com/default.aspx?scid=KB;EN-US;296861*) umożliwia administratorom instalację kilku uaktualnień jednocześnie bez potrzeby wielokrotnego ponownego uruchamiania komputerów. W celu skorzystania z tego narzędzia należy utworzyć plik wsadowy służący do aktualizacji konfiguracji bezpieczeństwa za pomocą

poprawek *hotfix*. Program QChain nie jest potrzebny w przypadku wykorzystywania systemu Windows 2000 z uaktualnieniem Service Pack 3 lub nowszym albo nowszej wersji systemu Windows (np. Windows XP lub 2003).

Program *Scanning Tool* opisany w artykule bazy wiedzy Microsoft numer 824146 (*http://support.microsoft.com/default.aspx?scid=kb;pl;827363*) służy do wyszukiwania w sieci komputerów, w których nie zainstalowano uaktualnień bezpieczeństwa 823980 (MS03-026) oraz 824146 (MS03-039).

## Narzędzia do automatycznego skanowania i aktualizacji systemów Windows i Office

Częste odwiedzanie witryny *Windows Update* (*http://windowsupdate.microsoft.com*) i pobieranie z niej publikowanych uaktualnień ułatwia zapewnienie aktualności systemu. W witrynie tej następuje skanowanie systemu operacyjnego zainstalowanego w komputerze użytkownika i wyszukiwanie uaktualnień odpowiadających zainstalowanemu systemowi operacyjnemu, programom i sprzętowi. W celu aktualizacji produktów pakietu Office, należy odwiedzić witrynę WWW *Microsoft Office Product Updates* (*http://office.microsoft.com/officeupdate/default.aspx*).

## Blokowanie, audyt i narzędzia do wykrywania intruzów

Kreator blokowania serwera IIS (*http://www.microsoft.com/technet/security/tools/tools.locktool.asp*) pozwala zmniejszyć ryzyko ataku na serwer IIS. Program wykorzystuje narzędzie *URLScan* zapewniające wielowarstwową ochronę przed napastnikami. Narzędzie jest przeznaczone wyłącznie dla serwera IIS5 (Windows 2000). W systemie Windows Server 2003 własność ta jest wbudowana i skorzystanie z niej nie wymaga pobierania dodatkowych programów.

Narzędzie *UrlScan Security Tool* (*http://www.microsoft.com/technet/security/tools/tools/URLScan.asp*) pozwala zabezpieczyć serwery IIS przed potencjalnie szkodliwymi żądaniami HTTP. Narzędzie to również jest przeznaczone głównie dla serwerów IIS5. Większość własności programu UrlScan (choć nie wszystkie) jest wbudowana w serwerze IIS6.

Program *EventCombMT* jest dostępny w witrynie *Security Guide Scripts Download* (*http:// www.microsoft.com/downloads/details.aspx?FamilyID=9989D151-5C55-4BD3-A9D2-B95A15C73E92*).

To wielowątkowe narzędzie analizuje dzienniki zdarzeń wielu serwerów jednocześnie. Jest to bardzo przydatna cecha umożliwiająca wyszukiwanie w dziennikach zdarzeń śladów działania intruzów.

Program *Cipher Security Tool for Windows 2000* (*http://www.microsoft.com/technet/security/tools/tools/cipher.asp*) umożliwia trwałe nadpisywanie usuniętych danych z twardych dysków. Narzędzie to zastępuje polecenie wiersza polecenia cipher, służące do zarządzania szyfrowanym systemem plików EFS (*Encrypted File System*).

## Zabezpieczenia przed wirusami i narzędzia do usuwania infekcji

Uaktualnienie *Office 2000 Update Service Pack 3* (*http://www.microsoft.com/downloads/detail.aspx?FamilyID=5C011C70-47D0-4306-9FA4-8E92D36332FE*) zawiera uaktualnienie bezpieczeństwa *Outlook 2000 SR1 E-mail Security Update* (OESU), które blokuje dostęp użytkownikom do niektórych, potencjalnie niebezpiecznych typów plików wysyłanych jako załączniki e-mail. Uaktualnienie to rozszerza również domyślną strefę zabezpieczeń programu Outlook.

Za pomocą narzędzia SQL Server 2000 Security Tools (*http://www.microsoft.com/downloads/details.aspx?FamilyId=9552D43B-04EB-4AF9-9E24-6CDE4D933600*) można sprawdzić, czy komputer lub sieć są wrażliwe na infekcję robakiem Slammer.

## Najważniejsze dokumenty RFC dotyczące bezpieczeństwa

W tym punkcie znajduje się lista kilku dokumentów RFC (*Request For Comments*), z którymi powinien się zapoznać każdy specjalista w dziedzinie zabezpieczeń. Dokumenty te dotyczą wszystkich korporacyjnych środowisk sieciowych — wyłącznie windowsowych, wyłącznie unikowych oraz mieszanych.

*RFC 2196 Site Security Handbook* (*ftp://ftp.rfc-editor.org/in-notes/rfc2196.txt*)
: Opisuje strategie zabezpieczeń i procedury dla sieci podłączonych do internetu.

*RFC 2504 Users' Security Handbook* (*ftp://ftp.rfc-editor.org/in-notes/rfc2504.txt*)
: Dokument o podobnej tematyce co *Site Security Handbook*, ale przeznaczony dla użytkowników.

*RFC 2350 Expectations for Computer Security Incident Response* (*ftp://ftp.rfc-editor.org/in-notes/rfc2350.txt*)
: Dokument opisuje oczekiwania wobec zespołu specjalistów obsługujących incydenty naruszenia zabezpieczeń.

Dodatkowo warto przejrzeć następujące dokumenty RFC:

*RFC 2828 Internet Security Glossary* (*ftp://ftp.rfc-editor.org/in-notes/rfc2828.txt*)
: Glosariusz pojęć i skrótów dotyczących bezpieczeństwa.

*RFC 2577 FTP Security Considerations* (*ftp://ftp.rfc-editor.org/in-notes/rfc2577.txt*)
: Wskazówki dotyczące bezpiecznej implementacji serwerów FTP.

*RFC 3013 Recommended Internet Service Provider Security Services and Procedures* (*ftp://ftp.rfc-editor.org/in-notes/rfc3013.txt*)
: Dokument opisuje oczekiwania dotyczące zabezpieczeń stosowanych przez dostawców usług internetowych.

*— Rod Trent i Mitch Tulloch*