Bezpieczeństwo w Windows NT/2000.
Ćwiczenia praktyczne

Autor: Piotr Czarny
ISBN: 83-7197-639-9
Format: B5, stron: 114

Z naruszeniem bezpieczeństwa domowego czy firmowego komputera kojarzy się przede wszystkim atak crakerów. Jednak niewielu użytkowników postrzega to zjawisko poprzez nieautoryzowany dostęp do rejestru systemu czy utratę spójności dysku lub kłopoty wynikające ze złych ustawień BIOS-u. Niniejsza książeczka służyć ma lepszemu zrozumieniu koncepcji bezpieczeństwa komputera.

Autor w serii kilkudziesięciu ćwiczeń naucza, jak zabezpieczyć swoje dane przed utratą lub kradzieżą. Z całą pewnością nie wyczerpuje to tematu, ale jest doskonałym zaproszeniem do lektury bardziej zaawansowanych publikacji.

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

Spis treści

Rozdział 5.

Magiczne sztuczki

Taki tytuł rozdziału może się wydawać dziwny w książce o tematyce technicznej. Zmiany, jakie za pomocą edycji *Rejestru* można wprowadzić w systemie operacyjnym, w pełni ten tytuł usprawiedliwiają.

Gdy podczas wykonywania ćwiczenia okaże się, że w *Rejestrze* nie występuje klucz, należy go utworzyć. Jeśli klucz już istnieje, należy nadać mu podaną wartość.

Zmiana ścieżki do plików instalacyjnych

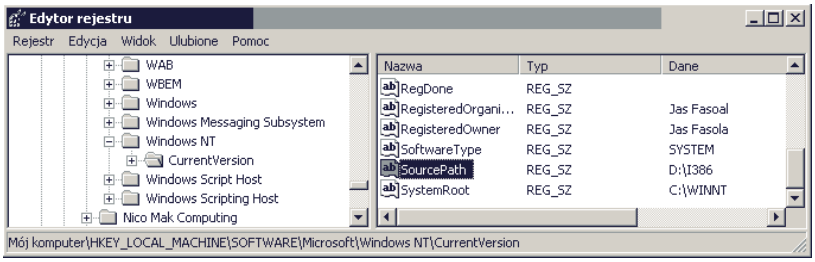
Podczas instalacji Windows 2000 zapisywana jest w Rejestrze ścieżka dostępu do plików źródłowych. Ścieżka ta może ulegać zmianom, na przykład wtedy gdy dodajemy do komputera nową partycję, dysk czy nagrywarkę CD-ROM. W systemie cały czas pozostaje jednak pierwotny zapis. Jest to kłopotliwe, gdyż przy instalowaniu nowych plików są one poszukiwane w pierwotnej lokalizacji. Użytkownik musi wpisywać ich aktualne położenie z klawiatury.

Ćwiczenie 5.1.

Zmień ścieżkę do plików instalacyjnych Windows.

1. Uruchom program *regedit* — patrz ćwiczenie 4.3.
2. Po wyświetleniu okna *Edytor rejestru* rozwiń klucz *HKEY_LOCAL_MACHINE*.
3. Rozwiń kolejno podklucze: *SOFTWARE\Microsoft\Windows NT\CurrentVersion* (rysunek 5.1).

Rysunek 5.1.
Wpis z informacją o ścieżce dostępu do plików źródłowych

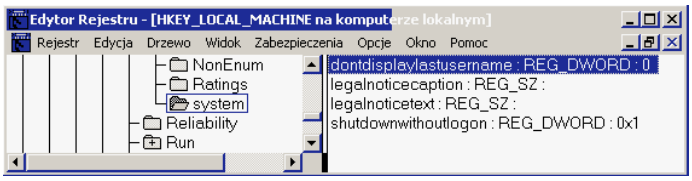


4. Dwukrotnie kliknij wartość *SourcePath*.
5. Po wyświetleniu okna *Edytowanie ciągu* wpisz w polu *Dane wartości* aktualną ścieżkę dostępu do plików instalacyjnych. Jeżeli do komputera dodawane były partycje lub napędy, wystarczy zmienić literę dysku.
6. Kliknij przycisk *OK*.
7. Zamknij okno edytora, wybierając polecenia: *Rejestr*, *Zakończ*.

Ukrywanie nazwy ostatnio zalogowanego użytkownika

Przed wejściem do systemu należy podać nazwę użytkownika oraz aktualne hasło. Domyślnie Windows 2000 pamięta identyfikator użytkownika, który ostatnio się logował. Z punktu widzenia użytkownika jest to wygodne. Trzeba wpisać tylko hasło. Dla włamywacza jest to również ułatwienie, ponieważ i jemu do odgadnięcia pozostaje tylko hasło.

Rysunek 5.2.
Domyślne ustawienia sprzyjają wygodzie użytkownika, a nie bezpieczeństwu systemu



Ćwiczenie 5.2.

Zablokuj wyświetlanie nazwy ostatnio logowanego użytkownika.

1. Uruchom program *regedit* — patrz ćwiczenie 4.3.
2. Po wyświetleniu okna *Edytor rejestru* rozwiń klucz *HKEY_LOCAL_MACHINE*.
3. Rozwiń kolejno podklucze:
   SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system.
4. Wybierz kolejno polecenia: *Edycja*, *Nowy*, *Wartość DWORD*.
5. Po utworzeniu wpisu nadaj mu nazwę *dontdisplaylastusername*.

6. Naciśnij klawisz *Enter*, aby zatwierdzić nową nazwę.
7. Naciśnij powtórnie klawisz *Enter*.
8. Wyświetlone zostanie okno *Edytowanie wartości DWORD*.
9. W polu *Dane wartości* wpisz liczbę *1*.
10. Kliknij przycisk *OK*.
11. Zamknij okno edytora, wybierając polecenia: *Rejestr*, *Zakończ*.

Wyświetlanie komunikatu ostrzegawczego

Jeżeli komputer przeznaczony jest do przetwarzania danych niejawnych, a czynności są rejestrowane, należy ostrzec użytkowników przed wykorzystywaniem systemu np. do celów prywatnych.

Ćwiczenie 5.3.

Włącz wyświetlanie ostrzegawczego komunikatu logowania.

1. Uruchom program *regedt32* — patrz ćwiczenie 4.4.
2. Po wyświetleniu okna *Edytor rejestru* rozwiń klucz *HKEY_LOCAL_MACHINE na komputerze lokalnym*.
3. Rozwiń kolejno podklucze: *SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system*.
4. Wybierz kolejno polecenia: *Edycja*, *Dodaj wartość*.
5. Po wyświetleniu okna *Dodawanie wartości* w polu *Nazwa wartości* wpisz *legalnoticecaption*.
6. Z listy *Typ danych* wybierz *REG_SZ*.
7. Kliknij przycisk *OK*.
8. Po wyświetleniu okna *Edytor ciągu* w polu *Ciąg* wpisz tytuł okna z ostrzeżeniem.
9. Kliknij przycisk *OK*.
10. Wybierz kolejno polecenia: *Edycja*, *Dodaj wartość*.
11. Po wyświetleniu okna *Dodawanie wartości* w polu *Nazwa wartości* wpisz *legalnoticetext*.
12. Z listy *Typ danych* wybierz *REG_SZ*.
13. Kliknij przycisk *OK*.
14. Po wyświetleniu okna *Edytor ciągu* w polu *Ciąg* wpisz tekst ostrzeżenia.
15. Kliknij przycisk *OK*.
16. Zamknij okno edytora, wybierając polecenia: *Rejestr*, *Zakończ*.

Ukrywanie dysków twardych

Jeżeli w komputerze jest więcej niż jeden dysk twardy, wówczas ten, który zawiera cenne dane, można uczynić niewidzialnym. Nie każdy włamywacz będzie rozbierał komputer, aby sprawdzić, ile jest w nim dysków.

Ćwiczenie 5.4.

Ukryj dysk twardy komputera.

1. Uruchom program *regedt32* — patrz ćwiczenie 4.4.
2. Po wyświetleniu okna *Edytor rejestru* rozwiń klucz *HKEY_LOCAL_MACHINE na komputerze lokalnym*.
3. Rozwiń kolejno podklucze: *SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer*.
4. Wybierz kolejno polecenia: *Edycja*, *Dodaj wartość*.
5. Po wyświetleniu okna *Dodawanie wartości* w polu *Nazwa wartości* wpisz *NoDrives*.
6. Z listy *Typ danych* wybierz *REG_DWORD*.
7. Kliknij przycisk *OK*.
8. Po wyświetleniu okna *Edytor ciągu* wpisz liczbę odpowiadającą dyskowi. Dla poszczególnych dysków są to liczby: A — 1, B — 2, C — 4, D — 8 itd.
9. Kliknij przycisk *OK*.
10. Zamknij okno edytora, wybierając polecenia: *Rejestr*, *Zakończ*.

Wyłączanie automatycznego uruchamiania płyt CD

Jeżeli do napędu CD włożona zostanie płyta, która ma możliwość samoczynnego uruchamiania, wówczas mogą zostać z niej załadowane aplikacje. Stwarza to potencjalne zagrożenie dla bezpieczeństwa systemu. Funkcję tę należy wyłączyć.

Wykonanie poniższej zmiany spowoduje zablokowanie samoczynnego uruchamiania płyt muzycznych.

Ćwiczenie 5.5.

Wyłącz automatyczne uruchamianie płyt CD.

1. Uruchom program *regedt32* — patrz ćwiczenie 4.4.

2. Po wyświetleniu okna *Edytor rejestru* rozwiń klucz *HKEY_LOCAL_MACHINE na komputerze lokalnym*.
3. Rozwiń kolejno podklucze: *System\CurrentControlSet\Services\CDRom.*
4. Dwukrotnie kliknij wpis: *Autorun*.
5. Po wyświetleniu okna *Edytor DWORD* w polu *Dane* wpisz wartość *0*.
6. Kliknij przycisk *OK*.
7. Zamknij okno edytora, wybierając polecenia: *Rejestr*, *Zakończ*.