

IDŹ DO

PRZYKŁADOWY ROZDZIAŁ



SPIS TREŚCI

KATALOG KSIĄŻEK

KATALOG ONLINE

ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK

DODAJ DO KOSZYKA

CENNIK I INFORMACJE

ZAMÓW INFORMACJE
O NOWOŚCIACH

ZAMÓW CENNIK

CZYTEL尼亚

FRAGMENTY KSIĄŻEK ONLINE

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

Wstęp.....	9
Autoryzacja dostępu	10
Ustawienia BIOS-u	10
Prawa Murphy'ego, a zmiany w konfiguracji sprzętu	10
Włamania przez Internet	11
Zapory sieciowe	11
Wirusy i programy antywirusowe	11
Programy IDS.....	12
Szyfrowanie danych	13
Wybór hasła	13
Zakres szyfrowania	14
Pretty Good Privacy	15
Nieodwracalne kasowanie danych z dysku	16
Awarie zasilania	17
Uszkodzenia mechaniczne	17
Podział dysku na dwie partycje	18
Defragmentacja danych	20
Kopie zapasowe	21
Rozdział 1. Wybór systemu plików	23
FAT	23
FAT32	24
NTFS 4.	24
NTFS wersja 5.....	24
Rozdział 2. Service Pack.....	27
Sprawdzanie wersji Service Pack.....	27
Instalacja Service Pack.....	28
Rozdział 3. Odtwarzanie aplikacji i systemu operacyjnego	31
Tworzenie awaryjnego dysku naprawczego.....	31
Tworzenie dyskietek startowych	32

Rozdział 4. Zasady edycji Rejestru	39
Kopia zapasowa Rejestru	39
Narzędzia do edycji Rejestru.....	41
Wyszukiwanie kluczy	42
Zapisywanie i odtwarzanie klucza	43
Wyszukiwanie wartości.....	44
Klucze i podklucze Rejestru.....	44
Tworzenie nowego klucza.....	45
Tworzenie nowej wartości	46
Zmiana nazwy klucza.....	47
Zmiana nazwy wartości.....	47
Edycja wartości	48
Usuwanie klucza z Rejestru	48
Usuwanie wartości z Rejestru	49
Eksportowanie Rejestru.....	49
Rozdział 5. Magiczne sztuczki	51
Zmiana ścieżki do plików instalacyjnych	51
Ukrywanie nazwy ostatnio zalogowanego użytkownika	52
Wyświetlanie komunikatu ostrzegawczego	53
Ukrywanie dysków twardych.....	54
Wyłączanie automatycznego uruchamiania płyt CD	54
Rozdział 6. Uprawnienia.....	57
Konta użytkowników	57
Zmiana hasła	59
Uprawnienia do plików	60
Uprawnienia do folderów	64
Rozdział 7. Zapora sieciowa.....	71
Tiny Personal Firewall 2.0	71
Wersja instalacyjna.....	71
Instalacja programu	73
Podstawy protokołu TCP/IP	75
Zasada działania zapory sieciowej.....	78
Wybór poziomu bezpieczeństwa	79
Zabezpieczanie programu hasłem.....	80
Automatyczne uruchamianie programu.....	81
Komunikaty programu.....	81
Tworzenie reguł filtrowania	82
Dodawanie reguły	84
Edycja reguły.....	86
Praca w sieci Microsoft	86
Sygnatury MD5	88
Log programu.....	89

Rozdział 8. Norton AntiVirus	91
Instalacja programu	91
Automatyczna aktualizacja bazy danych	93
Pierwsze skanowanie	94
Okno stanu programu	94
Raporty	96
Opcje pracy programu	97
Dodatkowe narzędzia	102
Usuwanie wirusa	103
Rozdział 9. PGP — czyli całkiem niezła prywatność	105
Instalacja programu	105
Generowanie kluczy	107
Wysyłanie zaszyfrowanej poczty	107
Szyfrowanie plików	108
Rozdział 10. „Wycieranie” danych z dysku	111

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.

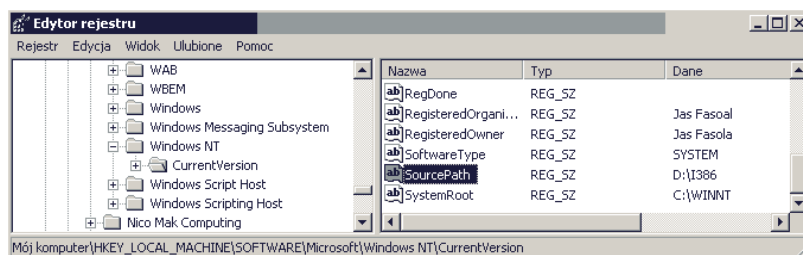
Ćwiczenie 5.1.

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.

Wpisz z informacją
o ścieżce dostępu
do plików źródłowych



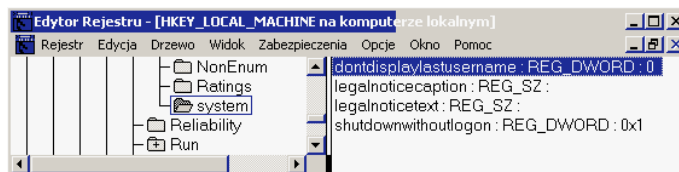
4. Dwukrotnie kliknij wartość *SourcePath*.
5. Po wyświetleniu okna *Edytowanie ciągu* wpisz w polu *Dane wartości* aktualną ścieżkę dostępu do plików instalacyjnych. Jeżeli do komputera dodawane były partycje lub napędy, wystarczy zmienić literę dysku.
6. Kliknij przycisk *OK*.
7. Zamknij okno edytora,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