

MySecureDoc

Ochrona danych na dyskach i pamięciach USB

- **Pełne zabezpieczenie informacji zapisanych na dysku dzięki mocnemu szyfrowaniu**
- **Gwarancja, że poufne dane nigdy nie trafią w niepowołane ręce**
- **Szyfrowanie wszystkich danych bez angażowania użytkownika**

MySecureDoc firmy WinMagic gwarantuje pełne bezpieczeństwo informacjom zgromadzonym na dyskach twardych i pamięciach USB. Olbrzymia skuteczność rozwiązania możliwa jest dzięki metodzie szyfrowania całej powierzchni nośnika, na którym zgromadzono cenne dane.

PEŁNE BEZPIECZEŃSTWO

SecureDoc szyfruje cały dysk, dzięki czemu użytkownik nie musi potem pamiętać o szyfrowaniu zapisywanych na nim zbiorów. Program umożliwia również szyfrowanie pamięci przenośnych USB (pendrive). Dyski są szyfrowane algorytmem AES z 256-bitowym kluczem, co jest jednym z najsilniejszych zabezpieczeń dostępnych na rynku. Algorytm AES został zatwierdzony jako standard szyfrujący na szczeblu federalnym w Stanach Zjednoczonych i w Kanadzie.

NIEWYSTARCZAJĄCE ZABEZPIECZENIA

Na rynku istnieje wiele rozwiązań szyfrujących. Użytkownik może wybrać rozwiązanie do szyfrowania wybranych plików - w takim przypadku po utworzeniu nowego zbioru, który powinien pozostać poufny, należy każdorazowo taki zbiór zaszyfrować. Inną opcją jest tworzenie wirtualnego zaszyfrowanego dysku - wszystkie pliki zapisywane na takim dysku są automatycznie szyfrowane, jednak należy pamiętać, by poufne zbiory zapisywać zawsze wyłącznie na wirtualnym dysku. Pozostawienie jakiegokolwiek kopii poza wirtualnym dyskiem wiąże się z dużym ryzykiem. Niestety obydwie powyższe metody, nawet jeśli skrupulatnie pamiętamy o zapisywaniu danych we właściwych miejscach, tak naprawdę nie gwarantują 100% pewności bezpieczeństwa danych. Dopiero szyfrowanie całego dysku daje optymalny poziom bezpieczeństwa. Dlaczego tak się dzieje? Zagrożenie dla poufności naszych danych wynika ze specyficznych cech działania systemu operacyjnego w naszym komputerze - o czym osoby niezainteresowane na codzień informatyką nie zawsze są poinformowane. Chociażby kasowanie plików poleceniem "usuń" tylko pozornie usuwa pliki z dysku. W rzeczywistości plik pozostaje na dysku, ale jest niewidoczny dla użytkownika korzystającego z komputera.

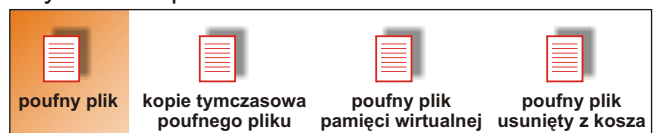
Dlatego też w zależności od wybranego rozwiązania szyfrującego możemy liczyć na różny poziom bezpieczeństwa naszych danych.

DLACZEGO NALEŻY SZYFROWAĆ CAŁY DYSK?

Program Windows zapisując plik umieszcza go w kilku miejscach na dysku:

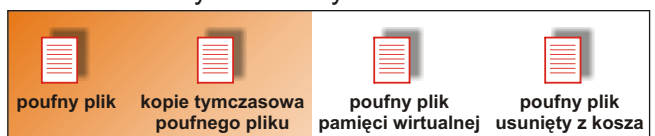
- jako oryginalny plik zapisywany we wskazanym przez nas miejscu,
- jako kopia tymczasowa,
- jako kopia w pamięci wirtualnej (tworzona kiedy brakuje pamięci RAM na przetwarzanie informacji).

Szyfrowanie plików



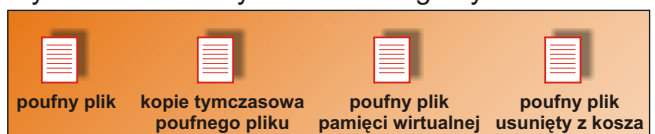
Szyfrowanie plików, pozwala na zaszyfrowanie pliku stworzonego przez użytkownika, ale pozostawia na dysku niezasyfrowane kopie tymczasowe, pliki pamięci wirtualnej oraz pliki teoretycznie usunięte z dysku.

Wirtualne zaszyfrowane dyski



Oprogramowanie tworzące wirtualne, zaszyfrowane dyski, również nie zapewnia pełnego bezpieczeństwa danych ponieważ pozostawia część kopii w formie niezasyfrowanej.

MySecureDoc - szyfrowanie całego dysku



Szyfrowanie całego dysku zabezpiecza wszystkie dane zapisane na dysku, zapewniając maksymalny poziom bezpieczeństwa danych.

MySecureDoc

JAK DZIAŁA SECUREDOK?

Do uruchomienia komputera, na którym jest zainstalowany SecureDoc, niezbędne jest podanie prawidłowej nazwy użytkownika oraz hasła. Dopiero po weryfikacji uruchamia się program Windows, a następnie SecureDoc pracuje w tle, w sposób niezauważalny dla użytkownika. Program pozwala opcjonalnie na awaryjne uruchomienie w przypadku zapomnienia hasła dostępu. Do tego celu użytkownik tworzy w programie listę pytań oraz odpowiedzi. Jeśli użytkownik zapomni hasła, wystarczy, że odpowie na wcześniej wprowadzone przez siebie pytania i w ten sposób odzyska dostęp do zaszyfrowanego dysku.

WYGODA UŻYTKOWANIA

SecureDoc w minimalnym stopniu angażuje użytkownika. Po podaniu prawidłowej nazwy użytkownika oraz hasła, praca na zaszyfrowanym komputerze przebiega zupełnie standardowo. Dzieje się tak ponieważ dane są automatycznie rozszyfrowywane w momencie otwierania pliku oraz szyfrowane w momencie zapisywania. Co ważne, samo szyfrowanie jest niedostrzegalne i nie wpływa na wydajność pracy z komputerem. Instalacja i konfiguracja programu oraz szyfrowanie dysku jest oparte na prostym kreatorze. Dzięki temu nawet początkujący użytkownik może korzystać z bardzo zaawansowanej ochrony.

W JAKIM CELU SZYFROWAĆ?

Ochrona cennych informacji.

Pracując na komputerze gromadzimy na nim zwykle cenne poufne dane. Numery kart kredytowych, dane osobowe, strategie firm, listy klientów, umowy, listy płac, karty chorobowe pacjentów to tylko przykład informacji, które traktujemy jako poufne.

W społeczeństwie opartym na wiedzy informacja jest najcenniejszym zasobem. Istnieje wiele sposobów zabezpieczania danych przed dostępem osób niepowołanych, ale najpewniejszym sposobem jest ich zaszyfrowanie.

Szyfrowanie nakazane przez prawo.

Co ważne, obowiązek szyfrowania niektórych danych wynika również z przepisów prawa. Zgodnie z polskim ustawodawstwem każdy wynoszony poza obręb firmy komputer, na którym przetwarzane są dane osobowe, powinien być zabezpieczony rozwiązaniem szyfrującym:

„Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.” (Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku.)

WERSJA ENTERPRISE DLA ŚREDNICH I DUŻYCH FIRM

Wersja korporacyjna programu pozwala na silne szyfrowanie danych dodatkowo oferując funkcje istotne dla administratorów sieci w przedsiębiorstwie:

- możliwość przechowywania zbioru z kluczami szyfrującymi na tokenie lub karcie,
- łatwe współdzielenie zasobów dzięki systemowi etykietowania kluczy szyfrujących,
- możliwość blokowania zapisu na dyskach USB,
- trwałe usuwanie danych.

Dzięki konsoli do zarządzania wersja Enterprise może być stosowana nawet w bardzo rozległych sieciach korporacyjnych.

MySecureDoc

Funkcja	MySecureDoc Personal Edition Plus	MySecureDoc Media Edition	SecureDoc Enterprise Edition
Szyfrowanie dysków twardej	✓	✗	✓
Szyfrowanie przenośnych dysków USB i kart pamięci	✓	✓	✓
Centralne zarządzanie	✗	✗	✓
Liczba użytkowników	1-15	1-15	Dowolna
Algorytm szyfrujący	AES 256	AES 256	AES 256
Możliwość zabezpieczenia zaszyfrowanego dysku tokenem	✗	✗	✓
Konieczność podania nazwy użytkownika i hasła przed uruchomieniem programu Windows.	✓	✗	✓
Obsługiwane systemy	Windows 2000 Windows XP	Windows 2000 Windows XP	Windows 2000 Windows XP Windows 2003 Windows Vista



WINMAGIC
DATA SECURITY