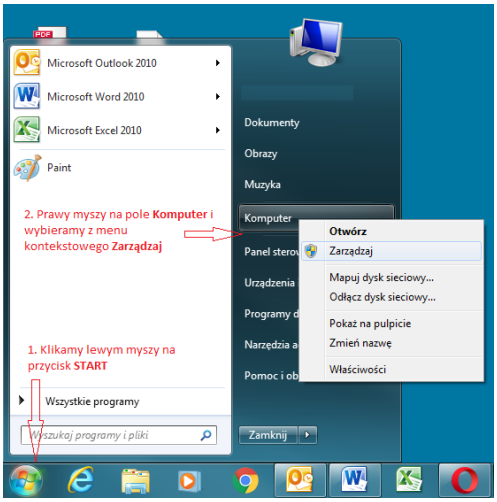
Szyfrowanie danych na laptopach

Proces szyfrowania danych jest środkiem ostrożności, który ma na celu zminimalizowanie niebezpieczeństwa, że nieupoważnione podmioty wejdą w posiadanie danych zapisanych na urządzeniu. Spośród wielu dostępnych na rynku programów służących do szyfrowania danych, proponujemy wykorzystanie jednego z nich, o nazwie DiskCryptor, który jest udostępniany bezpłatnie na stronie https://diskcryptor.net/wiki/Downloads. Poniżej przedstawiamy informacje pomocne w procesie instalacji oprogramowania na urządzeniu wyposażonym w system Microsoft Windows 7.

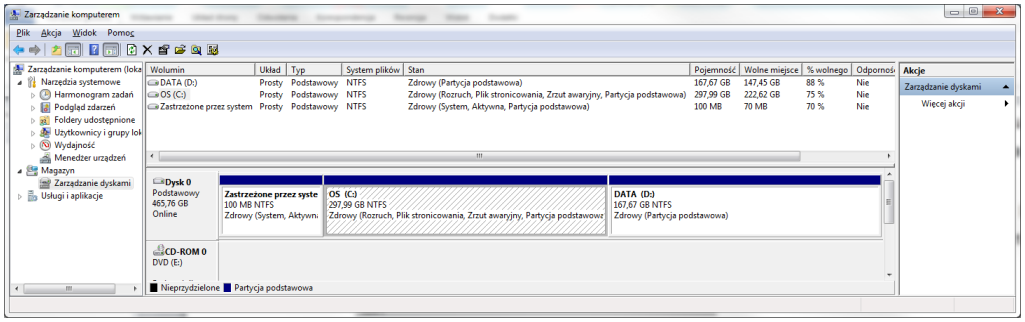
ETAP 1: Wykonanie kopii bezpieczeństwa, sprawdzenie systemu i przygotowanie do instalacji programu DiskCryptor

W pierwszej kolejności zaleca się wykonanie kopii bezpieczeństwa, tj. skopiowanie swoich plików na inny nośnik.
W kolejnym kroku należy sprawdzić, czy dysk w laptopie jest podzielony na partycje, bowiem szyfrowaniu będzie podlegać tylko jedna z nich. W tym celu należy z menu START wybrać pozycję Komputer, kliknąć prawy klawisz myszy i wybrać pozycję Zarządzaj.



Rysunek nr 1.

Na ekranie pojawi się okno dialogowe:



Rysunek nr 2.

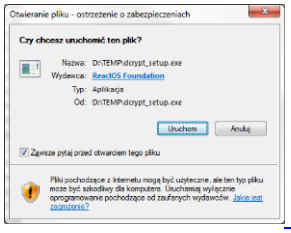
W kolejnym kroku w lewej części okna dialogowego wybieramy pozycję Magazyn, a dalej Zarządzanie dyskami. Powyżej przedstawiono przykładowe okno dialogowe, w którym widoczne są 3 partycje (obszary danych) o nazwach: *OS (C:), DATA (D:)* i *Zastrzeżone przez system*. W zależności od konfiguracji Państwa komputerów partycje mogą się różnić.
Dane wrażliwe, które będą szyfrowane powinny znajdować się na partycji innej niż systemowa (zwykle oznaczonej literą C:). Jeżeli w Państwa komputerach jest tylko jedna partycja należy dokonać jej podziału. Zaleca się, aby podziału dysku na partycję dokonała osoba legitymująca się wiedzą i doświadczeniem informatycznym.

W przedstawionym przykładzie dane do szyfrowania znajdują się na partycji D:

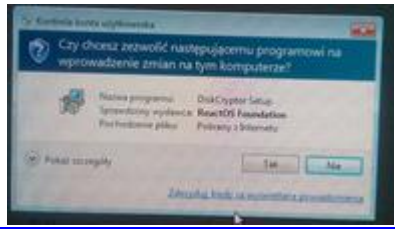
ETAP 2: DiskCryptor – instalacja i szyfrowanie danych

Proszę pobrać aplikację ze strony https://diskcryptor.net/wiki/Downloads i następnie uruchomić ją (plik o nazwie dcrypt_setup.exe). Instalacja polega na zatwierdzaniu kolejnych komunikatów wyświetlanych na ekranie monitora. Zaleca się pozostawienie bez zmian ustawień domyślnych.

Po instalacji należy dokonać restartu systemu. Po restarcie, proszę uruchomić program o nazwie DiskCryptor z menu START/PROGRAMY. Możemy zostać poproszeni o zatwierdzenie otwarcia aplikacji. Klikamy kolejno przyciski „Uruchom" a następnie „Tak", aby kontynuować (rysunki nr 6 i 7).

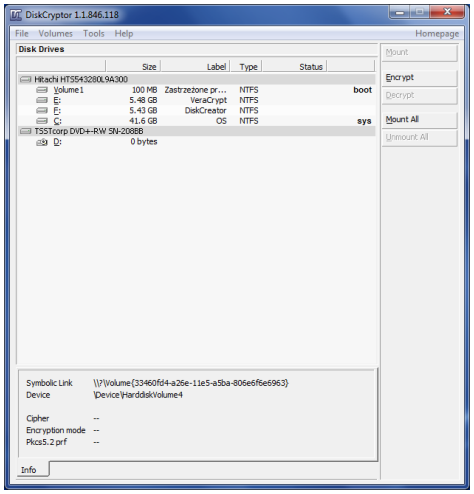


Rysunek nr 6.



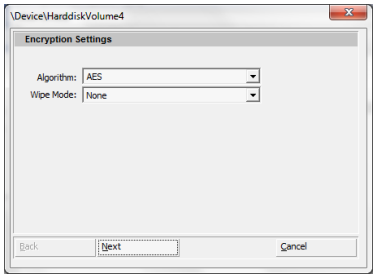
Rysunek nr 7.

Na ekranie monitora pojawi się następujące okno dialogowe:



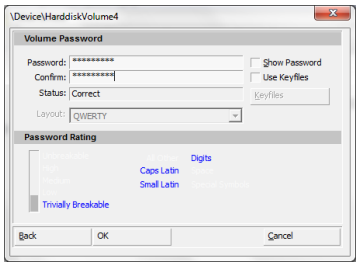
Rysunek nr 8.

Aby rozpocząć szyfrowanie danych za pomocą DiskCryptor wybieramy (zaznaczamy) wskaźnikiem myszy partycję, na której zapisane są dane do szyfrowania (w tym przykładzie jest to partycja D:) Proszę następnie kliknąć na przycisk „Encrypt". Powyższa akcja otworzy okno „ustawienia szyfrowania" (rysunek nr 9). W oknie tym można zmienić opcje: „Algorythm" i „Wipe Mode" lub pozostawić domyślne. Proszę wybrać przycisk „Next".



Rysunek nr . 9

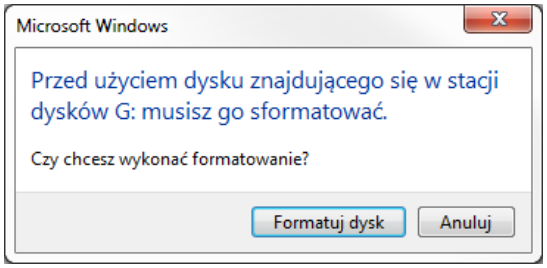
DiskCryptor poprosi o hasło (rysunek nr 10). Wskazane jest, aby nadane hasło składało się z minimum 12 znaków, zawierało wielkie i małe litery oraz cyfry lub znaki specjalne. Po zakończeniu wprowadzania hasła dwukrotnie, klikamy na przycisk "OK", aby uruchomić szyfrowanie.



Rysunek nr 10.

Po zakończeniu procesu szyfrowania należy ponownie uruchomić komputer.

Po ponownym uruchomieniu sytemu zaszyfrowana partycja będzie widoczna, jednakże próba jej użycia zakończy się komunikatem:



Rysunek nr 11.

Aby nie utracić danych zawartych na tej partycji należy wybrać opcję „Anuluj” i potwierdzić kolejny komunikat. W kolejnym kroku proszę wykonać czynności:

- uruchomić program DiskCryptor
- wskazać zaszyfrowaną partycję
- wybrać opcje „Mount” i potwierdzić wybranym wcześniej hasłem.

Więcej na temat szyfrowania można znaleźć pod adresami:

http://www.yac.mx/pl/pc-tech-tips/hardware/How_to_Use_DiskCryptor_to_Encrypt_Your_Hard_Drive.html
http://www.yac.mx/pl/pc-tech-tips/windows/How_to_Use_DiskCryptor_to_Encrypt_Partitions_in_Windows.html
https://diskcryptor.net/wiki/Main_Page/pl

UWAGA ważne!

Przy tego typu operacjach istnieje niewielkie ryzyko uszkodzenia lub utraty danych na nośniku, dlatego osoby nie mające doświadczenia powinny podchodzić bardzo ostrożnie do szyfrowania lub skorzystać z pomocy osób trzecich mających doświadczenie m.in. w zabezpieczeniu danych. Sąd Okręgowy w Warszawie nie ponosi odpowiedzialności za skutki uboczne i źle wykonane procedury związane z szyfrowaniem danych.