Co-funded by the Erasmus+ Programme of the European Union

Moduł treningowy InCyT

Bezpieczeństwo informacji dla pracowników **Część 3, Tydzień 6** **Moduł: Prywatność i ochrona danych**	
Zajęcia edukacyjne	❑ **Webinaria** ❑ **Ćwiczenia** ❑ **Warsztaty** ❑ **Prezentacja** ❑ **Inne**
Odpowiedzialni za zajęcia	• Mirosław Mazurek • Paweł Dymora
Cele aktywności edukacyjnej	1. Szyfrowanie dysków i partycji 2. Jak używać narzędzia VeraCrypt
Umiejętności do zdobycia	• **TS1** • **SS1** • **SS2**
Czas trwania okresu edukacyjnego	2 tygodnie
Wymagania wstępne	***Co jest potrzebne?***
	• Dostęp do Internetu • Przeglądarka Internetowa • Program VeraCrypt

Co-funded by the Erasmus+ Programme of the European Union

Krótka informacja o module

Opis
Celem modułu jest zdobycie wiedzy i praktycznych umiejętności związanych z ochroną danych i szyfrowaniem danych na dysku prywatnym lub firmowym.

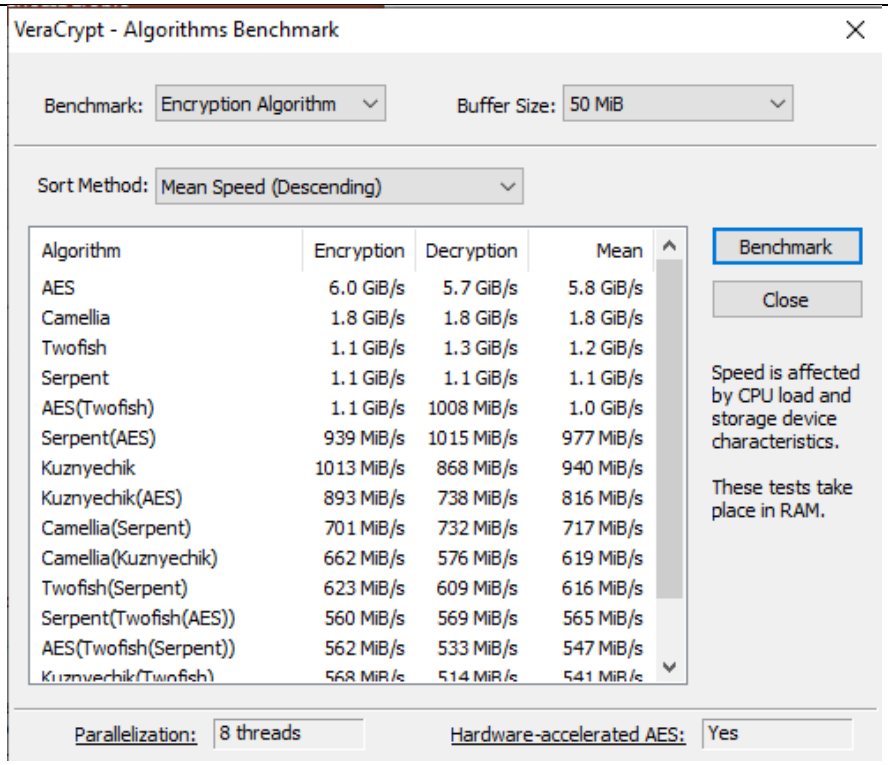
Treść materiałów dydaktycznych

1. Szyfrowanie dysków i partycji. Podstawy teoretyczne: zasada działania, algorytmy szyfrowania. Instalacja programu (konfiguracja, definiowanie dysku, wybór parametrów, generowanie kluczy).

Bezpieczeństwo systemów komputerowych wymaga ochrony nie tylko zasobów takich jak sam system operacyjny, aplikacje, ale przede wszystkim danych. Znane metody zabezpieczeń poprzez uniemożliwienie dostępu do zasobów, jak np. zapora sieciowa, nie zawsze są skuteczne. Dlatego należy łączyć ze sobą wiele metod zabezpieczeń. Przedstawiona metoda szyfrowania danych pozwala na wyeliminowanie wielu zagrożeń wynikających z dostępu intruza do naszego komputera.

Jednym z najczęściej stosowanych rozwiązań jest darmowy program do szyfrowania danych VeraCrypt. Pozwala on na szyfrowanie nie tylko całych dysków czy partycji, ale nawet przenośnych dysków USB oraz tworzenie wirtualnych zaszyfrowanych dysków o określonej pojemności. VeraCrypt umożliwia szyfrowanie przy użyciu następujących algorytmów: AES, Camellia, Kuznyechik, Serpent i Twofish; a także szyfrowanie wielokrotne z: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES, Twofish-Serpent.

W zależności od konfiguracji komputera szybkość szyfrowania i deszyfrowania dla każdego z tych algorytmów będzie różna, co przedstawia rysunek 1.



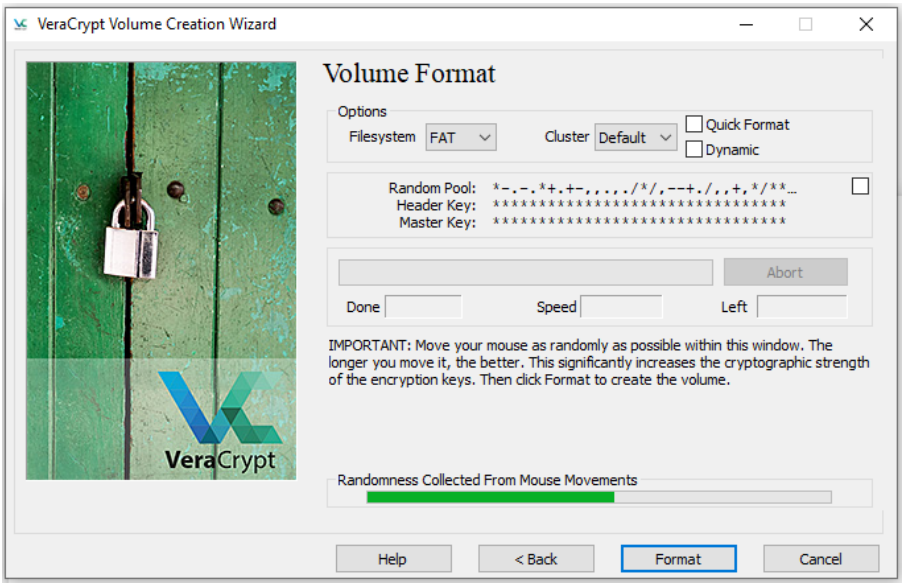
Rys. 1. Testowanie szybkości działania algorytmów

Proces szyfrowania rozpoczyna się od utworzenia woluminu. Można zaszyfrować cały dysk, partycję lub dowolny wolumin (rys. 2).

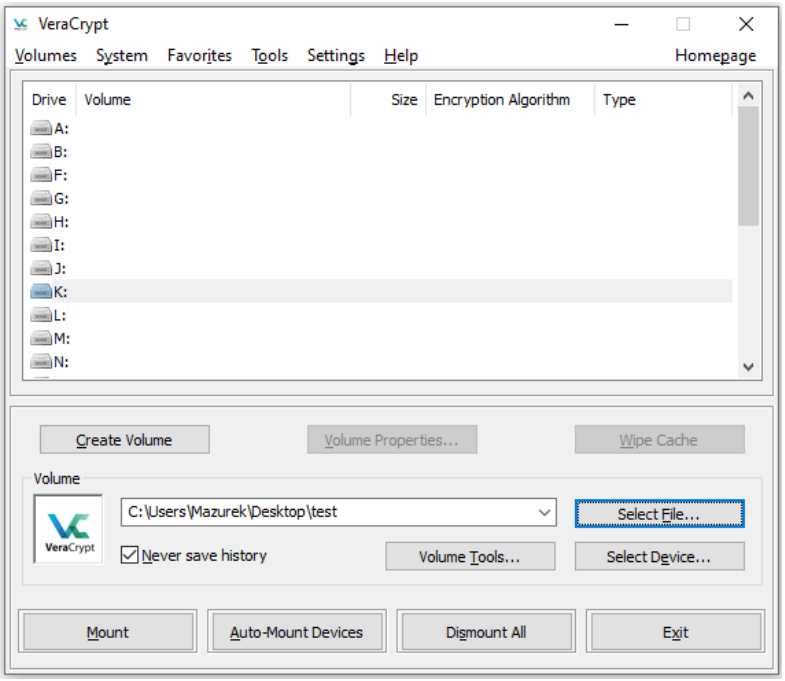
Rys. 2. Okno kreatora tworzenia woluminu VeraCrypt

Po wybraniu lokalizacji woluminu należy nadać mu nazwę. Wolumin VeraCrypt jest umieszczany w pliku, który można zapisać na dysku twardym lub dysku USB. Wolumen zachowuje

się jak zwykły plik, czyli możemy go kopiować, zmieniać jego nazwę itp. Kolejnym krokiem jest wybór odpowiedniego algorytmu szyfrowania, np. AES, oraz nadanie hasła dostępu zgodnego z odpowiednimi zasadami jakości (odpowiednia długość, duże i małe litery, cyfry, znaki specjalne). Następnie wolumin zostaje sformatowany. Dla zwiększenia jego bezpieczeństwa kreator prosi o wygenerowanie losowych ruchów myszką, co znacznie poprawia jakość kryptograficzną generowanych kluczy (rys. 3). Po sformatowaniu wolumin jest dostępny do użytku. Należy go tylko podłączyć, wpisując hasło (rys. 4).



Rys. 3. Proces formatowania woluminów VeraCrypt



Rys. 4. Okno połączenia woluminów VeraCrypt

W przypadkach, gdy zależy nam na wysokim poziomie ochrony, a nie zależy nam na czasie szyfrowania, należy wybrać szyfrowanie wielokrotne. Testując wydajność podczas szyfrowania dla woluminów o różnych pojemnościach z różnymi algorytmami jednocześnie, można zauważyć, że im silniejszy algorytm szyfrujący, tym mniejsza szybkość szyfrowania i deszyfrowania pliku. Nie każdy algorytm jednakowo reaguje na zmianę wielkości woluminu. Tworzenie woluminu jest szybkie i proste, dzięki przejrzystej instrukcji instalatora.

Pytania:

Pytania Forum dyskusyjne, na które należy odpowiedzieć z krótkim uzasadnieniem. Odpowiedzi zostaną omówione z mentorem podczas sesji mentorskich

1. Jak można chronić dane na dysku twardym komputera?
2. Jakich programów komputerowych możesz użyć, aby zabezpieczyć swoje dane?

Pytania do samooceny. Po udzieleniu odpowiedzi uczeń może zobaczyć wyniki i porównać je z tymi zapisanymi na platformie

1. Jaka jest najbezpieczniejsza metoda szyfrowania do zabezpieczenia plików?

Załączniki:

1. Prezentacja
2. Materiały wideo

Referencje:

1. https://www.veracrypt.fr/en/Home.html
2. https://github.com/veracrypt/VeraCrypt
3. https://veracrypt.eu/en/Beginner%27s%20Tutorial.html