

Module de instruire InCyT

Securitatea informațiilor pentru angajați

Unitatea 3 Săptămâna 6

Numele unității : Confidențialitate și protecție a datelor

<i>Activități de învățare</i>	☒ Webinar ☒ Exerciții ☐ Workshop ☐ Prezentare ☐ Alte
<i>Responsabil de învățare</i>	• Mirosław Mazurek • Paweł Dymora
<i>Obiectivele activității de învățare</i>	1. Criptarea discurilor și a partițiilor 2. Cum se utilizează instrumentul VeraCrypt
<i>Abilități de dobândit</i>	• TS1 • SS1 • SS2
<i>Durata activității de învățare</i>	2 săptămâni
<i>Cerințe de învățare</i>	Ce e necesar? • Internet access • Internet Browser • VeraCrypt program

Informații scurte despre modul



Descriere

Scopul acestui modul este de a dobândi cunoștințe și abilități practice legate de protecția datelor și criptarea datelor de pe discul tău privat sau corporativ.

Conținutul materialului de învățare

1. Criptarea discurilor și a partițiilor. Baze teoretice: principiu de funcționare, algoritmi de criptare. Instalarea programului (configurare, definirea discului, alegerea parametrilor, generarea cheilor).

Securitatea sistemelor informatice necesită protecția nu numai a resurselor precum sistemul de operare în sine, aplicațiile, ci mai ales a datelor. Metodele de securitate cunoscute prin împiedicarea accesului la resurse, cum ar fi un firewall, nu sunt întotdeauna eficiente. Prin urmare, mai multe metode de securitate ar trebui combinate între ele. Metoda prezentată de criptare a datelor permite eliminarea multor amenințări rezultate din accesul unui intrus la computerul nostru.

Una dintre cele mai utilizate soluții este software-ul gratuit de criptare a datelor VeraCrypt. Vă permite să criptați nu numai discuri sau partiții întregi, ci chiar și discuri USB portabile și să creați discuri virtuale criptate cu o anumită capacitate. VeraCrypt permite criptarea folosind următorii algoritmi: AES, Camellia, Kuznyechik, Serpent și Twofish; precum și criptare multiplă cu: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES, Twofish-Serpent.

În funcție de configurația computerului, viteza de criptare și decriptare pentru fiecare dintre acești algoritmi va varia, așa cum se arată în Figura 1.

VeraCrypt - Algorithms Benchmark

Benchmark: Encryption Algorithm Buffer Size: 50 MiB

Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
AES	6.0 GiB/s	5.7 GiB/s	5.8 GiB/s
Camellia	1.8 GiB/s	1.8 GiB/s	1.8 GiB/s
Twofish	1.1 GiB/s	1.3 GiB/s	1.2 GiB/s
Serpent	1.1 GiB/s	1.1 GiB/s	1.1 GiB/s
AES(Twofish)	1.1 GiB/s	1008 MiB/s	1.0 GiB/s
Serpent(AES)	939 MiB/s	1015 MiB/s	977 MiB/s
Kuznyechik	1013 MiB/s	868 MiB/s	940 MiB/s
Kuznyechik(AES)	893 MiB/s	738 MiB/s	816 MiB/s
Camellia(Serpent)	701 MiB/s	732 MiB/s	717 MiB/s
Camellia(Kuznyechik)	662 MiB/s	576 MiB/s	619 MiB/s
Twofish(Serpent)	623 MiB/s	609 MiB/s	616 MiB/s
Serpent(Twofish(AES))	560 MiB/s	569 MiB/s	565 MiB/s
AES(Twofish(Serpent))	562 MiB/s	533 MiB/s	547 MiB/s
Kuznyechik(Twofish)	568 MiB/s	514 MiB/s	541 MiB/s

Parallelization: 8 threads Hardware-accelerated AES: Yes

Benchmark Close

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

Fig. 1. Testarea vitezei algoritmilor

Procesul de criptare începe cu crearea volumului. Puteți cripta un întreg disc, partiție sau orice volum (Fig. 2).

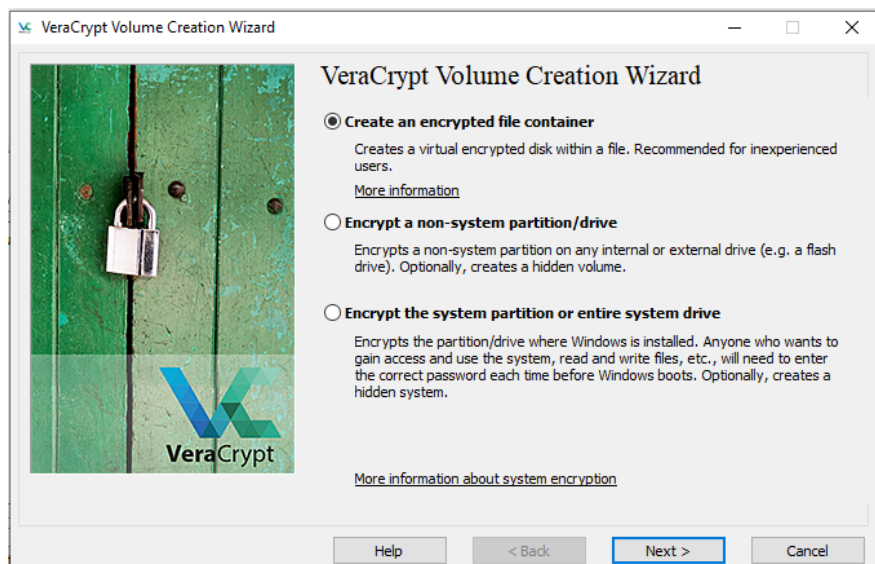


Fig. 2. Fereastra asistentului de creare a volumului VeraCrypt

După ce ați selectat locația volumului, ar trebui să îi dați un nume. Volumul VeraCrypt este plasat într-un fișier care poate fi salvat pe un hard disk sau pe o unitate USB. Volumul se comportă ca un fișier normal, adică îl putem copia, redenumi etc. Următorul pas este selectarea algoritmului

de criptare adecvat, de ex. AES și să atribuie o parolă de acces în conformitate cu regulile de calitate relevante (lungime adecvată, litere mari și mici, cifre, caractere speciale). Apoi volumul este formatat. Pentru a-i crește securitatea, vrăjitorul vă cere să generați mișcări aleatorii ale mouse-ului, ceea ce îmbunătățește semnificativ calitatea criptografică a cheilor generate (Fig. 3). După formatare, volumul este disponibil pentru utilizare. Trebuie doar conectat prin introducerea parolei (Fig. 4).

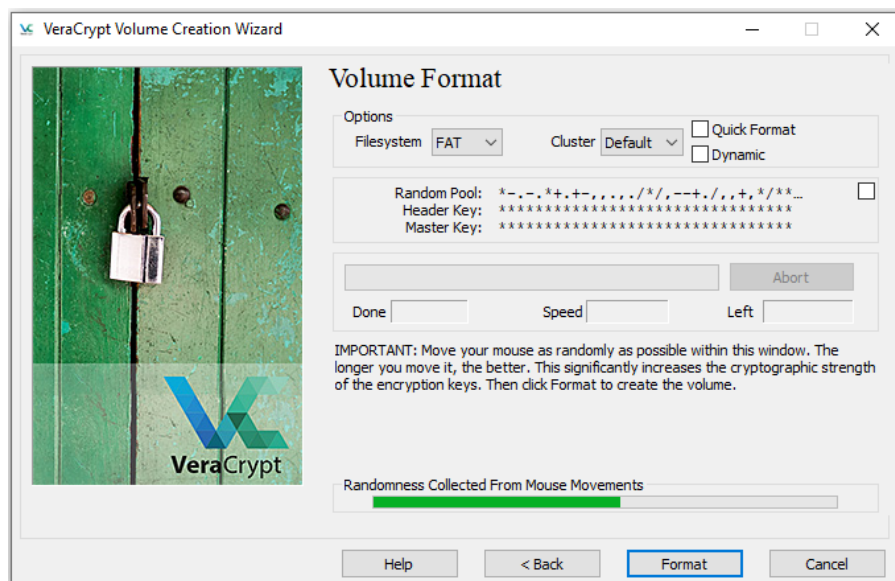


Fig. 3. Procesul de formatare a volumelor VeraCrypt

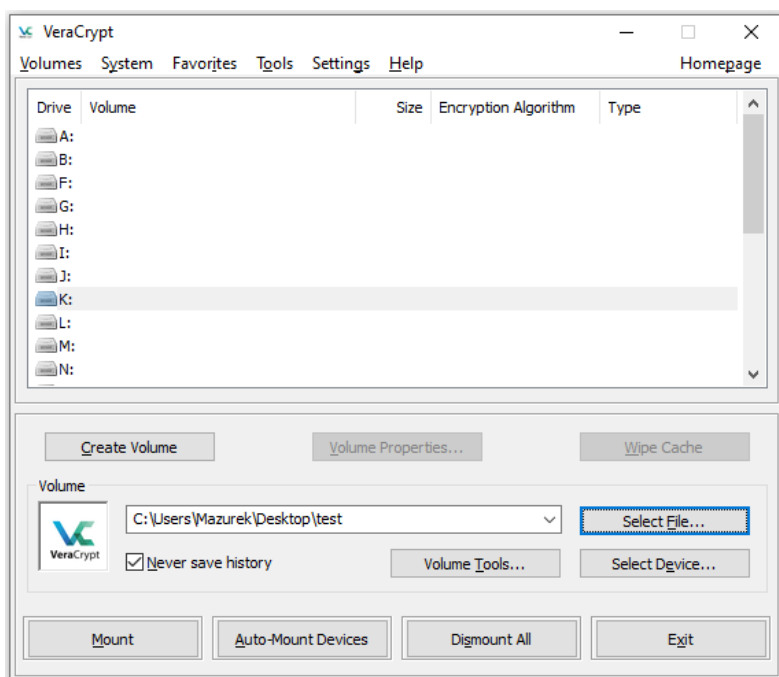


Fig. 4. Fereastra de conectare la volume VeraCrypt

În cazurile în care dorim un nivel ridicat de protecție și nu ne pasă de timpul de criptare, ar trebui

selectată criptarea multiplă. Testând performanța în timpul criptării pentru volume de diferite capacități cu diferiți algoritmi în același timp, se poate observa că cu cât algoritmul de criptare este mai puternic, cu atât viteza de criptare și decriptare a fișierului este mai mică. Nu orice algoritm răspunde în mod egal la o modificare a dimensiunii volumului. Crearea unui volum este rapidă și ușoară, datorită instrucțiunilor clare de la instalator.

Întrebări:

Forumul de discuții la care se răspunde cu o scurtă explicație. Răspunsurile vor fi discutate cu mentorul în timpul sesiunilor de mentorat.

1. Cum vă puteți proteja datele de pe hard diskul computerului?
2. Ce fel de programe de calculator puteți utiliza pentru a vă proteja datele?

Întrebări de autoevaluare. După ce răspunde, cursantul poate vedea rezultatele și le poate compara cu cele salvate pe platformă

1. Care este cea mai sigură metodă de criptare pentru a vă securiza fișierele?

Atasamente:

1. Prezentare
2. Video

Referințe:

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