

InCyT træningsmoduler

Informationssikkerhed for medarbejdere Enhedsnummer: (3) Uge 6 Enhedsnavn (modul): (Privatliv og databeskyttelse)	
Læringsaktiviteter	☐ Webinar ☐ Øvelser ☐ Værksted ☐ Præsentation ☐ Andet
Læringsansvarlig	• Mirosław Mazurek • Paweł Dymora
Læringsaktivitetsmål	1. Kryptering af diske og partitioner 2. Sådan bruger du VeraCrypt Tool
Færdigheder, der skal opnås	• TS1 • SS1 • SS2
Varighed af læringsaktivitet	2 uger
Læring krav	Hvad skal der til?
	• Internetadgang • Internet browser • VeraCrypt program

Kort information om modulet



Beskrivelse

Målet med dette modul er at opnå viden og praktiske færdigheder relateret til databeskyttelse og kryptering af data på din private eller virksomheds disk.

Lærematerialets indhold

1. Kryptering af diske og partitioner. Teoretisk basis: funktionsprincip, krypteringsalgoritmer. Installation af programmet (konfiguration, definering af disken, valg af parametre, generering af nøgler).

Sikkerheden af computersystemer kræver beskyttelse ikke kun af ressourcer såsom selve operativsystemet, applikationer, men mest af alle data. Kendte sikkerhedsmetoder ved at forhindre adgang til ressourcer, såsom en firewall, er ikke altid effektive. Derfor bør flere sikkerhedsmetoder kombineres med hinanden. Den præsenterede metode til datakryptering giver mulighed for at eliminere mange trusler, der skyldes en ubuden gæsts adgang til vores computer.

En af de mest brugte løsninger er den gratis VeraCrypt datakrypteringssoftware. Det giver dig mulighed for at kryptere ikke kun hele diske eller partitioner, men endda bærbare USB-diske og skabe virtuelle krypterede diske med en vis kapacitet. VeraCrypt muliggør kryptering ved hjælp af følgende algoritmer: AES, Camellia, Kuznyechik, Serpent og Twofish; samt multiple kryptering med: AES- Twofish, AES- Twofish -Serpent, Serpent-AES, Serpent- Twofish -AES, Twofish -Serpent.

Afhængigt af computerens konfiguration vil krypterings- og dekrypteringshastigheden for hver af disse algoritmer variere, som vist i figur 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

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

Fig. 1. Test af algoritmers hastighed

Krypteringsprocessen begynder med oprettelsen af volumen. Du kan kryptere en hel disk, partition eller en hvilken som helst diskenhed (fig. 2).

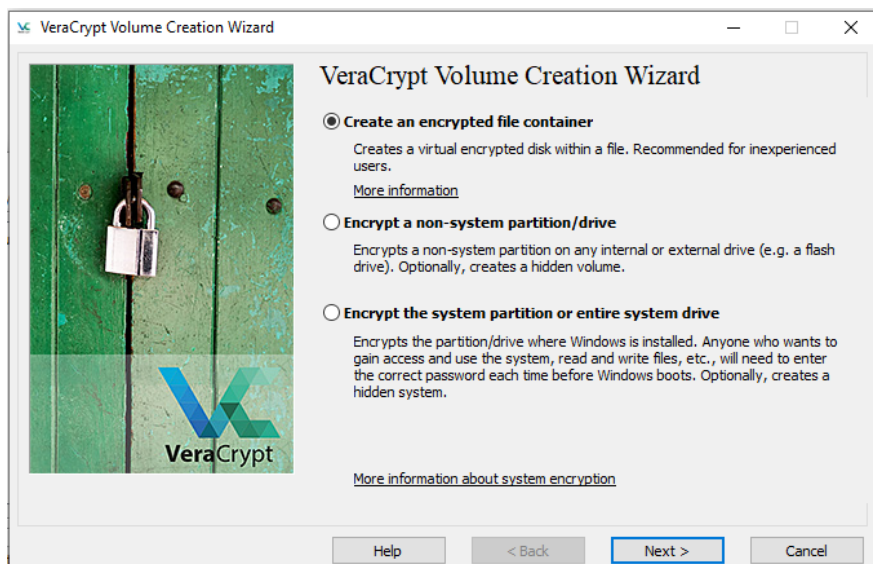


Fig. 2. Vindue i VeraCrypt-volumenoprettelsesguiden

Når du har valgt lydstyrkens placering, skal du give den et navn. VeraCrypt-volumen er placeret i en fil, der kan gemmes på en harddisk eller et USB-drev. Volumen opfører sig som en normal fil, dvs. vi kan kopiere den, omdøbe den osv. Næste trin er at vælge den passende krypteringsalgoritme

, f.eks. AES, og at tildele et adgangskodeord i overensstemmelse med de relevante kvalitetsregler (passende længde, store og små bogstaver, tal, specialtegn). Derefter formateres lydstyrken. For at øge dens sikkerhed beder guiden dig om at generere tilfældige musebevægelser, hvilket væsentligt forbedrer den kryptografiske kvalitet af de genererede nøgler (fig. 3). Efter formatering er lydstyrken tilgængelig til brug. Den skal kun tilsluttes ved at indtaste adgangskoden (fig. 4).

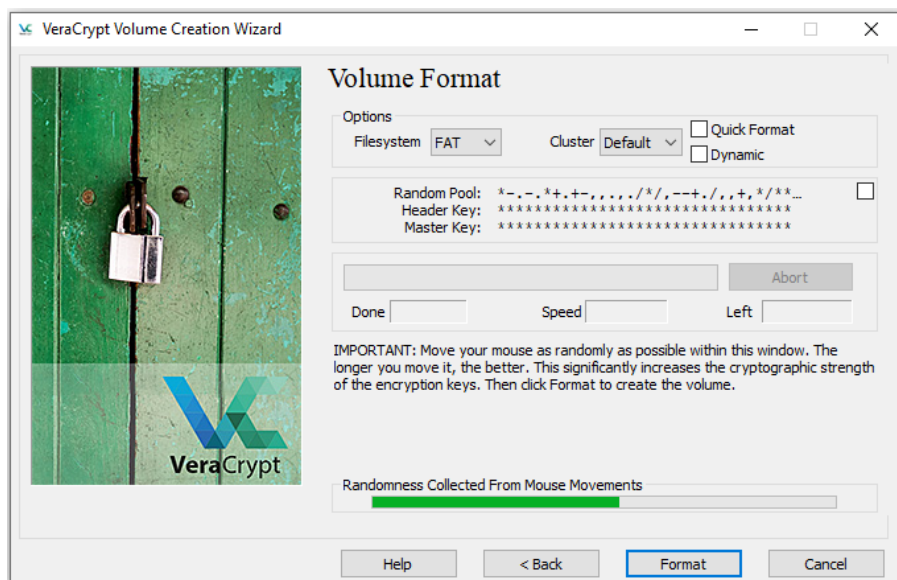


Fig. 3. Processen med at formatere VeraCrypt-volumener

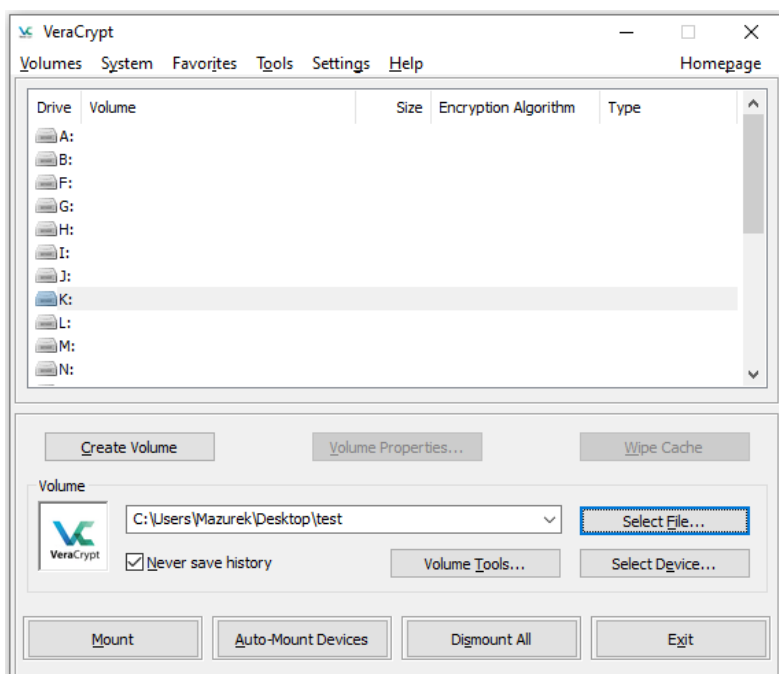


Fig. 4. Tilslutningsvindue til VeraCrypt-volumener

I tilfælde, hvor vi ønsker et højt beskyttelsesniveau, og vi er ligeglade med krypteringstiden, bør der vælges multikryptering. Ved at teste ydeevnen under kryptering for mængder af forskellig kapacitet

med forskellige algoritmer på samme tid, kan man bemærke, at jo stærkere krypteringsalgoritmen er, jo lavere er kryptering og dekryptering af filen. Ikke alle algoritmer reagerer lige meget på en ændring i volumenstørrelse. Det er hurtigt og nemt at oprette et volumen takket være de klare instruktioner fra installatøren.

Spørgsmål :

Spørgsmål Diskussionsforum skal besvares med en kort forklaring. Svarene vil blive drøftet med mentoren under mentorsessionerne.

1. Hvordan kan du beskytte dine data på din computers harddisk?
2. Hvilken slags computerprogrammer kan du bruge for at beskytte dine data?

Selvevalueringsspørgsmål. Efter besvarelsen kan eleven se resultaterne og sammenligne dem med disse gemt på platformen

1. Hvad er den sikreste krypteringsmetode til at sikre dine filer?

Vedhæftede filer:

1. Præsentation
2. Video

Referencer:

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