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

Moduli di formazione InCyT

Sicurezza delle informazioni per i dipendenti **Unità n.: (3) Settimana 6** **Nome dell'unità (modulo): (Privacy e protezione dei dati)**	
Attività di apprendimento	❑ **Webinar** ❑ **Esercizi** ❑ **Workshop** ❑ **Presentazione** ❑ **Altro**
Apprendimento responsabile	• Mirosław Mazurek • Paweł Dymora
Obiettivi dell'attività di apprendimento	1. Crittografia di dischi e partizioni 2. Come utilizzare lo strumento VeraCrypt
Competenze da acquisire	• **TS1** • **SS1** • **SS2**
Durata dell'attività di apprendimento	2 settimane
Apprendimento requisiti	***Cosa serve?***
	• Accesso a Internet • Browser Internet • Programma VeraCrypt

Brevi informazioni sul modulo

Descrizione
L'obiettivo di questo modulo è quello di acquisire conoscenze e competenze pratiche relative alla protezione e alla crittografia dei dati sul disco privato o aziendale.

Contenuto del materiale didattico

1. Crittografia di dischi e partizioni. Basi teoriche: principio di funzionamento, algoritmi di crittografia. Installazione del programma (configurazione, definizione del disco, scelta dei parametri, generazione delle chiavi).

La sicurezza dei sistemi informatici richiede la protezione non solo delle risorse, come il sistema operativo stesso e le applicazioni, ma soprattutto dei dati. I metodi di sicurezza conosciuti che impediscono l'accesso alle risorse, come ad esempio un firewall, non sono sempre efficaci. Pertanto, è necessario combinare più metodi di sicurezza tra loro. Il metodo di crittografia dei dati presentato consente di eliminare molte minacce derivanti dall'accesso di un intruso al nostro computer.

Una delle soluzioni più utilizzate è il software gratuito di crittografia dei dati VeraCrypt. Consente di crittografare non solo interi dischi o partizioni, ma anche dischi USB portatili e di creare dischi virtuali crittografati con una certa capacità. VeraCrypt consente la crittografia utilizzando i seguenti algoritmi: AES, Camellia, Kuznyechik, Serpent e Twofish; nonché la crittografia multipla con: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES, Twofish-Serpent.

A seconda della configurazione del computer, la velocità di cifratura e decifratura di ciascuno di questi algoritmi varierà, come mostrato nella Figura 1.

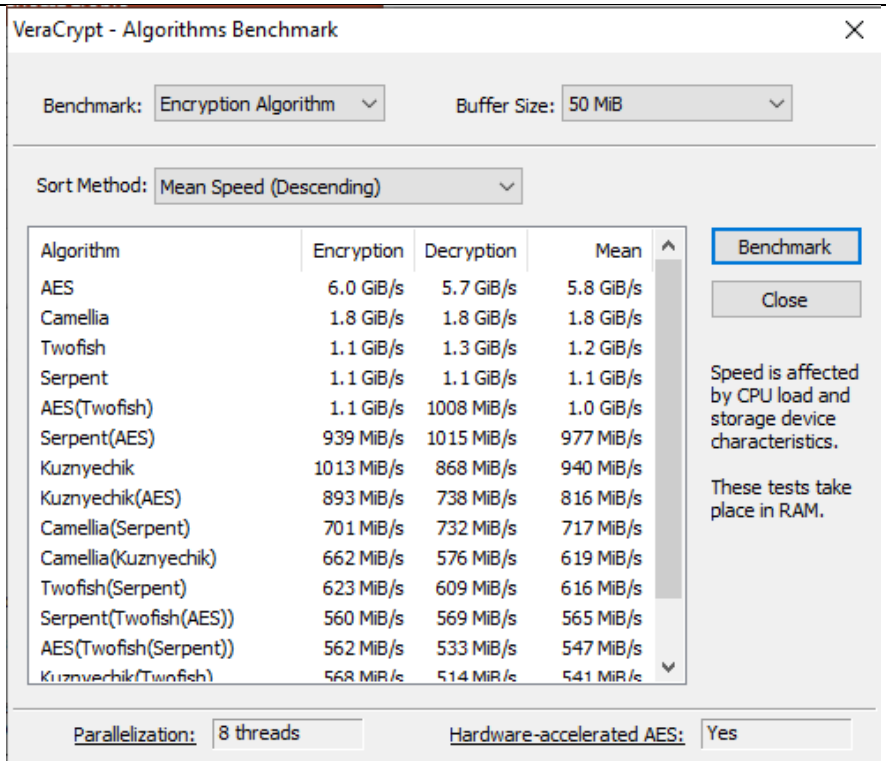

Fig. 1. Verifica della velocità degli algoritmi

Il processo di crittografia inizia con la creazione del volume. È possibile crittografare un intero disco, una partizione o qualsiasi volume (Fig. 2).

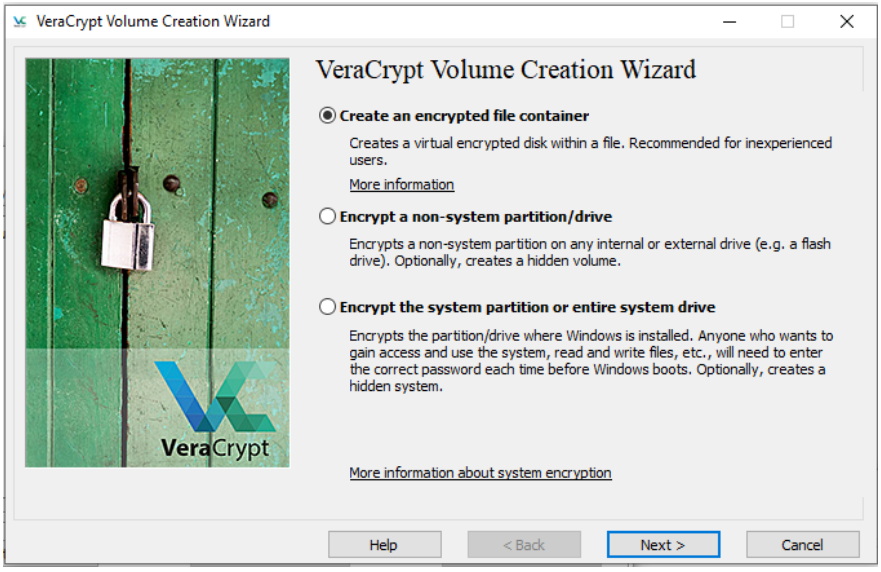

Figura 2. Finestra della procedura guidata di creazione del volume VeraCrypt

Dopo aver selezionato la posizione del volume, è necessario assegnargli un nome. Il volume VeraCrypt viene inserito in un file che può essere salvato su un disco rigido o su un'unità USB. Il volume si comporta come un normale file, cioè può essere copiato, rinominato, ecc. Il passo

successivo consiste nel selezionare l'algoritmo di crittografia appropriato, ad esempio AES, e nell'assegnare una password di accesso conforme alle norme di qualità pertinenti (lunghezza adeguata, lettere maiuscole e minuscole, numeri, caratteri speciali). Quindi il volume viene formattato. Per aumentarne la sicurezza, la procedura guidata chiede di generare movimenti casuali del mouse, che migliorano notevolmente la qualità crittografica delle chiavi generate (Fig. 3). Dopo la formattazione, il volume è disponibile per l'uso. È sufficiente collegarlo inserendo la password (Fig. 4).

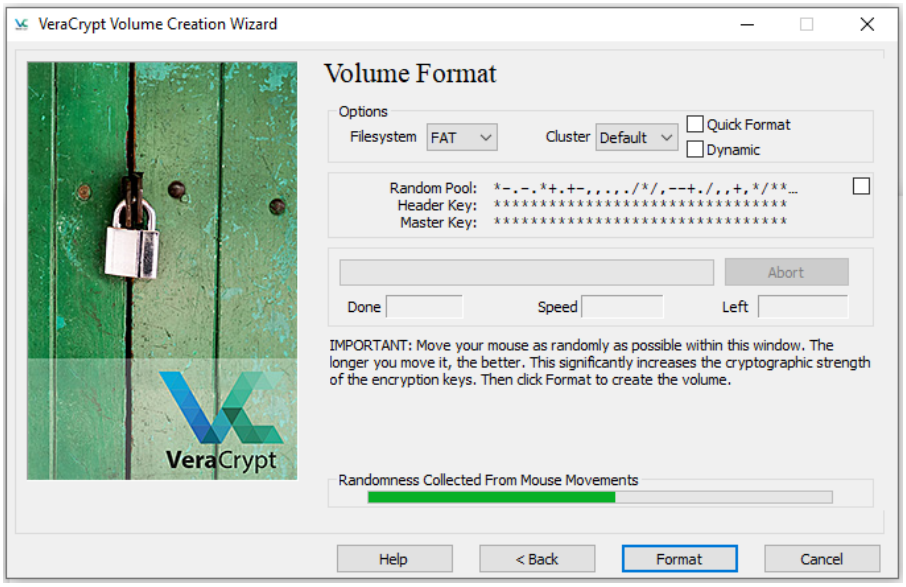

Figura 3. Il processo di formattazione dei volumi VeraCrypt

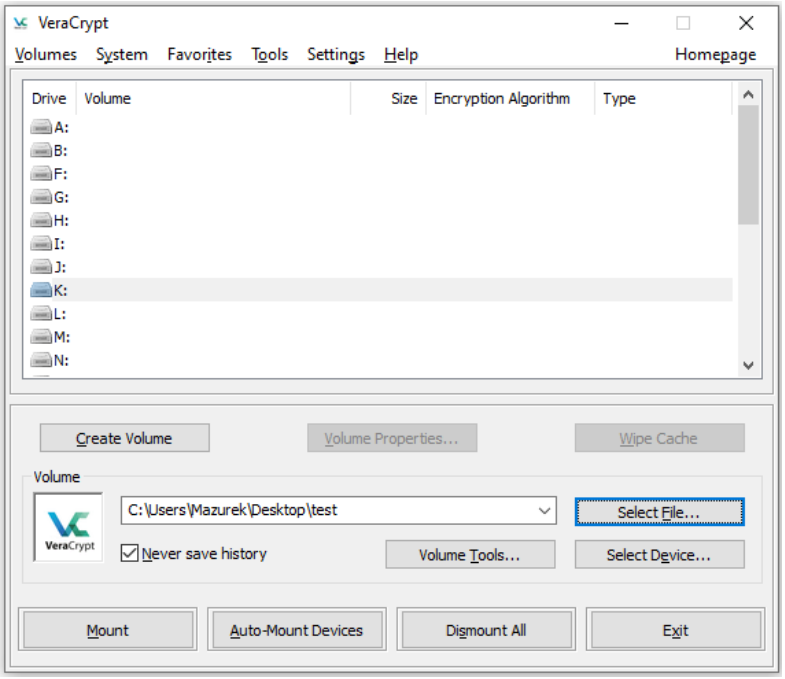

Figura 4. Finestra di connessione dei volumi VeraCrypt

Nei casi in cui si desidera un livello di protezione elevato e non ci si preoccupa del tempo di crittografia, è opportuno scegliere la crittografia multipla. Valutando le prestazioni durante la crittografia di volumi di diversa capacità con diversi algoritmi contemporaneamente, si può notare che più forte è l'algoritmo di crittografia, minore è la velocità di cifratura e decifratura del file. Non tutti gli algoritmi rispondono allo stesso modo alla variazione delle dimensioni del volume. La creazione di un volume è semplice e veloce, grazie alle chiare istruzioni del programma di installazione.

Domande:

Domande Forum di discussione a cui rispondere con una breve spiegazione.

1. Come si possono proteggere i dati sul disco rigido del computer?
2. Che tipo di programmi informatici potete utilizzare per proteggere i vostri dati?

Domande di autovalutazione.

1. Qual è il metodo di crittografia più sicuro per proteggere i vostri file?

Allegati:

1. Presentazione
2. Video

Riferimenti:

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