This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

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

InCyT-Trainingsmodule

Informationssicherheit für Mitarbeiter **Einheit Nr.: (3) Woche 6** **Name der Einheit (Moduls): (Privatsphäre und Datenschutz)**	
Lernaktivitäten	❑ **Webinar** ❑ **Übungen** ❑ **Workshop** ❑ **Präsentation** ❑ **Sonstiges**
Lehrverantwortliche	• Mirosław Mazurek • Paweł Dymora
Ziele der Lernaktivitäten	1. Verschlüsselung von Festplatten und Partitionen 2. Wie man VeraCrypt Tool benutzt
Zu erwerbende Fertigkeiten	• **TS1** • **SS1** • **SS2**
Dauer der Lernaktivität	2 Wochen
Lernanforderungen	***Was wird benötigt?*** • Zugang zum Internet • Internet-Browser • VeraCrypt-Programm

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

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

Kurze Informationen zum Modul

Beschreibung
Ziel dieses Moduls ist der Erwerb von Kenntnissen und praktischen Fähigkeiten im Zusammenhang mit dem Datenschutz und der Verschlüsselung von Daten auf Ihrer privaten oder betrieblichen Festplatte.

Inhalt des Lernmaterials

1. Verschlüsselung von Festplatten und Partitionen. Theoretische Grundlagen: Funktionsprinzip, Verschlüsselungsalgorithmen. Installation des Programms (Konfiguration, Definition des Datenträgers, Auswahl der Parameter, Schlüsselerzeugung).

Die Sicherheit von Computersystemen erfordert nicht nur den Schutz von Ressourcen wie dem Betriebssystem selbst, von Anwendungen, sondern vor allem von Daten. Bekannte Sicherheitsmethoden, die den Zugriff auf Ressourcen verhindern, wie z. B. eine Firewall, sind nicht immer wirksam. Daher sollten mehrere Sicherheitsmethoden miteinander kombiniert werden. Die vorgestellte Methode der Datenverschlüsselung ermöglicht die Beseitigung vieler Bedrohungen, die sich aus dem Zugriff eines Eindringlings auf unseren Computer ergeben.

Eine der am häufigsten verwendeten Lösungen ist die kostenlose Datenverschlüsselungssoftware VeraCrypt. Mit ihr können Sie nicht nur ganze Festplatten oder Partitionen verschlüsseln, sondern sogar tragbare USB-Festplatten und virtuelle verschlüsselte Festplatten mit einer bestimmten Kapazität erstellen. VeraCrypt ermöglicht die Verschlüsselung mit den folgenden Algorithmen: AES, Camellia, Kuznyechik, Serpent und Twofish; sowie die Mehrfachverschlüsselung mit: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES, Twofish-Serpent.

Je nach Konfiguration des Computers variiert die Geschwindigkeit der Ver- und Entschlüsselung für jeden dieser Algorithmen, wie in Abbildung 1 dargestellt.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

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

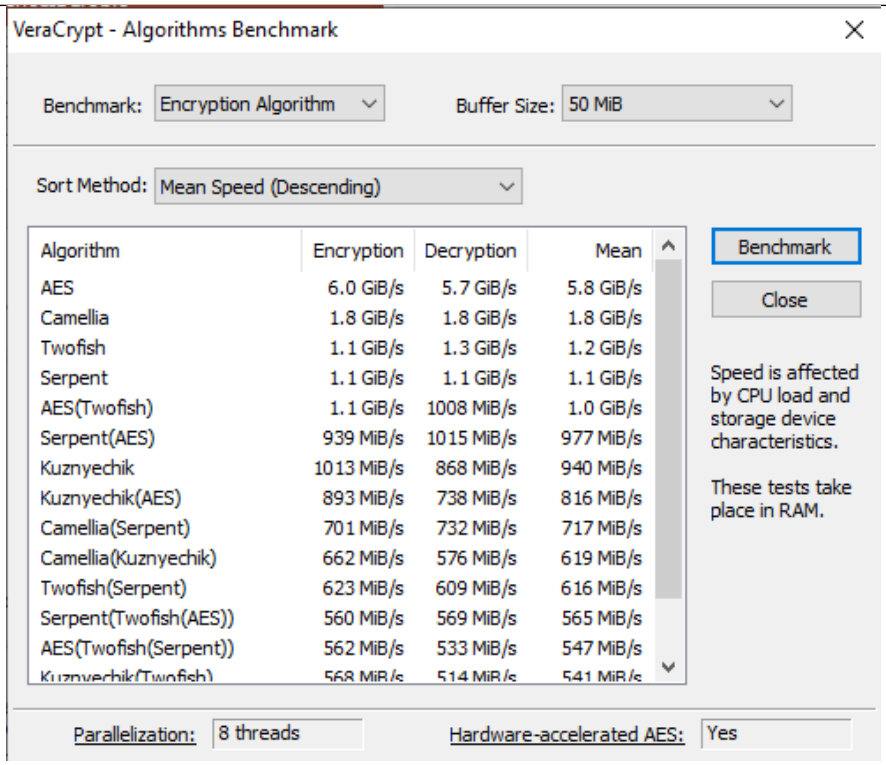


Abb. 1. Prüfung der Geschwindigkeit von Algorithmen

Der Verschlüsselungsprozess beginnt mit der Erstellung des Volumes. Sie können einen ganzen Datenträger, eine Partition oder ein beliebiges Volume verschlüsseln (Abb. 2).

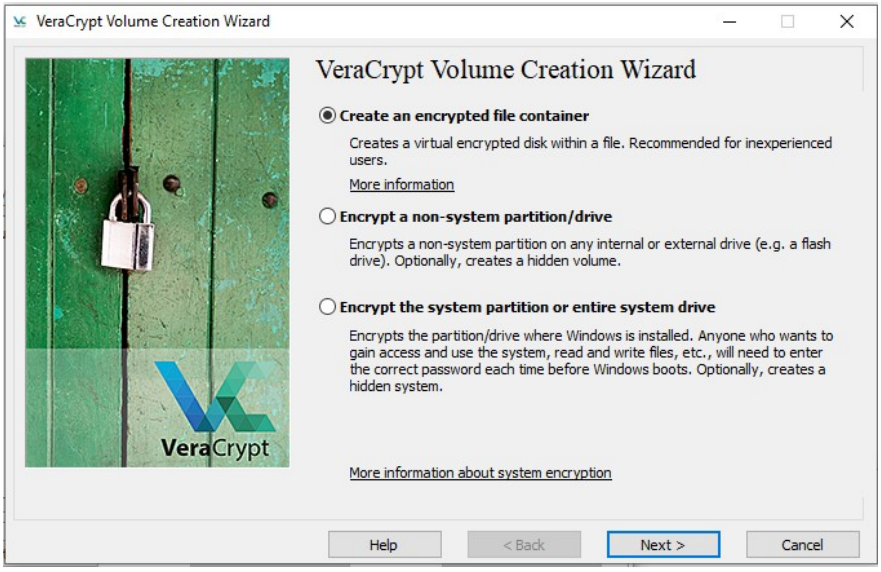


Abb. 2. Fenster des VeraCrypt-Volume-Erstellungsassistenten

Nachdem Sie den Speicherort für das Volume ausgewählt haben, sollten Sie ihm einen Namen geben. Das VeraCrypt-Volume wird in einer Datei abgelegt, die auf einer Festplatte oder einem USB-Laufwerk gespeichert werden kann. Das Volume verhält sich wie eine normale Datei,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

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

d. h. wir können es kopieren, umbenennen usw. Der nächste Schritt ist die Auswahl des geeigneten Verschlüsselungsalgorithmus, z. B. AES, und die Vergabe eines Zugangspassworts unter Einhaltung der entsprechenden Qualitätsregeln (angemessene Länge, Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen). Anschließend wird der Datenträger formatiert. Um die Sicherheit zu erhöhen, fordert der Assistent Sie auf, zufällige Mausbewegungen zu erzeugen, was die kryptografische Qualität der erzeugten Schlüssel deutlich verbessert (Abb. 3). Nach der Formatierung ist der Datenträger einsatzbereit. Es muss nur noch durch Eingabe des Passworts verbunden werden (Abb. 4).

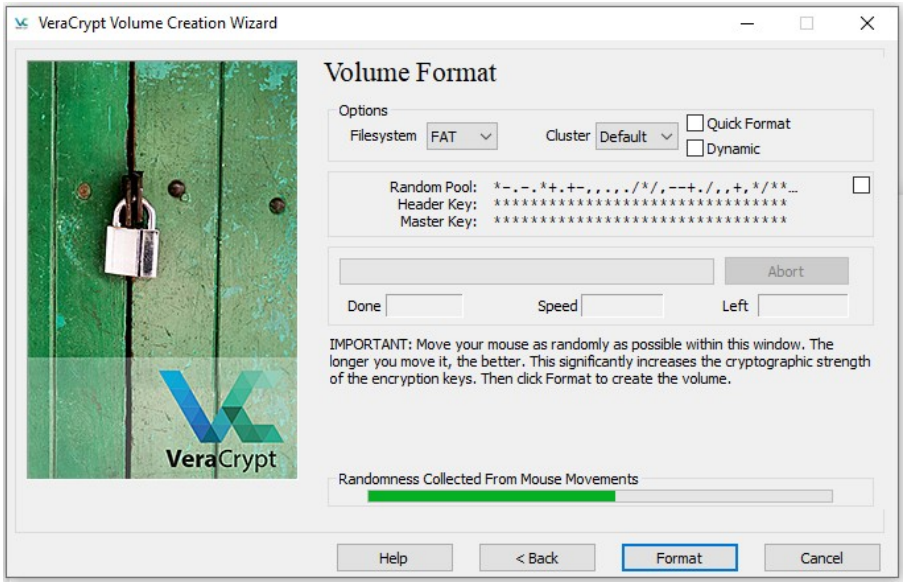
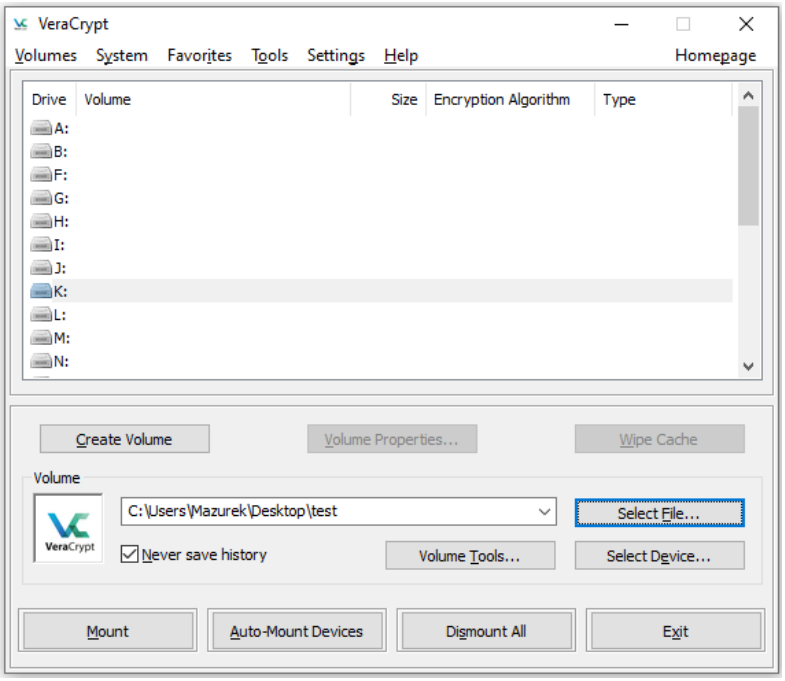


Abb. 3. Der Prozess der Formatierung von VeraCrypt-Volumes



Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

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

Abb. 4. VeraCrypt Volumes Verbindungsfenster

In Fällen, in denen wir ein hohes Maß an Schutz wünschen und uns die Verschlüsselungszeit egal ist, sollte die Mehrfachverschlüsselung gewählt werden. Wenn man die Leistung bei der Verschlüsselung von Datenträgern mit unterschiedlichen Kapazitäten und verschiedenen Algorithmen gleichzeitig testet, stellt man fest, dass die Geschwindigkeit beim Ver- und Entschlüsseln der Datei umso geringer ist, je stärker der Verschlüsselungsalgorithmus ist. Nicht jeder Algorithmus reagiert gleichermaßen auf eine Änderung der Datenträgergröße. Das Erstellen eines Volumes ist dank der klaren Anweisungen des Installationsprogramms schnell und einfach.

Fragen:

Fragen Diskussionsforum, die mit einer kurzen Erklärung beantwortet werden müssen. Die Antworten werden mit dem Mentor während der Mentoring-Sitzungen besprochen.

1. Wie können Sie Ihre Daten auf der Festplatte Ihres Computers schützen?
2. Welche Computerprogramme können Sie verwenden, um Ihre Daten zu schützen?

Fragen zur Selbsteinschätzung. Nach der Beantwortung kann der Lernende die Ergebnisse sehen und sie mit den auf der Plattform gespeicherten Ergebnissen vergleichen

1. Welches ist die sicherste Verschlüsselungsmethode zum Schutz Ihrer Dateien?

Anhänge:

1. Präsentation
2. Video

Referenzen:

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

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.