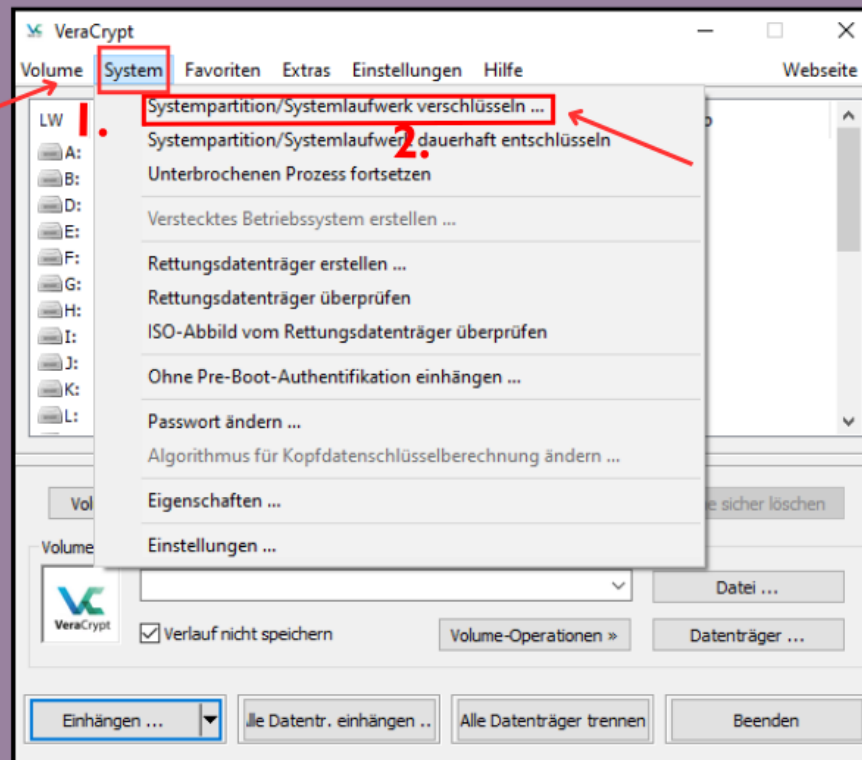


Grundlagen der IT Sicherheit

Teil 4 - PC

Verschlüsseln

I. Veracrypt starten, “System” und “Systempartition” auswählen



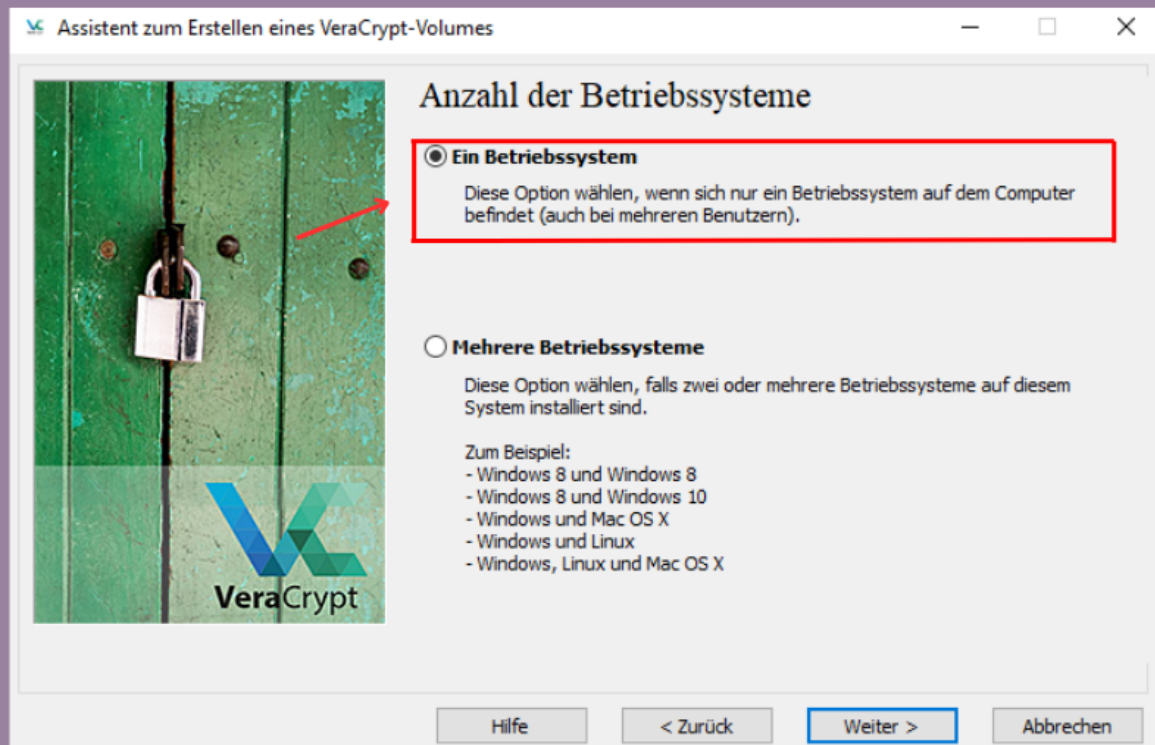
2. “Normale” Systemverschlüsselung auswählen



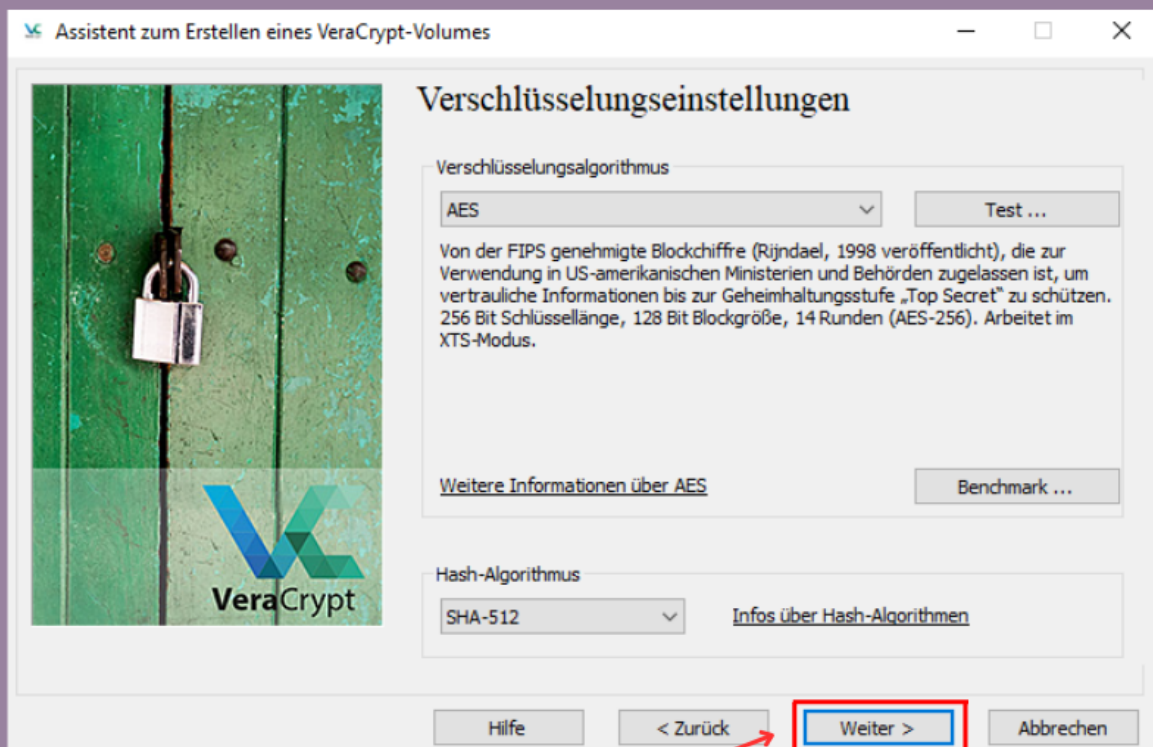
3. “Windows Systempartition verschlüsseln” anklicken



4. “Ein Betriebssystem” wählen, falls ihr nicht mehr installiert habt




5. Verschlüsselungsalgorithmus beibehalten



6. Passwort ausdenken

Assistent zum Erstellen eines VeraCrypt-Volumes



Passwort

Passwort:

Bestätigung:

☐ Schlüsseldat. verwenden Schlüsseldateien ...

☐ Passwort anzeigen

☐ PIM verwenden

Es wird dringend empfohlen, ein gutes Passwort zu wählen. Passwörter, die in einem Wörterbuch zu finden sind, und Kombinationen aus 2, 3 oder 4 solcher Wörter sollten nicht verwendet werden. Das Passwort sollte keine Namen oder Geburtstage enthalten und nicht leicht zu erraten sein. Ein gutes Passwort ist eine zufällige Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen wie @ ^ = \$ * + usw. Es ist zudem empfehlenswert, ein Passwort mit mehr als 20 Zeichen zu wählen (je länger, umso besser). Die mögliche Länge ist auf 128 Zeichen beschränkt.

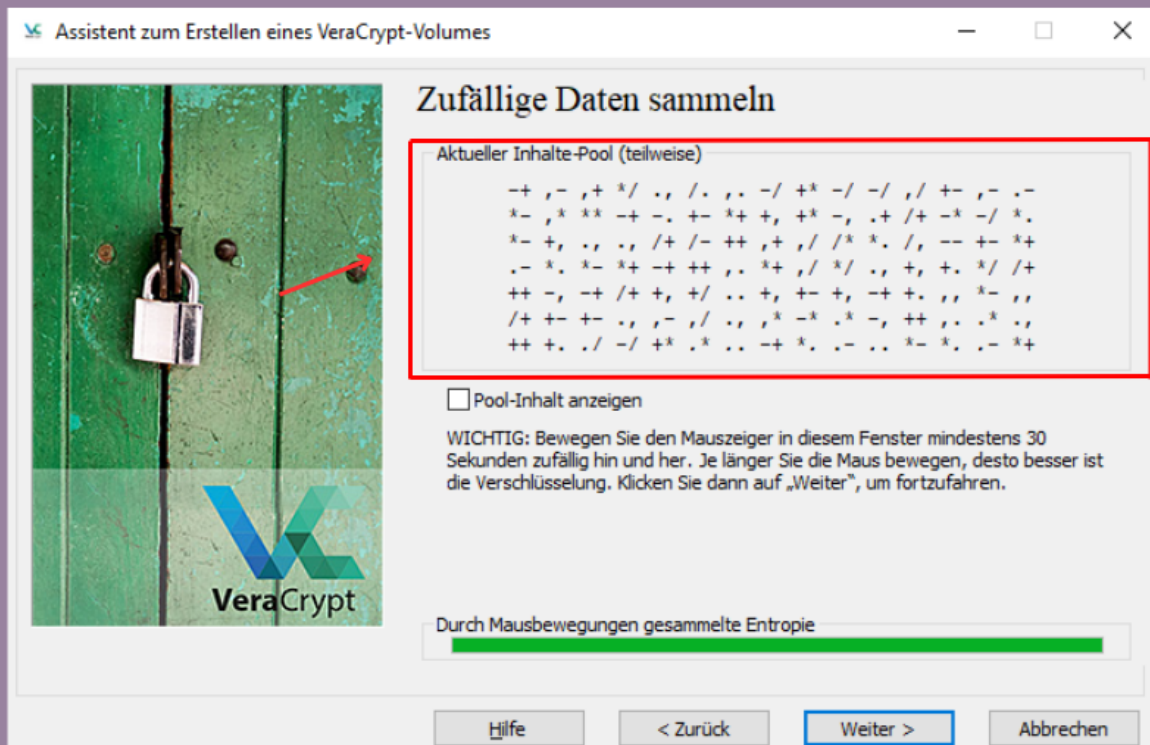
Hilfe

< Zurück

Weiter >

Abbrechen

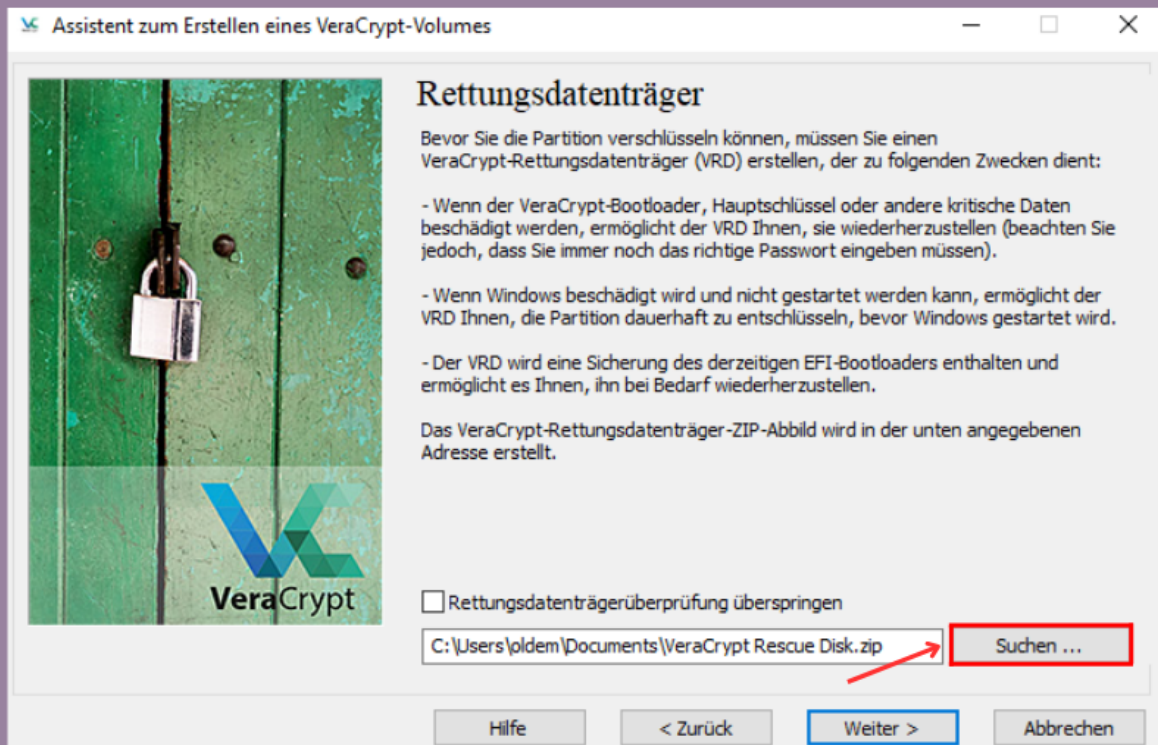
7. Verschlüsselung durch Mausbewegung generieren



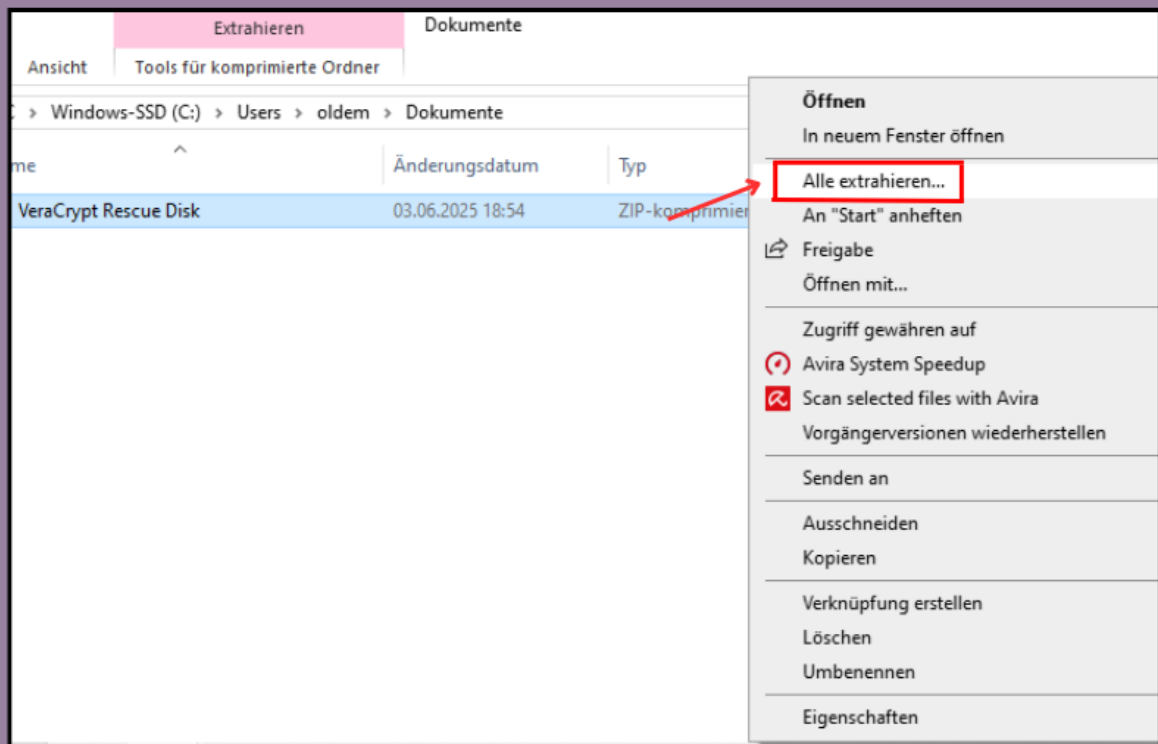
8. Neu erstellten Schlüssel bestätigen



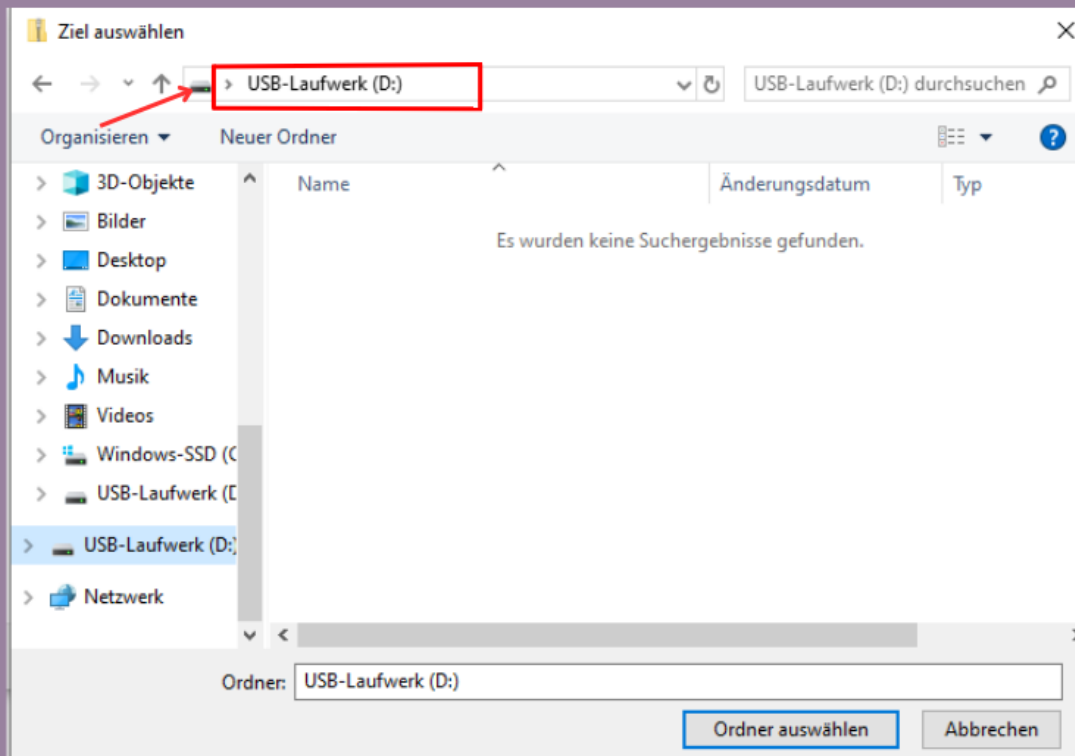
9. USB Stick anschließen und Rettungsdatei erstellen



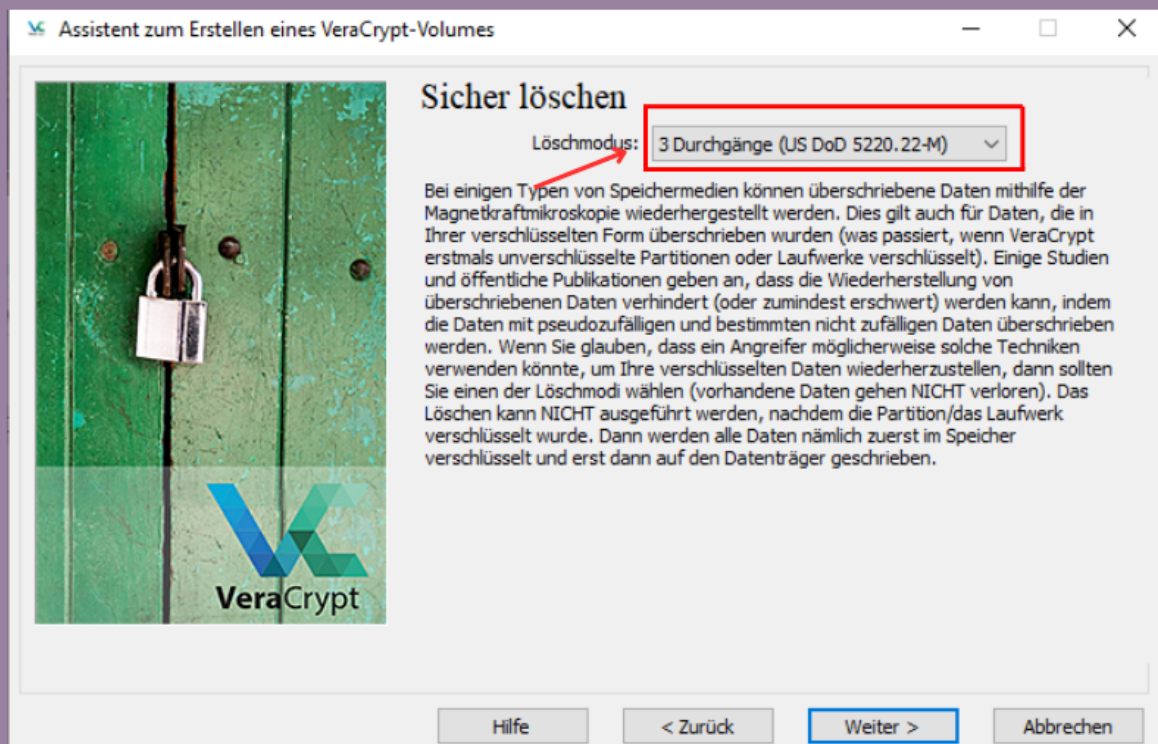
10. Heruntergeladene Datei mit Rechtsklick extrahieren



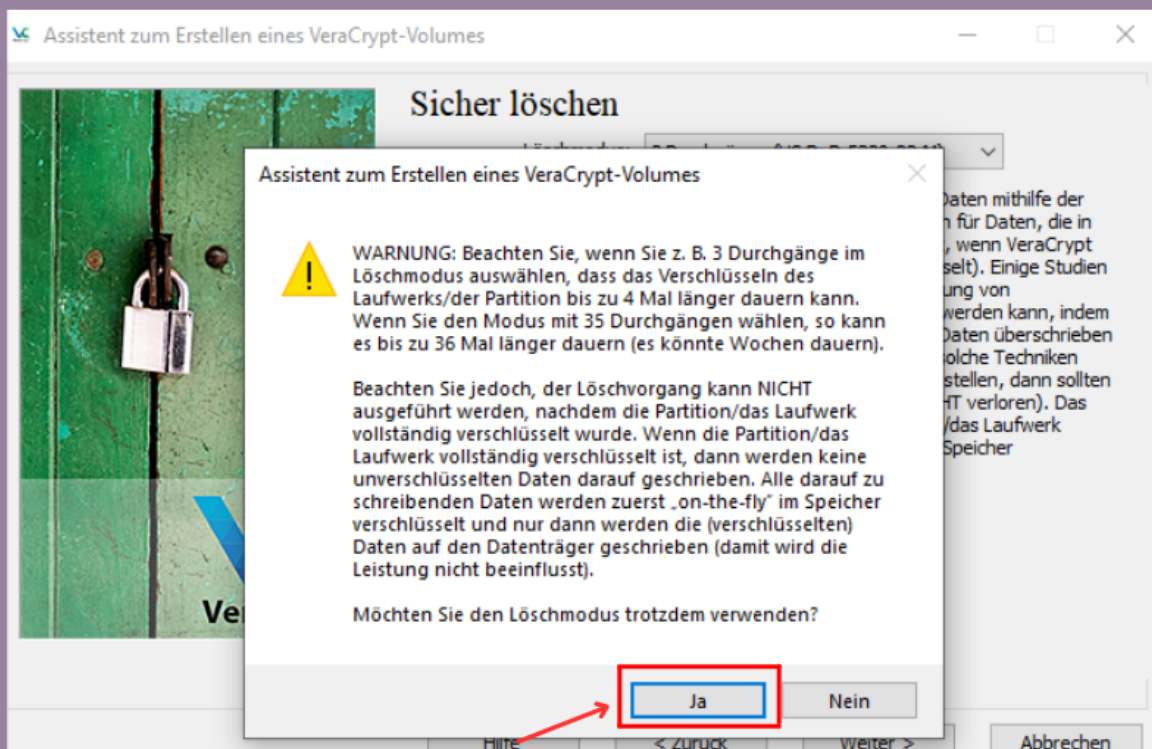
II. USB Stick als Extraktionsort auswählen



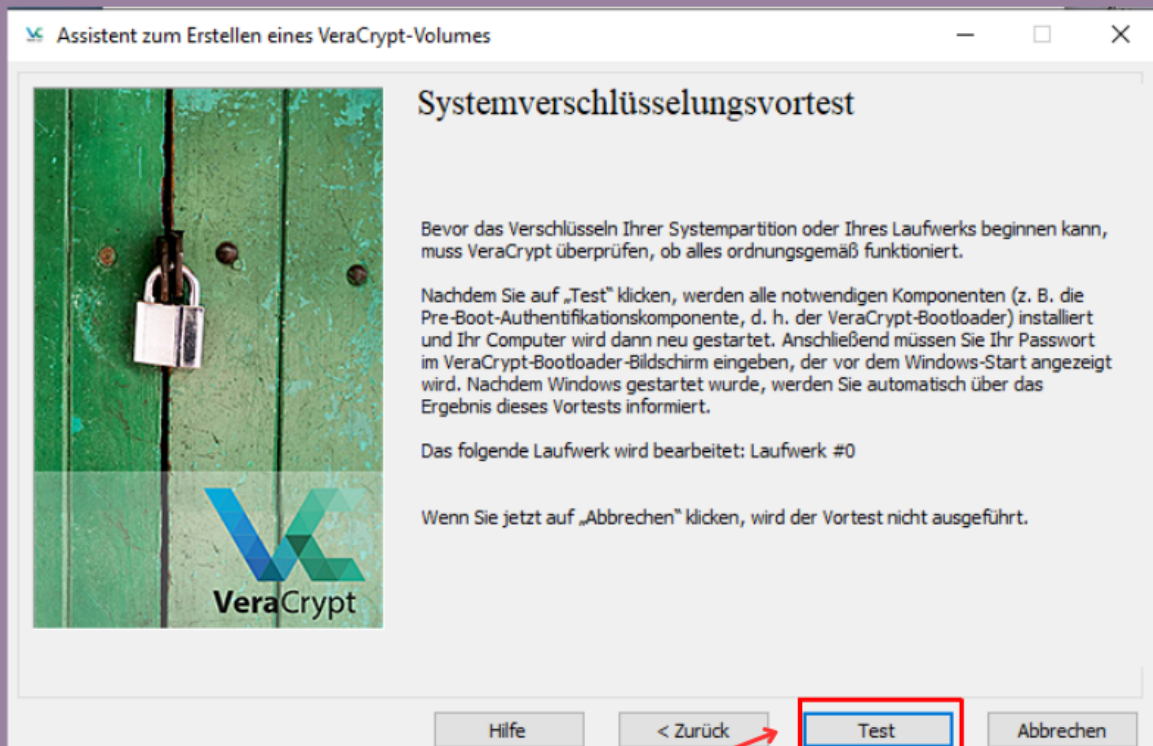
12. Anzahl Löschvorgänge auswählen: Mindestens 3 Durchgänge



13. Löschvorgang bestätigen



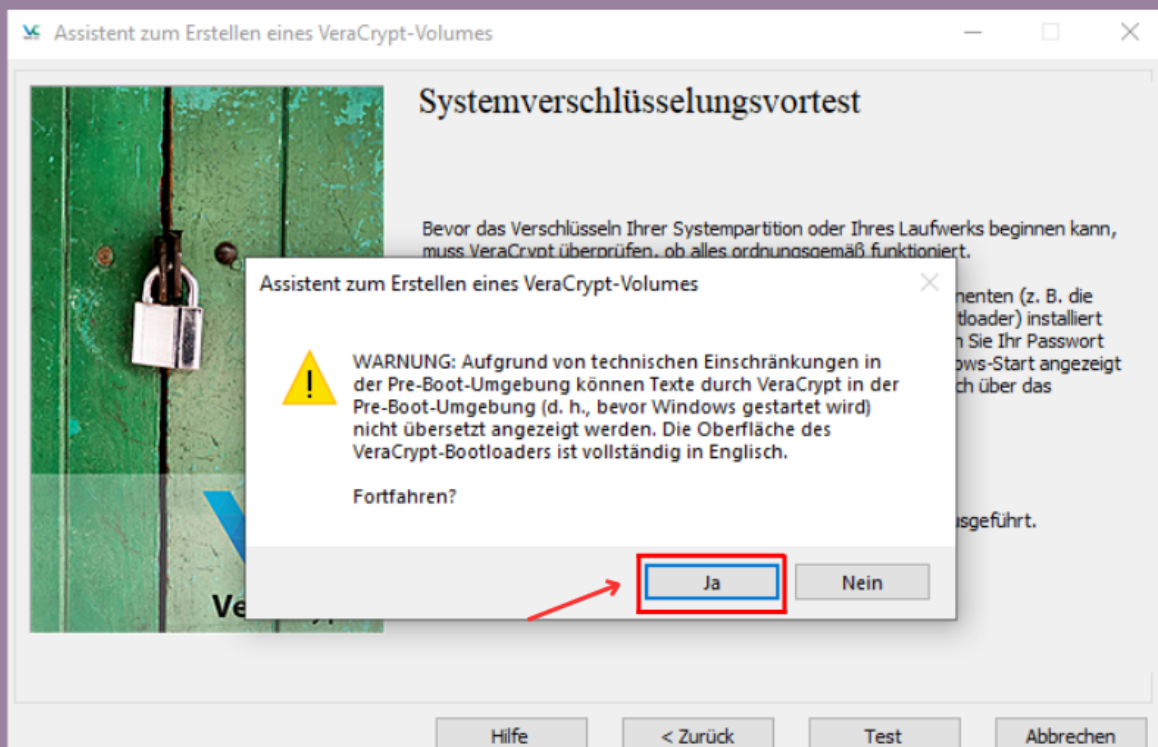
14. Testvorgang starten: PC startet neu und Kennwort eingeben



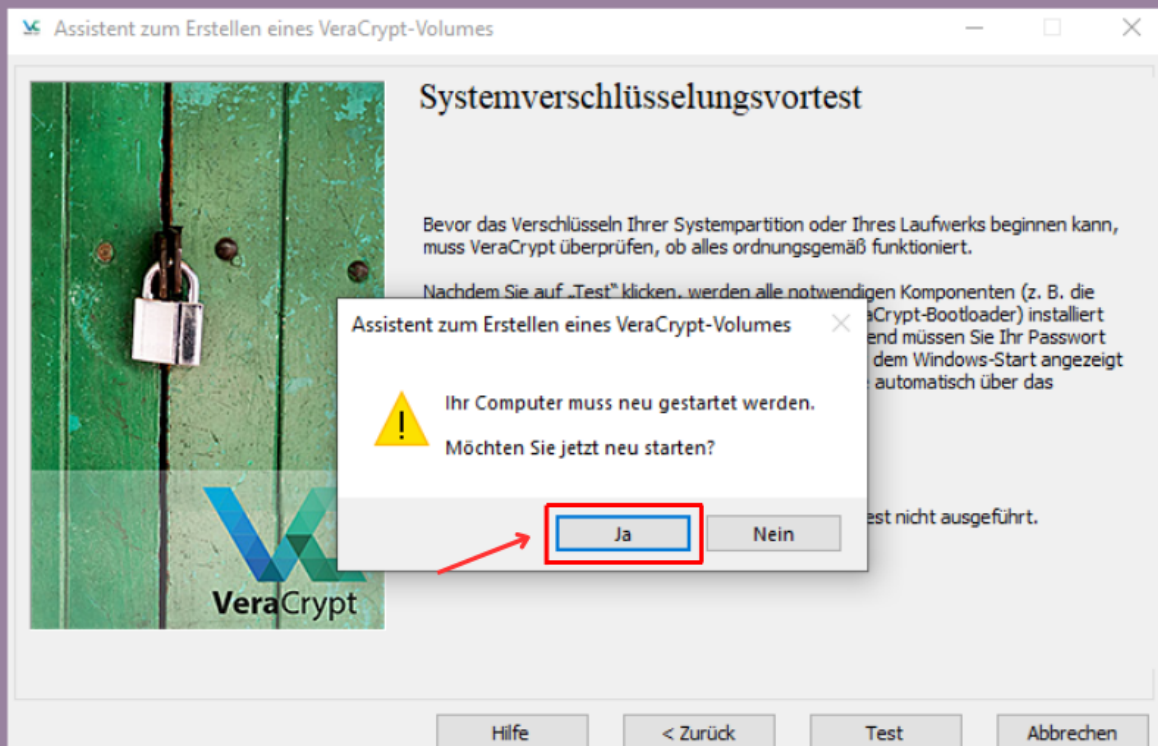
15. Testvorgang starten



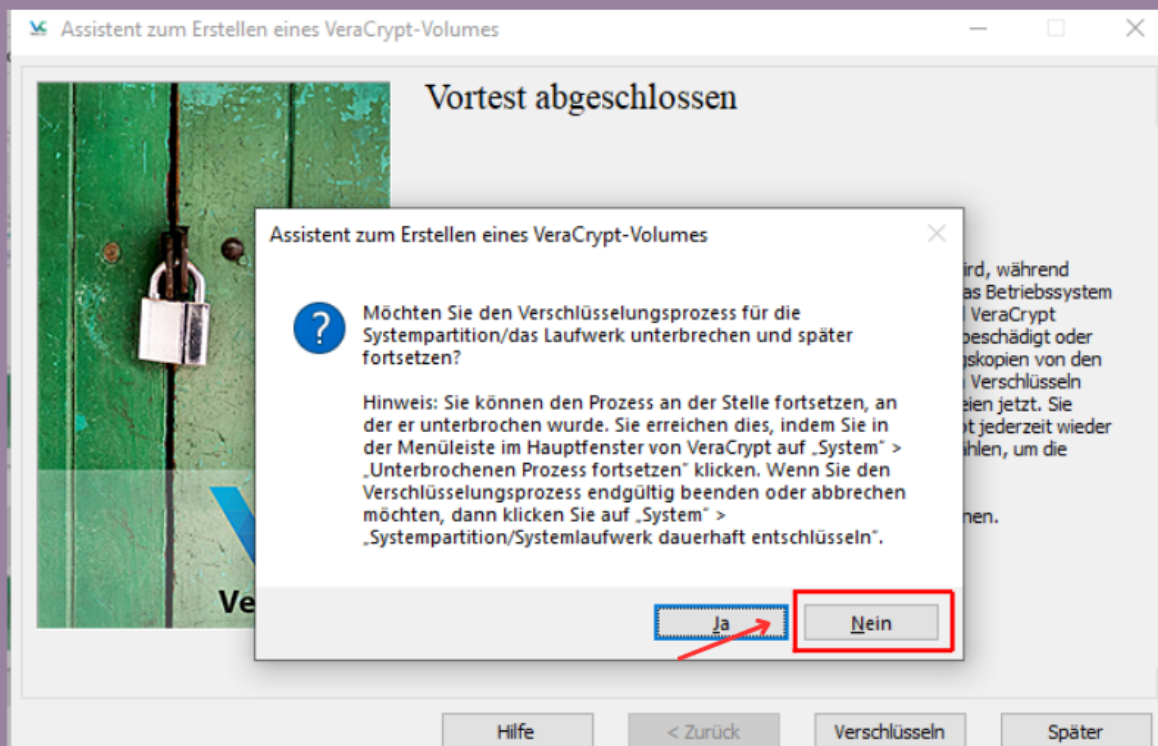
16. Warnung bestätigen



17. Neustart durchführen und Kennwort eingeben



18. Verschlüsselungsprozess fortsetzen



19. Rettungsdatenträger-Anleitung bestätigen

