Bitlocker

BitLocker ist ein Windows-Sicherheitsfeature, das die Verschlüsselung für ganze Volumes (Festplatten, USB-Sticks) bereitstellt und die Bedrohungen durch Datendiebstahl oder Offenlegung durch verlorene, gestohlene oder unangemessen außer Betrieb gesetzte Geräte angeht.

Praktische Anwendungsfälle

Daten auf einem verlorenen oder gestohlenen Gerät sind anfällig für nicht autorisierten Zugriff, entweder durch Ausführen eines Softwareangriffstools gegen das Gerät oder durch Übertragen der Festplatte des Geräts auf ein anderes Gerät. BitLocker trägt dazu bei, nicht autorisierten Datenzugriff zu mindern, indem der Datei- und Systemschutz verbessert wird, sodass der Zugriff auf Daten nicht mehr möglich ist, wenn bitLocker-geschützte Geräte außer Betrieb genommen oder wiederverwendet werden.

Folgenden Windows-Editionen, unterstützen die BitLocker-Aktivierung:

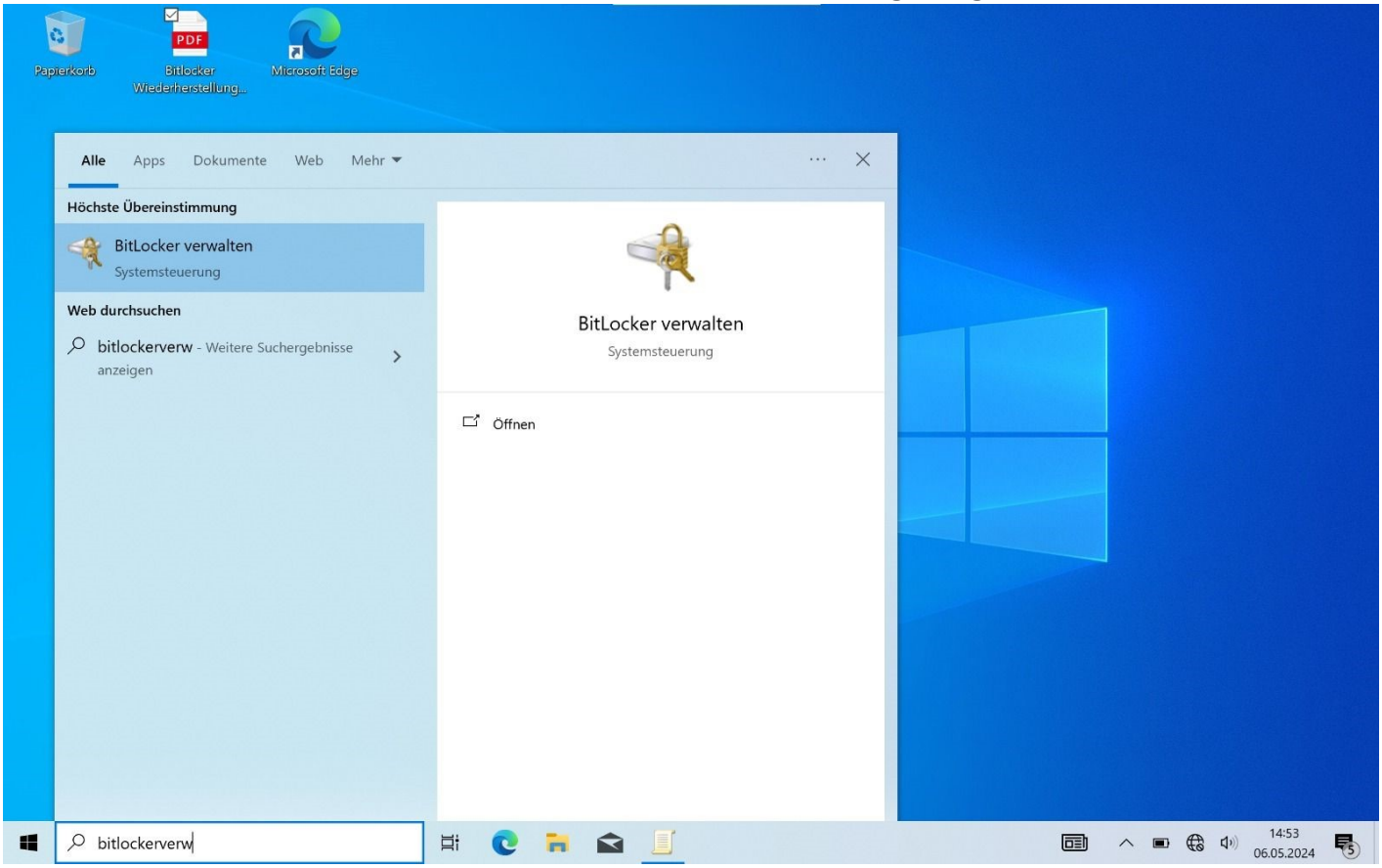
- Windows Pro
- Windows Enterprise
- Windows Pro Education/SE
- Windows Education

Weitere Informationen finden Sie auf der Microsoft Seite: https://learn.microsoft.com/de-de/windows/security/operating-system-security/data-protection/bitlocker/#system-requirements

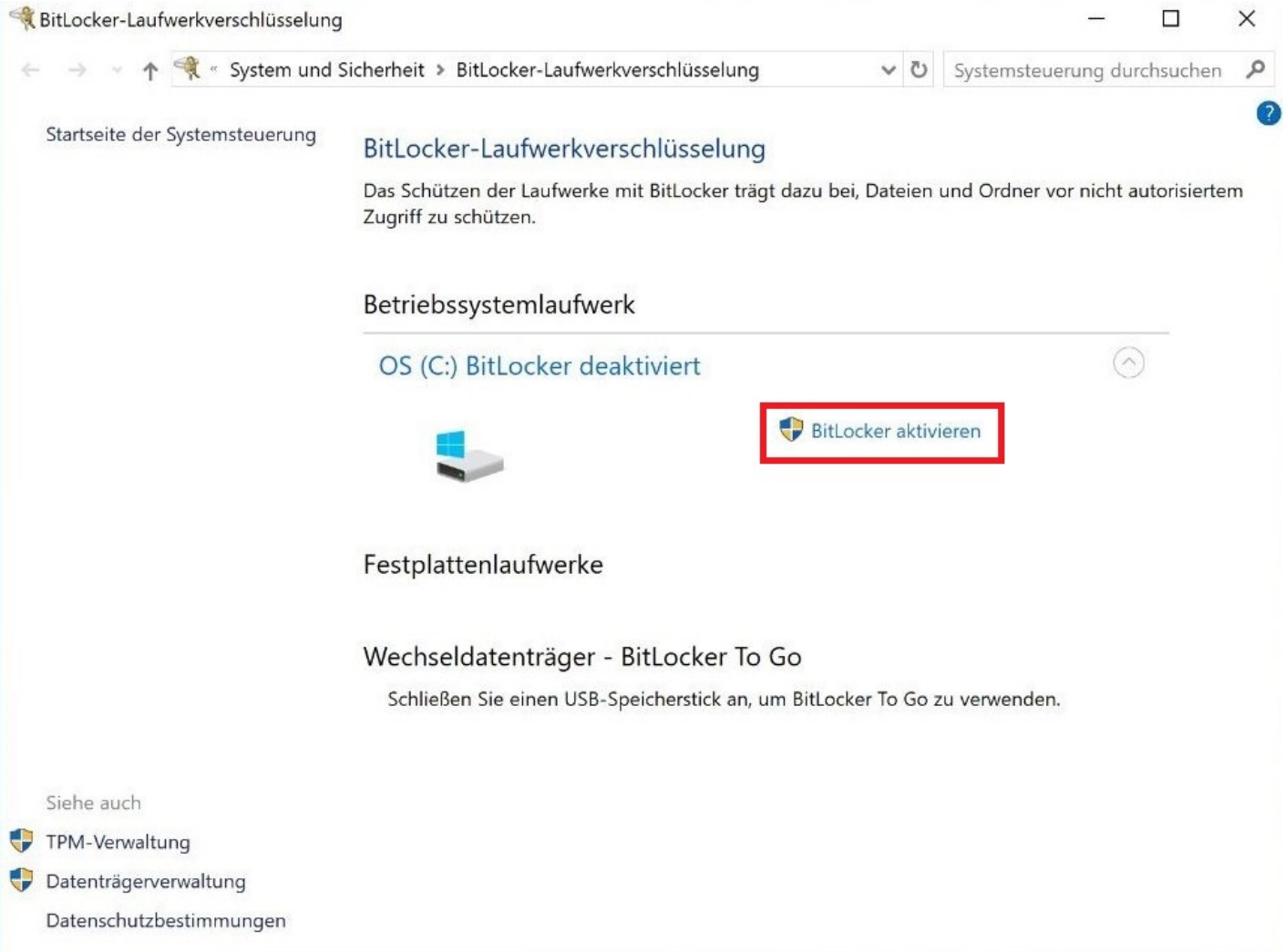
- Bitlocker aktivieren
- Bitlocker Pin einrichten

Bitlocker aktivieren

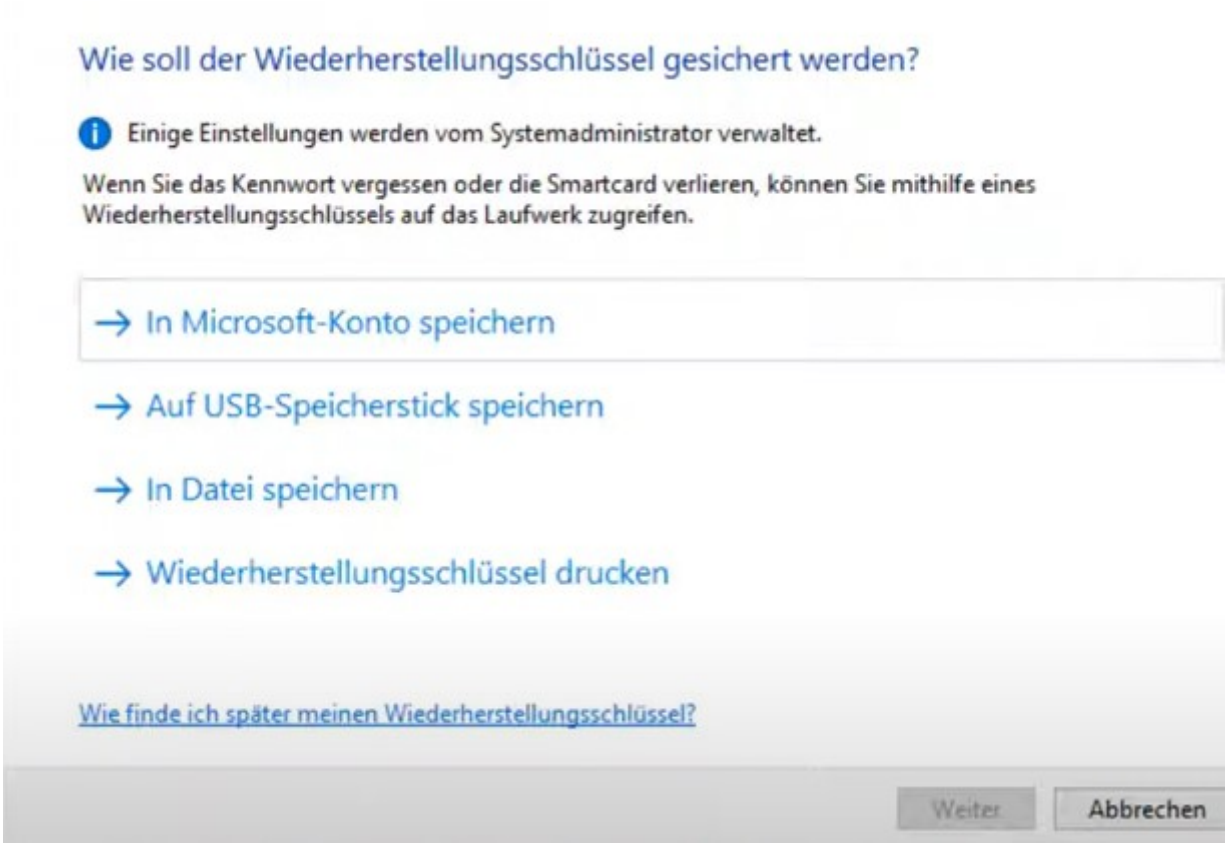
Schritt 1: In die Suchleiste „Bitlocker“ oder "Bitlockerverwaltung" eingeben.



Schritt 2: Es öffnet sich die Bitlocker-Laufwerksverschlüsselung



Schritt 3: Nachdem Sie auf „Bitlocker aktivieren“ geklickt haben, erscheint folgendes Fenster.



Hier können Sie auswählen wie der Wiederherstellungsschlüssel gesichert werden soll. Es werden mehrere Optionen angeboten.

- Direkt im Konto MS Konto abspeichern
- Den Schlüssel auf einem Stick kopieren
- Im Ordner abspeichern
- Den Wiederherstellungsschlüssel ausdrucken

> **FALLS MAN DIE BITLOCKER PIN VERGESSEN HABEN SOLLTE, KANN OHNE DEN WIEDERHERSTELLUNGSSCHLÜSSEL NICHT AUF DEN PC/LAPTOP ZUGEGRIFFEN WERDEN!**

Schritt 4: Beispiel eines Wiederherstellungsschüssels.

> **Diesen auf einem externen Gerät abspeichern oder ausdrucken und an einem Sicheren Ort aufbewahren!**

Wiederherstellungsschlüssel für die BitLocker-Laufwerkverschlüsselung

Um zu überprüfen, ob es sich um den richtigen Wiederherstellungsschlüssel handelt, vergleichen Sie den Beginn des folgenden Bezeichners mit dem auf dem PC angezeigten Bezeichnerwert.

Bezeichner:

1E0906AA-B5EC-4C7B-8B72-460FA3AD1589

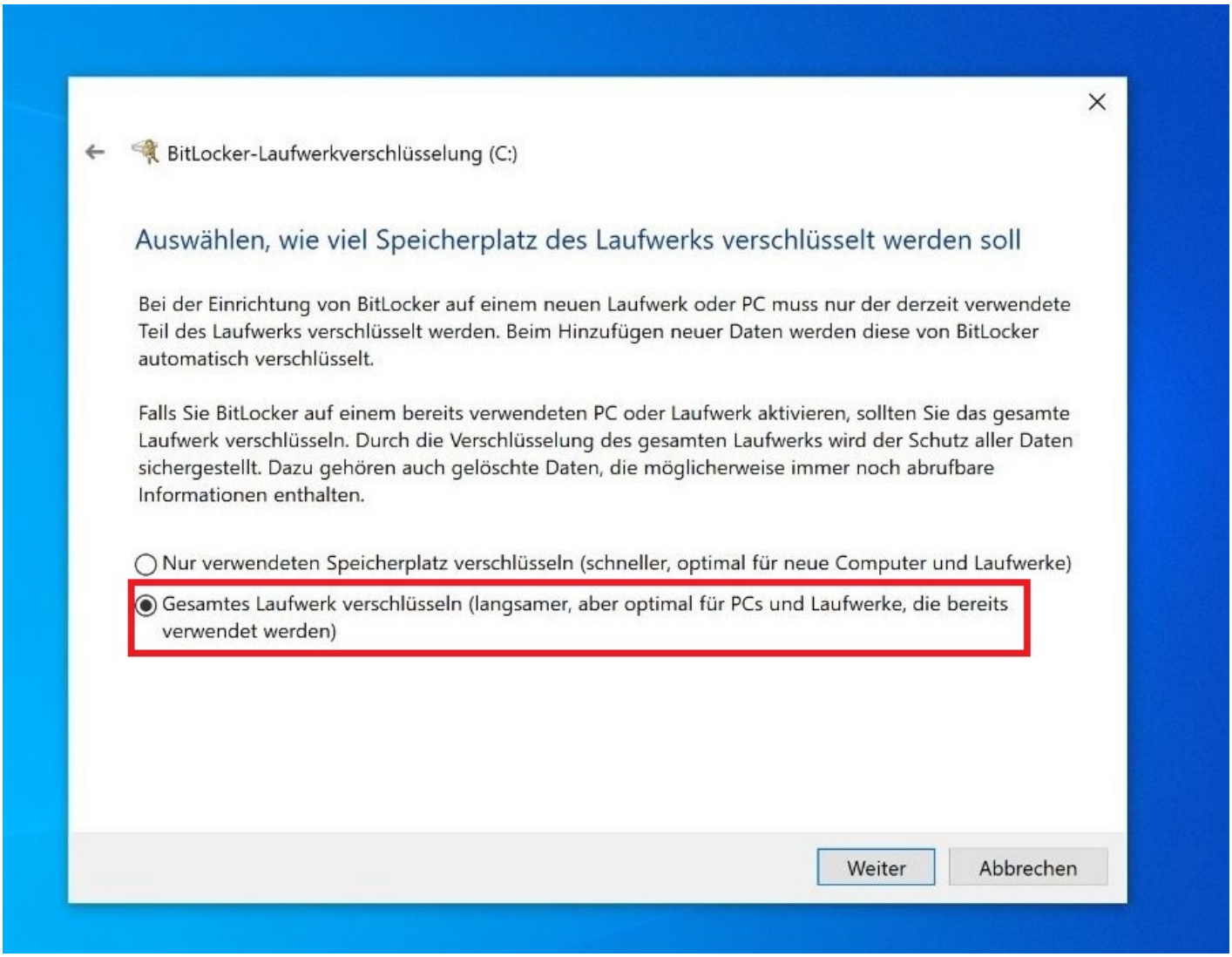
Falls der obige Bezeichner mit dem auf dem PC angezeigten Bezeichner übereinstimmt, sollten Sie den folgenden Schlüssel zum Entsperren des Laufwerks verwenden.

Wiederherstellungsschlüssel:

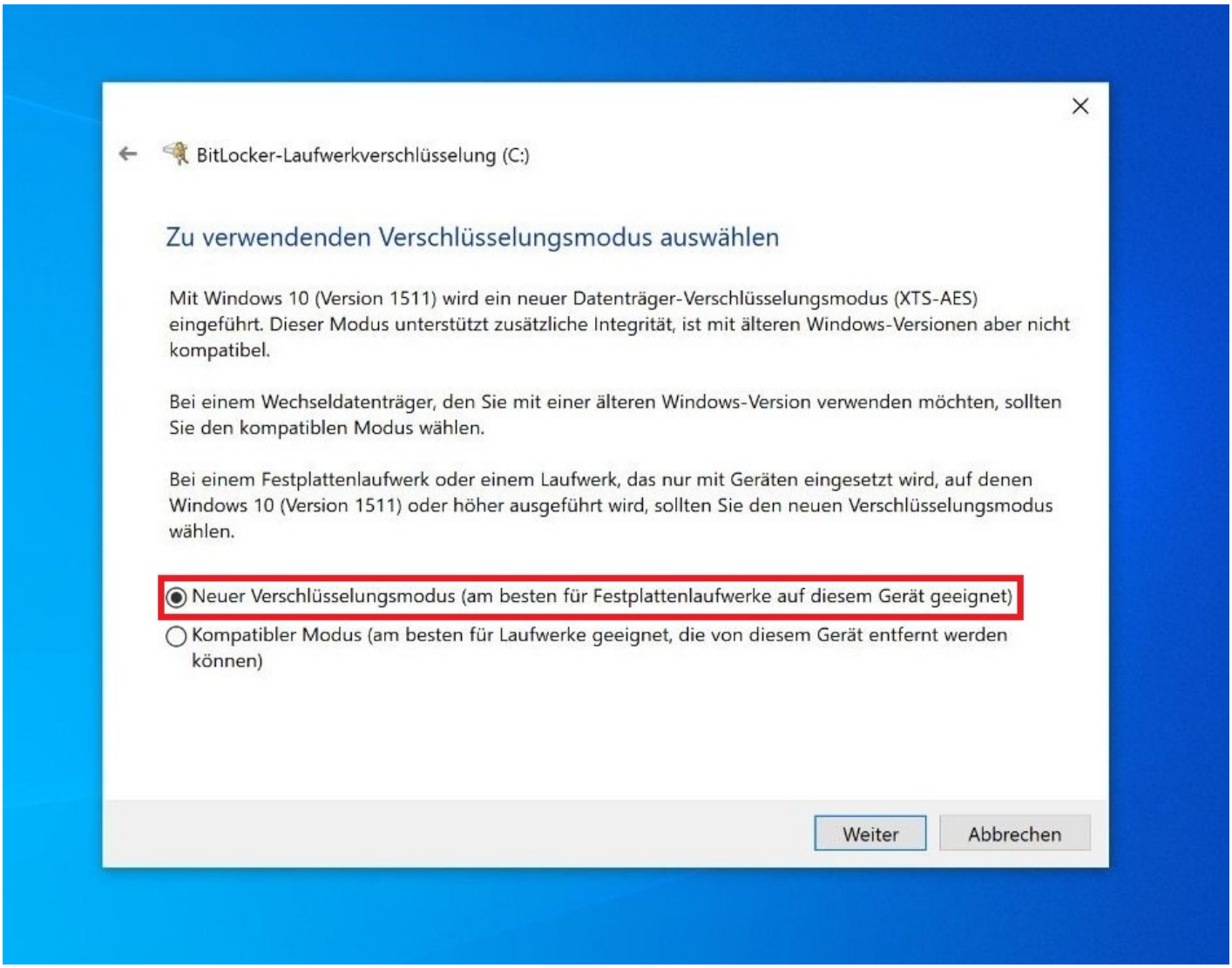
295735-501160-091399-549604-498531-459965-625548-334279

Falls der obige Bezeichner nicht mit dem auf dem PC angezeigten Bezeichner übereinstimmt, handelt es sich nicht um den richtigen Schlüssel zum Entsperren des Laufwerks.
Versuchen Sie es mit einem anderen Wiederherstellungsschlüssel, oder suchen Sie unter "https://go.microsoft.com/fwlink/?LinkID=260589" nach weiteren Informationen.

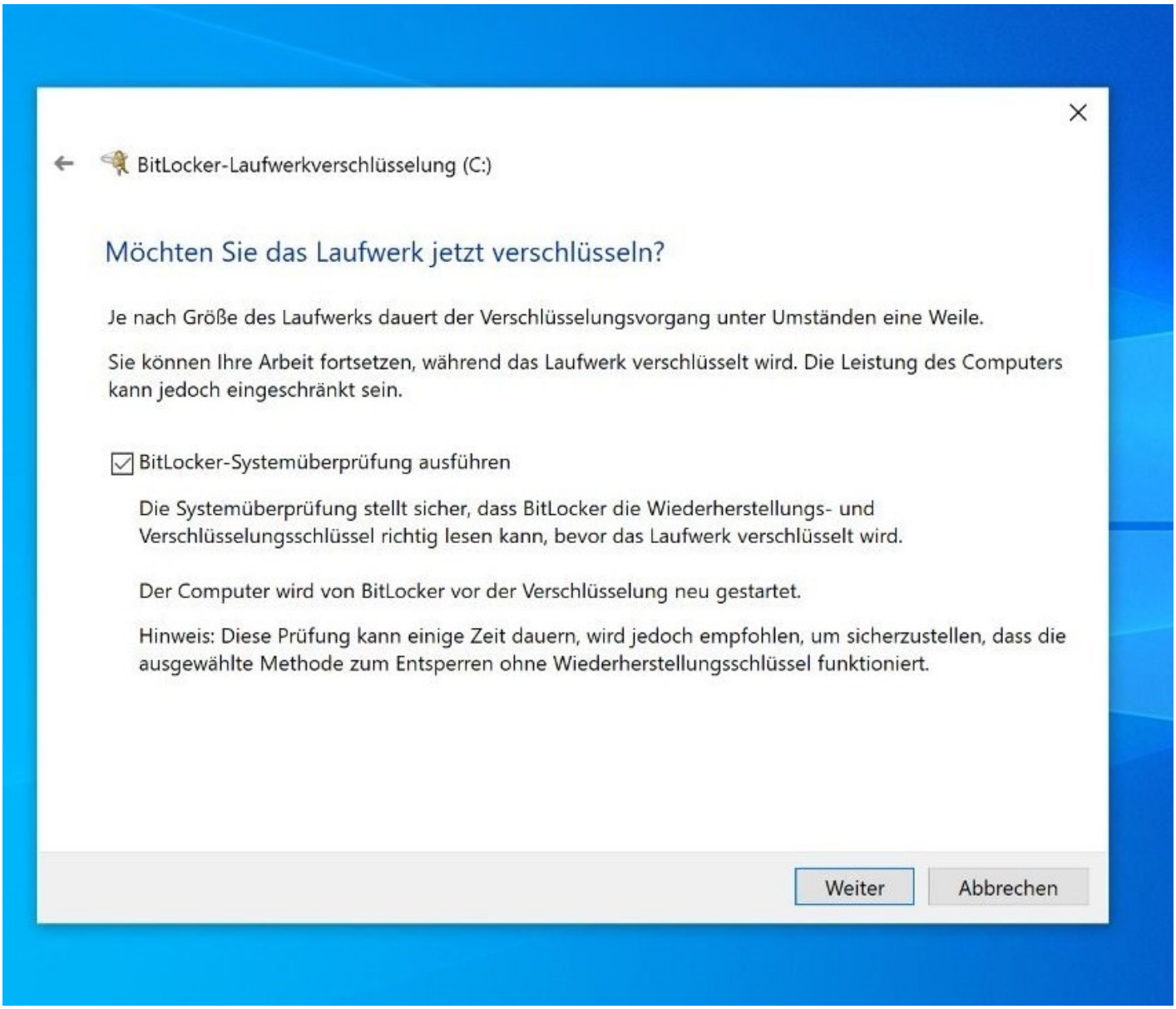
Schritt 5: Auswahl, wie viel Speicherplatz verschlüsselt werden soll. Empfehlung: "Gesamtes Laufwerk verschlüsseln"



Schritt 6: Verschlüsselungsmodus wählen. Es empfiehlt sich den "Neuer Verschlüsselungsmodus" zu wählen. Der "Kompatibler Modus" ist für USB-Sticks oder externe Festplatten geeignet.



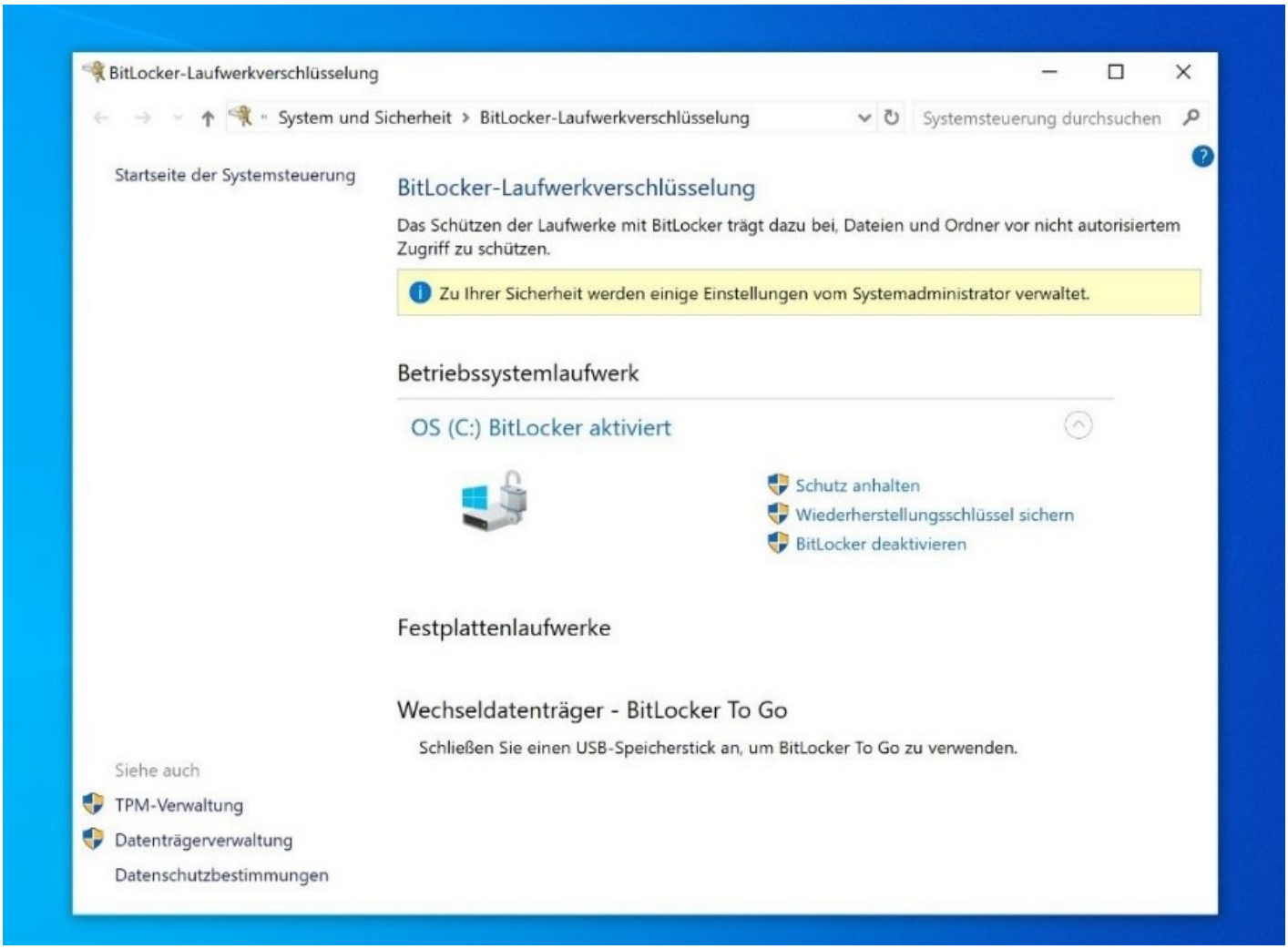
Schritt 7: Als nächster Schritt empfiehlt sich die Systemüberprüfung auszuführen.



Schritt 8: Durch klicken auf weiter wird die Verschlüsselung gestartet. Dies kann eine bestimmte Zeit in Anspruch nehmen.

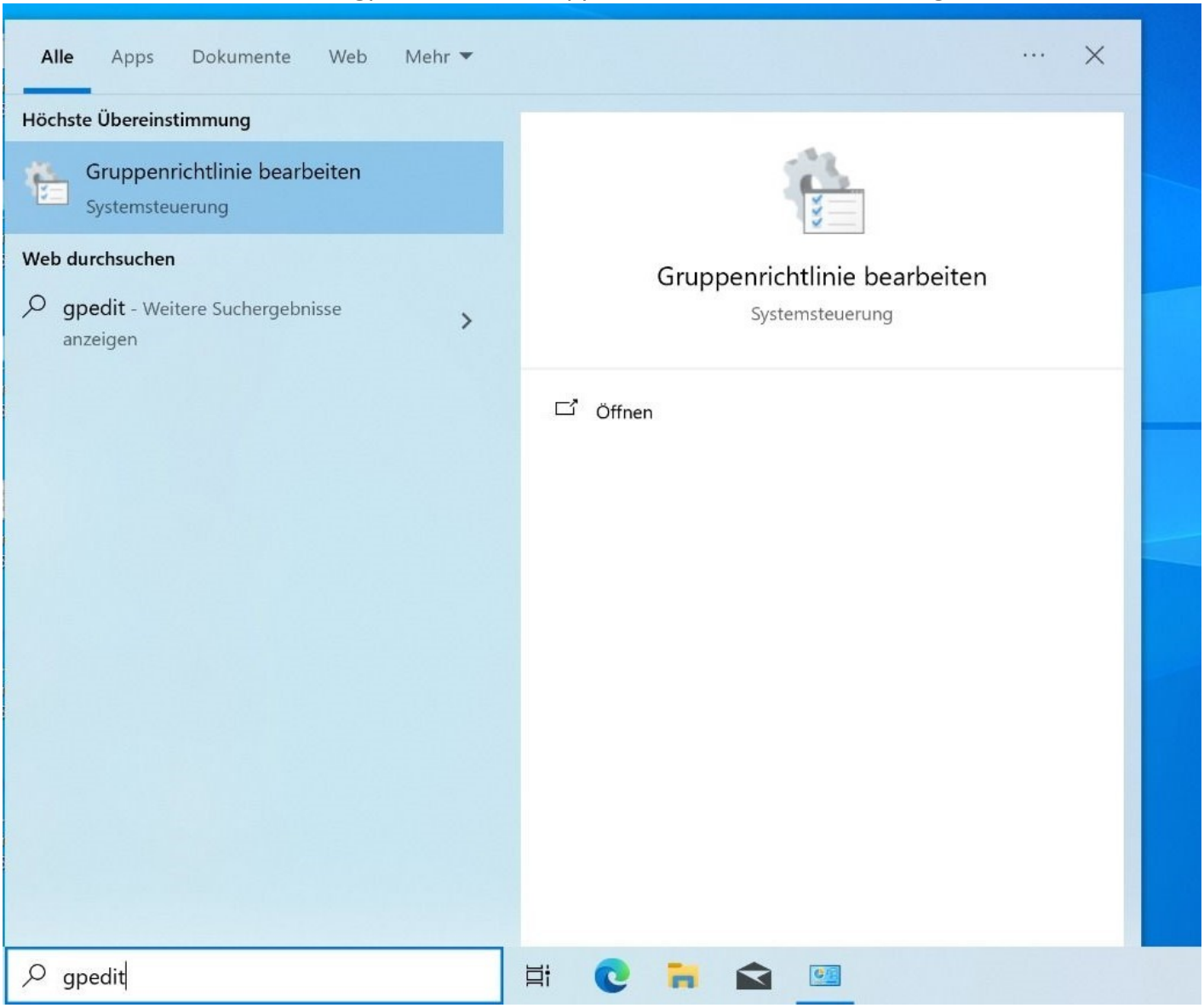
Schritt 9: Im letzten Schritt muss das System neu gestartet werden.

Schritt 10: Anschließend sollte es aktiviert sein.

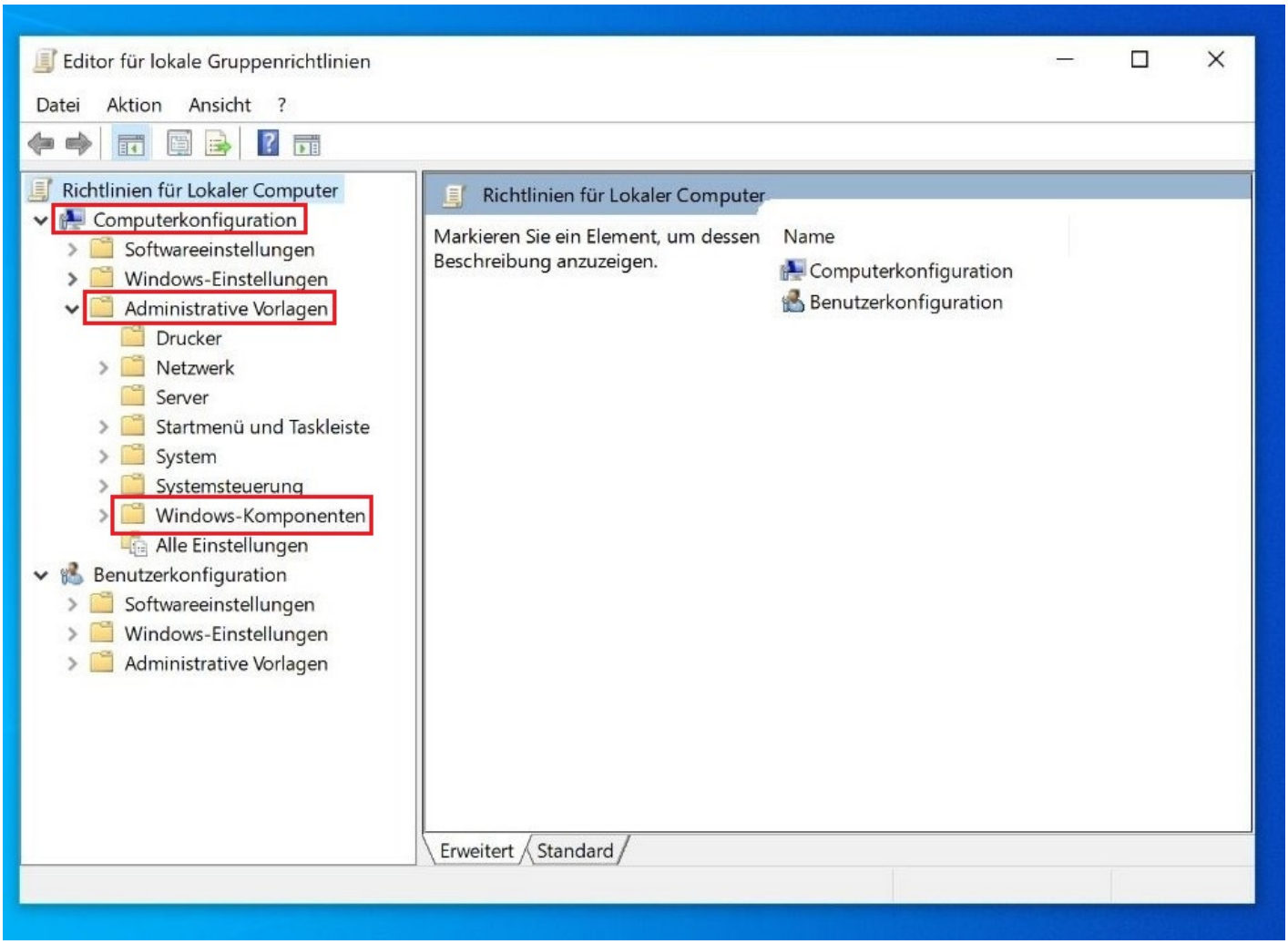

BitLocker-Laufwerkverschlüsselung
System und Sicherheit › BitLocker-Laufwerkverschlüsselung
Systemsteuerung durchsuchen
Startseite der Systemsteuerung
BitLocker-Laufwerkverschlüsselung
Das Schützen der Laufwerke mit BitLocker trägt dazu bei, Dateien und Ordner vor nicht autorisiertem Zugriff zu schützen.
Zu Ihrer Sicherheit werden einige Einstellungen vom Systemadministrator verwaltet.
Betriebssystemlaufwerk
OS (C:) BitLocker aktiviert
Schutz anhalten
Wiederherstellungsschlüssel sichern
BitLocker deaktivieren
Festplattenlaufwerke
Wechseldatenträger - BitLocker To Go
Schließen Sie einen USB-Speicherstick an, um BitLocker To Go zu verwenden.
Siehe auch
TPM-Verwaltung
Datenträgerverwaltung
Datenschutzbestimmungen

Bitlocker Pin einrichten

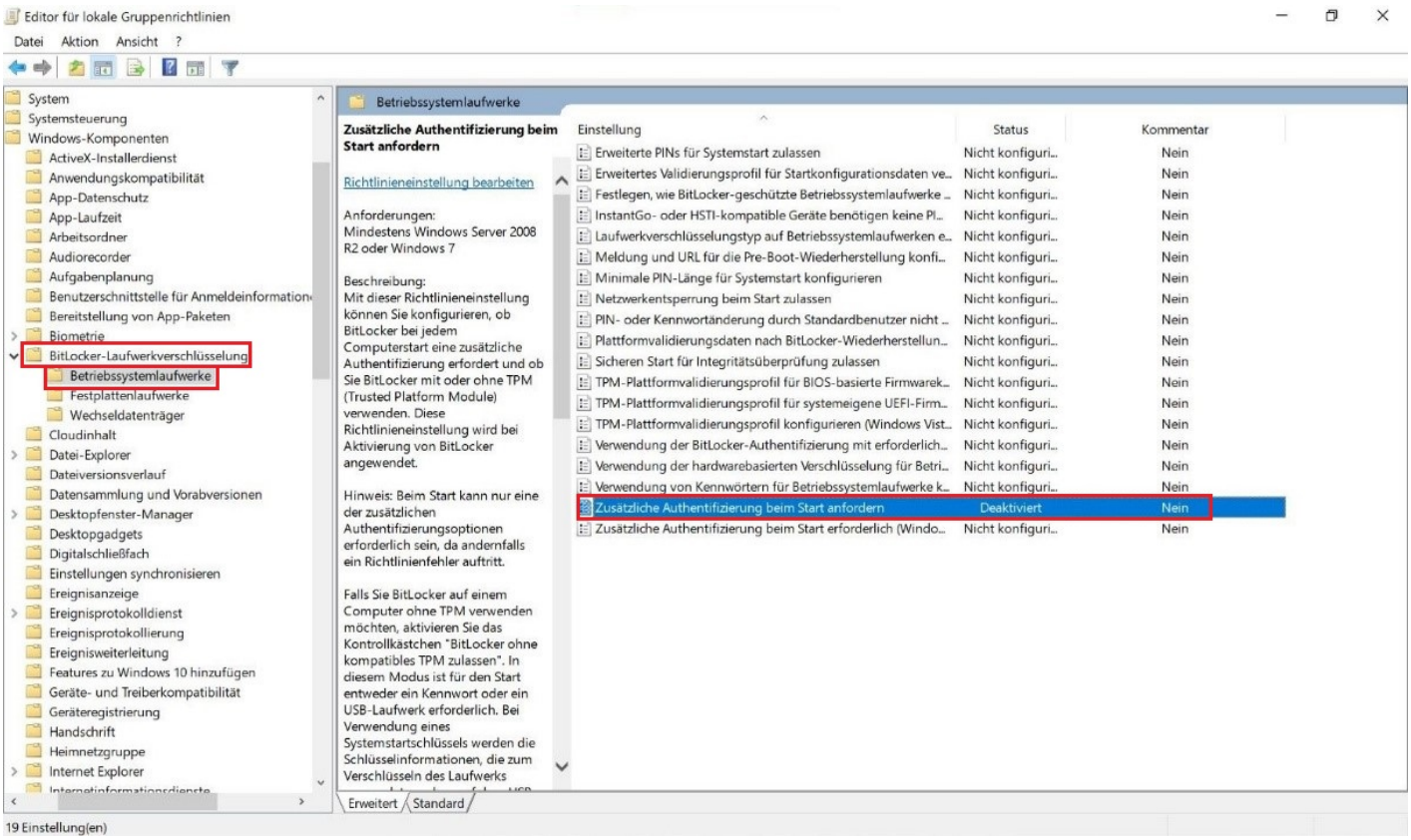
Schritt 1: In die Suchleiste „gpedit“ oder „Gruppenrechtlinie bearbeiten“ eingeben.



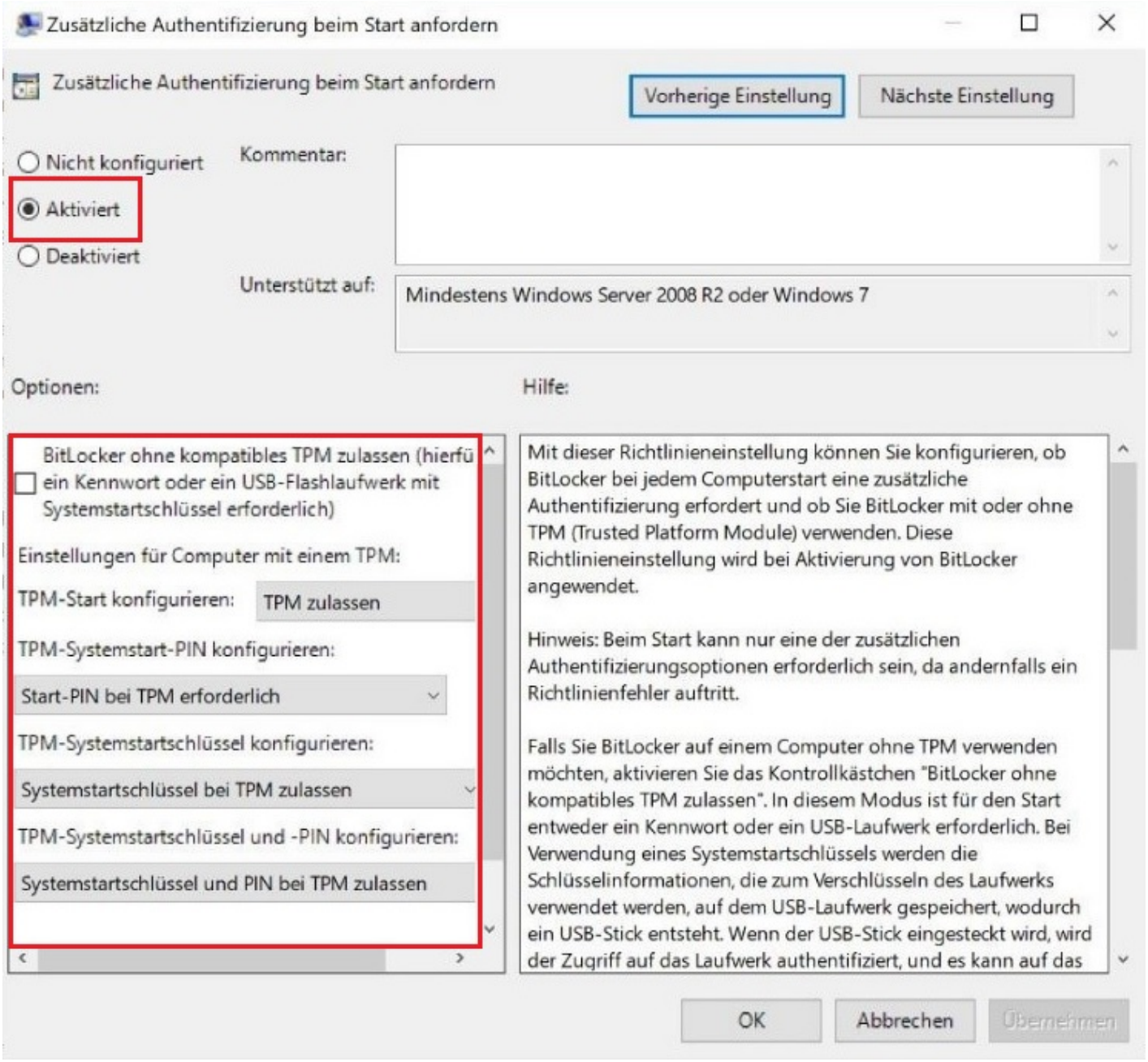
Schritt 2: Das Fenster "Editor für lokale Gruppenrichtlinen" öffnet sich. Dort Navigiert man zu "Computerkonfiguration" -> "Administrative Vorlagen" -> "Windows-Komponenten" ->



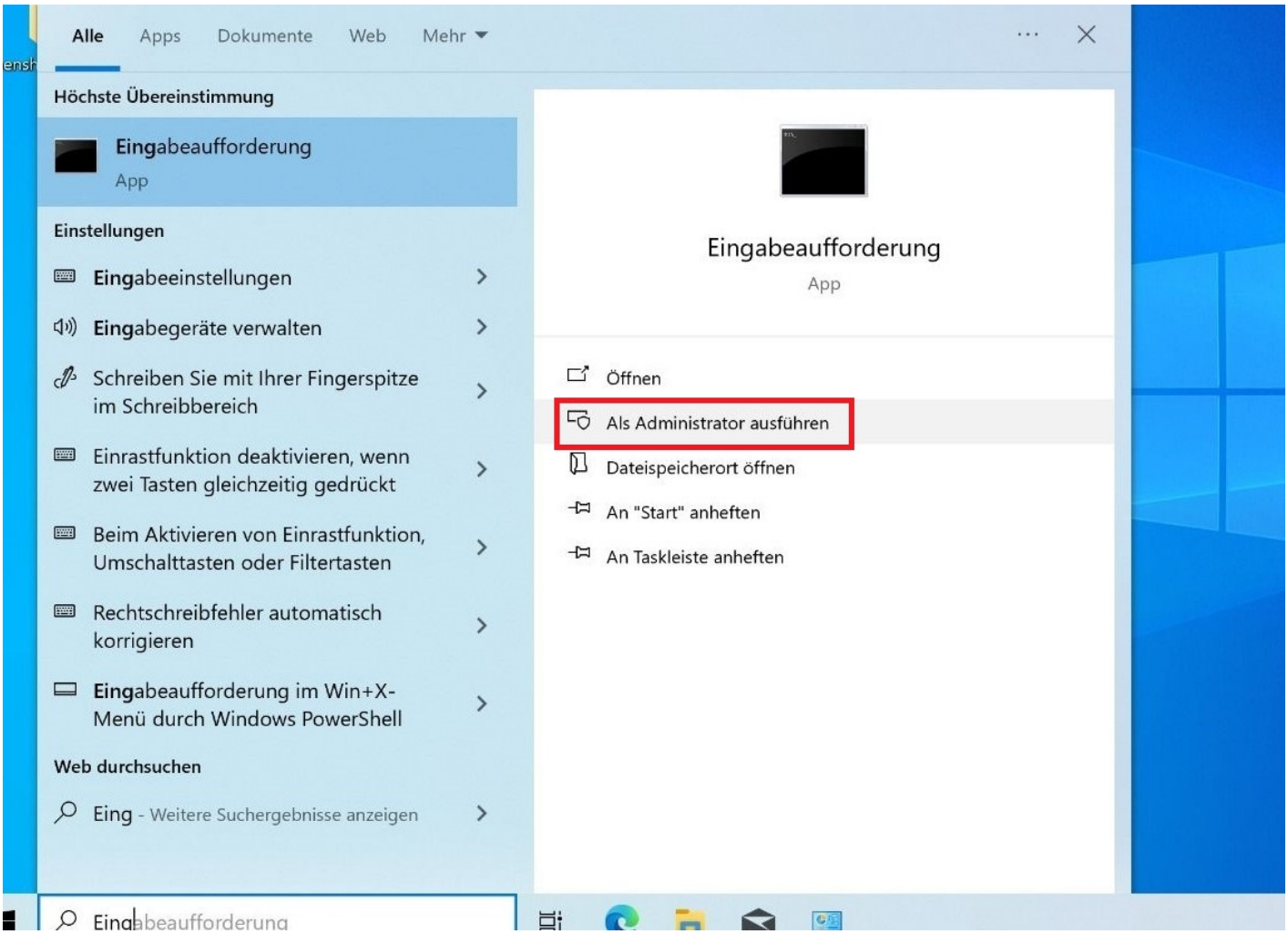
"Bitlocker-Laufwerksverschlüsselung" -> "Betriebssystemlaufwerke" -> doppelklick auf "Zusätzliche Authentifizierung beim Start anfordern"



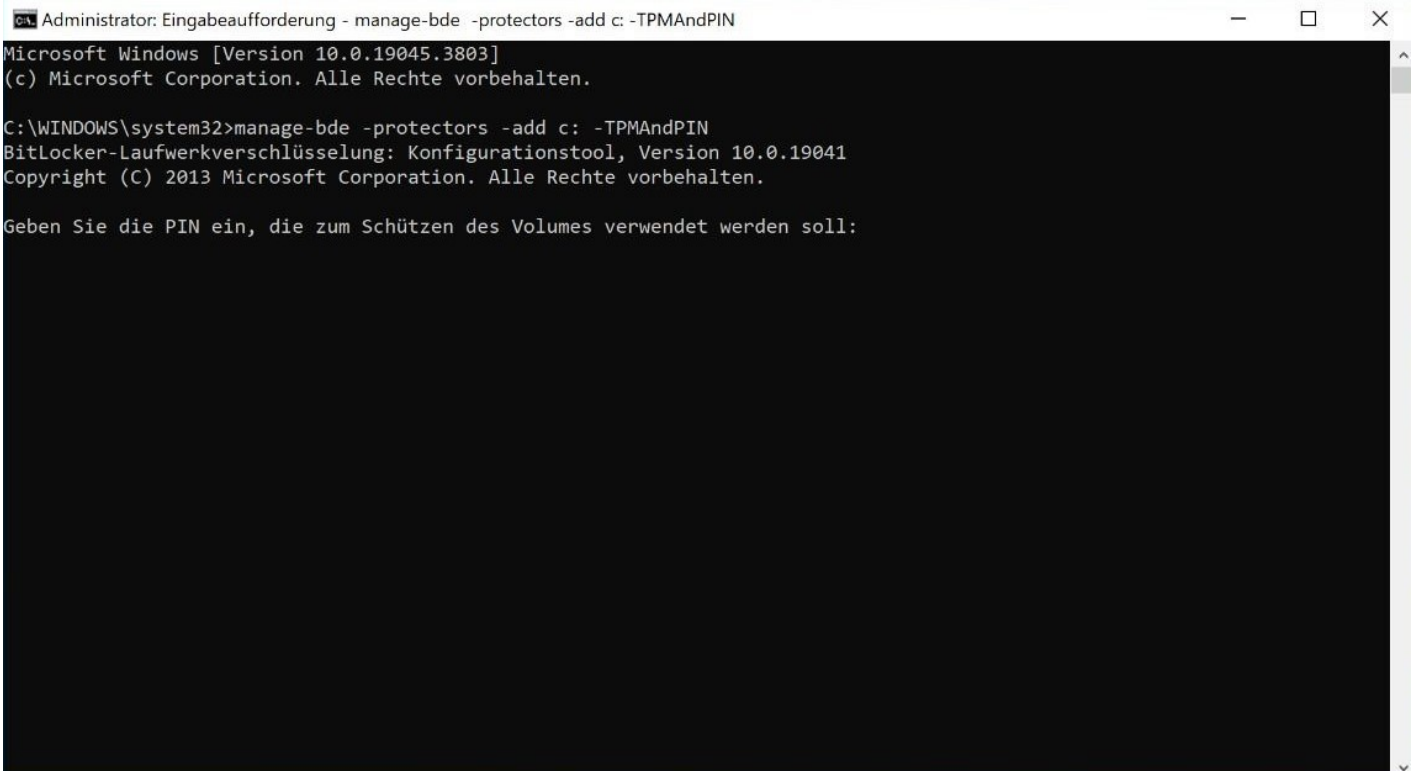
Schritt 3: Es öffnet sich folgendes Fenster. Das Modul oben links auf "Aktiviert" setzen und in den Optionen „Start Pin bei TPM erforderlich“ auswählen und mit "OK" bestätigen.



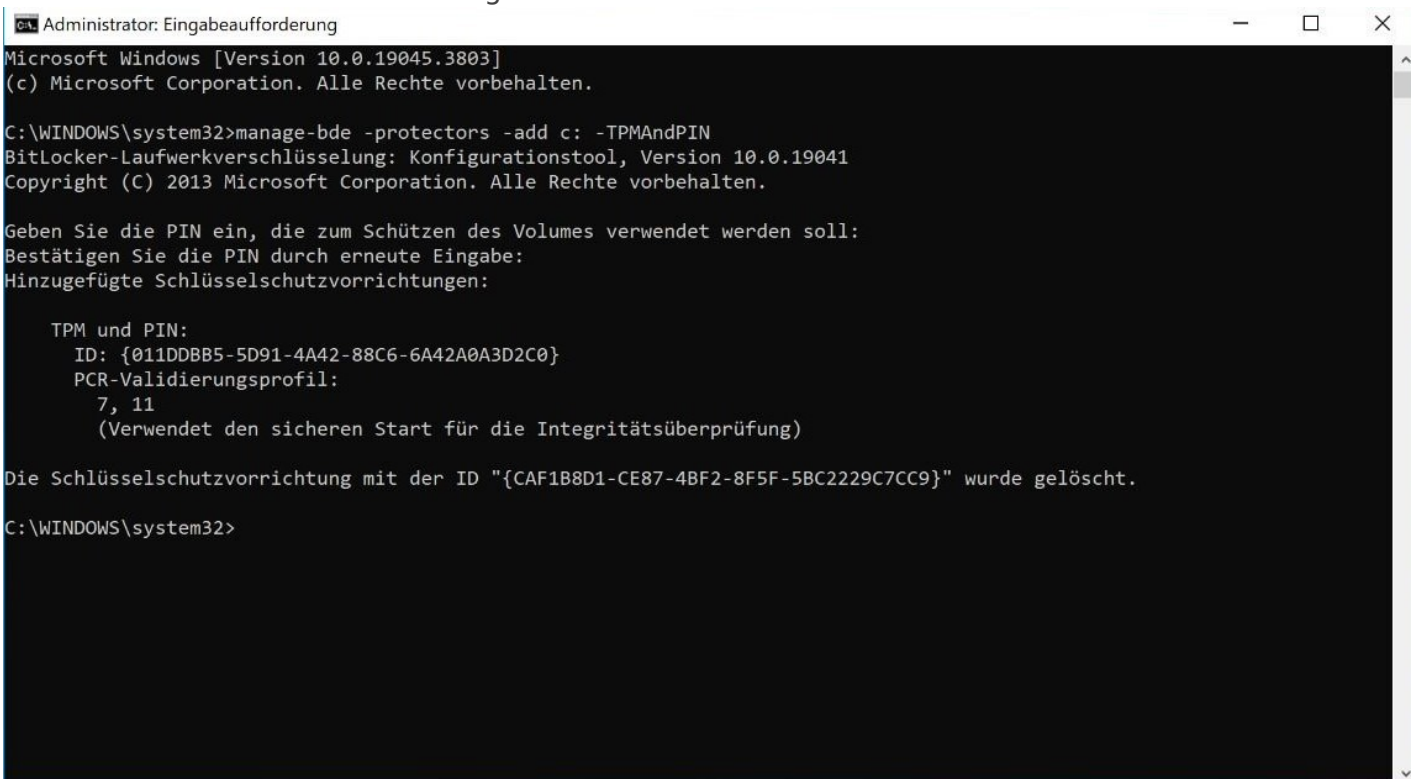
Schritt 4: Anschließend muss eine PIN vergeben werden. Dazu starten wir in die Eingabeaufforderung. Dafür im Suchfeld "cmd" eingeben. GANZ WICHTIG! Als Administrator ausführen.


Alle
Apps
Dokumente
Web
Mehr
Höchste Übereinstimmung
Eingabeaufforderung
App
Einstellungen
Eingabeeinstellungen
Eingabegeräte verwalten
Schreiben Sie mit Ihrer Fingerspitze im Schreibbereich
Einrastfunktion deaktivieren, wenn zwei Tasten gleichzeitig gedrückt
Beim Aktivieren von Einrastfunktion, Umschalttasten oder Filtertasten
Rechtschreibfehler automatisch korrigieren
Eingabeaufforderung im Win+X-Menü durch Windows PowerShell
Web durchsuchen
Eing - Weitere Suchergebnisse anzeigen
Eingabeaufforderung
Eingabeaufforderung
App
Öffnen
Als Administrator ausführen
Dateispeicherort öffnen
An "Start" anheften
An Taskleiste anheften

Schritt 5: Folgenden Befehl eingeben: *manage-bde –protectors –add C: -TPMAndPIN*
(C: ist der Laufwerksbuchstabe, bei mehreren Laufwerken ist auf die Bezeichnung zu achten.)
In der Oberen Zeile ist das Ganze aufgelistet Hinter C:\Windows\system32>.....
Das Ganze wird dann mit Enter bestätigt. ACHTUNG: DIE EINGABE DER PIN WIRD NICHT ANGEZEIGT



Schritt 6: Nun wird der PIN erzeugt.



Schritt 7: Um zu überprüfen ob der Schutz aktiviert ist, gibt man folgenden Befehl ein: *manage-bde -status*

Bei einer erfolgreichen Einrichtung steht unter Schutzstatus „Der Schutz ist aktiviert“.'