

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:

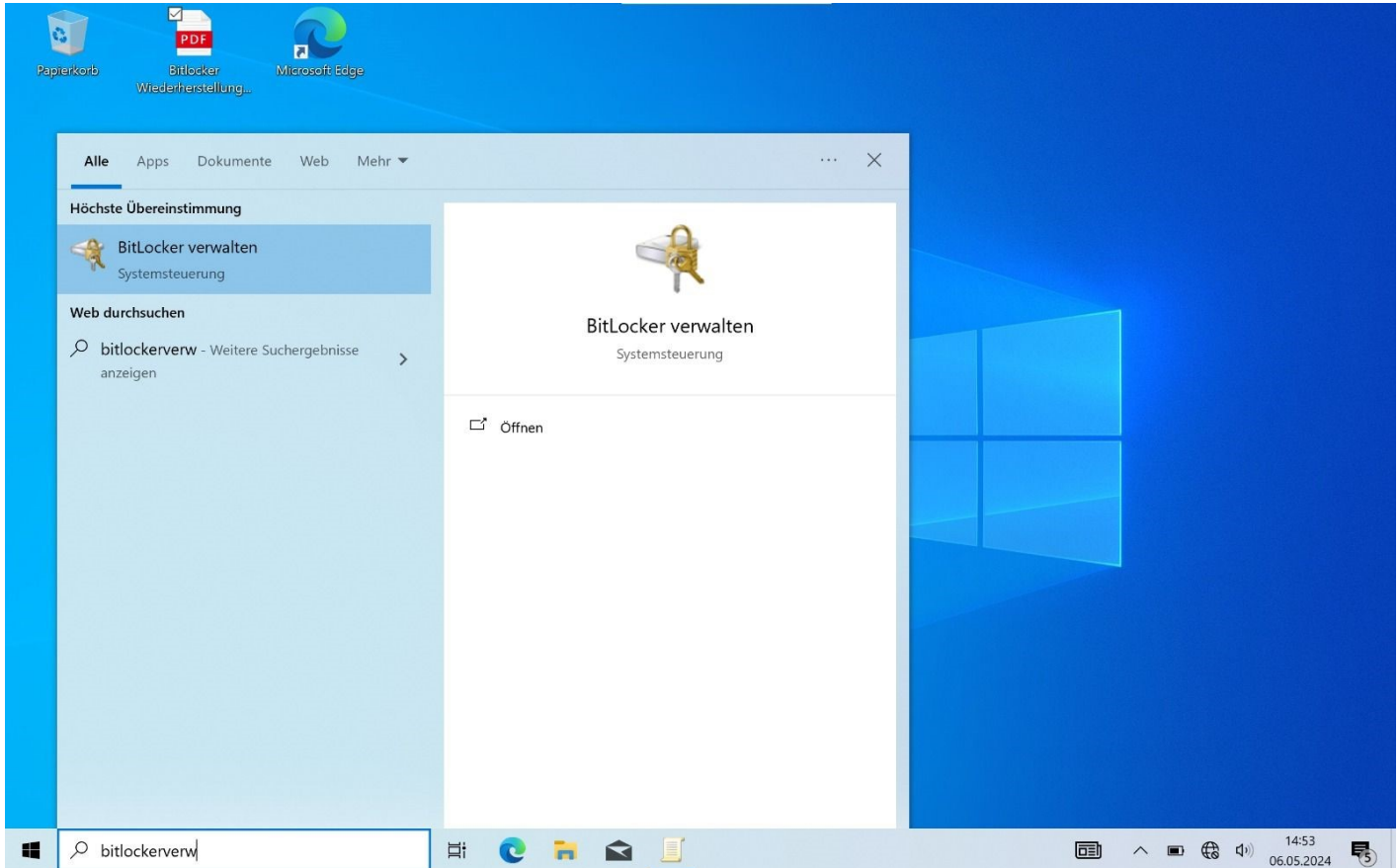
- Windows Pro
- Windows Enterprise
- Windows Pro Education/SE
- Windows Education

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

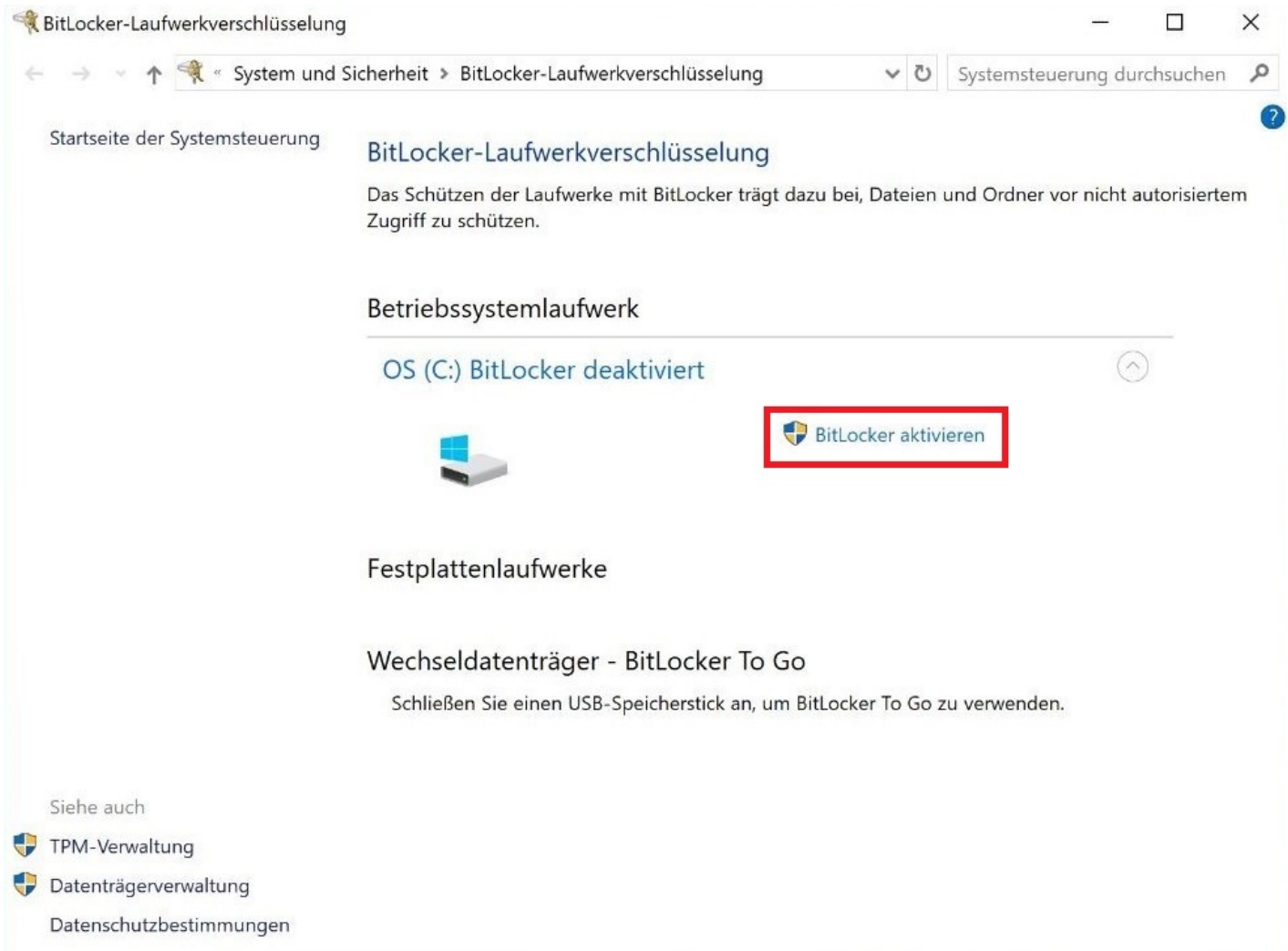
- [Bitlocker aktivieren](#)
- [Bitlocker Pin einrichten](#)

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.

Wie soll der Wiederherstellungsschlüssel gesichert werden?

 Einige Einstellungen werden vom Systemadministrator verwaltet.

Wenn Sie das Kennwort vergessen oder die Smartcard verlieren, können Sie mithilfe eines Wiederherstellungsschlüssels auf das Laufwerk zugreifen.

→ In Microsoft-Konto speichern

→ Auf USB-Speicherstick speichern

→ In Datei speichern

→ Wiederherstellungsschlüssel drucken

[Wie finde ich später meinen Wiederherstellungsschlüssel?](#)

Weiter

Abbrechen

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 Wiederherstellungsschlüssels.

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.

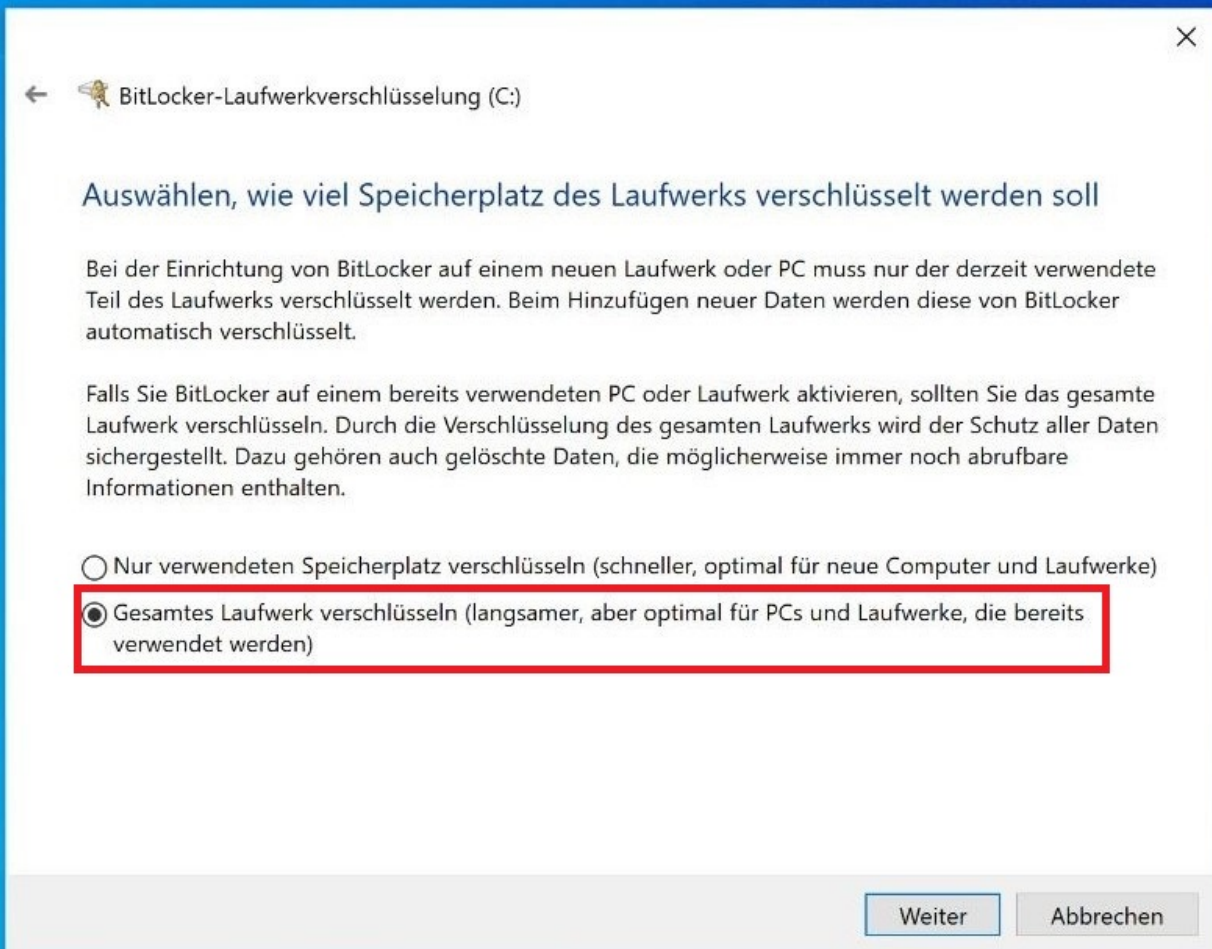
Wiederherstellungsschlüssel:

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

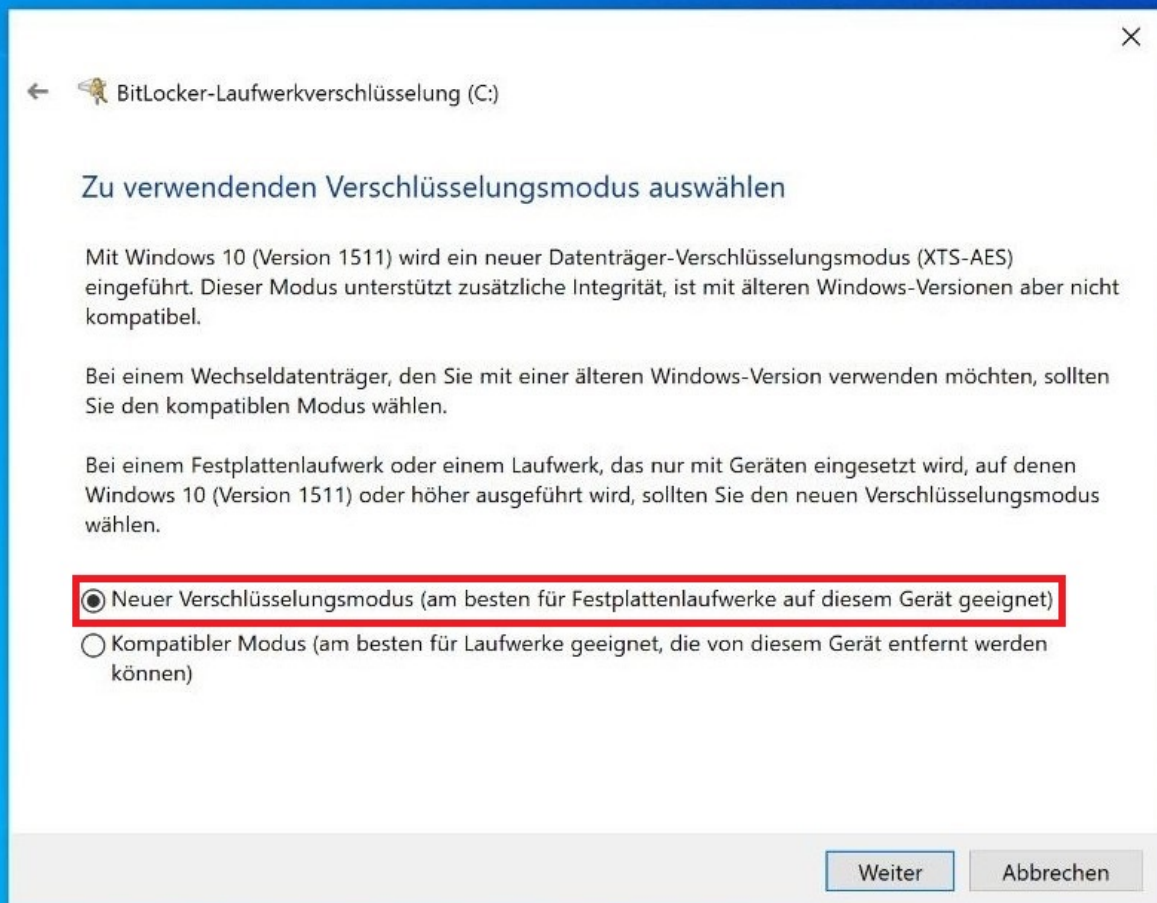
Falls der obige Bezeichner nicht mit dem auf dem PC angezeigten Bezeichner übereinstimmt, handelt es sich nicht um den richtigen Schlüssel zum Entsperren des Laufwerks.

Versuchen Sie es mit einem anderen Wiederherstellungsschlüssel, oder suchen Sie unter "<https://go.microsoft.com/fwlink/?LinkID=260589>" nach weiteren Informationen.

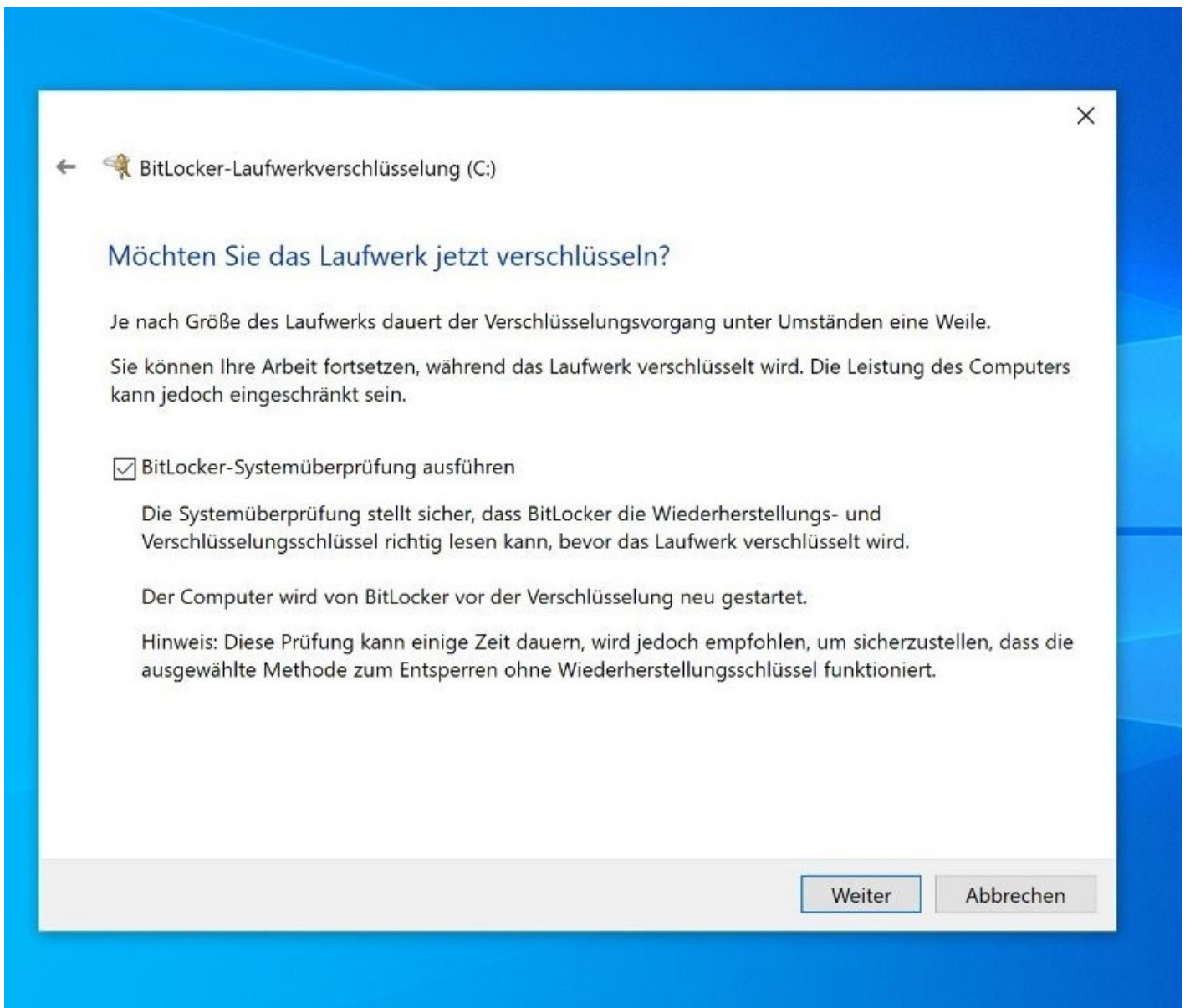
Schritt 5: Auswahl, wie viel Speicherplatz verschlüsselt werden soll. Empfehlung: "Gesamtes Laufwerk verschlüsseln"



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.

Startseite der Systemsteuerung

BitLocker-Laufwerkverschlüsselung

Das Schützen der Laufwerke mit BitLocker trägt dazu bei, Dateien und Ordner vor nicht autorisiertem Zugriff zu schützen.

i 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

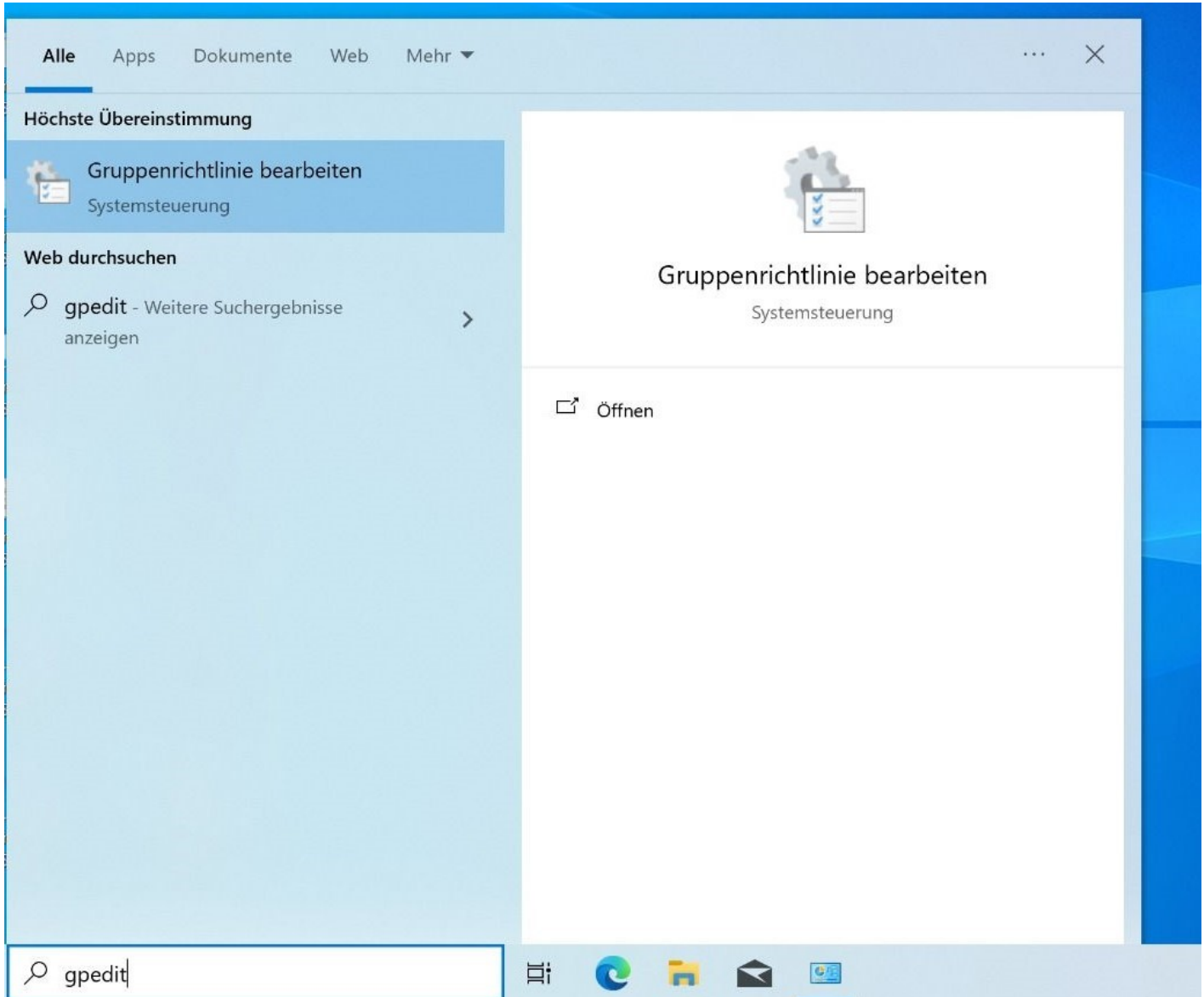
Schließen Sie einen USB-Speicherstick an, um BitLocker To Go zu verwenden.

Siehe auch

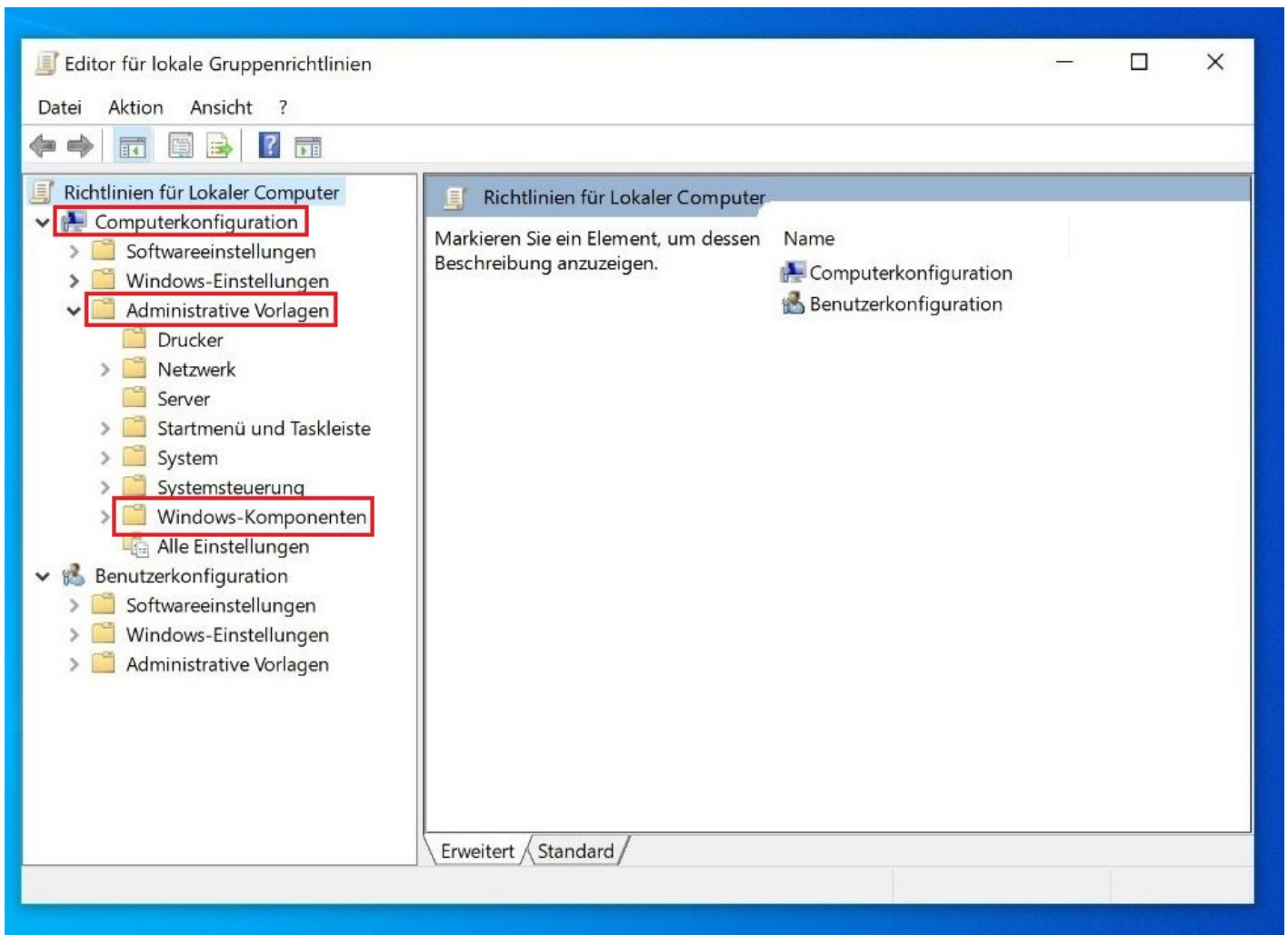
- TPM-Verwaltung
- Datenträgerverwaltung
- Datenschutzbestimmungen

Bitlocker Pin einrichten

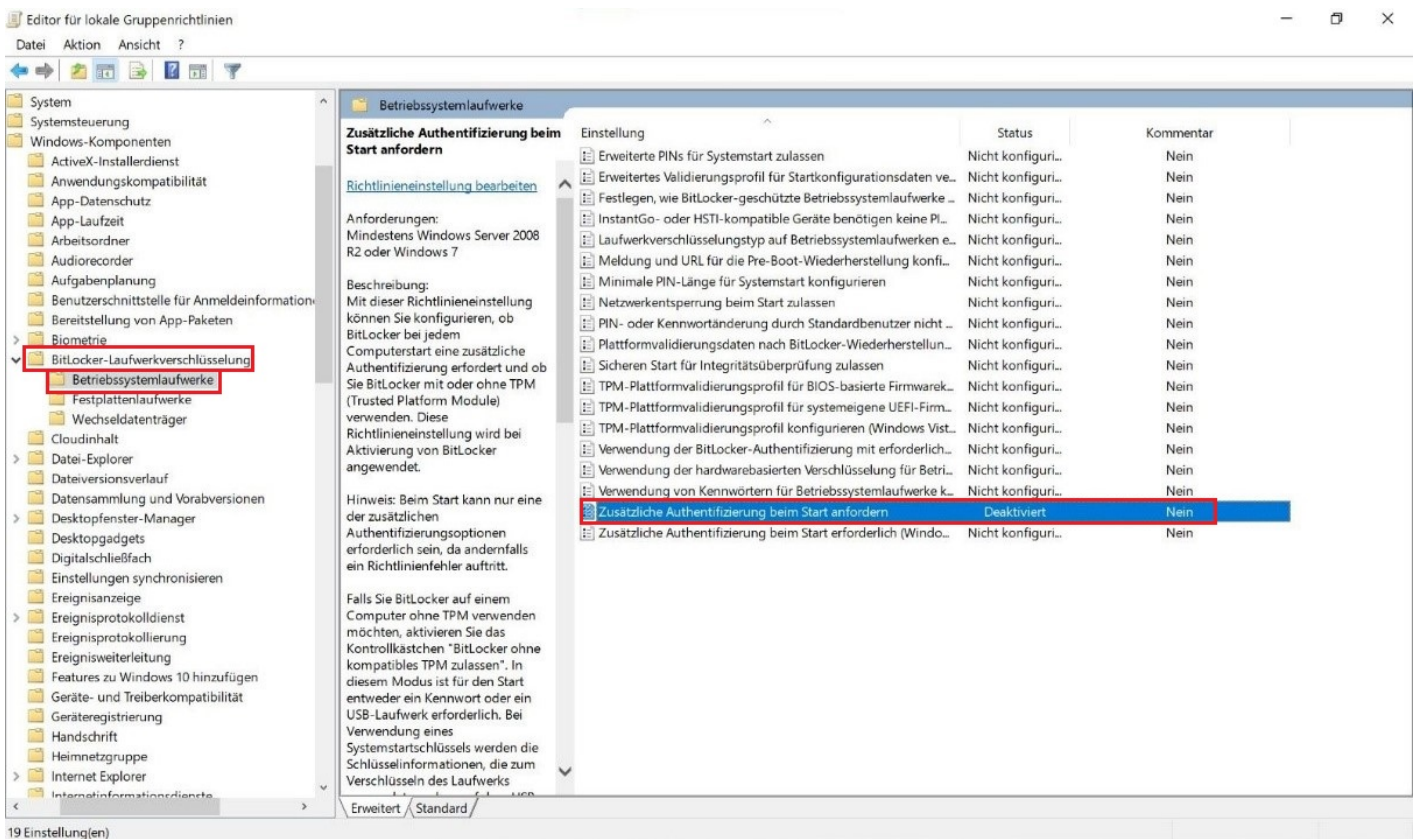
Schritt 1: In die Suchleiste „gpedit“ oder „Gruppenrichtlinie bearbeiten“ eingeben.



Schritt 2: Das Fenster "Editor für lokale Gruppenrichtlinien" 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.

Zusätzliche Authentifizierung beim Start anfordern

Zusätzliche Authentifizierung beim Start anfordern

Vorherige Einstellung Nächste Einstellung

☐ Nicht konfiguriert ☒ Aktiviert ☐ Deaktiviert

Kommentar:

Unterstützt auf: Mindestens Windows Server 2008 R2 oder Windows 7

Optionen:

Hilfe:

BitLocker ohne kompatibles TPM zulassen (hierfür ein Kennwort oder ein USB-Flashlaufwerk mit Systemstartschlüssel erforderlich)

Einstellungen für Computer mit einem TPM:

TPM-Start konfigurieren: TPM zulassen

TPM-Systemstart-PIN konfigurieren: Start-PIN bei TPM erforderlich

TPM-Systemstartschlüssel konfigurieren: Systemstartschlüssel bei TPM zulassen

TPM-Systemstartschlüssel und -PIN konfigurieren: Systemstartschlüssel und PIN bei TPM zulassen

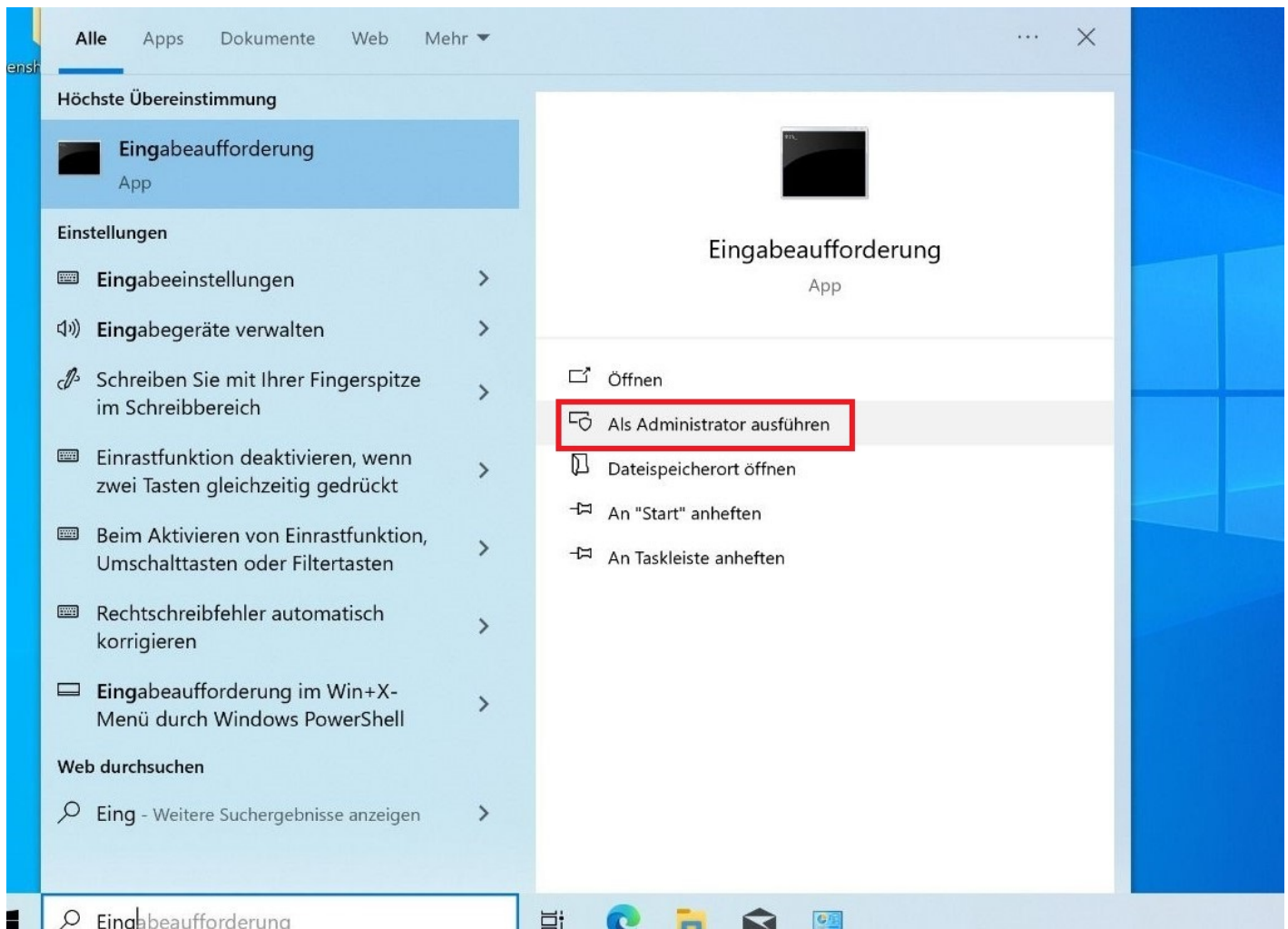
Mit dieser Richtlinieneinstellung können Sie konfigurieren, ob BitLocker bei jedem Computerstart eine zusätzliche Authentifizierung erfordert und ob Sie BitLocker mit oder ohne TPM (Trusted Platform Module) verwenden. Diese Richtlinieneinstellung wird bei Aktivierung von BitLocker angewendet.

Hinweis: Beim Start kann nur eine der zusätzlichen Authentifizierungsoptionen erforderlich sein, da andernfalls ein Richtlinienfehler auftritt.

Falls Sie BitLocker auf einem Computer ohne TPM verwenden möchten, aktivieren Sie das Kontrollkästchen "BitLocker ohne kompatibles TPM zulassen". In diesem Modus ist für den Start entweder ein Kennwort oder ein USB-Laufwerk erforderlich. Bei Verwendung eines Systemstartschlüssels werden die Schlüsselinformationen, die zum Verschlüsseln des Laufwerks verwendet werden, auf dem USB-Laufwerk gespeichert, wodurch ein USB-Stick entsteht. Wenn der USB-Stick eingesteckt wird, wird der Zugriff auf das Laufwerk authentifiziert, und es kann auf das

OK Abbrechen Übernehmen

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

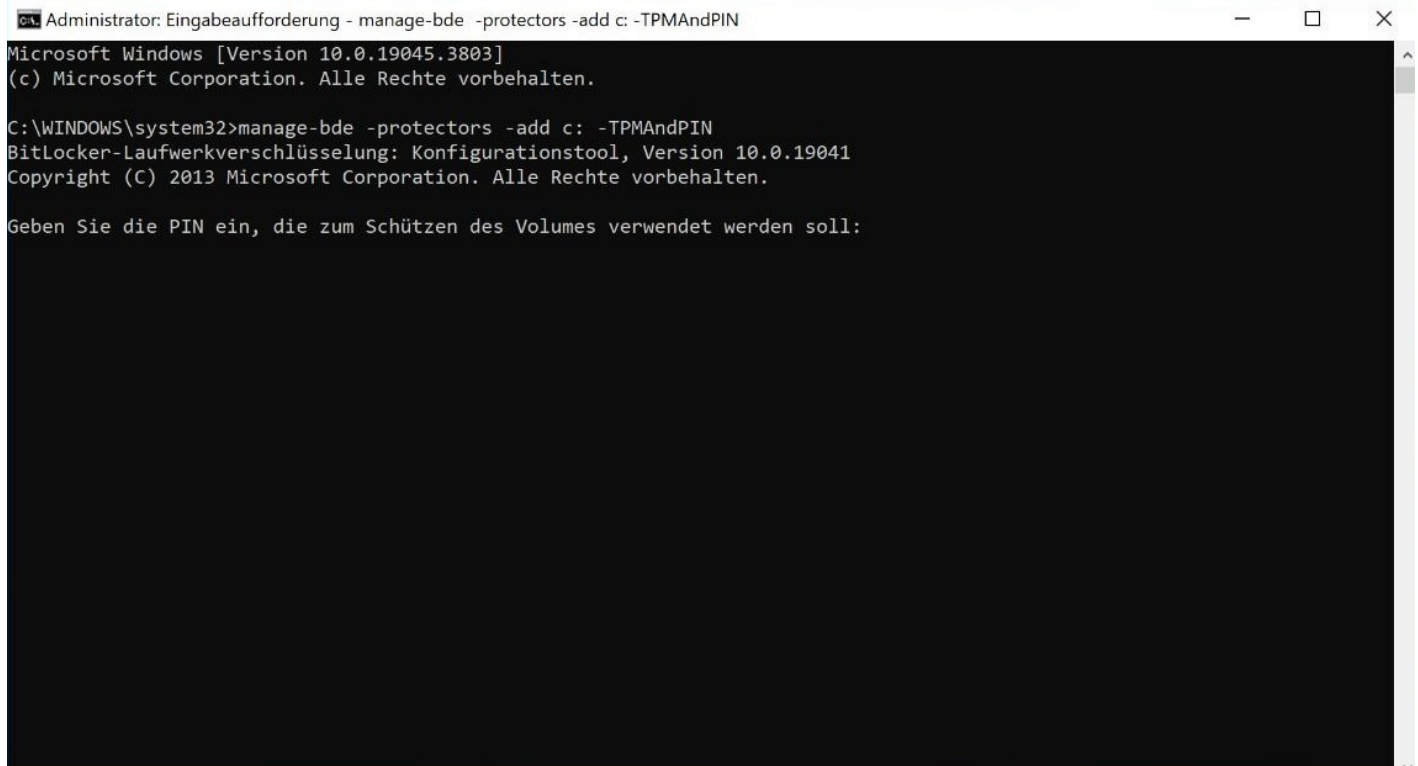


Schritt 5: Folgenden Befehl eingeben: *manage-bde -protectors -add C: -TPMAndPIN*

(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

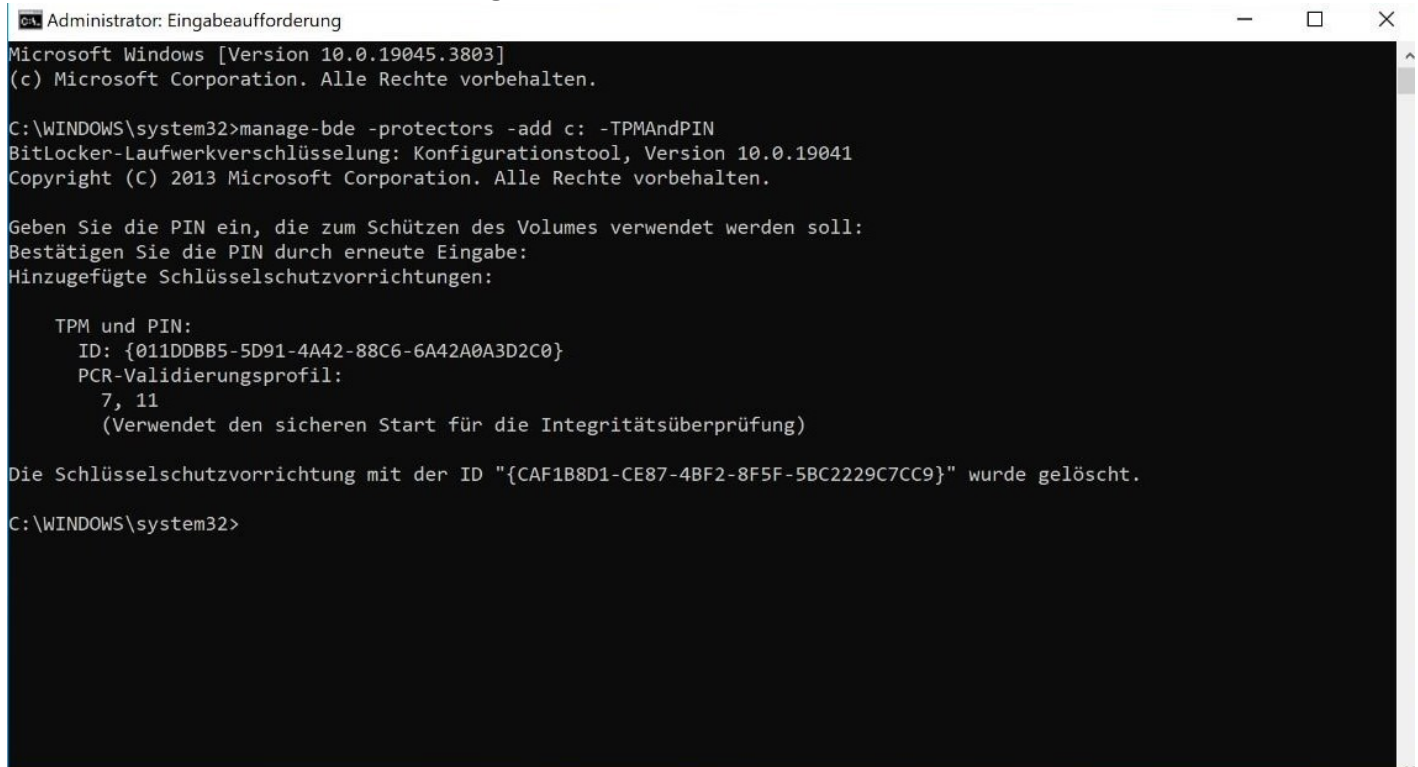


```
Administrator: Eingabeaufforderung - manage-bde -protectors -add c: -TPMAndPIN
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\WINDOWS\system32>manage-bde -protectors -add c: -TPMAndPIN
BitLocker-Laufwerkverschlüsselung: Konfigurationstool, Version 10.0.19041
Copyright (C) 2013 Microsoft Corporation. Alle Rechte vorbehalten.

Geben Sie die PIN ein, die zum Schützen des Volumes verwendet werden soll:
```

Schritt 6: Nun wird der PIN erzeugt.



```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\WINDOWS\system32>manage-bde -protectors -add c: -TPMAndPIN
BitLocker-Laufwerkverschlüsselung: Konfigurationstool, Version 10.0.19041
Copyright (C) 2013 Microsoft Corporation. Alle Rechte vorbehalten.

Geben Sie die PIN ein, die zum Schützen des Volumes verwendet werden soll:
Bestätigen Sie die PIN durch erneute Eingabe:
Hinzugefügte Schlüsselschutzvorrichtungen:

    TPM und PIN:
    ID: {011DDBB5-5D91-4A42-88C6-6A42A0A3D2C0}
    PCR-Validierungsprofil:
    7, 11
    (Verwendet den sicheren Start für die Integritätsüberprüfung)

Die Schlüsselschutzvorrichtung mit der ID "{CAF1B8D1-CE87-4BF2-8F5F-5BC2229C7CC9}" wurde gelöscht.

C:\WINDOWS\system32>
```

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“.

```
Administrator: Eingabeaufforderung
ID: {011DDBB5-5D91-4A42-88C6-6A42A0A3D2C0}
PCR-Validierungsprofil:
7, 11
(Verwendet den sicheren Start für die Integritätsüberprüfung)

Die Schlüsselschutzvorrichtung mit der ID "{CAF1B8D1-CE87-4BF2-8F5F-5BC2229C7CC9}" wurde gelöscht.

C:\WINDOWS\system32>manage-bde -status
BitLocker-Laufwerkverschlüsselung: Konfigurationstool, Version 10.0.19041
Copyright (C) 2013 Microsoft Corporation. Alle Rechte vorbehalten.

Datenträgervolumes, die mit BitLocker-Laufwerkverschlüsselung
geschützt werden können:
Volume "C:" [OS]
[Betriebssystemvolumen]

Größe: 474,05 GB
BitLocker-Version: 2.0
Konvertierungsstatus: Vollständig verschlüsselt
Verschlüsselt (Prozent): 100,0 %
Verschlüsselungsmethode: XTS-AES 128
Schutzstatus: Der Schutz ist aktiviert.
Sperrungsstatus: Entsperrt
ID-Feld: Unbekannt
Schlüsselschutzvorrichtungen:
Numerisches Kennwort
TPM und PIN

C:\WINDOWS\system32>
```