Systemadministration mit Windows Server 2022 und Windows 11 in 35 Tagen

Teil 3 - Weiterführende Themen

Tag 26-35: Netzwerk und Unternehmensumgebung

Nicole Laue

Verlag Nicole Laue

n|l|v

Inhaltsverzeichnis

Für wen ist dieses Buch?
- Übungsumgebung
- Software
- Wie benutze ich dieses Buch?
- Danksagung

26 Tag 26: Datendeduplizierung und BitLocker
- 26.1 Einrichten der Datendeduplizierung
- 26.2 BitLocker
- 26.3 BitLocker To Go
- 26.4 Wiederherstellung durch Active Directory
- 26.5 BitLocker mit der PowerShell

27 Tag 27: Speicherverwaltung
- 27.1 Einrichten der Serverspeicherung
- 27.2 Optimieren der Speicherverwaltung durch iSCSI
- 27.3 Multipath IO (MPIO)

28 Tag 28: Hochverfügbarkeit
- 28.1 Speicherreplikation
- 28.2 Fehlertoleranz durch Hyper-V Replica
- 28.3 Einrichten eines NLB-Clusters

29 Tag 29: Failover-Servercluster
- 29.1 Wie arbeitet ein Servercluster?
- 29.2 Konfiguration des gemeinsamen Speichers
- 29.3 Einrichten eines Failover-Clusters
- 29.4 Cluster ohne Active Directory in einer Arbeitsgruppe

29.5 Konfigurieren der Clustereinstellungen
29.6 Einrichten einer Clusterrolle
30 Tag 30: Hochverfügbarkeit: virtuelle Maschinen und Cluster
30.1 Einrichten von hochverfügbaren virtuellen Maschinen
30.2 Einrichten von Storage Spaces Direct
31 Tag 31: VPN und Routing auf dem Server
31.1 VPN und Routing
31.2 NAT (Network Adress Translating)
31.3 RAS und VPN
31.4 VPN-Richtlinien
32 Tag 32: Always On VPN
32.1 RADIUS (Remote Authentication Dial-In User Service)
32.2 Always on VPN einrichten
33 Tag 33: Die Serverumgebung betriebsbereit halten
33.1 Patchmanagement
33.2 Server überwachen
34 Tag 34: Erweiterte Themen
34.1 Sicherheit für DNS
34.2 NS und WINS: GlobalNamesZone
34.3 DNS Richtlinien
34.4 Sicherheit für DHCP
34.5 Planen einer DHCP-Infrastruktur
35 Tag 35: Was ist Azure Active Directory?
35.1 Grundlagen Azure Active Directory
35.2 Beispiele für Funktionen von Azure Active Directory
Index

Für wen ist dieses Buch?

Dieses Buch ist der dritte Teil einer Reihe von drei Büchern, in denen Sie durch alle relevanten Themengebiete der Serveradministration mit Windows Server 2022 und Windows 11 als Client geführt werden.

Diese Reihe führt Sie in insgesamt 35 Schulungstagen durch dieses komplexe Thema.

Sie sollten die beiden vorhergehenden Bücher

Systemadministration mit Windows Server 2022 und Windows 11 in 35 Tagen

Teil 1 – Grundlagen

Tag 1-15

und

Systemadministration mit Windows Server 2022 und Windows 11 in 35 Tagen

Teil 2 - Weiterführende Themen

Tag 16-25: Active Directory

vorher durchgearbeitet haben, oder zumindest die darin vermittelten Kenntnisse besitzen.

Das Buch ist für zwei Personengruppen gleichermaßen geeignet:

- Privatleute, die sich die Kenntnisse im Selbststudium aneignen möchten
- Schulungsunternehmen, die eine Schulungsunterlage benötigen

In Zusammenarbeit mit der GFN GmbH wurde die Reihe für die Ausbildung zum Fachinformatiker Systemintegration (FISI) konzipiert und wird dort als Schulungsunterlage eingesetzt.

Ein Schulungsbuch kann nur gut sein, wenn das Erlernte sofort in praktischen Übungen ausprobiert werden kann.

Aus diesem Grund finden Sie in jedem Kapitel viele Übungen.

Sowohl die Lösungen für diese Übungen als auch die PowerPoint Präsentationen für den Unterricht stehen auf der Homepage des Verlags http://www.laue-net.de zum Download bereit.

Übungsumgebung

Die Hardwarevoraussetzungen für eine Übungsumgebung sind nicht besonders hoch. Sie können jeden Computer dafür benutzen, der folgende Mindestvoraussetzungen erfüllt:

- 32 GB Arbeitsspeicher
- 1 - 2 TB freien Festplattenspeicher

Für die Übungen installieren Sie eine Virtualisierungssoftware, die Übungen sind auf Hyper-V ausgelegt.

Ansonsten benötigen Sie lediglich DVDs oder ISO-Dateien mit Windows Server 2022 und Windows 11.

Einrichtung der Übungsumgebung

Falls Sie den vorherigen Kurs mit den Schulungstagen 16 - 25 (Active Directory) bearbeitet haben, können Sie mit der Übungsumgebung nahtlos weiterarbeiten.

Setzen Sie diese einfach auf den Prüfpunkt „Basis“ zurück und beginnen Sie mit diesem Buch.

Falls Ihnen keine Übungsumgebung zur Verfügung steht, können Sie eine Installationsanleitung auf der Homepage des Verlags http://www.laue-net.de herunterladen.

Software

Für die Übungen benötigen Sie folgende Evaluierungskopien:

- Windows Server 2022
- Windows 11

Die meisten dieser Evaluierungskopien können Sie bei Microsoft erhalten: Natürlich können Sie auch Vollversionen verwenden, die dann nicht aktiviert werden müssen.

Wie benutze ich dieses Buch?

Dieser Kurs ist für eine Gesamtdauer von 35 Tagen ausgelegt.

Sie müssen sich nicht akribisch daran halten, an manchen Tagen geht es schneller, und Sie sind früher fertig, an manchen Tagen aber ist der Stoff für Sie nicht so einfach und Sie brauchen länger.

Das ist kein Problem!

Die Einteilung in Arbeitstage ist nur ein Anhaltspunkt, Sie sollten sich nach Ihren Bedürfnissen richten, damit Sie zum bestmöglichen Ergebnis kommen.

Für jeden Tag gibt es einige Übungen.

Diese Übungen sind von großer Bedeutung, Sie wiederholen damit die gelernte Theorie und trainieren Ihre Fähigkeiten.

Laden Sie sich für alle Übungen die Lösungen herunter, damit Sie überprüfen können, ob Sie alles richtig gemacht haben.

Sie kommen bei einer Übung nicht weiter?

Das ist auch kein Problem, denn die Lösungen sind als Schritt-für-Schritt Anleitung geschrieben, damit Sie jederzeit wieder den Anschluss finden.

Die Übungsumgebung ist so aufgebaut, dass Sie für jeden neuen Lerntag mit einer zuvor weggespeicherten Konfiguration arbeiten können.

Das ist wichtig, falls Sie einen bestimmten Lerntag noch einmal wiederholen möchten, Sie müssen dafür nur die Übungsumgebung auf einen bestimmten Stand zurücksetzen.

Wir wünschen Ihnen viel Erfolg auf Ihrem Weg zur Systemadministration!

Danksagung

An dieser Stelle möchte ich mich bei den vielen hilfreichen Freunden und Mitarbeitern bedanken, die erst ermöglicht haben, dass dieses Buch entstehen kann.

Ich bedanke mich bei folgenden Helfern:

Karin Feichtinger und meinem Mann Christian.

Sie waren mir als Betaleser eine große Hilfe und haben freiwillig ihre Freizeit geopfert. Mit ihrem großen Fachwissen waren sie ein wichtiger Bestandteil der Entstehung dieses Buches.

Besonderer Dank gilt den Mitarbeitern und Trainern der GFN GmbH, mit denen wir in enger Zusammenarbeit die Themen dieses Buchs abgestimmt haben.

26
Tag 26:
Datendeduplizierung und BitLocker

Willkommen zurück!

Nun tauchen wir gemeinsam in die Weilt der erweiterten Systemadministration ein.

26.1 Einrichten der Datendeduplizierung

Seit einigen Versionen ist die Datendeduplizierung Bestandteil des Windows Servers.

Mit dieser Funktion wird verhindert, dass identische Daten mehrfach gespeichert werden. Damit kann der Speicherplatz effektiver genutzt werden.

Hierbei werden nicht nur ganze Dateien betrachtet. Daten werden in Blöcke mit variabler Größe unterteilt (32 KB bis 128 KB). Doppelte Daten werden nun anhand der Blöcke identifiziert.

Ein Beispiel:

Sie speichern ein Word-Dokument mit dem Protokoll des letzten Seminars.

Ein Kollege kopiert diese Datei, ändert nur den Namen des Teilnehmers und speichert die Datei in seinem Speicherlaufwerk.

Hierbei sind die Daten zum allergrößten Teil identisch, da die Datei ja in Blöcke aufgeteilt wird. Also können 99% der zweiten Datei beseitigt werden, es muss lediglich ein Verweis auf die ursprünglichen Datenblöcke bestehen bleiben.

Windows Server 2022 erweitert die Funktionalität auch auf die virtuellen Systeme, in denen ja häufig doppelte Daten zu finden sind. Jetzt können sowohl physische, als auch virtuelle Festplatten mit diesem Feature bereinigt werden.

Allerdings müssen die Datenträger mit NTFS formatiert sein, ReFS wird nicht unterstützt.

Windows Server 2022 unterstützt die Optimierung von Volumes mit einer Größe bis zu 64 TB.

Die Voraussetzungen für die Datendeduplizierung bezüglich der Laufwerke sind folgende:

- Sie dürfen kein System- oder Startvolume sein
- Sie müssen mit dem NTFS-Dateisystem formatiert sein
- Sie können als Master Boot Record (MBR) oder GUID-Partitionstabelle (GPT) partitioniert sein
- Sie können sich in Speicherfreigaben befinden, z. B. Speicher mit einem Fibre Channel- oder SAS-Array oder einem iSCSI-SAN, wenn das Windows-Failoverclustering vollständig unterstützt wird
- Sie dürfen nicht vom Microsoft Resilient File System (ReFS) abhängig sein
- Sie dürfen nicht größer als 64 TB sein
- Sie müssen für das Betriebssystem als nicht austauschbare Laufwerke verfügbar gemacht werden. Remote zugeordnete Laufwerke werden nicht unterstützt

Die Datendeduplizierung ist sehr einfach einzurichten, sie wird zunächst als Rollendienst der „Datei-/Speicherdienste“ installiert.

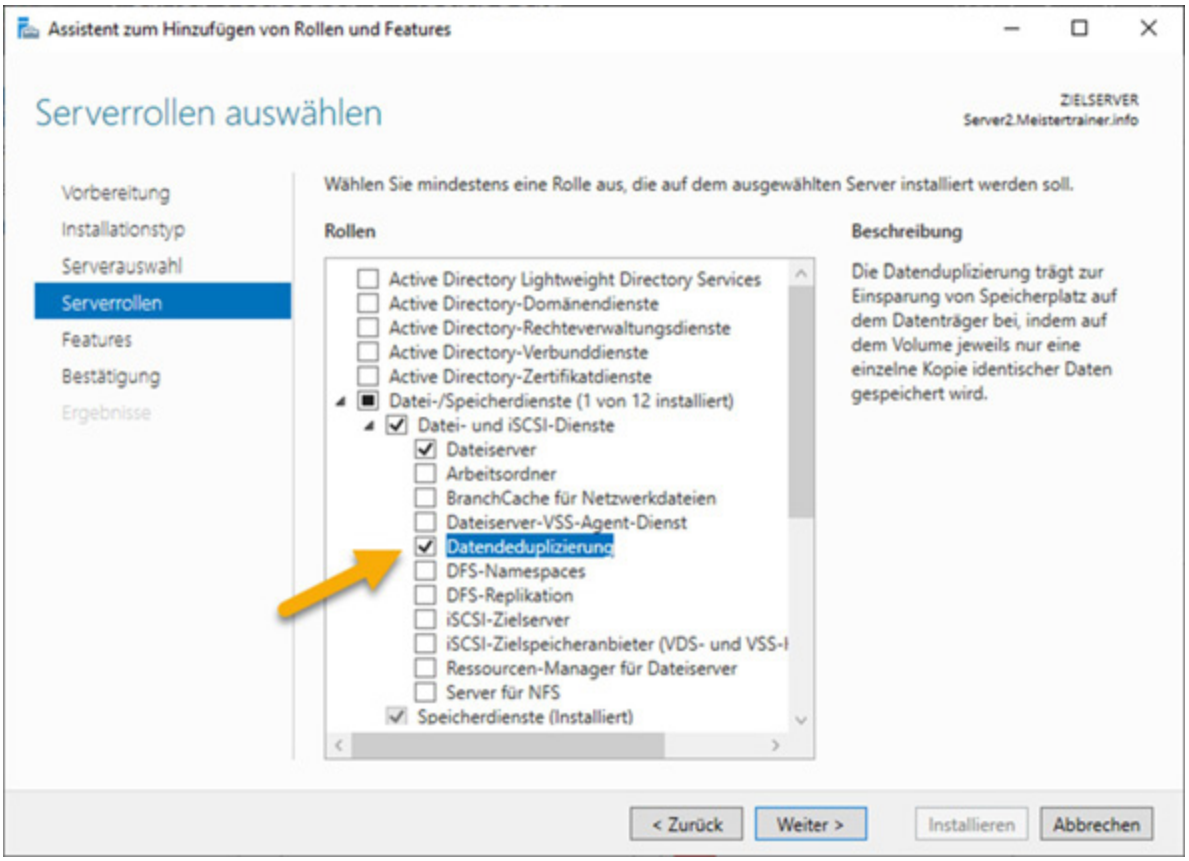

Abbildung 26.1: Installation

Nun kann sie konfiguriert werden.

Anders als die meisten Tools wird die Datendeduplizierung aber direkt im Server-Manager konfiguriert!

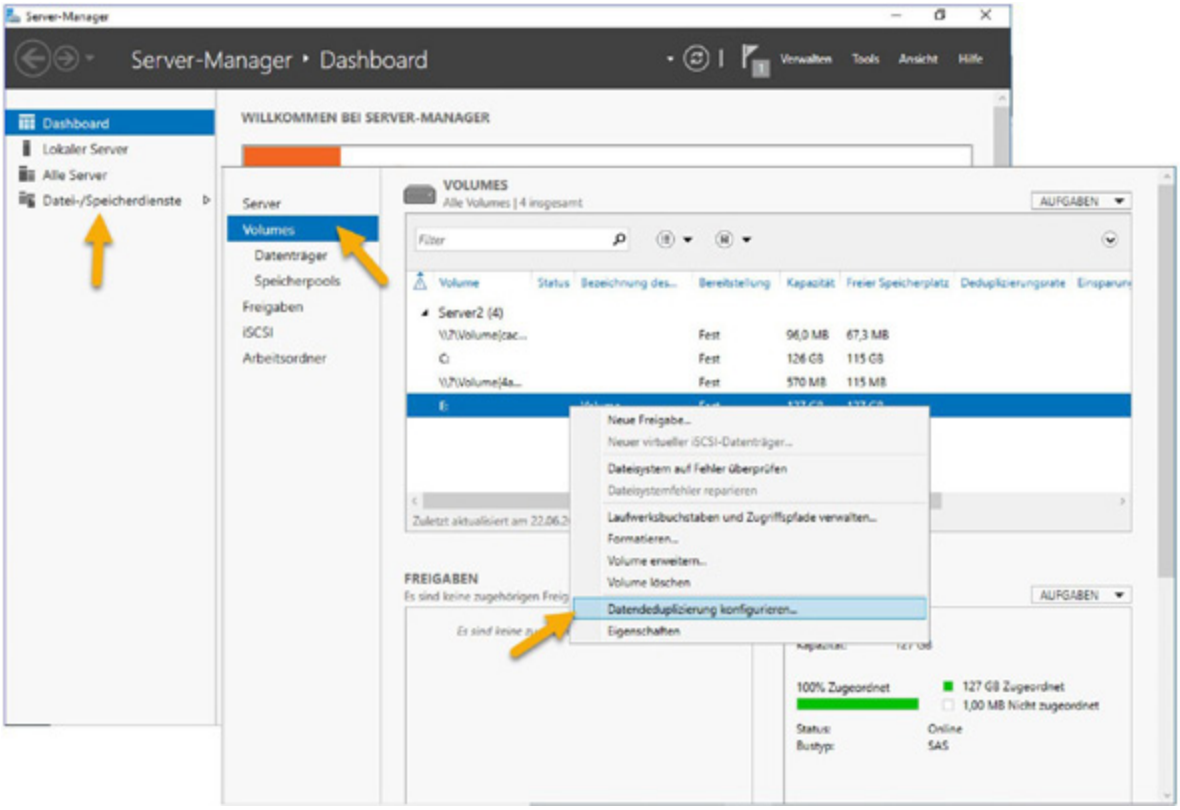

Abbildung 26.2: Konfiguration

Dazu wählen Sie „Datei- /Speicherdienste“ und klicken auf „Volumes“.

Im Kontextmenü können Sie nun „Datendeduplizierung konfigurieren“ wählen.

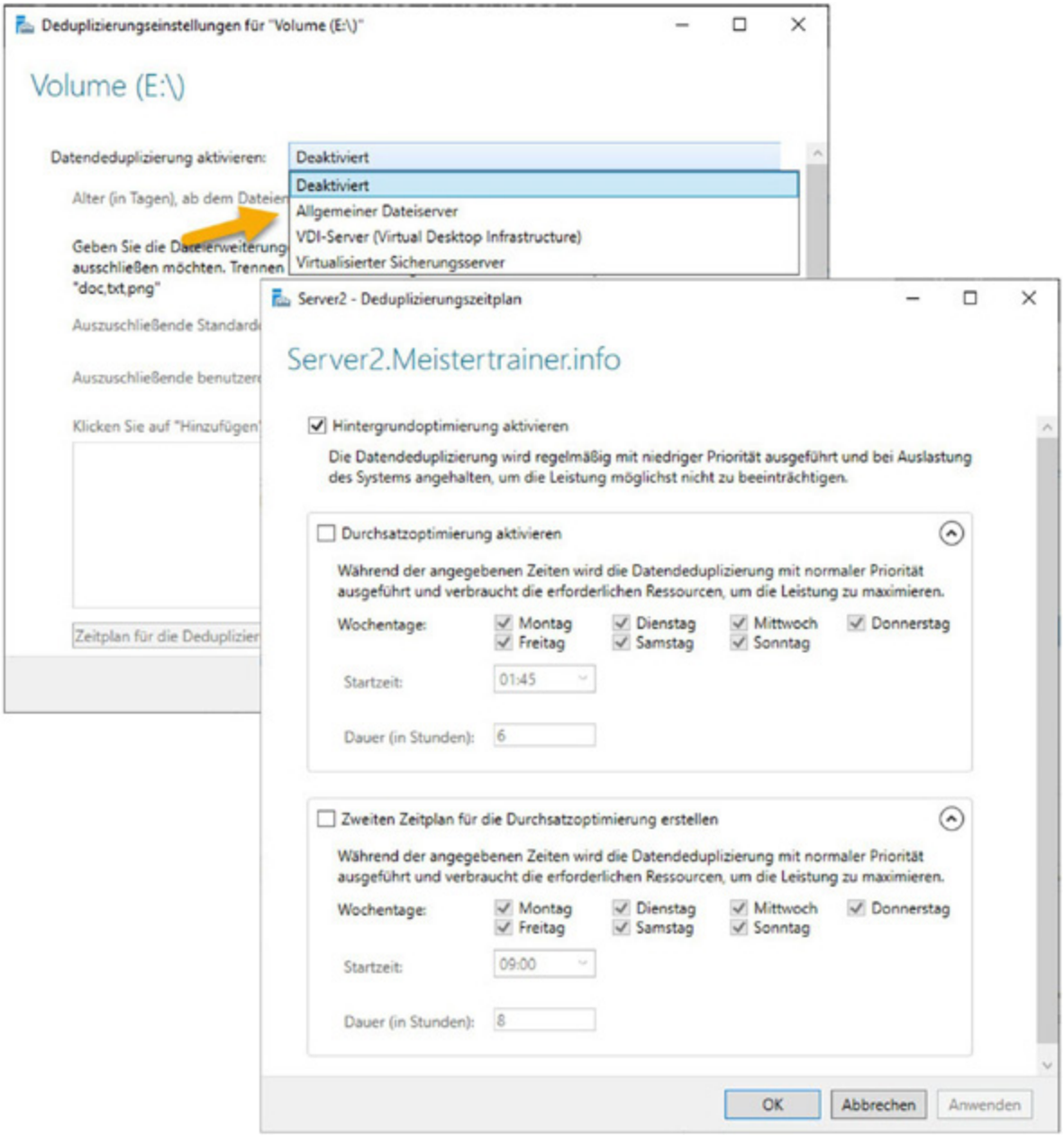

Abbildung 26.3: Datendeduplizierung

Hier wählen Sie die Art des Dateiservers aus und konfigurieren den Zeitplan.

Hier können Sie auch den Punkt „Virtualisierter Sicherungsserver“ wählen.

Die Datendeduplizierung in Windows Server 2022 eignet sich auch als Speicherplatz für Backups, da eine Größe bis zu 64 TB unterstützt wird.

Übung 26.1

- Richten Sie auf der virtuellen Maschine „Server2“ eine weitere Festplatte ein
- Aktivieren Sie auf dieser Festplatte die Datendeduplizierung für einen allgemeinen Dateiserver
- Aktivieren Sie die Hintergrundoptimierung

26.1.1 Überwachung der Datendeduplizierung

Zum Überwachen der Datendeduplizierung stehen einige PowerShell Cmdlets zur Verfügung.

GET-DEDUPSTATUS

Gibt den Status für Laufwerke mit Metadaten für die Datendeduplizierung an.

Abbildung 26.4: Get-DedupStatus

Get-DedupVolume

Gibt Laufwerke aus mit Metadaten für die Datendeduplizierung.

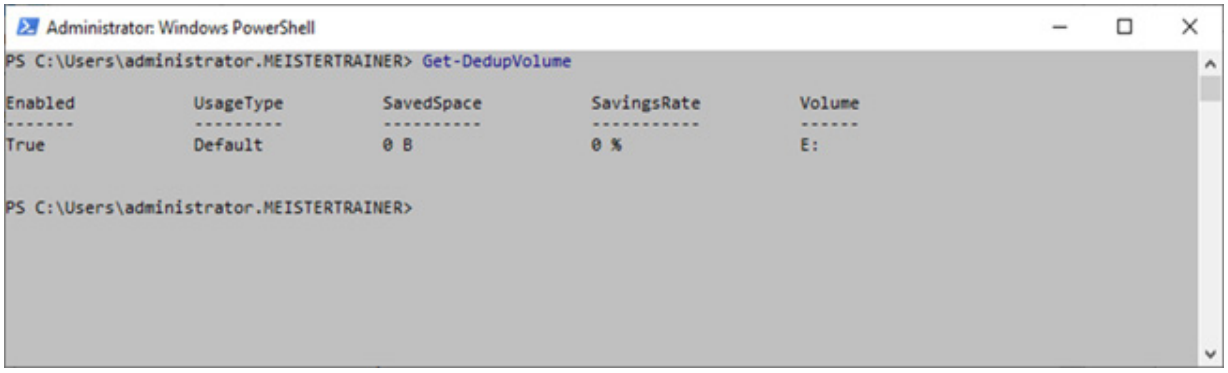

Abbildung 26.5:Get-DedupVolume

Get-DedupMetadata

Gibt die Metadaten für Laufwerke mit Datendeduplizierung aus.

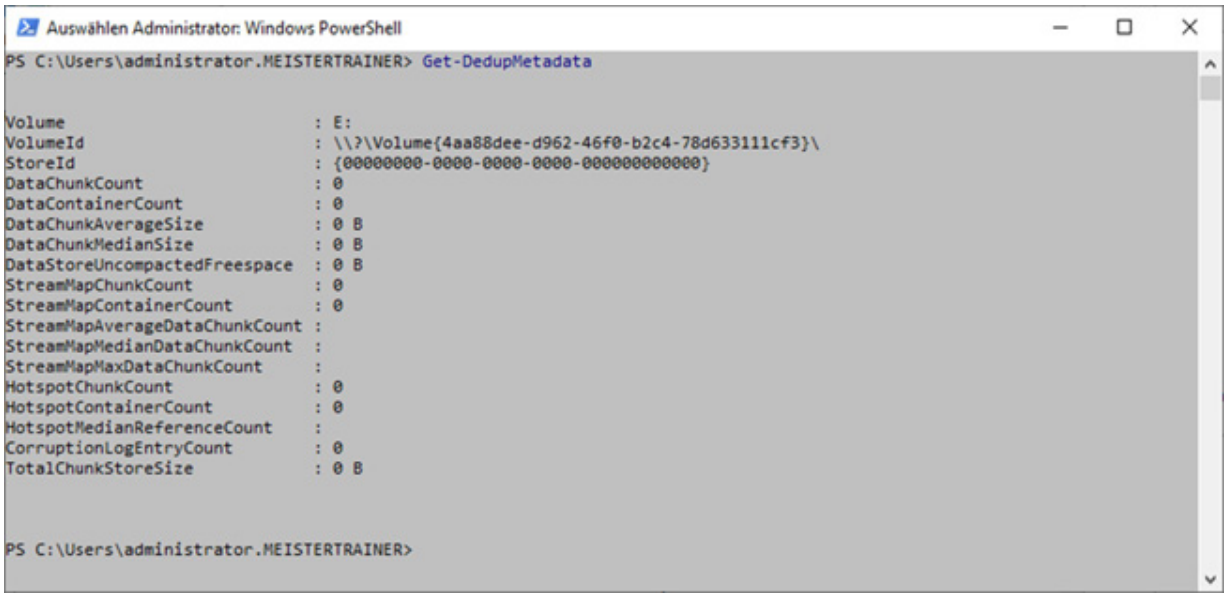

Abbildung 26.6: Get-DedupMetadata

Get-DedupSchedule

Gibt die geplanten Jobs für die Datendeduplizierung aus.

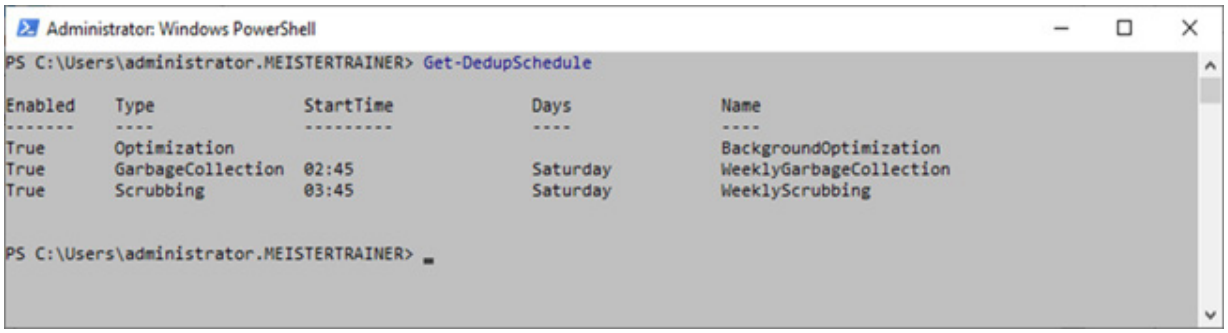

Abbildung 26.7: Get-DedupSchedule

Übung 26.1.1

- Betrachten Sie die eingerichtete Datendeduplizierung mithilfe der gelernten PowerShell cmdlets

26.2 BitLocker

BitLocker ist eine Möglichkeit, ganze Laufwerke komplett zu verschlüsseln, so dass beim Systemstart immer ein Verschlüsselungscode abgefragt wird. Da diese Funktion in den meisten Fällen eher auf dem Client als auf dem Server benutzt werden wird, zeigen wir hier die Einrichtung auf einem Windows 11 Client.

Damit wird sichergestellt, dass das Betriebssystem und die lokalen Festplatten sicher sind. Dies kann auf zwei verschiedene Arten erreicht werden:

Computer hat TPM (Trusted Platform Module) Chip 1.2

Die Computer der neuen Generation haben einen TPM Chip 1.2 oder höher. In diesem Fall kann die Verschlüsselung auf diesem Chip gespeichert werden.

Computer hat kein TPM (Trusted Platform Module) Chip 1.2

Alle anderen Computer, die den TPM Chip nicht haben, können BitLocker trotzdem verwenden, indem die Verschlüsselung auf einem USB Memory Stick gespeichert wird.

ACHTUNG!

Die Speicherung des Schlüssels auf einem USB-Stick kann natürlich nur ein Notbehelf sein. Ein USB-Stick ist ein Medium, das nicht die Zuverlässigkeit hat, wie ein Hardwarechip!

Sie sehen, bei einer BitLocker Verschlüsselung wird die Festplatte verschlüsselt und die Verschlüsselungsinformation wird auf der Hardware gespeichert.

Dadurch ergeben sich folgende Schutzszenarien, die durch BitLocker abgedeckt sind:

- Falls die Festplatte aus dem System ausgebaut wird und in ein anderes System eingebaut wird, ist die Entschlüsselungssequenz nicht verfügbar und das System kann nicht gestartet werden.

  Dies kann natürlich nur funktionieren, wenn der Schlüssel entweder auf dem TPM-Chip gespeichert worden ist, oder der USB-Stick nicht verfügbar ist, deswegen sollten Sie den USB-Stick immer abziehen, wenn Sie das System nicht benutzen!
- Falls Änderungen an den Startdateien, (die natürlich nicht verschlüsselt werden können) oder am BIOS

vorgenommen worden sind, stimmt der Schlüssel nicht mehr und das System kann ebenfalls nicht mehr gestartet werden.

ACHTUNG!

Natürlich gibt es für diese Fälle auch ein Wiederherstellungskennwort, denn es ist ja möglich, dass Startdateien geändert werden müssen, oder dass Sie eine Festplatte in ein anderes System übernehmen müssen.

Dieses Kennwort sollten Sie sehr gut verwahren!

Wenn Sie den BitLocker aktivieren wollen, gehen Sie folgendermaßen vor:

- Systemsteuerung
- System und Sicherheit
- BitLocker-Laufwerksverschlüsselung

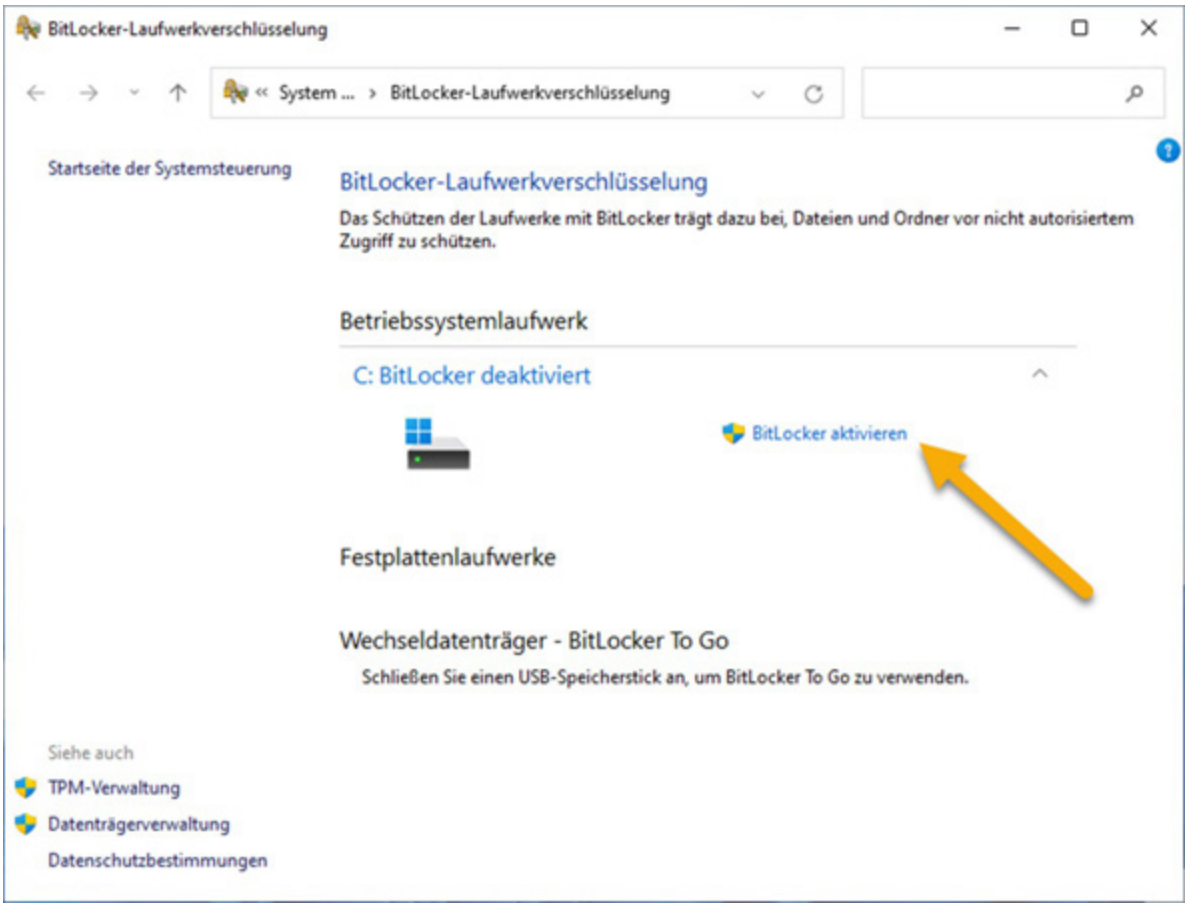

Abbildung 26.8: BitLocker Laufwerksverschlüsselung

Sie klicken hier auf „BitLocker aktivieren“.

Nun überprüft Windows das System.

Falls Sie einen startfähigen Datenträger im Laufwerk haben erkennt BitLocker das und lässt die Konfiguration nicht zu.

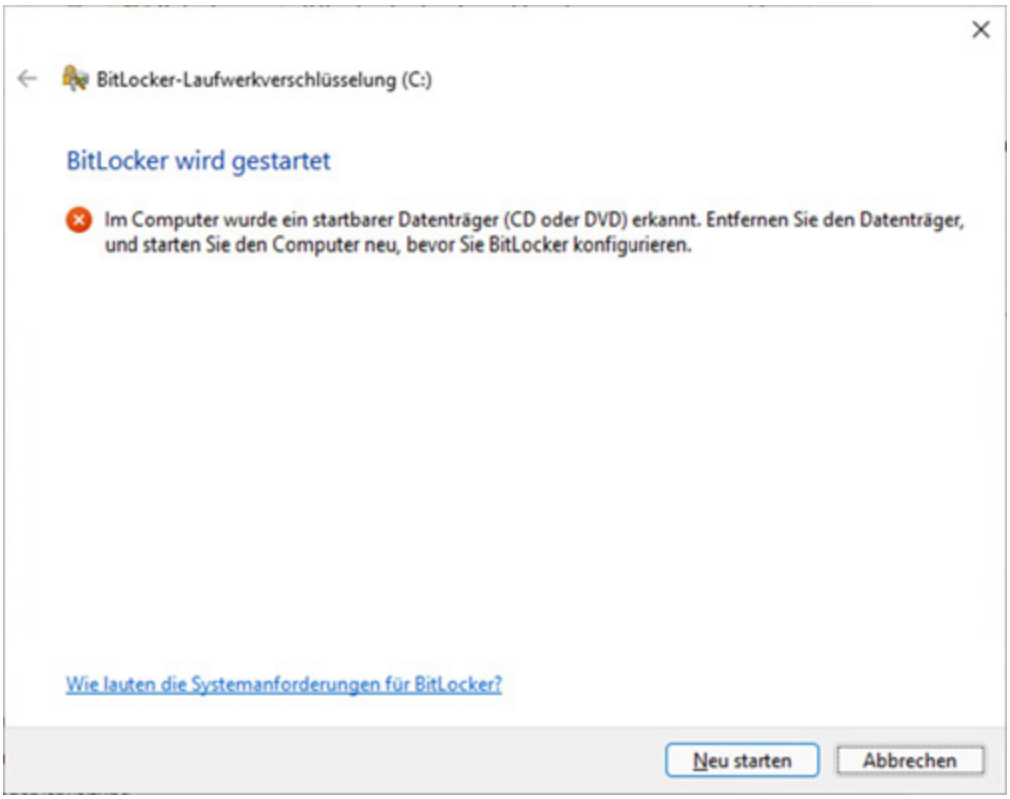

Abbildung 26.9: Startbarer Datenträger gefunden

Erst nach dem Entfernen des Datenträgers und einem Neustart können Sie BitLocker konfigurieren.

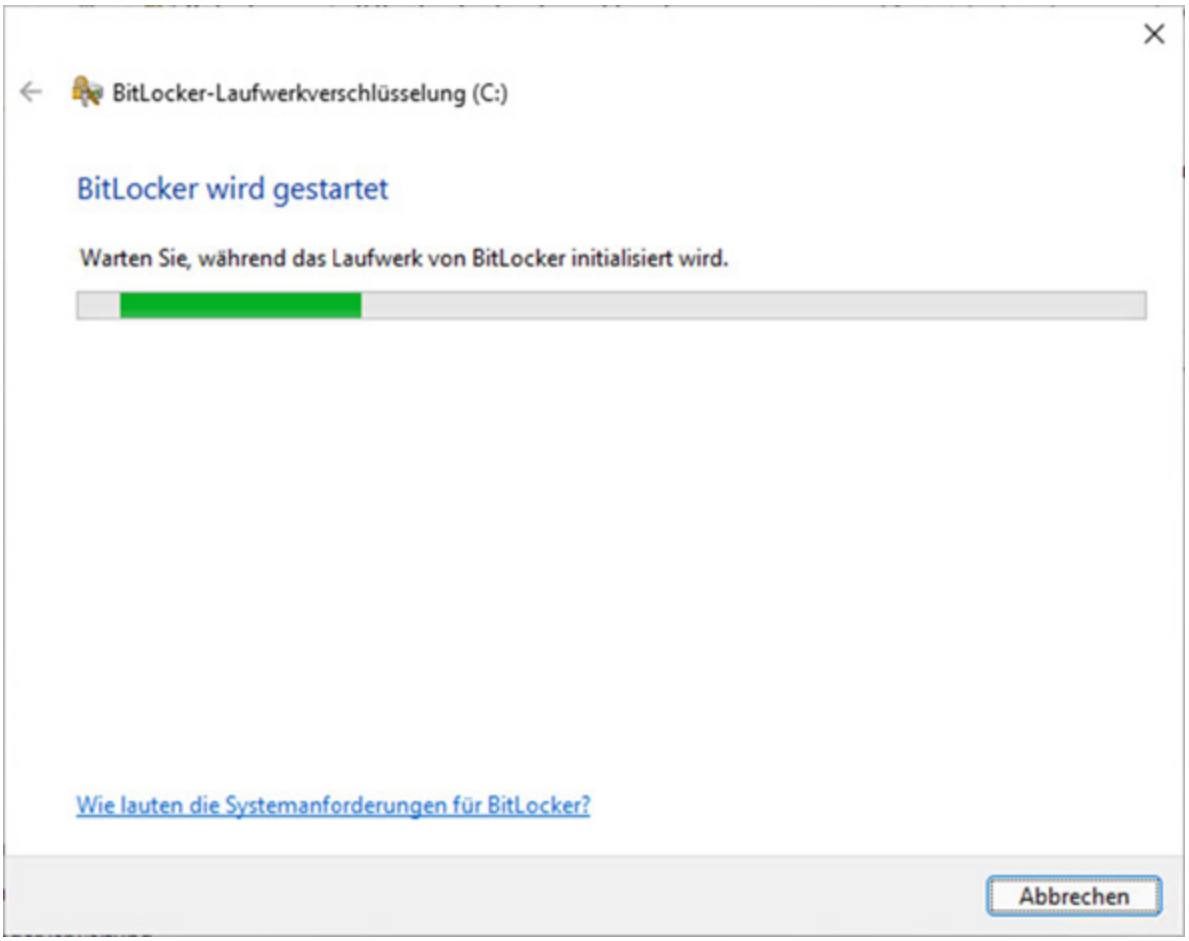

Abbildung 26.10: BitLocker wird gestartet

Nun wählen Sie aus, wo das komplexe Wiederherstellungskennwort gespeichert wird, das Sie benutzen müssen, wenn der Start von BitLocker verhindert wird.

Dies kann immer dann passieren, wenn Sie die Festplatte in ein anderes Gerät einbauen, oder wenn Sie beispielsweise die Startdateien geändert haben.

Dieses Kennwort wird in einer Datei gespeichert und kann auch ausgedruckt werden.

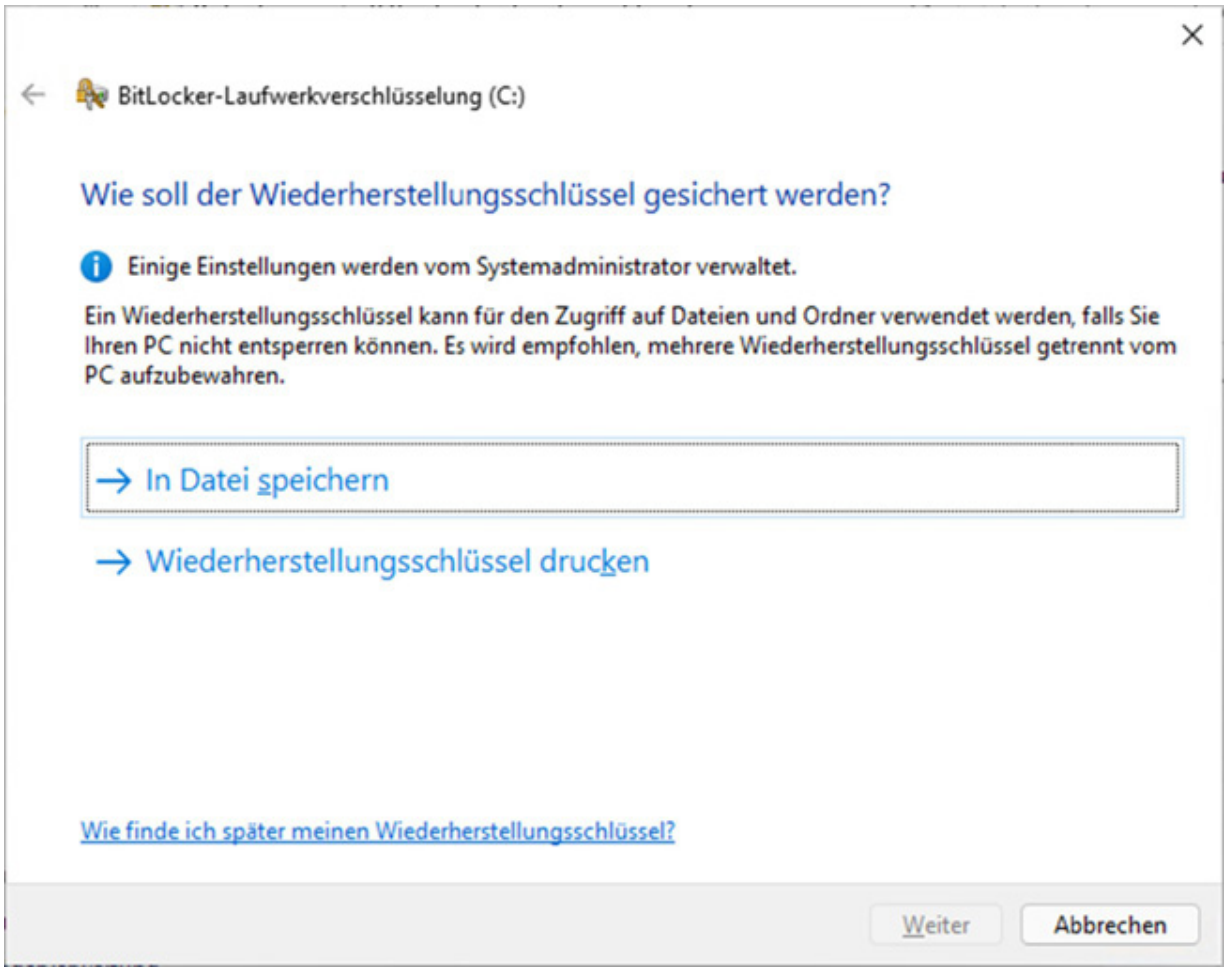

Abbildung 26.11: Wiederherstellungsschlüssel

ACHTUNG!

Sie können das Kennwort auf Diskette, auf dem USB-Stick oder auf der Festplatte speichern, nicht aber auf der

verschlüsselten Partition!

Bedenken Sie auch, dass es auf dem USB-Stick vielleicht nicht so gut aufgehoben ist, denn gerade bei einem Ausfall des Sticks brauchen Sie das Kennwort!

Der nächste Schritt ist die Auswahl, ob das gesamte Laufwerk verschlüsselt werden soll oder nur der verwendete Speicherplatz.

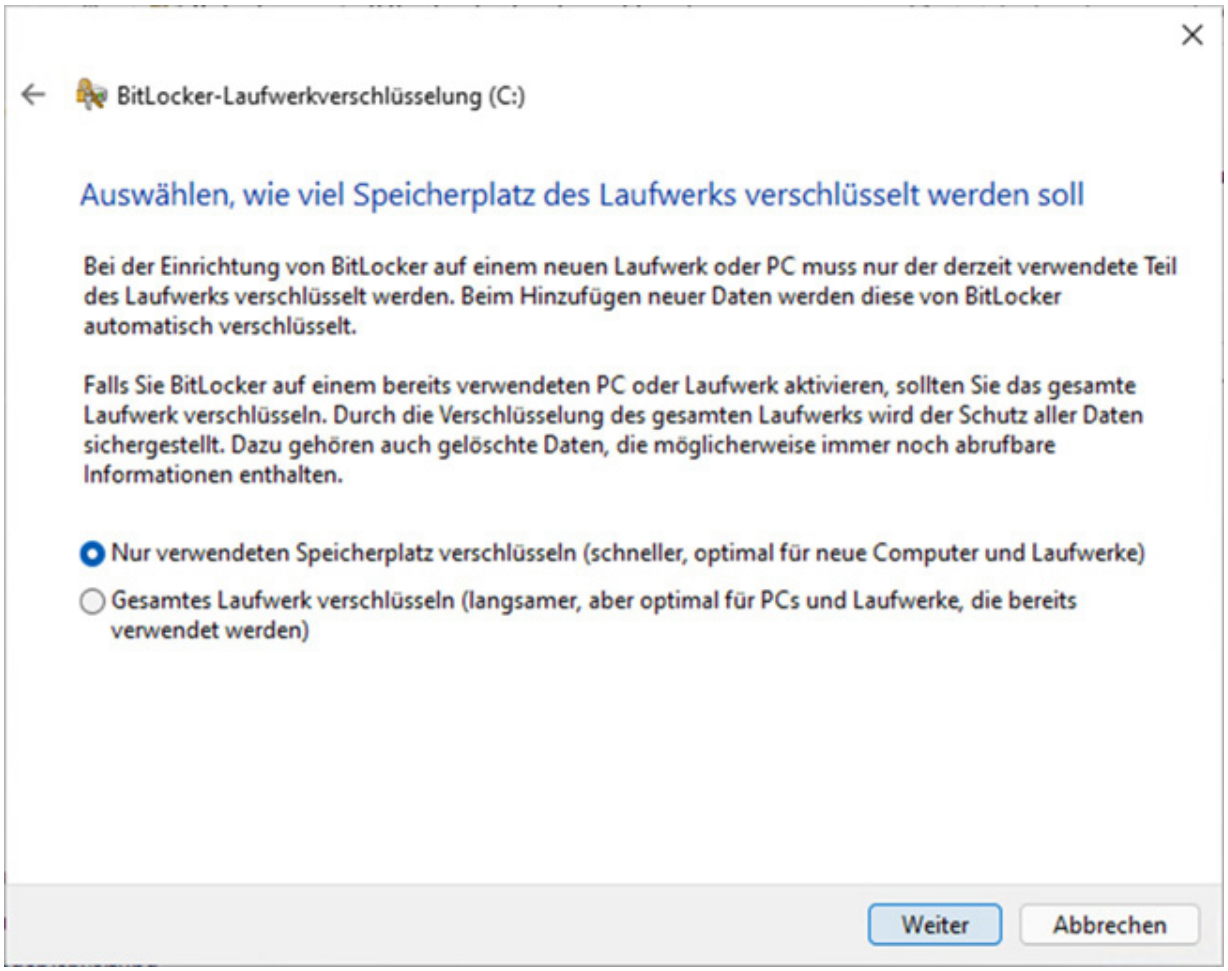

Abbildung 26.12: Auswahl Speicherplatz

ACHTUNG!

Auch wenn Sie wählen, dass nur der verwendete Speicherplatz verschlüsselt werden soll, bedeutet das nicht, dass die später hinzugefügten Daten unverschlüsselt sind.

Diese werden natürlich beim Hinzufügen auch verschlüsselt.

Der einzige, aber relevante Unterschied ist, dass bei einem Computer, der bereits in Gebrauch ist, unter Umständen Reste von zuvor gelöschten Daten vorhanden sind, die eventuell wiederhergestellt werden könnten.

Diese würden dann nicht verschlüsselt werden, da sie nicht als „verwendeter Speicherplatz“ betrachtet werden.

In diesem Fall sollten Sie immer das gesamte Laufwerk verschlüsseln, da dadurch auch diese Datenreste verschlüsselt und damit sicher sind.

Die letzte Auswahl ist der zu verwendende Verschlüsselungsmodus.

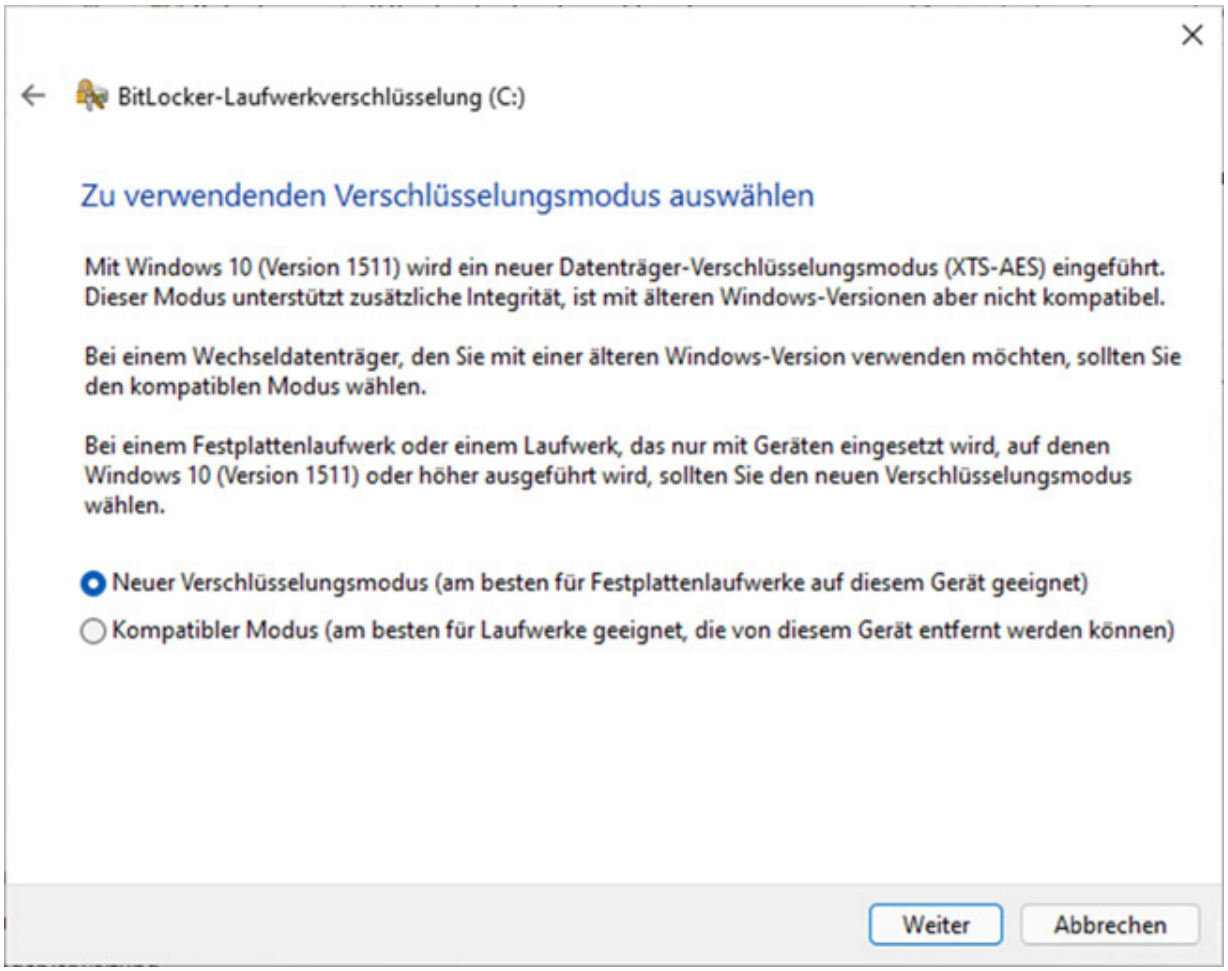

Abbildung 26.13: Verschlüsselungsmodus

BitLocker gibt es schon eine ganze Weile, dieses Feature ist permanent verbessert worden, oft, ohne dass man es bemerkt hat.

So wurde mit Windows 10 beim ersten großen Funktionsupdate im Herbst 2015 der Verschlüsselungsalgorithmus geändert.

Das hat zur Folge, dass nur Clients mit Windows 10 ab Version 1511 und Windows 11 diesen neuen Verschlüsselungsalgorithmus auch wieder entschlüsseln können.

Das sollte normalerweise kein Problem sein, nur wenn Sie dieses Laufwerk unter Umständen auch in älteren Systemen

einsetzen möchten, sollten Sie den „kompatiblen Modus“ wählen.

Er folgt noch eine Abfrage, bei der Sie die Systemüberprüfung aktivieren können.

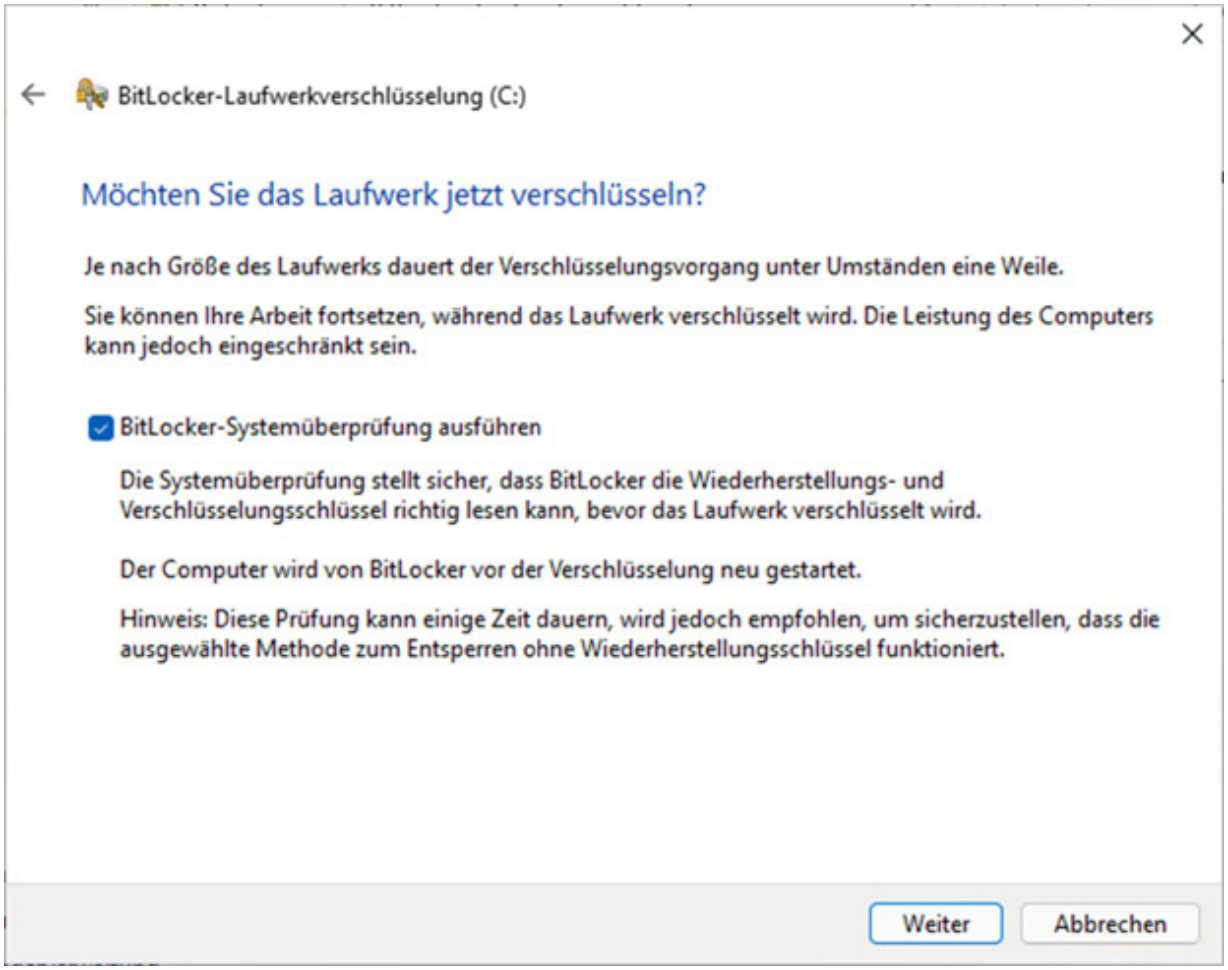

Abbildung 26.14: Systemüberprüfung

BitLocker verschlüsselt nun das Laufwerk und verlangt einen Neustart.

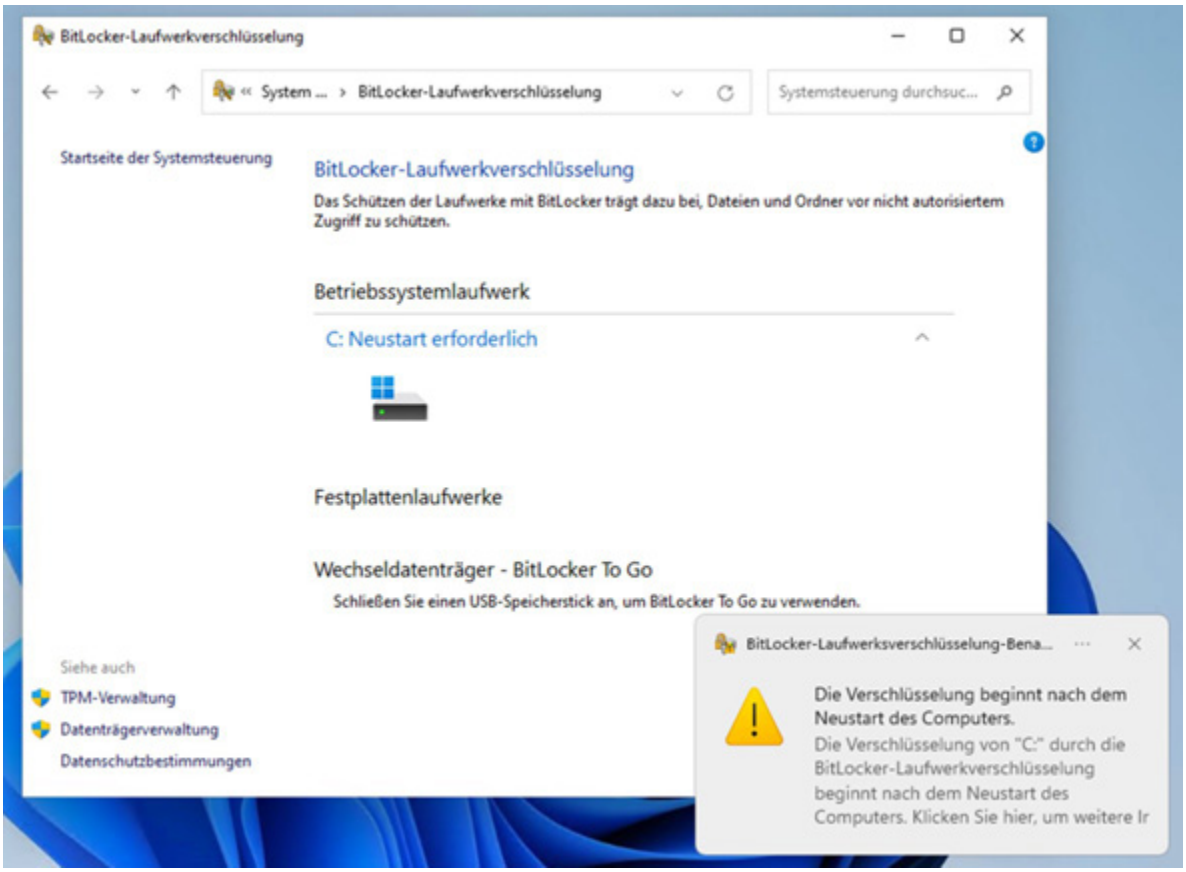

Abbildung 26.15: Neustart

Nach dem Neustart ist das Laufwerk verschlüsselt, kann aber vom Benutzer ohne Einschränkungen benutzt werden.

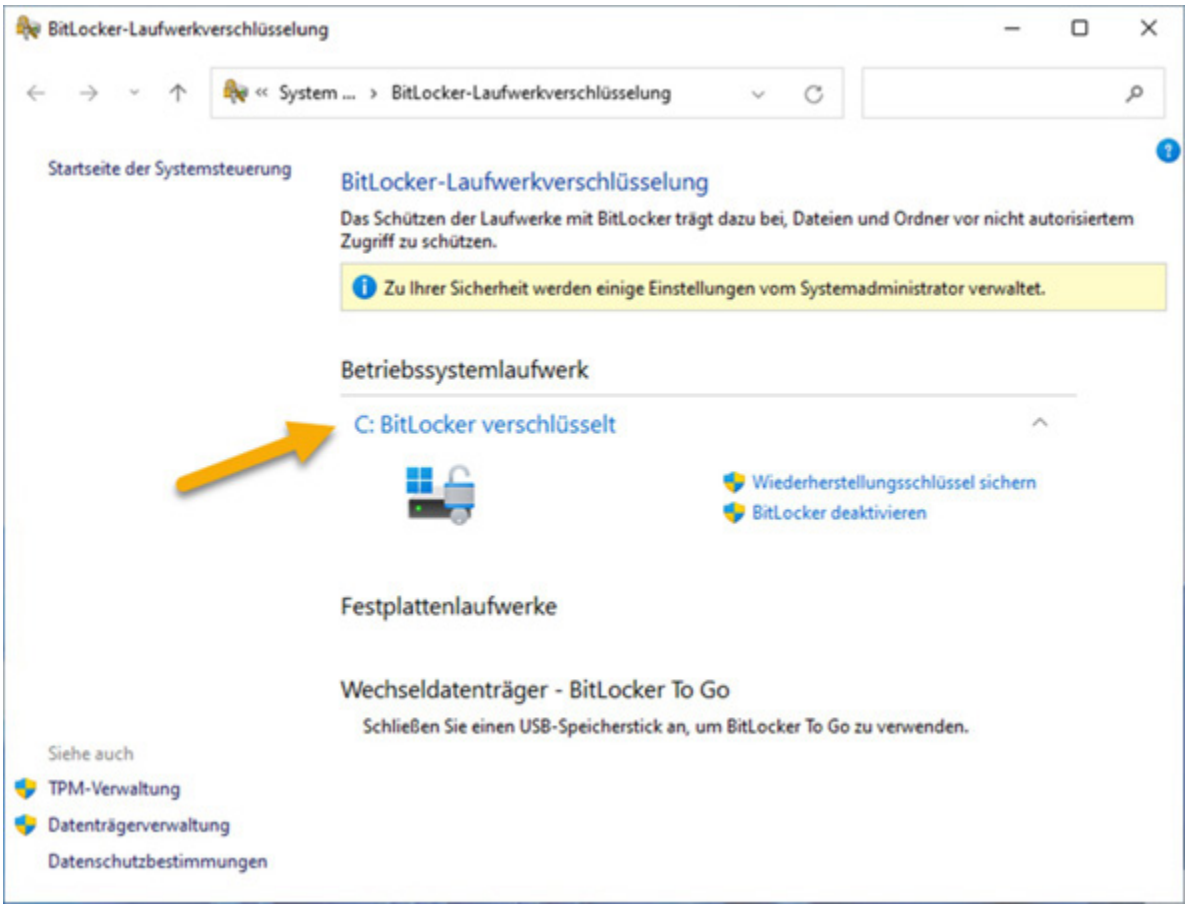

Abbildung 26.16: Laufwerk ist verschlüsselt

Übung 26.2

- Aktiveren Sie BitLocker auf W11
- Speichern Sie den Schlüssel in einer Freigabe mit Namen „Bitlocker“ auf Server2 unter dem Namen „BitLockerW11“

- Konfigurieren Sie BitLocker optimiert für einen bereits benutzten W11 Desktop und aktivieren Sie eine Systemüberprüfung

26.2.1 BitLocker mit USB-Stick

Windows 11 setzt ja für die Installation bereits einen TPM-Chip voraus, insofern gibt es mit diesem Betriebssystem im Normalfall keine Probleme.

Allerdings kann es durch Upgrades von Windows 10 in einigen Fällen dazu kommen, dass Windows 11 auch ohne TPM-Chip läuft.

In diesem Fall, oder falls Sie Windows 10 ohne TPM-Chip installiert haben, müssen Sie das Betriebssystem so konfigurieren, dass der BitLocker-Schlüssel nicht auf einem TPM-Chip gespeichert wird, sondern auf einem USB-Stick.

Dies können Sie wieder in der lokalen Gruppenrichtlinie konfigurieren.

Dafür erstellen Sie wieder eine MMC und fügen das Snap-In „Gruppenrichtlinienobjekt – Lokaler Computer“ ein.

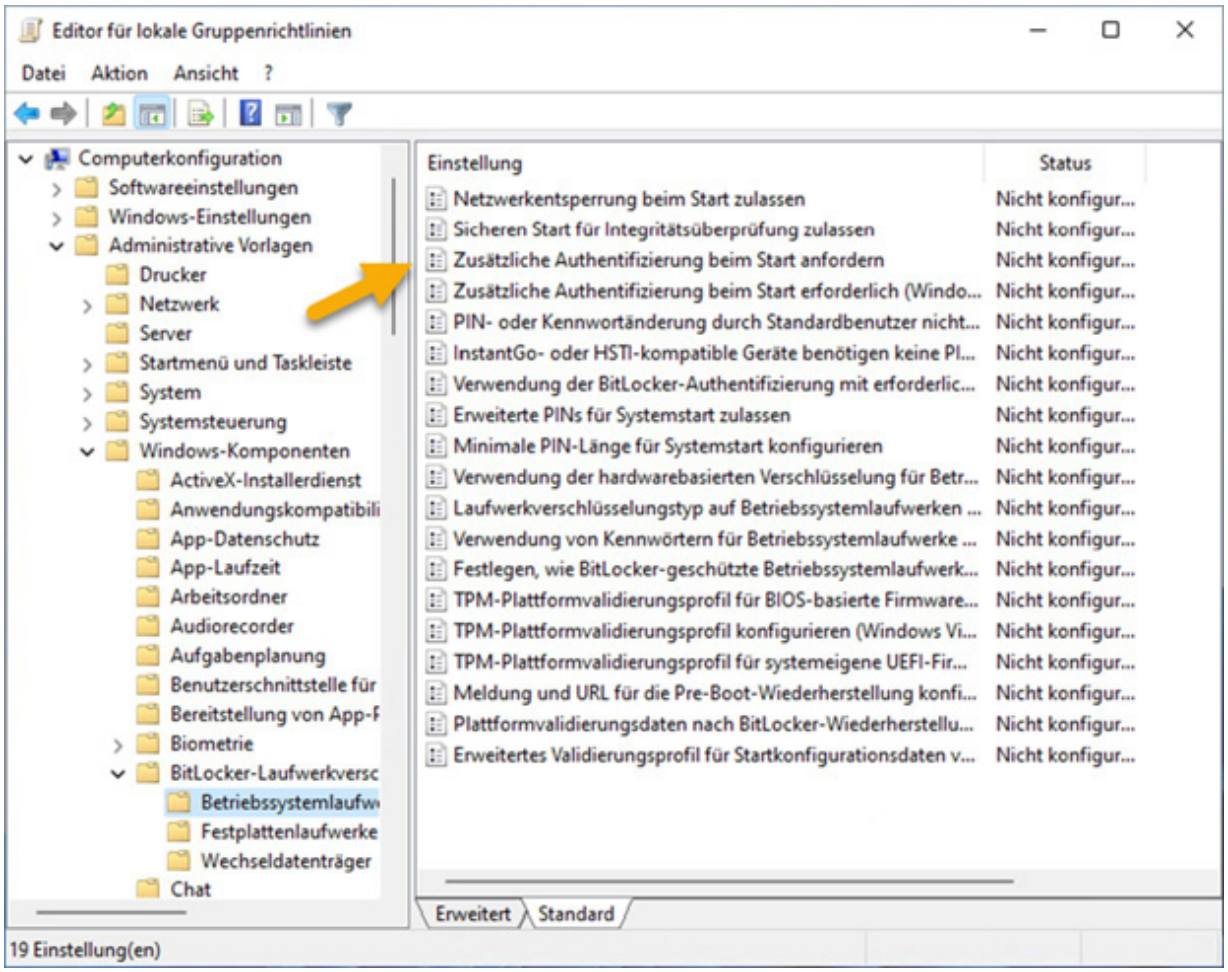

Abbildung 26.17: Gruppenrichtlinieneinstellung

Nun gehen Sie folgenden Weg:

- Computerkonfiguration
- Administrative Vorlagen
- Windows Komponenten
- BitLocker-Laufwerksverschlüsselung

Dort wechseln Sie ins Untermenü „Betriebssystemlaufwerk“ und wählen die Einstellung: „Zusätzliche Authentifizierung beim Start anfordern“ aus.