



Sicher verschlüsseln mit Bitlocker

Verschlüsselung ist nicht alles, aber ohne Verschlüsselung ist alles nichts.

Die Bitlocker Laufwerksverschlüsselung ist ein in Windows integriertes Feature, das Daten vor Bedrohungen durch Datendiebstahl oder durch Offenlegung verlorener, gestohlener oder nicht ordnungsgemäß außer Betrieb gesetzter Computer schützen soll.

Der Schutz von Festplatteninformationen gehört ja mittlerweile zum Standard, sei es im Server- oder Clientumfeld.

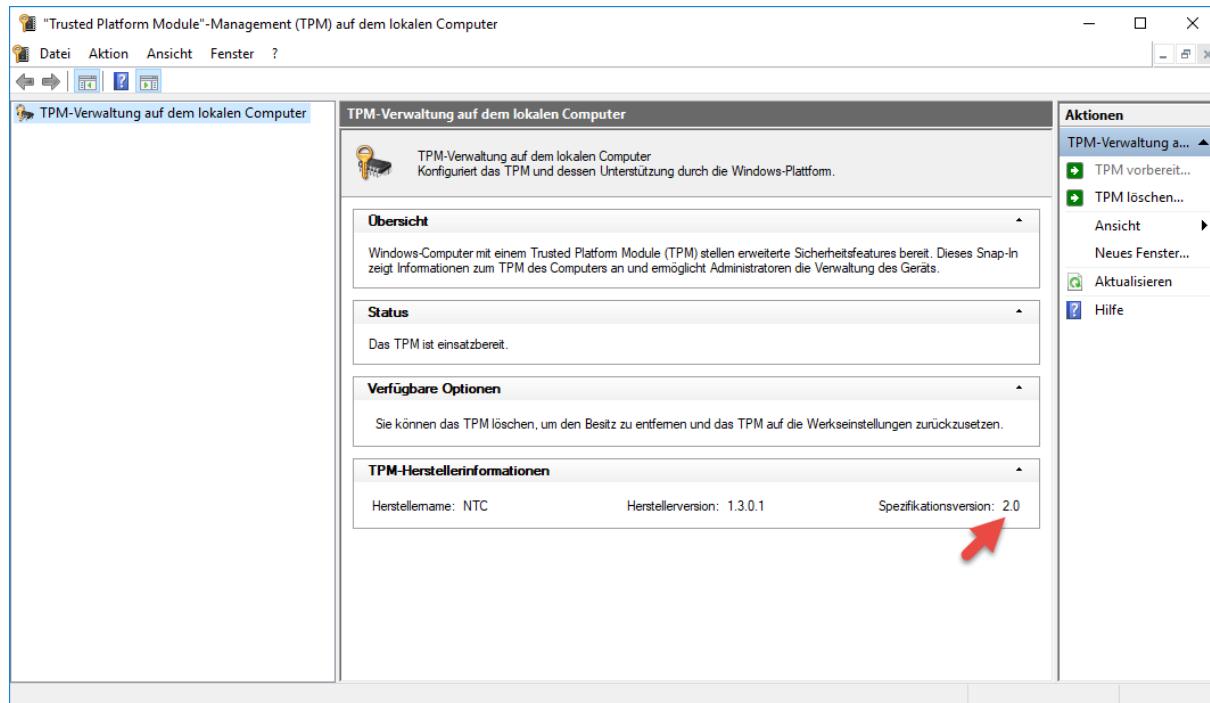
Clientsysteme gehören für mein Verständnis immer geschützt, egal ob es sich dabei um eine Workstation oder ein Notebook handelt. Auch Serversysteme in lokalen Niederlassungen, ohne Anbindung an ein Rechenzentrum, gehören abgesichert.

Was benötigen wir für eine Verschlüsselung mit Bitlocker?

Es gibt heute kaum noch ein Businessgerät, in dem kein TPM-Modul verbaut ist. TPM steht für (Trusted Platform Module) und überwacht die integrierte Hardware in einem Computer. Sollte die mit Bitlocker verschlüsselte Festplatte ausgebaut werden, wird diese ihren Dienst in einem anderen Computer verweigern. Denn die verschlüsselte Festplatte benötigt für die Entschlüsselung, das TPM Modul mit dem diese auch verschlüsselt wurde.

Wie prüfen wir denn ob ein TPM Modul verbaut ist?

Über die CMD führen wir den Befehl tpm.msc aus:



Das TPM Modul kann sofern eines vorhanden ist, erst dann in Windows angezeigt werden, wenn es im BIOS auch aktiviert wurde.

Zur Verschlüsselung einer Festplatte ist ein TPM Modul nicht zwingend notwendig. Bitlocker verschlüsselt Festplatten auch ohne Modul, aber dann nur mit einer softwarebasierten anstatt einer hardwarebasierten Verschlüsselung.



Sicher verschlüsseln mit Bitlocker

Dafür muss die lokale Richtlinie unter Windows angepasst werden.

Verwendung der hardwarebasierten Verschlüsselung für Betriebssystemlaufwerke konfigurieren

Vorherige Einstellung Nächste Einstellung

Nicht konfiguriert Kommentar:

Aktiviert ←

Deaktiviert Unterstützt auf:

Mindestens Windows Server 2012, Windows 8 oder Windows RT

Optionen: Softwarebasierte Verschlüsselung von BitLocker verwenden, wenn keine hardwarebasierte Verschlüsselung verfügbar ist

Zulässige Verschlüsselungsalgorithmen und Verschlüsselungssammlungen für die hardwarebasierte Verschlüsselung einschränken

Verschlüsselungsalgorithmen oder Verschlüsselungssammlungen wie folgt einschränken:
2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.

Hilfe:

Mit dieser Richtlinieneinstellung können Sie die Verwendung der hardwarebasierten Verschlüsselung durch BitLocker auf Betriebssystemlaufwerken verwalten und angeben, welche Verschlüsselungsalgorithmen für die hardwarebasierte Verschlüsselung verwendet werden können. Die Verwendung der hardwarebasierten Verschlüsselung kann die Laufwerksleistung beim Lesen oder Schreiben von Daten auf einem Laufwerk verbessern.

Wenn Sie diese Richtlinieneinstellung aktivieren, können Sie zusätzliche Optionen angeben, die steuern, ob auf Computern, die eine hardwarebasierte Verschlüsselung nicht unterstützen, stattdessen die softwarebasierte Verschlüsselung von BitLocker verwendet wird. Außerdem können Sie angeben, ob die bei der hardwarebasierten Verschlüsselung verwendeten Verschlüsselungsalgorithmen und Verschlüsselungssammlungen eingeschränkt werden sollen.

Wenn Sie diese Richtlinieneinstellung deaktivieren, kann

OK Abbrechen Übernehmen

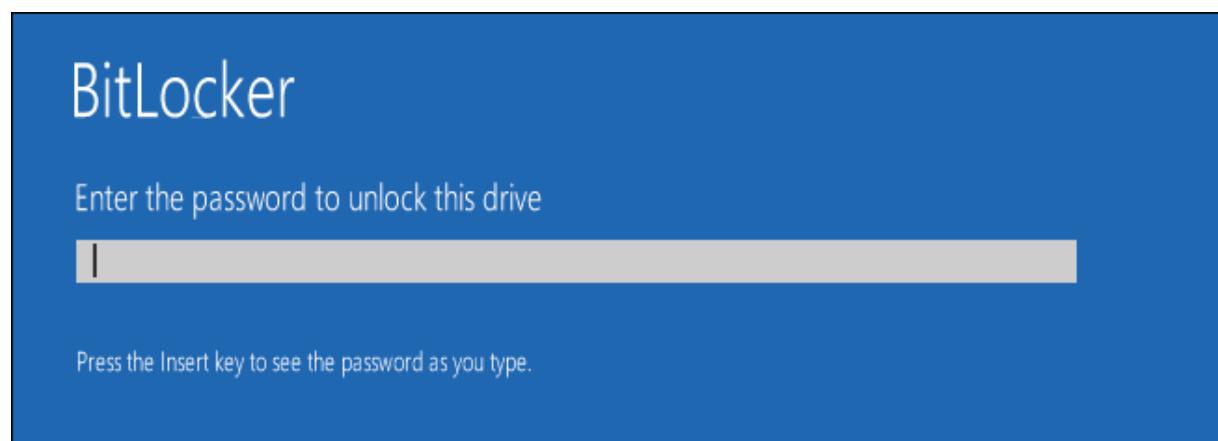


Sicher verschlüsseln mit Bitlocker

Wenn ein TPM-Module eingesetzt wird, kann das Verhalten so eingestellt werden, dass nach dem Start zusätzlich z.B. noch eine PIN eingegeben werden muss.

The screenshot shows the 'Zusätzliche Authentifizierung beim Start anfordern' (Additional authentication required at start) dialog box. The 'Aktiviert' (Enabled) radio button is selected, indicated by a red arrow. The 'Unterstützt auf:' (Supported on:) dropdown shows 'Mindestens Windows Server 2008 R2 oder Windows 7'. The 'Optionen:' (Options) section contains several dropdown menus: 'TPM-Start konfigurieren:' set to 'TPM zulassen', 'TPM-Systemstart-PIN konfigurieren:' set to 'Systemstart-PIN bei TPM zulassen', 'TPM-Systemstartschlüssel konfigurieren:' set to 'Systemstartschlüssel bei TPM zulassen', and 'TPM-Systemstartschlüssel und -PIN konfigurieren:' set to 'Systemstartschlüssel und PIN bei TPM zulassen'. A large red arrow points to the 'Systemstart-PIN bei TPM zulassen' dropdown. The 'Hilfe:' (Help) section provides detailed information about the policy settings. At the bottom are 'OK', 'Abbrechen' (Cancel), and 'Übernehmen' (Apply) buttons.

Es ist darauf zu achten, dass das Tastaturlayout nach dem Start des Computers „ENGLISCH“ ist!





Sicher verschlüsseln mit Bitlocker

Weitere wichtige Information zu Einrichtung und Konfiguration von Bitlocker:

[Bitlocker Guide](#)

[Bitlocker einsetzen](#)

[Bitlocker zum Neustart anhalten und wieder starten](#)

[Bitlocker CMD bde Commands](#)

[Bitlocker Active Directory Tab doppelt in der ADUC](#)

[Bitlocker Laufwerk per Verknüpfung sperren](#)

[Bitlocker Administration and Monitoring](#)