Bitlocker Guide

Was ist BitLocker?

Bitlocker ist eine Full Disk Encryption (FDE) Suite, die ganze Festplatten verschlüsseln kann und zum anderen Teil auch eine Full Volume Encryption (FVE), die einzelne Partionen sicher verschlüsselt.

Unter Windows 10 kommt die XTS-AES-256 Bit Verschlüsselung zum Einsatz. Diese Schlüssellänge wird für Daten eingesetzt die als Streng Geheim klassifiziert wurden. AES-128 ist weiterhin als sicher eingestuft.

Die Daten auf dem Notebook werden mit einem TPM-Chip (Trusted Platform Module) gesichert. Sollte die Festplatte aus dem Notebook entfernt werden, so ist eine Entschlüsselung der Daten nicht mehr möglich. Eine Entschlüsselung funktioniert nur mit dem TPM-Chip mit dem die Festplatte oder Partition verschlüsselt wurden. Somit ist der TPM-Chip der Dekodierungsschlüssel zum Entsperren der Daten. Sollte von einem externen Datenträger, einem USB-Stick oder einer DVD gebootet werden, so sind die Daten auf der verschlüsselten Festplatte oder Partition weiterhin geschützt. Nur durch die Eingabe einer PIN oder/und Passwort können die Daten zusammen mit dem TPM-Chip entsperrt werden.

Notebooks eines Unternehmens sollten mit der Bitlocker Technologie geschützt werden. Im Falles eines Verlustes oder Diebstahls, schützt die Festplattenverschlüsselungstechnologie die Daten vor ungewollten Zugriffen.

Werde ich einen Unterschied zu PGP bemerken?

Nein. Bitlocker verwendet einen TPM-Chip auf dem Mainboard um den Verschlüsselungsprozess sicher und schnell durchzuführen. Nach dem Einschalten des Notebooks beginnt Bitlocker bereits mit der Verschlüsselung der Festplatte und das ohne Beeinträchtigung.

Wie arbeitet Bitlocker?

Nach dem Einschalten des Notebook bzw. der Anmeldung muss durch den neuen Benutzer nur noch eine 10-stellige alphanumerische PIN vergeben werden. Diese PIN sollte jeder gültige Benutzer des Notebooks kennen. Nach Eingabe der PIN sind die Daten

entsperrt, also nicht mehr durch Bitlocker geschützt. Der Bitlocker Schutz greift entweder im Ruhezustand und das automatisch oder wenn das Notebook heruntergefahren wird

PIN erstellen:

Eine PIN ist eine Kombination aus Zahlen und Buchstaben und muss je nach Richtlinie entweder nach dem Einschalten des Notebooks eingegeben werden oder nach dem das Notebook aus dem Ruhezustand erweckt wurde. Eine PIN sollte niemals in der Nähe des Notebooks aufbewahrt oder transportiert werden.

PIN ändern:

Die PIN kann durch den Benutzer jederzeit geändert werden und zwar wie folgt:

1. Anmelden am Notebook
2. Windows-Einstellungen öffnen, Suche > BitLocker verwalten
   Systemsteuerung\System und Sicherheit\Bitlocker-Laufwerksverschlüsselung
3. Die Option PIN ändern auswählen

Hinweis: Das Ändern der PIN erfordert keine lokalen administrativen Rechte.

PIN vergessen, was nun?

Bitlocker erstellt und speichert im Active Directory automatisch einen Wiederherstellungsschlüssel. Nur autorisierte Mitarbeiter der IT haben Zugriff auf diesen Schlüssel. Nach der Vergabe einer PIN durch den gültigen Benutzer, hat dieser auch die Möglichkeit den Wiederherstellungsschlüssel auf einem vorgegeben Laufwerk abzuspeichern.

Ein Datenlaufwerk mit Bitlocker schützen?

Wenn das Notebook über weitere Festplatten verfügt, können auch diese mit Bitlocker verschlüsselt werden. Das Aktivieren erfordert keine lokalen administrativen Rechte. Sobald das Laufwerk verschlüsselt ist, wird zum Entsperren des Laufwerks ein Kennwort benötigt. Ein automatisches Entsperren des Laufwerks kann eingestellt werden.

USB Laufwerke mit Bitlocker schützen?

Das Schreiben von Daten auf externe Laufwerke zwingt den Benutzer automatisch zur Verschlüsselung des USB-Sticks oder der Festplatte. Ist das externe Laufwerk verschlüsselt und das Kennwort wurde vergessen, kann der während der Einrichtung abgelegte Wiederherstelungsschlüssel zum Entsperren des Laufwerks eingesetzt werden. Ein automatisches Entsperren des Laufwerks kann eingestellt werden.

Standby Mode (Sleep Option)

Notebooks können in den Ruhezustand versetzt werden aber nicht in den Stand-by-Modus. Wenn ein Notebook im Stand-by-Modus versetzt werden würde, würde keine PIN Abfrage erfolgen, aus diesem Grund steht dieser Modus nicht zur Auswahl.

Wird die Leistung des Notebooks beeinflusst?

Moderne Notebooks nutzen 3% der Leistung beim Verschlüsseln der Festplatte sowie im Betriebsmodus.

Kann die Verschlüsselung aufgehoben werden?

Sobald die IT ein Notebook ausgegeben hat, ist die Verschlüsselung aktiv und kann nicht deaktiviert werden.

Bitlocker Guide

Was bedeutet was?

TPM:

Das TPM (Trusted Pprotection Module) ist ein Mikroship, der in modernen Laptops verbaut ist. Dieser dient zur Erstellung von Schlüsseln die von Bitlocker und weiteren sicherheitsrelevanten Funktionen eingesetzt werden können. Das TPM und Bitlocker kann das System ohne Eingabe einer PIN oder Passwort automatisch entschlüsseln.

Aber Vorsicht! Viele Geräte sind bereits beim Kauf verschlüsselt. Wenn das Gerät jetzt zur Reparatur eingeschickt wird, oder der Techniker vor Ort das Motherboard austauscht, wird es schwer wieder an die Daten zu kommen.

Das System sofern möglich bitte vorher immer entschlüsseln oder Bitlocker deaktivieren.

Benutzer Kennwort:

Sobald das TPM aktiviert wurde, wird ein Benutzer/Besitzer Kennwort festgelegt. Mit diesem Kennwort hat man die Gewalt über das TPM.

FVEK:

Der "Full Volume Encryption Key" ist ein Schlüssel, den Bitlocker zum Verschlüsseln des gesamten Volumes C: einsetzt.

VMK:

Der "Volume Master Key" wird durch Bitlocker selbst generiert und entsperrt den FVEK wodurch das Laufwerk C: entsperrt wird. Ein Zugriff ist nun möglich. Der VMK wird wiederrum durch den "Key Protectors" verschlüsselt.

Key Protectors:

An dieser Stelle beginnt die Kette. Ein "KP" kann ein USB-Stick, ein Passcode oder Wiederherstellungsschlüssel sein. Ein "KP" entsperrt den "VMK", der "VMK" den "FVEK".

Recovery Key:

Wer einen automatischen roll-out von Bitlocker plant, der sollte sich Gedanken um die Wiederherstellungsschlüssel (RK) machen. Standardmäßig speichert Bitlocker keinen Wiederherstellungsschlüssel ab. Für jedes verschlüsselte Volume sollte ein RK im Active Directory abgelegt werden.

Computer mit installiertem und aktivem TPM:

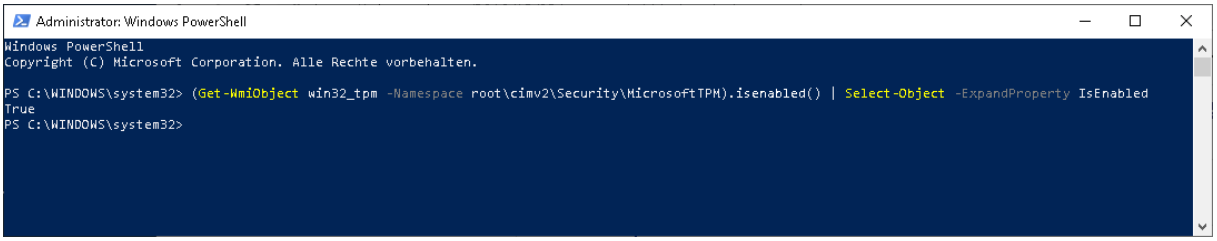
Für den automatischen roll-out von Bitlocker ist ein TPM erforderlich. Wäre kein TPM verbaut, so müsste der Benutzer manuell einen Key Protector erstellen. Mit einem aktiven TPM ist dies nicht nötig, weil der Computer während des Bootvorgangs mithilfe des TPM auf die Bitlockerverschlüsselung zugreift, und das Volume entsperrt sobald der PCR Test (Gefahreneinstufung) bestanden wurde. Soweit so gut. Diese Anforderung wäre mir persönlich zu schwach. Jetzt ist das Volume zwar vor Diebstahl geschützt aber wir haben keinen Zugriffsschutz. Setzt bitte einen Key Protector ein.

Bitlocker Guide

Ist meine Umgebung bereit für Bitlocker?

Das können wir auf dem Computer wie folgt überprüfen.

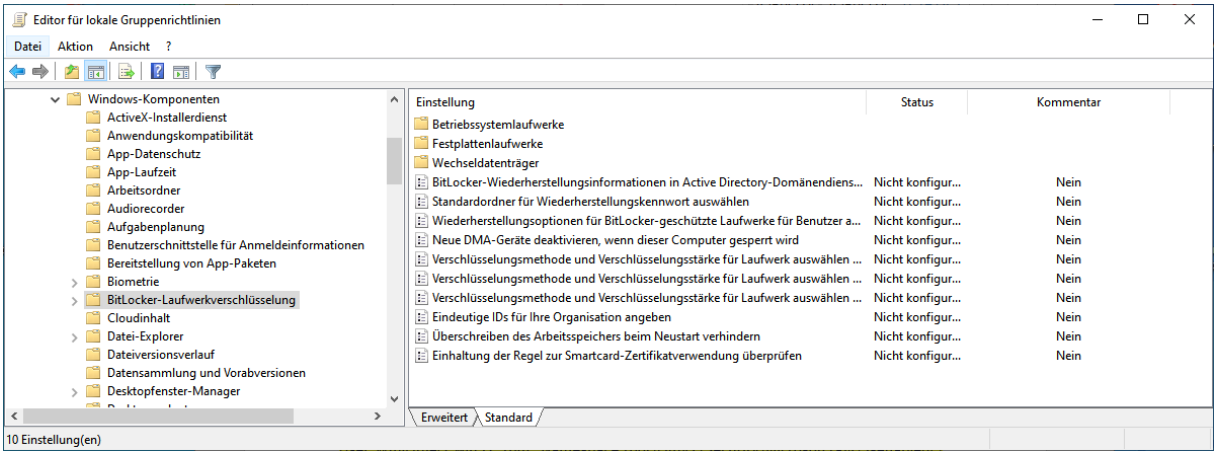
```
(Get-WmiObject win32_tpm -Namespace root\cimv2\Security\MicrosoftTPM).isenabled()
| Select-Object -ExpandProperty IsEnabled
```



Wie manage ich Bitlocker in einem Firmennetzwerk?

Dafür stehen uns seine Menge an Richtlinien bereit. Was sollte umgesetzt werden?

- Die Verschlüsselungsstärke sollte auf XTS-AES-256 Bite eingestellt werden
- Den Wiederherstellungsschlüssel im Active Directory abspeichern
- Bitlocker-Wiederherstellungsinformationen in AD speichern, aber bitte das ganze Schlüsselpaket



Bitlocker Guide

Was ist noch einmal ein PCR Test?

PCR steht für Platform Configuration Register. Diese Einstellungen legen die Bitlocker Integritätsprüfungen fest, die während des Bootvorgangs bestanden werden müssen. Sonst kann Bitlocker die im TPM gespeicherten Schlüssel (FVEK, VMK usw.) nicht freigegeben geben und das Volume würde nicht entsperrt werden.
Dieser Vorgang schützt vor Manipulationsversuchen.

Die Einstelungen finden wir in den Gruppenrichtlinien wieder.