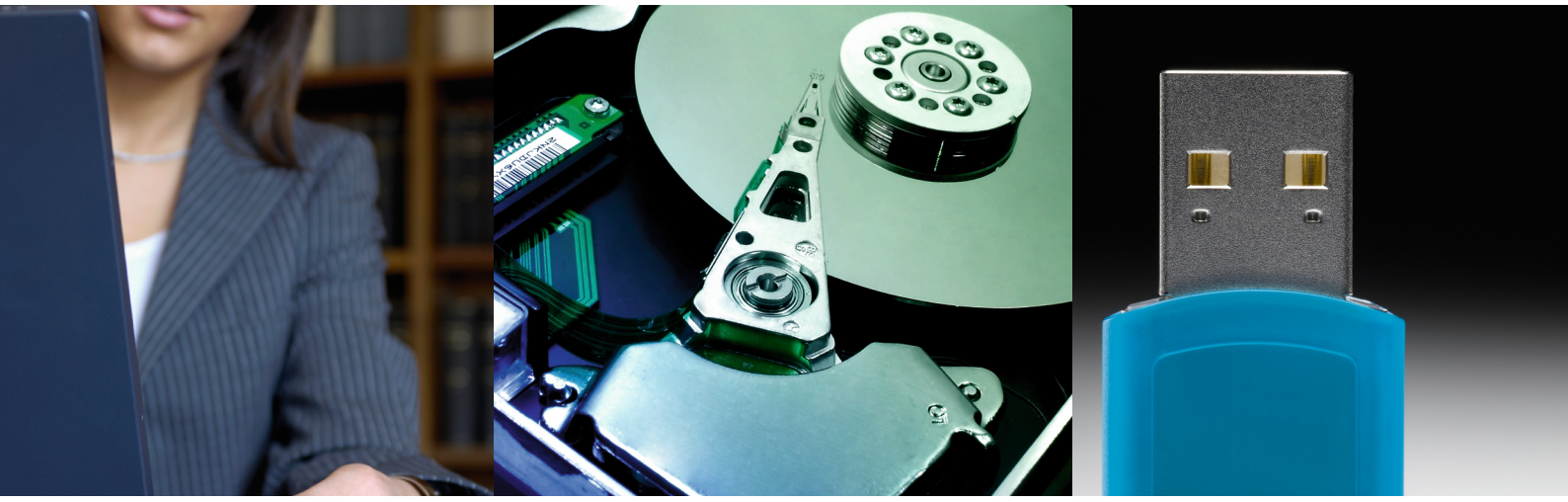
Fraunhofer Institut
Sichere Informations-
Technologie

BitLocker Drive Encryption im mobilen und stationären Unternehmenseinsatz

Ein Leitfaden für Anwender



Bundesamt
für Sicherheit in der
Informationstechnik

Autoren:
Jan Steffan, Andreas Poller, Jan Trukenmüller, Jan-Peter Stotz, Sven Türpe

Fraunhofer-Institut für Sichere Informationstechnologie
- Testlabor IT-Sicherheit -
Rheinstraße 75
64295 Darmstadt
Tel.: +49 6151 869 0
E-Mail: info@sit.fraunhofer.de
Web: http://www.sit.fraunhofer.de

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-5452
E-Mail: Thomas.Caspers@bsi.bund.de
Web: http://www.bsi.bund.de

Zusammenfassung

Der Leitfaden »*BitLocker Drive Encryption im mobilen und stationären Unternehmenseinsatz*« unterstützt Anwender von Microsoft Windows Vista dabei, die in einige Versionen integrierte Datenträgerverschlüsselung zu nutzen. Er wendet sich an IT-Verantwortliche, Sicherheitsbeauftragte und Administratoren in Unternehmen und Behörden. Der Leitfaden erläutert Funktionsweise, Fähigkeiten und Einsatzmöglichkeiten von BitLocker, zeigt das erzielbare Sicherheitsniveau, dessen Grenzen sowie mögliche Nebenwirkungen beim Einsatz und gibt Anwendern konkrete Handreichungen.

BitLocker Drive Encryption (BDE) verschlüsselt Partitionen und sichert den Bootprozess des Systems gegen Manipulationen. Voraussetzung ist ein Trusted Platform Module (TPM) und das passende BIOS. BitLocker ist damit die erste Sicherheitskomponente in Windows, die sich auf das Trusted Computing stützt. Schlüssel lassen sich mit oder ohne PIN-Schutz im TPM speichern, als weiterer Sicherheitsanker kann ein USB-Speicher verwendet werden. Für Nutzer und Anwendungen ist die Verschlüsselung weitgehend transparent.

Der Leitfaden geht vom Stand im Herbst 2007 aus. Er berücksichtigt jedoch auch voraussichtliche Änderungen in Service Pack 1 für Windows Vista sowie in Windows Server 2008, soweit sie derzeit bekannt sind.

Inhalt

1 Über diesen Leitfaden

Eine Neuerung von Microsoft Windows Vista ist die Partitionsverschlüsselung *BitLocker Drive Encryption (BDE)*. Anwendern der Vista-Versionen *Enterprise* und *Ultimate* sowie von Windows Server 2008 verspricht BitLocker, Daten auf der Festplatte vertraulich zu halten. Im Vordergrund stehen dabei Situationen, in denen Unbefugte physischen Zugriff auf einen PC erlangen. Dazu gehören zum Beispiel der Diebstahl oder der versehentliche Verlust des Geräts, aber auch Zugriffe vor Ort auf ausgebaute Datenträger oder mit Hilfe mitgebrachter Software. BitLocker nutzt dabei die Trusted-Computing-Plattform v1.2 der Trusted Computing Group (TCG, www.trustedcomputinggroup.org)

BitLocker ist damit eine interessante Sicherheitskomponente sowohl für Laptops als auch für ortsfeste Arbeitsplätze und die übrige stationäre IT-Infrastruktur einer Organisation. Auf einem einzelnen PC mit geeigneter Hardware lässt sich BitLocker auch ohne größere Schwierigkeiten aktivieren. Der sichere und reibungsarme Einsatz erfordert jedoch einige weitergehende Erwägungen. Das Fraunhofer-Institut für Sichere Informationstechnologie SIT hat deshalb in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) diesen Leitfaden für Anwender erstellt.

Für wen ist dieser Leitfaden?

Der vorliegende Leitfaden unterstützt IT-Verantwortliche, Administratoren und Sicherheitsbeauftragte bei diesen Überlegungen. Er soll die vorhandene Dokumentation nicht ersetzen, sondern um Empfehlungen für die Praxis ergänzen. Mitbringen sollten die Leser ein solides Basiswissen zum einen in der IT-Sicherheit, zum anderen im Betrieb von Windows-Systemen und -Netzen. Spezialkenntnisse setzt der Leitfaden jedoch nicht voraus. Wer auf die Stichworte *Blockchiffre*, *Active Directory*, *TPM* und *Gruppenrichtlinie* nicht nur mit einem ahnungslosen Schulterzucken reagiert, dürfte beim Lesen keine größeren Schwierigkeiten haben.

Was steht drin?

Zum besseren Verständnis erläutert Abschnitt 2 die Arbeitsweise von BitLocker und die wichtigsten Begriffe. Empfehlungen sind in den Abschnitten 3 und 4 zu finden. Abschnitt 3 diskutiert die Eignung von BitLocker und den damit möglichen Sicherheitsgewinn. Der darauffolgende 4. Abschnitt gibt Empfehlungen für den Einsatz. Er orientiert sich am Lebenszyklus eines Systems vom Einkauf bis zur Ausmusterung und zeigt für jede Phase die erforderlichen Erwägungen

auf. Er gibt einen Überblick über die Funktionsweise von BitLocker, seine Einbettung ins System und die unterstützten Betriebsarten. Im Anschluss an die Empfehlungen skizziert Abschnitt 5, wie BitLocker im Vergleich zu den Alternativen TrueCrypt und das Encrypting File System (EFS) abschneidet und inwieweit Kombinationen aus BitLocker und diesen beiden Werkzeugen sinnvoll sind. Jedoch ist es nicht Ziel dieses Leitfadens, BitLocker systematisch mit den erhältlichen Alternativen zu vergleichen. Auch eine vollständige Sicherheitsanalyse von BitLocker selbst ist nicht beabsichtigt.

Bezeichnungen

Dieser Leitfaden verwendet einige Bezeichnungen und Abkürzungen synonym:

- Volume und Partition; die subtilen Unterschiede sind hier bedeutungslos
- BitLocker, Bitlocker Drive Encryption und die Abkürzung BDE
- Volume-Schlüssel, Full Volume Encryption Key und die Abkürzung FVEK
- Diffuser und Diffusor benutzt auch Microsoft wechselweise

Erläutert werden diese Begriffe in Abschnitt 2 sowie im Glossar.

Typografische Konventionen

Wiedergegebene Kommandos im Text sind durch *`eine andere Schriftart`* gekennzeichnet. Wichtige Stichworte sind **fett** gedruckt. Andere Hervorhebungen erfolgen durch *schräggestellte Schrift*. URLs sind als Hyperlinks markiert.

2 BitLocker im Überblick

2.1 Was ist BitLocker Drive Encryption?

BitLocker Drive Encryption (BDE, BitLocker) verschlüsselt den Inhalt von NTFS-Volumes mit AES. Die Windows-Versionen Vista Enterprise, Vista Ultimate und Server 2008 enthalten BitLocker und integrieren damit eine Sicherheitsfunktion in das System, die bisher Produkten von Drittanbietern vorbehalten war. BitLocker ergänzt die Sicherheitsfunktionen von Windows, ersetzt jedoch keine davon vollständig.

Grundsätzlich eignet sich BitLocker für alle NTFS-Volumes, in der Praxis aber nur für solche auf fest installierten bzw. zugeordneten Datenträgern. Der mobile Einsatz auf Wechseldatenträgern an verschiedenen PC ist nicht praktikabel. Gegenwärtig[1] erstreckt sich die Unterstützung nur auf die Systempartition der jeweiligen Windows-Installation. Dies soll sich mit dem Erscheinen von Service Pack 1 im Frühjahr 2008 ändern, BitLocker wird dann auch Daten-Volumes auf derselben oder weiteren Festplatten verschlüsseln. In der Ursprungsversion von Vista ist diese Möglichkeit bereits als undokumentierte Funktion enthalten.

BitLocker bedient sich der Trusted-Computing-Technik. Das Trusted Platform Module (TPM) in der PC-Hardware speichert Schlüssel und gibt sie nur frei, nachdem es den Systemzustand geprüft hat. Darüber hinaus kann das TPM je nach Konfiguration auch eine PIN zur Authentisierung des Benutzers verlangen. Als Nebeneffekt der Verschlüsselung schützt BitLocker damit die Integrität des Systems; dieser Schutz hat jedoch Grenzen.

In der vorliegenden Form richtet sich BitLocker vor allem an Anwender in Unternehmen und Behörden. Neben den Grundfunktionen stehen ihnen Mittel zur lokalen und zentralen Systemadministration sowie für die Schlüsselhinterlegung zur Verfügung.

2.2 Eine grobe Einordnung

Verschlüsselungslösungen für Dateien und Datenträger gibt es wie Sand am Meer. Grob klassifizieren kann man sie nach der verwendeten Verschlüsselungstechnik sowie nach dem Grundkonzept, das sich aus dem Gegenstand der

[1] Stand November 2007

Verschlüsselung ergibt. Sicherheit und praktische Brauchbarkeit in konkreten Einsatzszenarien hängen jedoch noch von einer Reihe weiterer Faktoren ab, so dass die Einordnung keine Bewertung darstellt.

Verschlüsselungstechnik

BitLocker nutzt als Algorithmus den De-facto-Standard AES. Auch die Festlegung auf einen einzelnen Algorithmus ist sehr verbreitet.

In der Schlüsselverwaltung geht Microsoft einen eigenen Weg. Einerseits bietet BitLocker keine Unterstützung für Smartcards und die Integration in Public-Key-Infrastrukturen und ist damit anderen Produkten unterlegen. Bemerkenswert ist andererseits die Nutzung des Trusted Computing.

Gegenstand der Verschlüsselung

Daten sind in Dateien gespeichert, Dateien in Dateisystemen, Dateisysteme in Volumes und Volumes auf Datenträgern. BitLocker verschlüsselt Volumes und unterscheidet sich darin grundlegend vom bereits seit Windows 2000 von Microsoft angebotenen Encrypting File System (EFS). Das Sicherheitsniveau und die Einsatzmöglichkeiten hängen davon ab, auf welcher Ebene die Verschlüsselung erfolgt:

- Die Verschlüsselung einzelner Dateien lässt alle Metadaten (z.B. Dateinamen und -länge, Timestamps etc.) ungeschützt und bietet zahlreiche Möglichkeiten für Datenlecks. Beispiele sind EFS sowie allerlei kleine Tools für den Hausgebrauch, etwa bcrypt[2].
- Bei der Containerverschlüsselung liegt ein ganzes Dateisystem verschlüsselt in einer großen Datei. Der passende Schlüssel öffnet diesen Container und macht das Dateisystem zugänglich, in der Windows-Welt meist unter einem eigenen Laufwerksbuchstaben. Metadaten werden mit verschlüsselt, die Gefahr von Datenlecks z.B. durch temporäre Dateien ist aber auch hier hoch. Beispiele sind Steganos Safe, TrueCrypt und die Funktion FileVault in Mac-OS X.
- Nur die Verschlüsselung ganzer Volumes oder Datenträger kann zuverlässig alle möglichen Speicherorte im System erfassen. Darüber hinaus kann sie – als Nebeneffekt oder Zusatzfunktion – dabei helfen, die Integrität des Betriebssystems gegen Manipulationen am Datenträger zu schützen. Neben BitLocker gehören in diese Kategorie zum Beispiel die Produkte SafeGuard Easy und SafeGuard Device Encryption von Utimaco.

[2] http://bcrypt.sourceforge.net/

BitLocker beruht auf dem umfassendsten Ansatz der Volume-Verschlüsselung, beschränkt sich aber auf permanent verfügbare Datenträger sowie vorerst auf die Systempartition. Eine BitLocker-geschützte Systempartition erfasst alle auf dieser Partition gespeicherten Dateien, die zugehörigen Metadaten (Namen, Timestamps, Längenangaben, Ordnerstrukturen usw.) sowie in der Regel die Auslagerungsdatei von Windows.

2.3 Komponenten und Begriffe

Zum besseren Verständnis erklärt dieser Abschnitt die wichtigsten Komponenten und Begriffe, ohne die Zusammenhänge und die Funktionsweise von BitLocker vollständig zu erläutern. Einen groben Überblick gibt Abbildung 1.

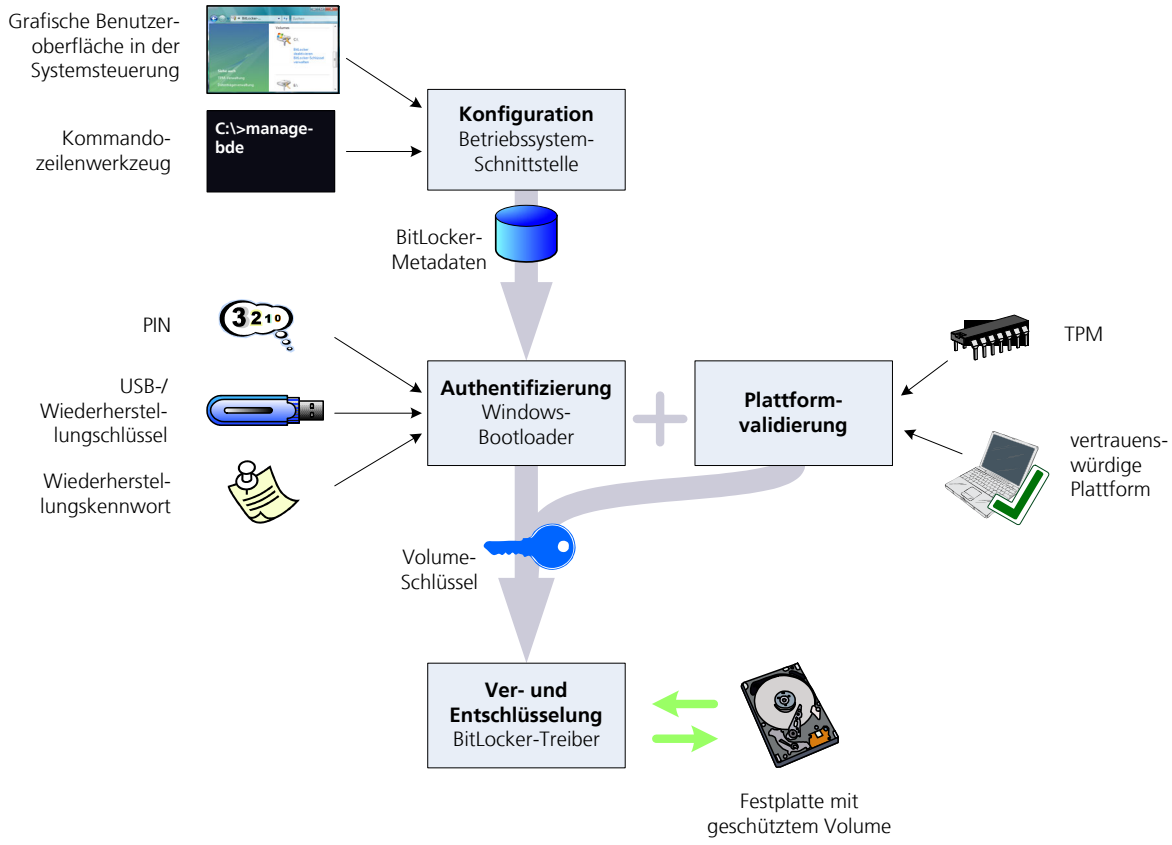


Abbildung 1: BitLocker-Komponenten.

Die Rollen sind wie folgt verteilt:

- Das **geschützte Volume** ist eine mit BitLocker verschlüsselte Partition[3] auf einem Datenträger, in der Regel einer eingebauten Festplatte. Microsoft unterscheidet zwischen dem Betriebssystem-Volume, von dem Windows Vista startet[4], und zusätzlichen Daten-Volumes.
- Der **BitLocker-Treiber** ver- und entschlüsselt die Volume-Daten. Details zur Verschlüsselung sind unter 2.4 beschrieben. Der Treiber arbeitet transparent für alle darauf aufbauenden Teile des Systems. Er ist unterhalb des NTFS-Dateisystemtreibers angesiedelt. Für Programme und Anwendungen im laufenden System ist BitLocker unsichtbar, sie bemerken nichts von seiner Existenz oder seinem Zustand.
- Der BitLocker-Treiber benötigt zu jedem Volume den passenden **Full Volume Encryption Key (FVEK)**, hier auch kurz **Volume-Schlüssel** genannt. Für die Systempartition muss der Bootloader diesen Schlüssel bereitstellen, für andere Daten-Volumes genügt die Bereitstellung nach dem Systemstart vor dem ersten Zugriff.
- Der **Windows-Bootloader** fragt den Benutzer nach Passwort, PIN oder Schlüsseln und ermittelt daraus den Volume-Schlüssel. Die Einzelheiten sind weiter unten in Abschnitt 2.5 genauer beschrieben. Neben Eingaben des Benutzers benötigt der Bootloader auch Metadaten aus dem verschlüsselten Volume sowie das TPM.
- Die **BitLocker-Metadaten** enthalten den FVEK in verschlüsselter Form. Sie liegen in einem reservierten Bereich des geschützten Volumes, den BitLocker nicht wie die übrigen Teile bearbeitet.
- Über die **BitLocker-Betriebssystem-Schnittstelle** greifen Programme aus dem laufenden System auf BitLocker zu. Windows Vista stellt eine Benutzerschnittstelle in der Systemsteuerung und das Kommandozeilenwerkzeug *manage-bde* zur Verfügung. Berechtigte Nutzer können damit Einstellungen abfragen und ändern sowie zusätzliche Daten-Volumes freigeben. Zeitaufwändige Operationen[5] erledigt BitLocker im Hintergrund, ohne dass der Nutzer warten muss.
- Um auf ein Volume zugreifen zu können, muss der Benutzer einen **Schlüssel** oder ein **Authentisierungsmerkmal** eingeben. Konfigurations- und situationsabhängig verwendet BitLocker eine **PIN**, einen **USB-Schlüssel**, einen **Wiederherstellungsschlüssel** oder ein **Wiederherstellungskennwort**, um den Volume-Schlüssel zu ermitteln. Möglich ist auch ein rein TPM-

[3] Dieser Leitfaden unterscheidet nicht zwischen den Begriffen *Volume* und *Partition*.
[4] Sind mehrere Instanzen des Systems auf einem PC installiert, so ist das Betriebssystem-Volume die Startpartition des jeweils laufenden oder zu startenden Systems. Alle anderen Volumes sind für diese Instanz Daten-Volumes.
[5] Insbesondere die Verschlüsselung der gesamten Partition nach dem Aktivieren sowie das Entschlüsseln nach dem Deaktivieren von BitLocker.

gestützter Betrieb ohne weitere Eingabe. Die Einzelheiten sind weiter unten in Abschnitt 2.5 erklärt.
- Das **Trusted Platform Module (TPM)** gehört zur PC-Hardware und dient als manipulationsresistenter Sicherheitsanker. Es speichert Schlüsselmaterial, mit dessen Hilfe BitLocker den Volume-Schlüssel (FVEK) gewinnt. Zugänglich ist dieses Material nur in einem bestimmten, vertrauenswürdigen Systemzustand, den das TPM durch »Messungen« der Konfiguration und der Software feststellt. Für Notfälle kann der Administrator auch TPM-unabhängige Schlüssel erzeugen und aufbewahren.

2.4 Verschlüsselung

BitLocker verwendet zur Verschlüsselung den Advanced Encryption Standard (AES), eine symmetrische Blockchiffre mit einer Blocklänge von 128 Bit (16 Bytes). Die Schlüssellänge von ist variabel, sie kann 128, 192 oder 256 Bit (16, 24 oder 32 Bytes) betragen. Der Algorithmus ist seit etwa zehn Jahren bekannt und vom US-amerikanischen National Institute of Standards and Technology (NIST) als U.S. FIPS PUB 197 (FIPS 197) standardisiert. Wesentliche kryptografische Schwächen haben sich bisher nicht gezeigt.

Als Kernfunktion von BitLocker arbeitet AES sektorweise im Cipher Block Chaining (CBC). Das bedeutet:

- Ver- oder entschlüsselt werden Sektoren von 512 bis 8192 Bytes Länge, das entspricht 32 bis 512 AES-Blöcken. Es gibt keine sektorübergreifende Verkettung.
- Innerhalb eines Sektors sind die Blöcke im CBC-Modus miteinander verkettet. Den erforderlichen Initialisierungsvektor (IV) berechnet BitLocker bei Bedarf jeweils neu aus dem Volume-Schlüssel (FVEK, siehe unten) und der Sektornummer.
- Der AES-Schlüssel ist für alle Sektoren und für alle Blöcke identisch.

BitLocker verschlüsselt alle Sektoren, in denen Dateiinhalte oder Metainformationen des NTFS-Dateisystems enthalten sind. Unverschlüsselt bleiben lediglich der BIOS Parameter Block der Partition mit grundlegenden Informationen über die Partition sowie die BitLocker-Metadaten.

Der Anwender kann zwei Aspekte der Verschlüsselungsmethode beeinflussen:

- Die **Schlüssellänge** beträgt wahlweise **128** oder **256 Bit**. Die mittlere Schlüssellänge von 192 Bit unterstützt BitLocker nicht.
- Ein zusätzlicher Algorithmus, der **Diffuser**, soll Schwächen des CBC-Verfahrens beheben. Der Diffuser vermischt Daten innerhalb eines Sektors und verknüpft sie mit einem zusätzlichen Sektorschlüssel.

In der **Standardeinstellung** arbeitet BitLocker mit **128 Bit** Schlüssellänge und der **Diffuser ist aktiviert**. Einzelheiten des Verfahrens und insbesondere die Arbeitsweise des Diffusers hat Microsoft in [1] veröffentlicht.

Grundlage der Verschlüsselung ist in allen Einstellungen der Full Volume Encryption Key (FVEK). Er enthält den gemeinsamen AES-Schlüssel für alle Sektoren und Blöcke einer Partition und dient zur Berechnung der Initialisierungsvektoren. Läuft BitLocker mit Diffuser, so liefert der FVEK neben dem AES-Schlüssel auch eine Eingabe zur Berechnung der einzelnen Sektorschlüssel.

2.5 Schlüsselverwaltung und Authentisierung

2.5.1 Überblick

Die Schlüsselverwaltung hat zwei Funktionen: Im Normalbetrieb soll sie sicherstellen, dass nur berechtigte Nutzer ein BitLocker-geschütztes Volume entschlüsseln und nutzen können. Die dafür verwendeten Mittel müssen im Alltag handhabbar sein. Daneben gibt es Mechanismen für den Notfall, bei denen es in erster Linie auf Funktionsfähigkeit in allen möglichen Situationen ankommt.

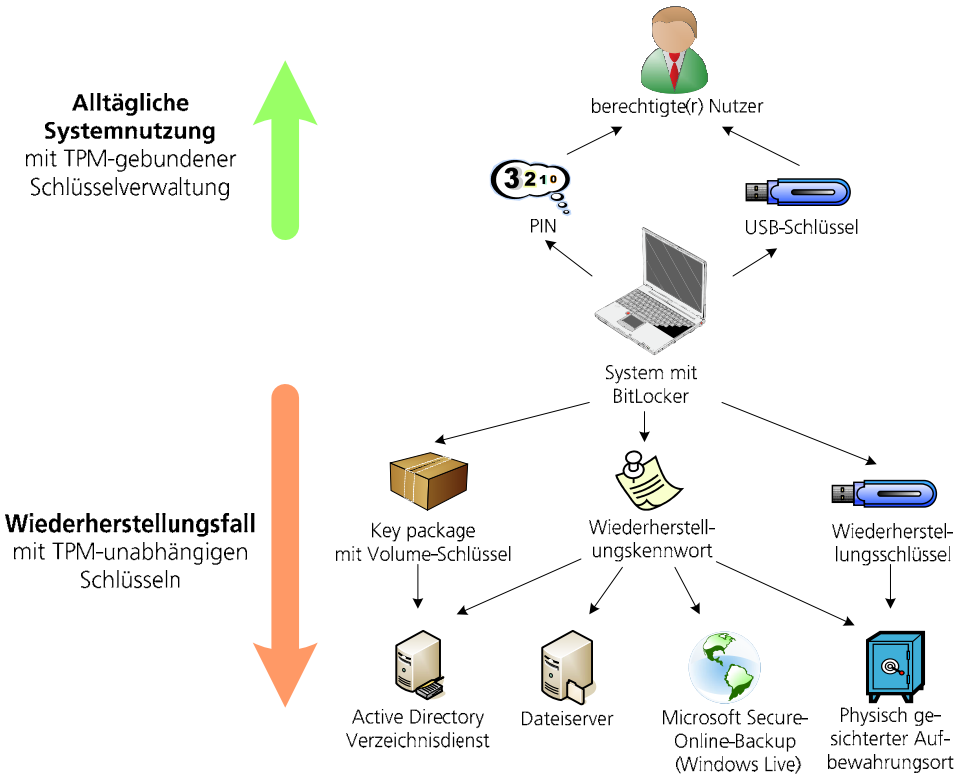
Es gibt zwei Verfahren, das Schlüsselmaterial nur Berechtigten zugänglich zu machen. Zum einen kann es der Benutzer selbst aufbewahren, etwa im Gedächtnis oder auf einem gewöhnlichen, passiven Datenträger. Datenträger bergen dabei ein recht hohes Verlustrisiko; das Gedächtnis ist mit den üblichen Schlüssellängen klar überfordert und jede Kürzung schwächt das Verfahren. Zum anderen kann man Schlüssel aber auch in einem aktiven Chip wie dem TPM einsperren und mit einer PIN oder einem Passwort schützen. Der Benutzer erhält auf diese Weise ein kurzes, leicht zu merkendes Geheimnis, ohne dass man die Schlüssel des Kryptosystems schwächen muss. BitLocker nutzt beide Möglichkeiten, das TPM und Schlüssel außerhalb des Systems, sowie Kombinationen daraus. Tabelle 1 zeigt, welche Möglichkeiten BitLocker im Einzelnen bietet.

Für den **Alltag** bietet BitLocker die **TPM-gebundene** Schlüsselverwaltung. Das gesamte Schlüsselmaterial oder ein Teil davon ist im TPM gespeichert und der Zugriff darauf an den Systemzustand gebunden. Optional kann das TPM eine Nutzerauthentisierung verlangen und weiteres Schlüsselmaterial außerhalb des Systems gespeichert sein. Zur **Wiederherstellung** des Systems in Notfällen gibt es darüber hinaus **TPM-unabhängige** Schlüssel. Sie sollen nur selten verwendet werden. In der Praxis lässt sich diese klare Einteilung nicht immer einhalten. Nutzer werden auch im Normalbetrieb zuweilen in Situationen geraten, die eine Wiederherstellung erfordern. Mehr dazu unter 4.7.

Tabelle 1:
Schlüssel und Authentisierungsmittel.

Merkmal	TPM-gebunden	Ist Schlüssel?	Aufbewahrung beim …
PIN	Ja	Nein, wird im TPM geprüft	Benutzer
USB-Schlüssel	Ja	Ja, Zwischenschlüssel mit 256 Bit Länge	Benutzer
Wiederherstellungskennwort	Nein	Ja, Zwischenschlüssel der Länge 128 Bit. Wird mit Erweiterungsalgorithmus auf 256 Bit gestreckt	Administrator
Wiederherstellungsschlüssel	Nein	Ja, Zwischenschlüssel mit 256 Bit Länge	Administrator

Abbildung 2:
Schlüsselverwaltung im Überblick.



Die beiden nachfolgenden Abschnitte beleuchten diese Mechanismen im Detail. Abbildung 2 zeigt die Anwendungsfälle und Mechanismen im Überblick. Als Faustregel gilt:

- **PIN** und **USB-Schlüssel** sind TPM-gebundene Authentisierungsmerkmale und werden an den Systemnutzer ausgehändigt
- **Wiederherstellungsschlüssel** und **Wiederherstellungskennwort** sind TPM-unabhängige Authentisierungsmerkmale und werden im systemadministrativen Bereich hinterlegt

Darüber hinaus ist BitLocker auch in der Lage, Klartextschlüssel für den einmaligen Gebrauch auf dem Datenträger zu speichern und den Schutz damit vorübergehend aufzuheben. Dies soll einzelne unbeaufsichtigte Neustarts ermöglichen, etwa zur Installation von Updates. Während dieses Zeitraums ist das Volume dann ungeschützt.

2.5.2 Betriebsarten

BitLocker unterstützt mehrere Varianten des Schlüsselmanagements, deren Sicherheitsniveau sich unterscheidet. Ein Großteil des Planungsaufwandes entfällt daher auf die Wahl der richtigen Betriebsart. Nähere Hinweise dazu gibt Abschnitt 4.3.1. In allen Betriebsarten benötigt BitLocker das passende Schlüsselmaterial, um den Volume-Schlüssel aus den Metadaten zu entschlüsseln. Dieses Schlüsselmaterial kommt aus verschiedenen Quellen:

- **Nur TPM:** Nur das TPM speichert Schlüsselmaterial und gibt es frei, wenn der vorgegebene Systemzustand erreicht ist. Eingaben des Benutzers sind nicht erforderlich. Das ist die Defaulteinstellung.
- **TPM mit PIN:** Nur das TPM speichert Schlüsselmaterial. Zusätzlich zum Systemzustand prüft das TPM eine PIN, die der Nutzer eingibt. Es gibt zu jedem Zeitpunkt nur eine PIN pro System.
- **TPM mit USB-Schlüssel:** Das Schlüsselmaterial ist auf das TPM und einen USB-Speicher verteilt. Das TPM gibt seinen Teil abhängig vom Systemzustand frei, den USB-Speicher mit dem anderen Teil soll der Nutzer getrennt vom System aufbewahren.
- Zukünftig **TPM mit PIN und USB-Schlüssel:** Wie TPM mit USB-Schlüssel, aber das TPM prüft zusätzlich eine PIN.
- **USB-Schlüssel (»Startup Key«) ohne TPM:** Das gesamte Schlüsselmaterial liegt auf einem USB-Speicher, das TPM spielt keine Rolle. Diese Variante mit grundlegend anderen Sicherheitseigenschaften wird hier nicht weiter berücksichtigt.

Die **PIN** ist ein numerisches Kennwort mit einer Länge von 4 bis 20 Ziffern. Das TPM prüft die PIN gegen einen internen Vergleichswert und gibt bei Übereinstimmung den Zugriff auf das Schlüsselmaterial frei. Das TPM verhindert Brute-

Force-Angriffe, d.h. das Ausprobieren aller möglichen Werte, sowie das Auslesen der PIN.

USB-Schlüssel sind Schlüsseldateien, die auf einem gewöhnlichen USB-Datenträger mit FAT-Dateisystem gespeichert werden. Der Schlüssel ist 256 Bit lang und entschlüsselt über Zwischenschritte den Volume-Schlüssel.

BitLocker enthält keine eigene Benutzerverwaltung. Sollen mehrere Benutzer ein BitLocker-geschütztes System starten können, so muss jeder von ihnen dieselbe PIN und/oder eine Kopie desselben USB-Schlüssels verwenden. Folgerichtig bietet BitLocker auch keine generelle Möglichkeit, die Windows-Anmeldung durch eine Authentisierung beim Systemstart (»Pre-Boot-Authentisierung«) zu ersetzen[6]. Im Gegensatz dazu erlauben die Wiederherstellungsmechanismen (vgl. 2.5.3) die Erzeugung und Hinterlegung verschiedener Schlüssel für ein System.

Der Zugriff auf BitLocker-geschützte Volumes mit TPM-gebundenen Schlüsseln ist ausschließlich mit dem Windows-Bootloader beim Systemstart möglich, da nur dann der vertrauenswürdige Systemzustand vorliegt.

2.5.3 Schlüsselhinterlegung und Wiederherstellung

Die Mechanismen der Schlüsselverwaltung hängen mit einer Ausnahme alle vom TPM ab. Der damit verbundene Sicherheitsgewinn hat eine Kehrseite: ohne den korrekten Systemzustand und ggf. die korrekte PIN führt kein Weg zu den darin gespeicherten Schlüsseln. Eine PIN aber kann in Vergessenheit geraten und der Systemzustand ändert sich unter Umständen durch die Reparatur nach einem Hardwaredefekt. Dann tritt ein sogenannter *Wiederherstellungsfall* ein.

BitLocker bietet für die Wiederherstellung zwei Mechanismen:

- Das **Wiederherstellungskennwort**, ein numerisches Kennwort aus 48 Zahlen in acht Sechsergruppen. Jede dieser Sechsergruppen ist durch 11 teilbar. Das Wiederherstellungskennwort wird auf einen 128 Bit langen Schlüssel abgebildet. Dieser Schlüssel wird mittels eines sogenannten Schlüsselerweiterungsalgorithmus auf 256 Bit vergrößert. Dazu wird er in einer großen Anzahl von Runden mit einem fixen Zufallswert (sogenannter *Salt*)

[6] BitLocker bietet jedoch eine Programmierschnittstelle, die Entwicklern die Integration ihrer eigenen Mechanismen gestattet. Einzelheiten beschreibt das Dokument *BitLocker Drive Encryption: Value Add Extensibility Options*, das Microsoft frei zum Download anbietet.

mithilfe einer SHA-256-Hashfunktion verknüpft. Der erhaltene Zwischenschlüssel entschlüsselt über mehrere Schritte den Volume-Schlüssel.
- Den **Wiederherstellungsschlüssel** auf einem USB-Stick. Er entspricht technisch dem *Startup Key* ohne TPM-Nutzung, d.h. er enthält das gesamte erforderliche Schlüsselmaterial. *Beachte: Microsoft verwirrt den Anwender hier mit wechselnden Bezeichnungen. Der Wiederherstellungsschlüssel ist in der Systemsteuerung als »Kennwort auf einem USB-Laufwerk« bezeichnet, womit je nach Konfiguration der BitLocker-Gruppenrichtlinien aber auch die zusätzliche Speicherung des Wiederherstellungskennworts in einer Textdatei gemeint sein kann.*

Im Gegensatz zu den Verfahren für den Normalbetrieb können zu einem BitLocker-geschützten Volume mehrere Wiederherstellungsmechanismen existieren. Administratoren können also mehrere Wiederherstellungsschlüssel oder -kennwörter erzeugen, falls dies erforderlich sein sollte.

Hinterlegung

Für die Hinterlegung der Wiederherstellungsschlüssel und -kennwörter sieht BitLocker mehrere Möglichkeiten vor:

- Im Verzeichnisdienst **Active Directory** dem jeweiligen System zugeordnet
- Als Datei auf einem **Dateiserver** mit einer **Netzwerkfreigabe**
- **Physisch gesichert** außerhalb der IT-Infrastruktur als ausgedrucktes Kennwort oder als USB-Schlüssel
- Als »Secure Online Backup« auf einem **Microsoft-Server im Internet** unter einem Windows-Live-Account.

In der Regel wird das Wiederherstellungs*kennwort* hinterlegt, das sich in Notfällen auch zum Beispiel telefonisch übermitteln lässt. Was dabei zu beachten ist, diskutiert Abschnitt 4.7.

Rettung beschädigter Datenträger

Der Wiederherstellungsschlüssel und das Wiederherstellungskennwort sind nur zu gebrauchen, solange die BitLocker-Metadaten auf dem Datenträger noch intakt sind (vergleiche Abschnitt 2.3).

Sind sie beschädigt, zum Beispiel wegen eines Plattenfehlers, so bleibt als letzte Möglichkeit zur Entschlüsselung ein sogenanntes *Key Package*. Das ist ein Datenobjekt, welches den Volume-Schlüssel mit einem Wiederherstellungskennwort verschlüsselt speichert. Damit lassen sich die unbeschädigten Sektoren einer Festplatte auch ohne die BitLocker-Metadaten entschlüsseln. Erforderlich ist

dafür ein besonderes *Repair Tool* (vgl. 2.7). Key Packages können nur im Active Directory abgelegt werden.

2.5.4 Bezeichnungen

Die PIN schützt einen Schlüssel im TPM vor unbefugter Benutzung. Die anderen beschriebenen Mechanismen geben dem Benutzer oder Administrator einen Teil des Schlüsselmaterials in die Hand, das BitLocker mit anderen Schlüsselteilen kombiniert und indirekt zum Entschlüsseln des Volume-Schlüssels (FVEK) einsetzt.

Microsoft bezeichnet diese Mittel in Dokumenten und Benutzerschnittstellen allesamt als **Schlüsselschutzvorrichtungen** verschiedener Art. Diese Bezeichnung ist formal korrekt, jedoch ist sie etwas sperrig und suggeriert eher Mechanik denn Software. Da alle diese Mittel letzten Endes dem Zweck dienen, BitLocker im Namen berechtigter Benutzer Zugriff auf den Volume-Schlüssel zu geben, werden in diesem Leitfaden auch die Bezeichnung **Authentisierungsmittel** oder **Authentisierungsmerkmal** verwenden. Sie betont den Aspekt der Berechtigung und des berechtigten Benutzers, soll jedoch nicht zu dem Fehlschluss verleiten, BitLocker biete an dieser Stelle ausgefeilte Konzepte der Berechtigungsverwaltung.

2.6 BitLocker und Trusted Computing

Um sich selbst vor Manipulationen zu schützen, verwendet BitLocker die Trusted-Computing-Plattform. Deren Kern ist das **Trusted Platform Module (TPM)**, auf das Software wie BitLocker über BIOS-Funktionen zugreift. Beide, TPM und BIOS-Funktionen, müssen der Spezifikation **1.2** der Trusted Computing Group (TCG) entsprechen. Genaueres zur Hardware-Auswahl steht in Abschnitt 4.2. Den Betrieb ohne TPM betrachten wir in diesem Leitfaden nur für den Wiederherstellungsfall.

Das Prinzip ist einfach. Während des Bootvorgangs erfasst das TPM – ein besonderer Microcontroller in der PC-Hardware – wichtige Aspekte der Systemkonfiguration. Dieser Vorgang heißt *Messung*, sein Ergebnis ist eine kryptografische Prüfsumme (Hash-Wert) zum Beispiel über den Programmcode des BIOS oder den Bootsektor. Veränderungen, egal ob sie zufällig oder bewusst herbeigeführt wurden, schlagen sich in veränderten Hash-Werten nieder.

Das TPM misst jedoch nicht selbst, sondern verwaltet lediglich die anfallenden Hash-Werte. Die **Platform Configuration Register (PCR)** des TPM nehmen diese Werte auf und repräsentieren so die Systemkonfiguration als eine Folge voneinander abhängender Messergebnisse. Eine Vertrauenskette ergibt sich dadurch, dass jeweils eine geprüfte Komponente das Messergebnis der nächs-

ten ermittelt, also zum Beispiel das überprüfte BIOS seinerseits eine Prüfsumme über den Master Boot Record bildet.

Die Vertrauenskette beginnt stets mit der *Core Root of Trust for Measurement (CRTM)*, einem Teil der Firmware. Das Ende der Kette bildet in diesem Fall BitLocker. Sobald BitLocker den Volume-Schlüssel der zu startenden Partition kennt, endet die TPM-gestützte Integritätssicherung. Später gestartete Komponenten, und dazu gehört ein Großteil des Betriebssystems, schützt nicht mehr das TPM, sondern lediglich die Verschlüsselung der Systempartition vor gezielten Manipulationen (vgl. auch Abschnitt 3.3).

Das TPM greift nicht aktiv in den Bootvorgang ein, das heißt ein manipuliertes System kann den Bootvorgang fortsetzen. Jedoch verwendet BitLocker die Sealing-Funktion des TPM, um Teile seines Schlüsselmaterials zu sichern. **Sealing** bedeutet, dass das TPM die ihm übergebenen Daten mit einem geheimen Schlüssel verschlüsselt. Zusätzlich fließen die PCR-Werte der Referenzkonfiguration in die Berechnung ein. Zum Entschlüsseln (»Unsealing«) ist folglich dasselbe TPM (wegen des Schlüssels) sowie derselbe Systemzustand erforderlich. Der versiegelte und damit an das TPM und die Systemkonfiguration gebundene Zwischenschlüssel ist in den Metadaten abgelegt.

Wird BitLocker mit PIN-Schutz eingesetzt, so fließt auch die PIN in diese Berechnung ein. Zuständig für die PIN-Prüfung ist also das TPM. Gemäß Spezifikation muss das TPM Brute-Force-Angriffe abwehren können. Dem Benutzer zeigt sich diese Sicherheitsfunktion als Verzögerung, die mit jeder Fehleingabe zunimmt.

Aus dem laufenden System lassen sich die PIN sowie die PCR-Referenzwerte ohne weiteres ändern. Der Integritätsschutz kann daher prinzipbedingt nur gegen Offline-Angriffe wirken, die nicht von einem gestarteten System ausgehen.

Löscht man das TPM, so gehen die dort gespeicherten Schlüssel verloren. BitLocker-geschützte Volumes lassen sich danach nur noch mit den TPM-unabhängigen Wiederherstellungsmitteln entsperren.

Weiterführende Informationen und Stellungnahmen zum Trusted Computing stellt das Bundesamt für Sicherheit in der Informationstechnik auf seiner Website bereit [11].

2.7 Werkzeuge zur Konfiguration und Administration

Neben den bereits erwähnten Werkzeugen zur Administration – Systemsteuerung und Gruppenrichtlinien – stellt Microsoft einige weitere Hilfsmittel bereit. Sie sind über die Update-Funktion von Windows Vista beziehungsweise über den Microsoft-Support erhältlich.

- Das *Drive Preparation Tool* bereitet die Festplatte auf den Einsatz von BitLocker vor. Einzelheiten beschreibt der Knowledge-Base[7]-Artikel 930063.
- Das *Repair Tool* sichert Daten aus beschädigten BitLocker-geschützten Volumes. Es ist im Knowledge-Base-Artikel 928201 beschrieben.
- Der *Recovery Password Viewer*, ein Werkzeug zur Verwaltung von Wiederherstellungsschlüsseln im Active Directory (Knowledge-Base-Artikel 928202).
- Das *TCG BIOS DOS Test Tool* (TCGBIOS.exe) überprüft eine BIOS-Funktion, die BitLocker benötigt. Es ist über das Microsoft Developer Network (MSDN) erhältlich.

Keines dieser Werkzeuge ist für den Einsatz von BitLocker zwingend erforderlich. Unsere Empfehlungen in Kapitel 4 dieses Leitfadens greifen jedoch teils auf sie zurück.

2.8 Änderungen in Service Pack 1 und Windows Server 2008

Voraussichtlich in der ersten Jahreshälfte von 2008 soll Service Pack 1 für Windows Vista (SP1) erscheinen. Mit SP1 werden sich die Fähigkeiten von BitLocker geringfügig erweitern:

- Die neue Betriebsart *TPM mit PIN und USB-Schlüssel* kommt hinzu. Damit steht eine Zwei-Faktor-Authentisierung zur Verfügung.
- BitLocker wird die Verschlüsselung von Daten-Volumes auch offiziell unterstützen. Bisher war diese Funktion auch schon vorhanden, aber nur über das Kommandozeilenwerkzeug *manage-bde* zugänglich. Nun soll sie auch im GUI der Systemsteuerung erscheinen.

Windows Server 2008 wird bei Erscheinen ebenfalls auf dem Stand von Service Pack 1 für Vista sein.

[7] http://support.microsoft.com/

Kapitel 2
BitLocker im Überblick

3 Sicherheitseigenschaften und Einsatzgebiete

Microsoft verspricht wenig: BitLocker soll es schwerer machen, vertrauliche Daten aus einem gestohlenen oder verlorenen Laptop zu lesen [1]. Was leistet BDE tatsächlich? Dieser Abschnitt betrachtet die Sicherheitseigenschaften näher. Er zeigt, welches Sicherheitsniveau und welchen Sicherheitsgewinn Anwender erzielen können.

3.1 Schutzziele

Die drei klassischen Schutzziele der IT-Sicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Schutzziele gelten jeweils für konkrete Objekte oder Werte und zwischen den einzelnen Zielen kann es Abhängigkeiten geben. BitLocker schützt gespeicherte Daten sowie Teile der Software und setzt die Schutzziele in eine klare Hierarchie.

In erster Linie soll BitLocker die **Vertraulichkeit gespeicherter Daten** gewährleisten. Von vornherein ist dabei nur ein Teil der Bedrohungen berücksichtigt. Die Verschlüsselung soll vor Angriffen schützen, die mit physischem Zugriff auf das System verbunden sind. Gegen solche Angriffe ist der Zugriffsschutz innerhalb des Betriebssystems wirkungslos.

Die Ver- und Entschlüsselung muss in einer vertrauenswürdigen IT-Umgebung erfolgen. Strenggenommen gehören dazu die gesamte Hardware, das Betriebssystem sowie alle Anwendungen. Die Umgebung darf Angreifern weder die Klartextdaten noch Schlüssel oder Authentisierungsmittel zugänglich machen. Sie darf sich insbesondere auch nicht so manipulieren lassen, dass sie dies tut. Ein wichtiges Nebenziel ist daher die **Integrität der Software**. Aus Anwendersicht kann sie auch das Hauptziel sein.

Auf das dritte klassische Schutzziel, die **Verfügbarkeit** des Systems und der gespeicherten Daten, kann sich die Verschlüsselung negativ auswirken. Sie schafft zusätzliche Fehlerquellen und Angriffsmöglichkeiten. In professionellen IT-Umgebungen wird man jedoch ohnehin gegen Datenverlust vorsorgen, zumal BitLocker ja gerade auf solche Systeme zielt, die verloren gehen können. Die Forderung nach Verfügbarkeit bedeutet daher in der Praxis vor allem, dass BitLocker die Benutzer und Administratoren des Systems nicht übermäßig belasten soll.

3.2 Bedrohungen und Angriffe

Diesen Schutzzielen steht eine Reihe von Angriffen gegenüber. An dieser Stelle geht es zunächst darum, was ein Angreifer versuchen könnte, unabhängig von den Voraussetzungen und Erfolgschancen. Der Angreifer hat jeweils das Ziel, die Vertraulichkeit oder Integrität zu verletzen. Für ein BitLocker-geschütztes System sind die wichtigsten Bedrohungen:

- **Verlust oder Diebstahl**
  Der Angreifer gelangt in den Besitz des geschützten Datenträgers oder des gesamte Systems (gezielt durch Diebstahl oder auch zufällig zum Beispiel nach einem Verkauf oder versehentlichen Verlust) und versucht anschließend, die vertraulichen Daten zu entschlüsseln. Wenigstens gegen diesen Angriff sollte BitLocker angemessen schützen.
- **Kopie**
  Der Angreifer verschafft sich eine Kopie des geschützten Volumes und versucht diese zu entschlüsseln. Im Unterschied zum Diebstahl steht dem Angreifer dabei das TPM nicht zur Verfügung, und der Angriff kann unbemerkt bleiben.
- **Ausspähen von Schlüsseln**
  Der Angreifer verschafft sich die kryptografischen Schlüssel oder die TPM-PIN und greift damit auf die vertraulichen Daten zu.
- **Manipulation**
  Der Angreifer, meist ein berechtigter Nutzer des Systems, versucht durch Manipulationen am Datenträger, Sicherheitsmechanismen des Betriebssystems zu umgehen. Dazu kann es bereits genügen, gezielt Daten auf dem Volume zu beschädigen.
- **Angriffe mit Mehrfachzugriffen**
  Der Angreifer besucht das System mehrfach. Der erste Besuch dient dazu, die spätere Fortsetzung vorzubereiten. Zu einem späteren Zeitpunkt kehrt der Angreifer zurück, um den Angriff zu vervollständigen. Zum Beispiel könnte ein erster Besuch dazu dienen, die Software so zu manipulieren, dass sie Schlüssel auf dem Datenträger ablegt. Nach einem späteren Diebstahl wäre das Volume damit leicht zu entschlüsseln.
- **Online-Angriffe**
  Online-Angriffe erfolgen nach dem Start von BitLocker im laufenden System oder durch das System hindurch. Ein Beispiel sind Angriffe mit Schadsoftware. Solche Angriffe liegen klar außerhalb des Wirkungsbereichs von BitLocker; für ihre Abwehr sind andere Mechanismen und Maßnahmen erforderlich.

Diese Liste ist keine abschließende Bedrohungsanalyse. Sie soll lediglich als Rahmen für die folgenden Betrachtungen dienen.

Angriffe können von externen Dritten, Innentätern oder auch berechtigten Benutzern mit eingeschränkten Rechten ausgeführt werden. Variieren können auch die Randbedingungen, etwa die verfügbare Zeit oder der vorgefundene Systemzustand.

3.3 Sicherheitsgewinn durch BitLocker

Gegen ein ungeschütztes Vista-System werden alle genannten Angriffe erfolgreich sein. Welchen Sicherheitsgewinn bietet demgegenüber BitLocker und von welchen Randbedingungen hängt die Sicherheit ab?

Obergrenze

Eine natürliche Schranke der erreichbaren Sicherheit ergibt sich daraus, gegen welche Bedrohungen überhaupt Mechanismen vorhanden sind, also aus den tatsächlich umgesetzten Entwurfszielen. Diese Betrachtung ergibt den maximalen Sicherheitsgewinn; mehr kann ein Anwender beim Einsatz von BitLocker nicht erreichen, je nach Konfiguration und Stärke der Mechanismen aber durchaus weniger.

Tabelle 2 gibt zu den oben betrachteten Angriffen jeweils die bedrohten Schutzziele sowie den Umfang des mit BitLocker maximal möglichen Schutzes an. Wechselseitige Abhängigkeiten sind dabei nicht berücksichtigt. Ob sich der Schutz gegen alle Bedrohungen gleichzeitig optimieren lässt, bleibt daher zunächst offen, ebenso die tatsächliche Wirksamkeit der einzelnen Mechanismen.

Tabelle 2:
Die Grenzen von BitLocker.

Angriff	Bedrohte Schutzziele	Mechanismen vorhanden?
Verlust oder Diebstahl	Vertraulichkeit der Daten, Verfügbarkeit	Ja (nur Vertraulichkeit)
Kopie	Vertraulichkeit der Daten	Ja
Ausspähen von Schlüsseln	Integrität der Software, Vertraulichkeit der Daten	Nein
Manipulation	Integrität der Software, Vertraulichkeit der Daten	Teilweise (Integrität)
Mehrfachzugriff	Integrität der Software, Vertraulichkeit der Daten	Teilweise (Integrität)
Online-Angriff	Integrität der Software, Vertraulichkeit der Daten	Nein

Konfigurationsmöglichkeiten

Im Wesentlichen bietet BitLocker an vier Stellen Konfigurationsmöglichkeiten mit Auswirkungen auf die Sicherheit:

- Wahl der AES-Schlüssellänge (128 oder 256 Bit).
  Nach derzeitigem Kenntnisstand ist sie in der Praxis belanglos. Beide Längen bieten genügend Schutz gegen Brute-Force-Angriffe, d.h. gegen systematisches Durchprobieren von Schlüsseln. Angriffe gegen AES, bei denen die Schlüssellänge eine wesentliche Rolle spielt, sind derzeit nicht bekannt.
- Verwendung des Diffusers (ja oder nein).
  Die AES-Verschlüsselung alleine schützt die Integrität der gespeicherten Daten kaum. Der Diffuser ergänzt AES und erschwert gezielte Manipulationen. Veränderungen an den verschlüsselten Daten führen mit dem Diffuser dazu, dass sich ein ganzer Sektor der Partition auf eine vom Angreifer nicht vorhersehbare Weise ändert. AES ohne Diffuser würde – mit Nebenwirkungen – die gezielte Manipulation einzelner Bits gestatten.
- Schlüsselverwaltung und Authentisierung für Benutzer (Betriebsart wie in 2.5.2 beschrieben).
  Empfehlenswert sind die Betriebsarten, die das TPM in Verbindung mit einer PIN oder einem USB-Schlüssel verwenden. Die übrigen Einsatzmöglichkeiten (nur TPM, nur USB-Schlüssel) sind mit erheblichen Abstrichen bei der Sicherheit verbunden. Das TPM ist wichtig für den Integritätsschutz der Software.
- Schlüsselhinterlegung (vgl. 2.5.3).
  Wiederherstellungsmittel funktionieren unabhängig vom TPM und sind daher ein besonders attraktives Ziel für Ausspähversuche. Wichtig für die Si-

cherheit ist vor allem, ob man sie überhaupt nutzt und wie man mit ihnen umgeht.

Für Sonderfälle existieren weitere Einstellmöglichkeiten, etwa zur Verwendung der PCR des TPM. In der Regel sollten sie jedoch in der Standardeinstellung belassen werden.

In der Praxis spricht nichts gegen den Betrieb mit AES-256 und Diffuser, so dass lediglich hinsichtlich der Schlüsselverwaltung und Wiederherstellung noch Fragen offen bleiben. Weitere Hinweise zur Auswahl gibt Abschnitt 4.3, hier soll lediglich die Sicherheitsbewertung interessieren.

Abhängigkeit von anderen Systemkomponenten

Die Sicherheit der Gesamtlösung hängt nicht allein von BitLocker ab, sondern auch von einer Reihe von Randbedingungen und anderen Systemkomponenten:

- Vom TPM und dem TCG-BIOS, die den Bootprozess überwachen.
- Von den übrigen Teilen des Betriebssystems, die erst nach BitLocker starten und den Schutz zur Laufzeit übernehmen.
- Von der sicheren Handhabung aller Schlüssel und PINs.

Fehler an diesen Stellen können den Schutz durch BitLocker schwächen oder auch gänzlich unwirksam machen. Die Handhabung von Schlüsseln und PINs obliegt dem Anwender. In den übrigen Fällen ist sein Einfluss beschränkt. Zu vermeiden sind Eingriffe, die vorhandene Mechanismen schwächen, z.B. Änderungen an der Integritätsprüfung des TPM. Ferner ist der Einsatz von BitLocker nur sinnvoll, wenn er in ein umfassendes Sicherheitskonzept eingebettet wird.

Schutz der Vertraulichkeit

Sofern dem Angreifer vorher keine Schlüssel oder PIN bekannt sind, schützt BitLocker in allen TPM-gestützten Betriebsarten gegen:

- Das Auslesen des Volumes in einem anderen Rechner. Davor schützt die Abhängigkeit vom TPM.
- Zugriffe auf das Volume mit einer nicht auf dem System installierten Betriebssysteminstanz (z.B. Boot-CD). Auch davor schützt das TPM; bootfähige Medien wie eine CD oder ein USB-Stick ändern die Systemkonfiguration, ebenso Veränderungen am BIOS oder anderen Bootkomponenten

Algorithmus, Schlüssellängen und die Schlüsselverwendung innerhalb von BitLocker sind nach gegenwärtigem Stand der Technik hinreichend sicher. Ohne

Kenntnis der Schlüssel ist es nicht möglich, die Daten aus einem *ausgeschalteten* System oder einer Kopie des Datenträgers zu entschlüsseln.

Im Gegensatz dazu ist BitLocker bei *laufendem* Vista im *eingeschalteten* System als Sicherheitsmechanismus praktisch bedeutungslos. In dieser Situation müssen andere Sicherheitsmechanismen des Systems die Vertraulichkeit gewährleisten, wie sich bereits aus dem in Tabelle 2 skizzierten Konzept ergibt. Ohnehin wird der Einsatz einer Volume-Verschlüsselung nur dann sinnvoll sein, wenn begleitend auch an anderen Stellen wenigstens die üblichen Maßnahmen des Grundschutzes umgesetzt sind.

Eine wichtige Trennlinie verläuft zwischen den Betriebsarten mit PIN oder USB-Schlüssel einerseits und der Verwendung allein mit dem TPM andererseits. Ohne Authentisierungsmittel oder Schlüssel in Nutzerhand kann ein Angreifer das System jederzeit hochfahren, also vom ausgeschalteten in den laufenden Zustand bringen. Falls ein Angreifer also ohne Mitwirkung legitimer Benutzer eine Schwachstelle im Betriebssystem oder in automatisch startenden Diensten und Anwendungen ausnutzen kann, bietet der Nur-TPM-Modus deutlich weniger Schutz als die anderen TPM-gestützten Betriebsarten. Über die Wahrscheinlichkeit solcher Schwachstellen lässt sich keine allgemeingültige Aussage treffen, da sie stark von der Softwareausstattung und Konfiguration des jeweiligen Systems abhängt.

Eine ausgespähte PIN oder ein ausgespähter USB-Schlüssel genügt nicht zum Entschlüsseln, wenn dem Angreifer nur eine Kopie der Daten vorliegt oder er zum Zugriff seine eigene Betriebssysteminstanz starten möchte bzw. muss. Im Gegensatz dazu erlauben die Wiederherstellungsmittel (vgl. 2.5.3) in diesen Situationen die Entschlüsselung. Dasselbe gilt für den *Startup Key* beim – technisch äquivalenten – Betrieb von BitLocker ohne TPM.

Integritätsschutz

BitLocker nutzt zwei unterschiedliche Mechanismen zur Integritätssicherung, die einander ergänzen sollen: die Sealing-Funktion des TPM sowie den Diffuser bei der Volume-Verschlüsselung.

Das TPM-Sealing prüft die Integrität aller Komponenten, die den Bootprozess bis zum Start von BitLocker beeinflussen. Es schützt einen Teil des Schlüsselmaterials vor der Kompromittierung, falls eine dieser Komponenten verändert wurde. Veränderte Hardware, zusätzliche bootfähige Medien, Veränderungen am BIOS oder an BitLocker selbst und andere Veränderungen führen dazu, dass das TPM seinen Teil des Schlüsselmaterials nicht freigibt.

Nachdem BitLocker die benötigten Schlüssel erhalten hat, spielt das TPM keine Rolle mehr. Alle später gestarteten Softwarekomponenten vom Vista-Kern bis zu den Anwendungen schützt nur noch die Volume-Verschlüsselung durch BitLocker. Ein Integritätsschutz im strengen Sinne, etwa mit kryptografischen Prüfsummen, fehlt hier. Veränderungen an den verschlüsselt gespeicherten Daten bleiben daher grundsätzlich unentdeckt, solange sie nicht im Betriebssystem oder einer Anwendung auffallen.

Der Integritätsschutz für gespeicherte Daten und Software beschränkt sich also auf Nebenwirkungen der Verschlüsselung, die wenigstens *gezielte* Manipulationen genügend erschweren soll. AES-CBC allein genügt dafür nicht. Der Cipher-Block-Chaining-Modus hat hier bekannte Schwächen. Um den Preis unkontrollierter Veränderungen an einem anderen 16-Byte-Block lassen sich gezielt einzelne Bitpositionen beeinflussen, ohne dass der Angreifer den AES-Schlüssel kennt. Darüber hinaus verwendet BitLocker in diesem Fall mit einen einzigen AES-Schlüssel für alle Sektoren, was zum Beispiel Manipulationen durch Vertauschung sowie Replay-Angriffe ermöglicht.

Der Diffuser führt zum einen zusätzlich einen Sektorschlüssel ein. Zum anderen sorgt er dafür, dass gezielte Manipulationen einzelner Bits unmöglich werden. Veränderungen an einzelnen Bits der verschlüsselten Daten führen mit Diffuser dazu, dass sich der gesamte betroffene Sektor unkontrolliert ändert, alle anderen Sektoren hingegen überhaupt nicht. Möglich und unerkannt bleiben jedoch Angriffe, bei denen ein ganzer Sektor zerstört oder ausgetauscht wird.

Die Kombination aus TPM und Diffuser schützt teilweise gegen Manipulation sowie gegen Angriffe mit mehrfachem Zugriff. Viele naheliegende Angriffsmöglichkeiten sind erfasst, andere bleiben aber offen. Neben den bereits diskutierten Online-Angriffen zur Laufzeit, die ja zunächst auch die Integrität verletzen, bleiben beispielweise auch Hardware-Keylogger zum Ausspähen von PINs unentdeckt.

Wiederherstellungsmittel umgehen den Integritätsschutz des TPM. Wer in ihrem Besitz ist, kann sowohl die Vertraulichkeit verletzen als auch die Integrität. Sie sind daher besonders gut zu schützen.

Verfügbarkeit der verschlüsselten Daten

Die Verfügbarkeit der geschützten Daten wird durch die Verschlüsselung zunächst negativ beeinflusst. Insbesondere TPM-gebundene Authentisierungsmittel werden unbenutzbar, wenn die vertrauenswürdige Plattform nicht mehr besteht, auch wenn das nur vorübergehend der Fall ist. In solchen Situationen ist dann zunächst kein Zugriff auf den Klartext mehr möglich. Ähnliche Probleme treten beim Schlüsselverlust auf (Vergessen der PIN oder Verlust des USB-Schlüssels).

BitLocker stellt für diese Fälle Wiederherstellungsschlüssel und -kennwörter zur Verfügung, die TPM-unabhängig sind. Diese können den Zugang zum BitLocker-geschützten Volume wiederherstellen. Für den Ad-hoc-Einsatz sind sie jedoch nicht zu gebrauchen, da sie dem berechtigten Nutzer aus Sicherheitsgründen nur bei unmittelbarem Bedarf (Wiederherstellung) ausgehändigt werden sollten. Empfehlungen dazu gibt Abschnitt 4.7.

Zusammenfassung

BitLocker eignet sich als Grundschutzmaßnahme zur Sicherung vertraulicher Daten in Arbeitsplatzrechnern und mobilen Systemen:

- Einem Angriff auf die Vertraulichkeit von Daten in einem *ausgeschalteten* System setzt BitLocker geeignete Sicherheitsmechanismen entgegen. Bei sorgfältigem Umgang mit dem PC ist das ein wirksamer Schutz der Vertraulichkeit bei Diebstahl oder Verlust.
- BitLocker erschwert die Manipulation der Bootkomponenten und der Daten und Programme im geschützten Volume. Jedoch kann BitLocker Veränderungen der gespeicherten Daten nicht erkennen und weniger gezielte Manipulationen (z.B. Beschädigung von Sektoren) bleiben möglich.
- Keinen Schutz bietet BitLocker gegen Angriffe auf das eingeschaltete System mit entsperrten Volumes (Online-Angriffe). Solche Angriffe liegen außerhalb des Wirkungsbereichs.
- Risiken durch Schlüsselverluste können nur durch organisatorische Maßnahmen kompensiert werden. BitLocker bietet Mechanismen, die diese Maßnahmen unterstützen (Wiederherstellungsschlüssel und -kennwort und deren Ablagemöglichkeiten).

Tabelle 3 fasst zusammen, gegen welche Angriffe aus 3.2 BitLocker geeignete Gegenmaßnahmen bereitstellt.

Tabelle 3: Tatsächliches Sicherheitsniveau von BitLocker.

Angriff	Wirksamer Schutz?	Einschränkungen, Bemerkungen
Verlust oder Diebstahl	Ja	Bei laufendem System abhängig von der Sicherheit von Vista und Anwendungen
Kopie	Ja	
Ausspähen von Schlüsseln	Nein	Ausspähen oder Missbrauch in einigen Fällen erschwert durch TPM
Manipulation	Teilweise	Weniger gezielte Angriffe bleiben möglich und unerkannt
Mehrfachzugriff	Teilweise	TPM erkennt nicht alle Manipulationen, z.B. Hardware-Keylogger
Online-Angriff	Nein	

3.4 Einsatzgebiete

Aus den Sicherheitseigenschaften, den vorhandenen Funktionen sowie aus praktischen Erwägungen ergibt sich, für welche Einsatzzwecke sich BitLocker eignet und für welche nicht.

Geeignet ist BitLocker für den Einsatz auf Laptops und Arbeitplatzrechnern mit *einem* Betriebssystem und *einem* fest zugeordneten Nutzer. Hier liegt auch das Haupteinsatzgebiet der Software. BitLocker verbessert hier den Schutz gegen eine Reihe von Angriffen und ist gleichzeitig praxistauglich. Allerdings muss der PC die Voraussetzungen für Windows Vista und BitLocker mitbringen (Hardwareleistung, Speicherkapazität, geeignetes TPM und TCG-BIOS).

Weniger empfehlenswert ist der Einsatz auf Serversystemen. Dann bleibt zu klären wie die eventuell notwendige Authentisierung ohne direkten Zugang zum System durchzuführen ist und welche Anforderungen bezüglich der Verfügbarkeit zu stellen sind. Da der physische Zugang zu Servern in der Regel beschränkt ist, wäre der Nutzen von BitLocker hier allerdings sowieso gering.

Ungeeignet ist BitLocker für die Verschlüsselung mobiler Datenträger (USB-Speichermedien, mobile Festplatten etc.). Ferner eignet sich BitLocker nicht für virtuelle Maschinen; für den Einsatz auf dem Hostsystem gilt das oben zu Servern Gesagte. Aufgrund seiner Hardware-Anforderungen kann BitLocker

außerdem keine einheitliche Lösung bieten, wenn die IT-Infrastruktur auf älterer und aktueller Hardware aufbaut oder verschiedene Windows-Betriebssysteme (Vista, XP, 2000) nebeneinander existieren. Bei Systemen mit zwei Betriebssystemen (sogenannter Dual-Boot) ist vom Einsatz BitLocker abzuraten.

4 BitLocker im Einsatz

Dieses Kapitel gibt Empfehlungen zum praktischen Einsatz von BitLocker in Unternehmen und Behörden. In Anlehnung an das Lebenszyklus-Modell des BSI-Standard 100-1 ([13], Seite 13 ff.) werden die Phasen Planung, Beschaffung, Installation (Umsetzung), Betrieb, Notfallvorsorge und Außerbetriebnahme betrachtet.

Wir gehen von einer Situation aus, wie sie typischerweise anzutreffen ist: Laptops, PCs und Software werden zentral beschafft. Die Software-Installation und -Konfiguration, und die Benutzerverwaltung erfolgen ebenfalls zentral. Alle Rechner befinden sich in einer Windows-Domäne.

Die gegebenen Empfehlungen können ohne weiteres auch auf lokal administrierte Systeme übertragen werden.

4.1 Planung

BitLocker wirkt sich auf den kompletten Lebenszyklus eines damit geschützten Systems aus, von der Beschaffung über die Konfiguration, Wartung und Benutzung bis zur Außerbetriebnahme. Die in diesem Kapitel gegebenen Empfehlungen und Erläuterungen sollen dazu dienen, die Einführung von BitLocker zu planen und die eigenen Prozesse anzupassen. Für alle Phasen muss ermittelt werden, wie die Verwendung von BitLocker mit den bestehenden Prozessen in Einklang gebracht werden kann.

Ein weiterer wichtiger Aspekt ist das richtige Handeln in Notfällen, in denen die Vertraulichkeit oder Verfügbarkeit der BitLocker-geschützten Daten gefährdet ist, sowie die Vorbereitung auf solche Situationen.

Berücksichtigung bei der Hardware-Beschaffung

BitLocker wird zurzeit nicht auf allen Systemen vollständig und problemlos unterstützt. Da es hierfür keine eindeutigen Kriterien oder Kennzeichen gibt, muss die Eignung eines bestimmten Gerätetyps für den Einsatz von BitLocker individuell getestet werden. Beschaffungsprozesse müssen eventuell so angepasst werden, dass die BitLocker-Eignung an einer Teststellung geprüft und möglichst einheitliche Hardware angeschafft wird.

Da sich bei manchen Herstellern selbst Geräte mit identischer Modellbezeichnung unterscheiden können, sollte man sich die Eignung für BitLocker vertraglich zusichern lassen.

Anpassung des Roll-out Prozesses

Die Aktivierung von BitLocker erfordert eine Reihe von Konfigurationsschritten, die teilweise global in der Windows-Domäne vorgenommen werden können, oder zu bestimmten Zeitpunkten während der Einrichtung der Einzelsysteme erfolgen müssen. In den Abschnitten 4.3 bis 4.5 geben wir Empfehlungen, wie die Aktivierung von BitLocker in den Roll-out Prozess für neue Systeme integriert werden kann.

Auswirkungen bei Wartung und Betrieb

BitLocker ist zwar so konzipiert, dass die Arbeit mit einem BitLocker-geschützten System möglichst wenig beeinflusst wird, dennoch gibt es Einschränkungen. In den von uns für Arbeitsplatzrechner und Laptops empfohlenen Betriebsarten ist beim Systemstart ein externes Authentisierungsmerkmal notwendig. Automatische Neustarts wie sie beispielsweise für zentralisierte Software-Updates benötigt werden, sind bei so geschützten Systemen nicht möglich. Auch eine Offline-Datensicherung ist nicht möglich. Bei Änderungen der Hard- und Software muss BitLocker unter Umständen neu aktiviert werden, um Schlüssel mit dem neuen Plattformzustand zu verknüpfen.

Helpdesk für Probleme im Zusammenhang mit BitLocker

Es muss damit gerechnet werden, dass Benutzer die BitLocker-PIN vergessen oder den USB-Schlüssel verlieren, oder dass die Freigabe und Entschlüsselung mit diesen Authentisierungsmerkmalen auf Grund von Änderungen an Hardware oder Boot-Komponenten nicht möglich ist. Benutzer können in diesem Fall weder ihr System benutzen noch auf die Daten zugreifen, die auf dem BitLocker-geschützten Volume abgelegt sind. Die Fortsetzung der Arbeit ist nur nach Eingabe des Wiederherstellungsschlüssels oder des Wiederherstellungskennworts möglich.

Um Arbeitsunterbrechungen und Schäden durch die Nichtverfügbarkeit von Systemen und Daten zu vermindern, sollte ein Helpdesk eingerichtet werden, der bei Bedarf Wiederherstellungskennwörter übermittelt und den Benutzer bei der Problembehebung behilflich ist. Falls Laptop-Benutzer häufig in anderen Zeitzonen unterwegs sind, kann es sinnvoll sein, den Helpdesk rund um die Uhr zu besetzen.

Wichtig ist auch die stets aktuelle Datensicherung, da BitLocker die Datenrettung auf anderen Wegen verhindert oder erheblich erschwert.

Mögliche Konflikte mit Sicherheitsrichtlinien

BitLocker lässt sich nur in sehr begrenztem Maße an die Erfordernisse lokaler Sicherheitsrichtlinien anpassen. Hierdurch können sich Konflikte ergeben, die vorab ermittelt und geklärt werden müssen.

Ein möglicher Konfliktpunkt ist insbesondere die Ausgestaltung von Authentisierungsmerkmalen. Bei der PIN-basierten Authentisierung sind ausschließlich aus Ziffern gebildete PINs möglich. BitLocker sieht keine Möglichkeit vor, PINs in regelmäßigen Abständen zu erneuern, oder dies zu erzwingen. Zudem ist es nicht möglich, individuelle Authentisierungsmerkmale für mehrere Benutzer desselben Systems anzulegen.

Die Verwendung von USB-Speichermedien zur Speicherung von Schlüsseln setzt voraus, dass USB-Anschlüsse zugänglich und nutzbar sind. Die Nutzung von USB-Anschlüssen wird aus Sicherheitsgründen häufig verboten und durch technische Maßnahmen unterbunden.

Weiterhin besitzt BitLocker keine Logging-Funktion zur Auditierung von Anmeldeversuchen.

4.2 Beschaffung

Checkliste Beschaffung
Nur Windows Vista Ultimate oder Enterprise bzw. Windows 2008 Server beschaffen.
Für Windows Vista geeignete Hardware auswählen (Vista Logo).
TPM und System-BIOS nach TCG-Spezifikation 1.2 in den Herstellerangaben überprüfen.
Weitere manuelle Tests zur Feststellung der Kompatibilität durchführen.

Da BitLocker ein Bestandteil von Windows Vista ist, gelten dessen Mindestanforderungen an die Leistungsfähigkeit der Hardware. Der Einsatz von BitLocker kommt daher vor allem auf neu zu beschaffender Hardware in Frage.

BitLocker ist nicht Bestandteil von Windows Vista Business, das häufig bei neuen Rechnern mitgeliefert wird. Windows Vista Ultimate oder Enterprise oder ein Upgrade auf eine dieser Versionen muss dann extra beschafft werden. Windows Server 2008 wird in allen Versionen BitLocker enthalten.

BitLocker stellt zusätzlich zur Lauffähigkeit von Windows Vista Anforderungen an die Hardware. Insbesondere Trusted Plattform Module (TPM) und das BIOS des Rechners muss eine Reihe von Anforderungen erfüllen. Beide müssen mindestens der TCG-Spezifikation 1.2 entsprechen. Dies allein ist jedoch noch kein hinreichendes Kriterium zur Kompatibilität mit BitLocker.

Die Eignung eines konkreten Gerätetyps kann gegenwärtig nur durch folgende manuelle Tests ermittelt werden:

1 Beim Hersteller erfragen, ob Probleme beim Einsatz von BitLocker bekannt sind. Eignung für BitLocker vertraglich zusichern lassen.
2 Keine Geräte mit nachrüstbarem TPM-Modul verwenden (nur noch vereinzelt im Handel).
3 Update des System-BIOS auf die aktuellste verfügbare Version.
4 Fehlerfreier Durchlauf des Testprogramms TCGBIOS.exe bestätigt Vorhandensein der notwendigen BIOS-Funktionen. Falls hierbei Fehler auftreten, so erübrigen sich weitere Tests, da das Gerät nicht geeignet ist.
5 Installation von Windows Vista Ultimate oder Enterprise.
6 Aktivieren von BitLocker im Modus TPM+PIN wie in den folgenden Abschnitten beschrieben.
7 Bei folgenden Tests darf BitLocker nicht die Fehlermeldung *»Die Informationen zum Starten des Betriebssystems wurden seit dem Aktivieren von BitLocker geändert.«* anzeigen:
a) Systemstart nach Einschalten
b) Systemstart nach Neustart
c) Aufwecken aus dem Ruhezustand.
8 Neustart des Systems und Eingabe von 20 absichtlich falsch gewählten BitLocker PINs. Nach spätetestens 20 Fehleingaben sollte die Meldung erscheinen, dass das TPM gegen weitere Eingaben gesperrt ist. Falls dies nicht der Fall ist, so eignet sich das Gerät nicht für den Modus TPM+PIN.
9 Um die Sperre aufzuheben muss das TPM in der Regel vollständig zurückgesetzt werden.

BitLocker kann auf inkompatiblen Systemen zwar auch ohne Verwendung des TPM eingesetzt werden, bietet dann aber ein wesentlich geringeres Sicherheitsniveau. Bei der Neubeschaffung von Systemen empfehlen wir daher, solche Systeme auszuschließen.

Geräte mit IEEE1394-Anschluss (auch als Firewire und iLink bezeichnet) sollten vermieden werden. Bei laufendem System sind über diese Schnittstelle Angriffe denkbar.

Damit PINs und Wiederherstellungskennwörter nicht leicht abgehört werden können, dürfen keine drahtlosen Tastaturen verwendet werden.

4.3 Installationsvorbereitung

Um die Erstinstallation mehrerer Laptops oder Arbeitsplatzrechner zu rationalisieren wird üblicherweise eine Musterinstallation aufgesetzt, die anschließend mit Hilfe von Imaging-Software auf die einzelnen Geräte repliziert wird. Da die Einrichtung von BitLocker relativ viele manuelle Schritte erfordert, empfehlen wir diese Vorgehensweise und erläutern im Folgenden, wie dabei vorzugehen ist.

Wir gehen davon aus, dass es im Netzwerk einen Windows Domänen-Controller gibt. Einige Einstellungen von BitLocker können durch Gruppenrichtlinien auf Ebene der Domäne festgelegt werden, was weitere Konfigurationsarbeiten an jedem Einzelsystem erspart.

Gruppenrichtlinien, für die wir im Folgenden keine andere Empfehlung geben, sollten in der Standardeinstellung belassen werden. Das gilt insbesondere für die Gruppenrichtlinien *»Überschreiben des Arbeitsspeichers beim Neustart verhindern«* und *»TPM-Plattformvalidierungsprofil konfigurieren«*. Die Änderung dieser Gruppenrichtlinien verschlechtert die Sicherheit ohne relevante Vorteile zu bringen.

In der Gruppenrichtlinie *»Verschlüsselungsmethode konfigurieren«* kann die Schlüssellänge von 128 auf 256 erhöht und der Diffuser abgeschaltet werden. Der Diffuser sollte auf keinen Fall deaktiviert werden, da ohne Diffuser gezielte Manipulationen an verschlüsselten Sektoren erheblich erleichtert werden. Eine AES-Schlüssellänge von 128 Bit ist in der Regel ausreichend, so dass auch diese Gruppenrichtlinie in der Standardeinstellung belassen werden kann.

Für größere Netze empfehlen wir die Verwendung eines Active Directory Servers zur automatischen zentralen Hinterlegung von Wiederherstellungsschlüsseln.

4.3.1 Auswahl des Authentisierungsverfahrens

Checkliste Auswahl des Authentisierungsverfahrens
TPM+PIN oder TPM+USB-Schlüssel verwenden. TPM+USB-Schlüssel besser für Arbeitsplatzrechner geeignet. TPM+PIN für Laptops und Systeme ohne USB-Anschluss geeignet.
Gruppenrichtlinie in Domäne für gewähltes Authentisierungsverfahren konfigurieren.

Wir empfehlen, BitLocker ausschließlich in einer TPM-gebundenen Betriebsart mit Nutzerauthentisierung beim Systemstart zu verwenden, also entweder im Modus TPM+PIN oder TPM+USB-Schlüssel.

Hinsichtlich ihrer Sicherheit sind beide Betriebsarten praktisch gleichwertig. Aus folgenden Erwägungen schlagen wir jedoch vor, bei Laptops die Betriebsart TPM+PIN zu bevorzugen, bei Arbeitsplatzrechnern dagegen TPM+USB:

- USB-Schlüssel dürfen auf keinen Fall zusammen mit dem BitLocker-geschützten System aufbewahrt werden. Bei mobilen Geräten ist eine Verletzung dieses Grundsatzes auf Grund des üblichen Benutzerverhaltens wahrscheinlicher. Am Arbeitsplatz können USB-Schlüssel gegebenenfalls auch eingeschlossen werden.
- Bei Arbeitsplatzrechnern besteht die Gefahr, dass PINs durch einen unbemerkt installierten Hardware-Keylogger protokolliert werden.

Falls USB-Anschlüsse aus Sicherheitsgründen generell deaktiviert oder blockiert werden sollen, so kommt nur die Verwendung der PIN in Frage.

In der Standardeinstellung verwendet BitLocker keines der beiden Verfahren, sondern nutzt alleine das TPM zur Sicherung des Schlüssels. Diese Betriebsart hat mehrere Schwächen und wird nicht empfohlen.

Damit BitLocker bei der Aktivierung eine der beiden Betriebsarten mit Authentisierung verwendet, muss eine Gruppenrichtlinie angepasst werden. Wir empfehlen, die Einstellung in der Domäne vorzunehmen. Falls verschiedene Betriebsarten für unterschiedliche Rechnertypen verwendet werden sollen, können hierfür separate Organisationseinheiten (OU) in der Domäne angelegt werden. (Falls BitLocker auf einem System installiert wird, das nicht Teil einer Domäne ist, können die gleichen Einstellungen natürlich auch lokal vorgenommen werden.)

Gruppenrichtlinien können mit dem Programm *gpedit.msc* angepasst werden. Die Einstellungen zur Wahl der BitLocker-Betriebsart befinden sich im Pfad *»Computerkonfiguration – Administrative Vorlagen – Windows Komponenten – BitLocker-Laufwerkverschlüsselung – Systemsteuerungssetup: Erweiterte Startoptionen aktivieren«* (siehe Abbildung 3).

Um den Betriebsmodus TPM+PIN vorzugeben, muss diese Gruppenrichtlinie wie in Abbildung 4 gezeigt eingestellt werden: »BitLocker ohne kompatibles TPM zulassen« deaktiviert, *»Startschlüssel bei TPM nicht zulassen« und »Start-PIN bei TPM erforderlich«*.

Für die Betriebsart TPM+USB-Schlüssel sind die umgekehrten Einstellungen zu wählen, also »*Startschlüssel bei TPM erforderlich*« und »*Start-PIN bei TPM nicht zulassen*«.

Abbildung 3: Gruppenrichtlinien für BitLocker.

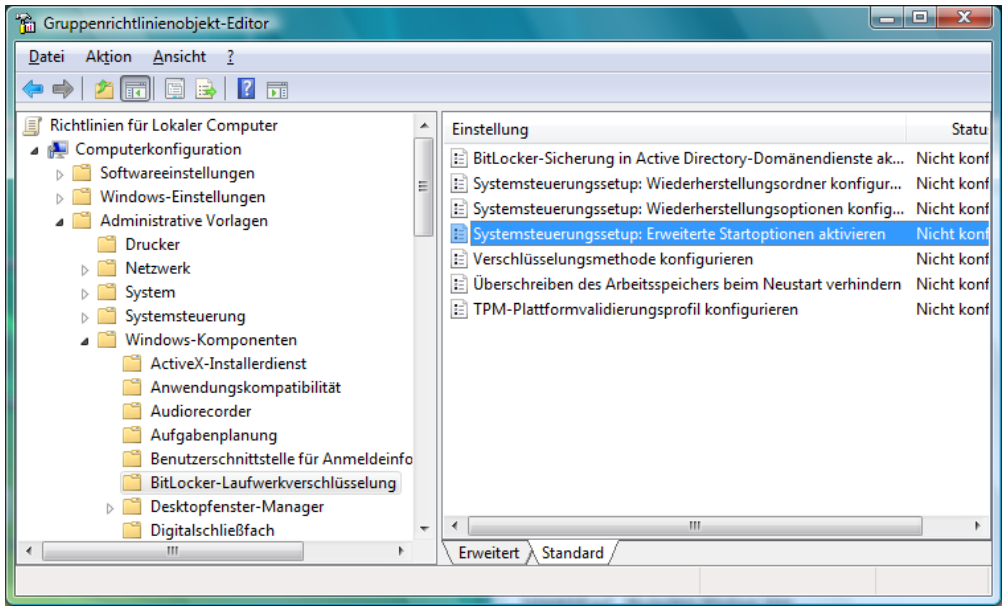
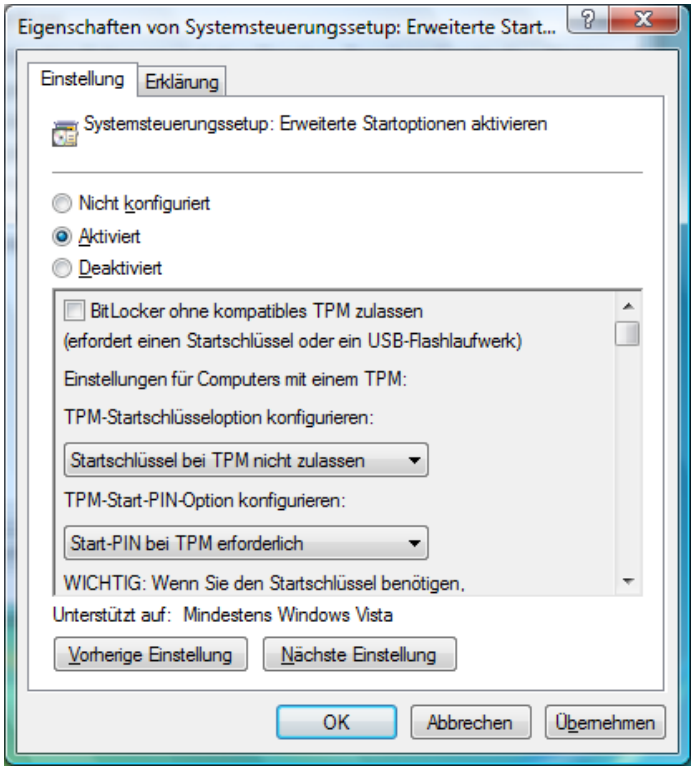


Abbildung 4: Einstellungen für die Betriebsart TPM+PIN.



4.3.2 Vorbereitung zur Schlüsselhinterlegung

Checkliste Vorbereitung der Schlüsselhinterlegung
Variante: Active Directory Server - Verzeichnisstruktur des AD-Servers anpassen. - AD-Server und Datensicherung davon durch Rechtevergabe und physikalische Maßnamen vor unbefugtem Zugriff schützen. - Gruppenrichtlinie zur Schlüsselhinterlegung in AD konfigurieren.
Variante: Ausdruck von Wiederherstellungskennwörtern - geeignet aufgestellten Drucker in Domäne einrichten. - Ordnungssystem für Ausdrucke schaffen. - Ausdrucke sicher verschließen.
Option: USB-Speichermedium zu Wartungszwecken - Nur ein oder wenige Schlüssel pro USB-Speichermedium. Schlüssel sinnvoll gruppieren, z.B. nach Abteilung oder Stockwerk. - USB-Speichermedien immer unter Verschluss halten.

Windows startet nicht, falls beim Systemstart die Plattformüberprüfung fehlschlägt oder das primäre Authentisierungsmerkmal (PIN oder USB-Schlüssel) fehlt. In dieser Situation ist ein Systemstart und Zugriff auf die BitLocker-geschützten Daten nur mit Hilfe eines Wiederherstellungsschlüssels oder -kennworts möglich. Auf die Erstellung dieser Notfallschlüssel sollte nur dann verzichtet werden, wenn die Verfügbarkeit des BitLocker-geschützten Systems und der darauf gespeicherten Daten keine Rolle spielt.

In Bezug auf ihre Sicherheit sind Wiederherstellungsschlüssel und -kennwörter vergleichbar. Für die Auswahl des Verfahrens spielen vor allem praktische Erwägungen eine Rolle.

Wiederherstellungskennwörter bestehen aus 48 Ziffern und können deshalb im Notfall telefonisch übermittelt werden, etwa wenn ein Nutzer mit einem Laptop unterwegs ist. Wiederherstellungskennwörter empfehlen wir daher vor allem für Laptops. Falls USB-Ports aus Sicherheitsgründen deaktiviert oder blockiert sind, müssen ebenfalls Wiederherstellungskennwörter verwendet werden.

Wiederherstellungsschlüssel werden auf einem USB-Speichermedium gespeichert. Um den Wiederherstellungsschlüssel zum Systemstart zu verwenden, muss das USB-Speichermedium angeschlossen werden. Der Vorteil gegenüber Wiederherstellungskennwörtern ist hierbei, dass die manuelle Eingabe entfällt. Zudem können die Wiederherstellungsschlüssel mehrerer Systeme auf demselben USB-Speichermedium abgelegt werden. Wiederherstellungsschlüssel eignen sich daher besonders als Zweitschlüssel für Wartungsaufgaben durch einen Systemadministrator. Um das Schadenspotential durch Verlust eines solchen USB-Speichermediums gering zu halten, muss die Maximalzahl der darauf gespeicherten Schlüssel begrenzt werden. Bei Verlust müssen alle betroffenen Systeme umgehend mit einem neuen Schlüssel versehen werden können (Die Vorgehensweise ist in Abschnitt 4.7 beschrieben.)

Sowohl Wiederherstellungskennwörter als auch Wiederherstellungsschlüssel müssen so aufbewahrt und verwendet werden, dass Unbefugte keinen Zugang erlangen können. Wiederherstellungsschlüssel sind immer an ein USB-Speichermedium gebunden. Dieses muss physisch gesichert werden, etwa durch Einschließen in einen Tresor. Wiederherstellungskennwörter können ausgedruckt werden oder auf einem USB-Speichermedium, in einem Ordner auf einem Netzlaufwerk, oder in einem Active Directory Dienst (AD) abgespeichert werden. Welcher Aufbewahrungsort am besten geeignet ist, hängt vorwiegend von der Anzahl der verwalteten Systeme ab.

Für große Netze empfehlen wir die zentrale Speicherung in einem gut gesicherten Active Directory Dienst. Bei der BitLocker-Aktivierung werden Wiederherstellungskennwörter dadurch automatisch hinterlegt, wodurch Sicherheitsrisiken durch Bedienungsfehler vermieden werden können. Falls kein AD-Server

vorhanden ist, kann ein nur für Administratoren schreib- und lesbarer Ordner auf einem Netzlaufwerk als zentraler Speicherort verwendet werden. Wir empfehlen jedoch stattdessen die Einrichtung eines AD-Servers. Die Ablage auf einem USB-Speichermedium bringt keine Vorteile. Für kleine Netze empfehlen wir stattdessen den Ausdruck der Wiederherstellungskennwörter auf Papier, das in einem Tresor eingeschlossen wird.

Vorgehensweise bei Nutzung von BitLocker mit Active Directory

In einem zentralen AD-Server können Wiederherstellungskennwörter und optional Schlüsselpakete abgelegt werden. Schlüsselpakete sind nur zusammen mit einem AD-Server verwendbar und unterscheiden sich von allen anderen Schlüsselarten. Ein Schlüsselpaket enthält keinen Zwischenschlüssel, sondern den FVEK selbst, mit dem das BitLocker-geschützte Volume direkt entschlüsselt werden kann. Der FVEK ist lediglich durch Verschlüsselung mit dem ebenfalls im AD hinterlegten Wiederherstellungskennwort vor direktem Zugriff geschützt. Der Vorteil von Schlüsselpaketen ist, dass ein BitLocker-geschütztes Volume auch dann noch entschlüsselt werden kann, wenn alle drei Kopien von dessen Metadaten zerstört sind. Dieser unwahrscheinliche Fall kann beispielsweise durch Hardwaredefekte an der Festplatte auftreten. Zur Entschlüsselung mittels Schlüsselpaket ist ein spezielles Werkzeug notwendig, das bei Microsoft angefordert werden muss (vgl. 2.7).

Bevor Wiederherstellungskennwörter und Schlüsselpakete in einem AD-Server hinterlegt werden können, müssen dessen Struktur und Zugriffsrichtlinien angepasst werden. Wie hierbei vorzugehen ist, ist in [12] beschrieben.

Damit die Schlüsselhinterlegung im AD bei der Aktivierung von BitLocker automatisch erfolgt, muss die Gruppenrichtlinie *»BitLocker-Sicherung in Active Directory-Domänendienste aktivieren«* aktiviert werden. Wir empfehlen die in Abbildung 5 gezeigte Standardeinstellung: *»BitLocker-Sicherung in AD DS erforderlich«* und *»Wiederherstellungskennwörter und Schlüsselpaket«*.

Die auf dem AD-Server gespeicherten Daten dürfen nur für berechtigte Domänen-Administratoren zugänglich sein. Wir empfehlen ein physisch gut gesichertes System, das neben dem AD-Dienst keine weiteren Aufgaben erfüllt. Für die Datensicherung gelten die gleichen Anforderungen.

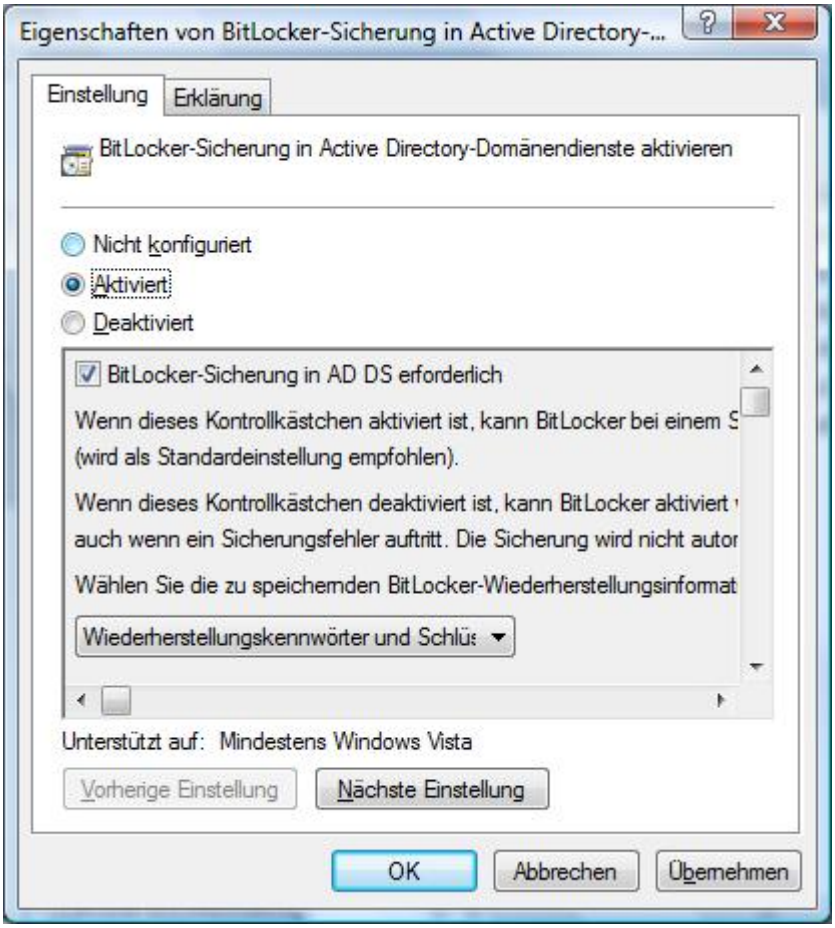


Abbildung 5: Einstellungen für die Schlüsselhinterlegung im Active Directory.

Vorgehensweise bei Nutzung von BitLocker ohne Active Directory

Generell muss beim Aktivieren von BitLocker mindestens ein Wiederherstellungsschlüssel oder -kennwort erstellt werden. In der Standardeinstellung stehen bei der Aktivierung alle Varianten und Kombinationen daraus zur Auswahl.

Falls Wiederherstellungskennwörter ausgedruckt werden sollen, so muss in der Domäne ein geeigneter Drucker vorkonfiguriert werden. Der Drucker sollte in unmittelbarer Nähe des Arbeitsplatzes augestellt sein, an dem die BitLocker-Aktivierung erfolgt. Der zu einem bestimmten System gehörende Ausdruck muss bei Bedarf schnell auffindbar sein. Die Ausdrucke sollten daher in geeigneter Form sortiert werden. Die Ausdrucke dürfen unter keinen Umständen für Unbefugte zugänglich sein. Sie sollten daher in einem Tresor eingeschlossen und nur bei Bedarf kurzzeitig entnommen werden.

Als zusätzliche Maßnahme sollten Ausdrucke von Wiederherstellungskennwörtern in versiegelten Umschlägen verschlossen werden, damit ein unbefugter Zugriff sofort erkannt wird.

4.3.3 Konfiguration des Mustersystems zur Image-Erstellung

Checkliste Image-Erstellung
Installation von Vista Ultimate oder Enterprise.
Gesamte Festplatte für die Systempartition verwenden (Kein zweites Betriebssystem, Datenpartition erst ab SP1 verschlüsselbar.)
System ans Internet anschließen, Windows Update aufrufen und Ultimate-Extras »*BitLocker- und EFS-Verbesserungen*« nachinstallieren.
BitLocker-Laufwerksvorbereitungstool ausführen und den Anweisungen folgen.

Der Zweck eines Imaging-Verfahrens zur Einrichtung von Systemen für Benutzer ist es, Zeit zu sparen, Systeme einheitlich zu konfigurieren und Konfigurationsfehler zu vermeiden. Dieses Ziel wird umso besser erreicht, je mehr Konfigurationsschritte bereits in das Image des Mustersystems einfließen können.

Bei der Einrichtung von BitLocker gibt es mehrere Schritte, die gut geeignet sind bei der Konfiguration des Mustersystems ausgeführt zu werden. Andere Schritte dürfen jedoch auf keinen Fall am Mustersystem erfolgen, sondern müssen immer am individuellen System durchgeführt werden.

Wir empfehlen, folgende Schritte vor der Image-Erstellung auf dem Mustersystem durchzuführen:

Installation von Vista Ultimate oder Enterprise und Partitionierung der Festplatte

Obwohl BitLocker eine spezielle Partitionierung der Festplatte benötigt, ist das Installationsprogramm von Vista nicht in der Lage, diese Partitionierung vorzunehmen. Die Festplatte wird daher wie bei einer normalen Windows Installation eingerichtet. BitLocker eignet sich in der Praxis nicht für Multi-Boot Systeme, bei denen beispielsweise ein Linux-System parallel installiert ist. Es ist somit nicht sinnvoll, bei der Partitionierung hierfür Platz vorzusehen. Eine von der Systempartition getrennte Datenpartition empfehlen wir nur, wenn diese ebenfalls mit BitLocker verschlüsselt wird. Diese Funktion wird jedoch erst ab Service Pack 1 (SP1) offiziell unterstützt werden. Wir gehen daher im Folgenden davon aus,

dass bei der Installation die gesamte Festplattenkapazität für die Systempartition verwendet wird.

Updates und Ultimate-Extras installieren

BitLocker benötigt zusätzlich zur Systempartition eine weitere unverschlüsselte Partition von mindestens 1,5 GB, auf die zum Systemstart notwendige Software-Komponenten kopiert werden. Das BitLocker-Laufwerksvorbereitungstool erledigt alle Schritte zur Einrichtung dieser Partition vollautomatisch. Die Systempartition wird dazu falls notwendig um 1,5 GB verkleinert.

Das BitLocker-Laufwerksvorbereitungstool muss über das Internet nachinstalliert werden, da es nicht auf der Installations-DVD enthalten ist. Zur Installation sind folgende Schritte durchzuführen:

1 Herstellung einer Internetverbindung
2 Aufruf von *Windows Update* über das Startmenü oder die Systemsteuerung
3 Liste der verfügbaren Updates gegebenenfalls aktualisieren
4 Liste der verfügbaren »*Ultimate-Extras*« anzeigen und »*BitLocker- und EFS-Verbesserungen*« zur Installation auswählen.
Gegebenenfalls weitere verfügbare Updates zur Installation selektieren.
5 Updates installieren

Aufruf des BitLocker-Laufwerksvorbereitungstools

Das Programm BitLocker-Laufwerksvorbereitungstool befindet sich im Ordner »*Zubehör – Systemprogramme – BitLocker*« des Startmenüs. Das Programm erfordert außer der Bestätigung der Lizenzvereinbarung und des Einrichtungsprozesses keine Interaktion. Nach seiner erfolgreichen Ausführung befindet sich die für BitLocker notwendige Partition auf der Festplatte.

Falls die Replikation mehrerer Partitionen von der verwendeten Imaging-Software nicht unterstützt wird, so kann dieser Schritt unterbleiben. Das BitLocker-Laufwerksvorbereitungstool muss dann jeweils nach dem Einspielen des Partitions-Images auf den Einzelsystemen aufgerufen werden.

Weitere Konfiguration und Software-Installation

Alle im Zusammenhang mit BitLocker stehenden Schritte, die vor der Erstellung eines Festplatten-Images durchgeführt werden können oder dürfen, sind hiermit abgeschlossen. Vor der Erstellung des Images kann nun noch weitere individuelle Software installiert oder die Systemkonfiguration angepasst werden.

Das System kann zur Aufnahme in die Windows-Domäne vorbereitet werden. Sollen Wiederherstellungskennwörter bei der Aktivierung von BitLocker ausgedruckt werden, so sollte ein Drucker oder Druckserver vorkonfiguriert werden.

Erstellung des Festplatten-Images

Sowohl die Systempartition als auch die vom BitLocker-Laufwerksvorbereitungstool angelegte Partition haben das NTFS-Format und sind zu diesem Zeitpunkt unverschlüsselt. Zur Erstellung des Images kann jedes Programm verwendet werden, das mit NTFS-Partitionen umgehen und ein Image mehrerer Partitionen inklusive Partitionstabelle und Bootsektor erstellen kann.

4.4 Installation am Einzelsystem

4.4.1 Vorbereitung

Checkliste Vorbereitung des Einzelsystems
Festplatten-Image einspielen, System starten.
TPM aktivieren, TPM-PIN braucht nicht aufbewahrt zu werden.
Gegebenenfalls BIOS-Einstellungen vornehmen.

Festplatten-Image einspielen

Der erste Schritt zur Einrichtung eines neuen Systems ist das Wiederherstellen des vom Mustersystem erstellten Festplatten-Image. Nach der Wiederherstellung müssen sich die BitLocker-Startpartition (normalerweise S:) sowie die Systempartition C: auf der Festplatte befinden. Nach dem Systemstart muss das Betriebssystem Windows Vista starten.

TPM aktivieren

Das Trusted Platform Module (TPM) muss aktiviert und initialisiert sein, damit es von BitLocker verwendet werden kann. In der Regel werden Rechner mit deaktiviertem TPM ausgeliefert.

Zur Aktivierung des TPM gibt es geräteabhängig zwei alternative Möglichkeiten:

1 Bei allen Systemen kann das TPM im BIOS-Setup aktiviert werden.

2 Bei vielen neueren Systemen kann die Aktivierung des TPM durch das Betriebssystem veranlasst werden. Die eigentliche Aktivierung muss dann beim nächsten Systemstart bestätigt werden.

Wir empfehlen, in der Systemsteuerung die Seite »*Sicherheit – BitLocker-Laufwerksverschlüsselung*« aufzurufen. Dort befindet sich unten links ein Verweis auf das Programm zur TPM-Verwaltung. Alternativ kann versucht werden, BitLocker zu aktivieren. Falls das TPM noch nicht aktiviert und initialisiert ist, erscheint eine Meldung und Verweis auf das Programm zur Einrichtung des TPM. Das Programm leitet durch alle notwendigen Schritte.

Bei der Aktivierung und Initialisierung muss ein Benutzerkennwort (TPM-Owner-PIN) erzeugt werden. Wir empfehlen, das Kennwort vom System generieren zu lassen. Das Kennwort wird später weder im normalen Betrieb noch in Notfallsituationen benötigt. Eine Aufbewahrung des Kennworts ist daher nicht notwendig.

BIOS-Einstellungen vornehmen

Bei manchen Geräten kann BitLocker in der Betriebsart TPM+USB-Schlüssel nicht verwendet werden, wenn im BIOS-Setup das Booten von USB-Speichermedien aktiviert ist. Diese Option muss dann im BIOS-Setup deaktiviert werden. Da nicht auszuschließen ist, dass auch andere BIOS-Einstellungen Einfluss auf die Plattformvalidierung durch BitLocker haben, sollten möglichst alle BIOS-Einstellungen vor dem Aktivieren von BitLocker durchgeführt werden.

Um zu vermeiden, dass Benutzer durch Änderung von BIOS-Einstellungen oder durch Löschen des TPM die Funktion von BitLocker stören, kann das BIOS-Setup durch ein Passwort geschützt werden.

Zusätzliche Maßnahmen

Zum Schutz vor spezialisierten Hardware-basierten Angriffen kann bei besonders hohem Sicherheitsbedarf im Windows Gerätemanager der PCMCIA-Controller deaktiviert (siehe Abbildung 6) und der Firewire-Treiber deinstalliert werden. Alternativ können die entsprechenden Schnittstellen durch ausgießen mit Epoxid-Harz oder ähnliche Maßnahmen mechanisch unbrauchbar gemacht werden.

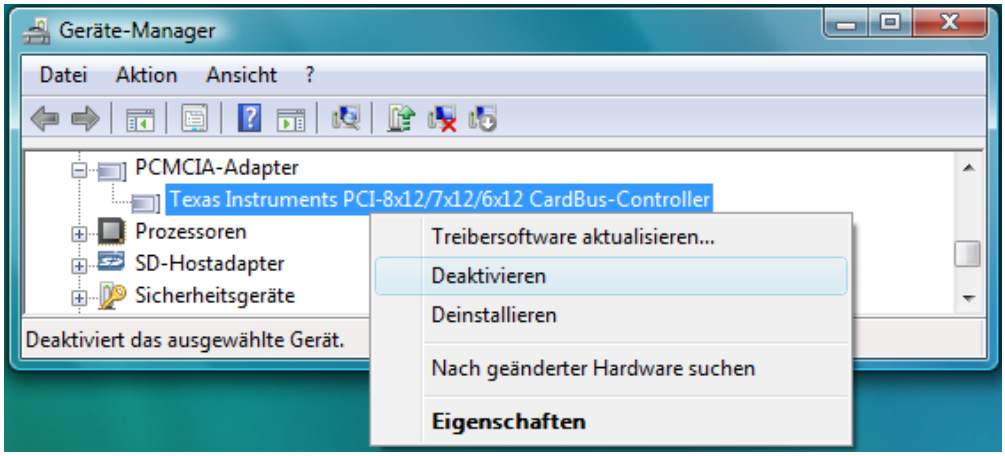


Abbildung 6: Deaktivieren des PCMCIA-Controllers im Gerätemanager

4.4.2 BitLocker aktivieren

Checkliste BitLocker aktivieren
BitLocker in Systemsteuerung für Systempartition C: aktivieren.
Authentisierungsmerkmal PIN oder USB-Schlüssel erstellen.
Wiederherstellungsschlüssel oder -kennwort erstellen und sicher aufbewahren.
Gegebenenfalls Datenpartitionen verschlüsseln.

Sobald alle Schritte zur Einrichtung des TPM abgeschlossen sind, kann BitLocker auf der Seite »*Sicherheit – BitLocker-Laufwerksverschlüsselung*« in der Systemsteuerung aktiviert werden.

Authentisierungsmerkmal erstellen

Wurde in den Gruppenrichtlinien die Betriebsart TPM+PIN festgelegt, so muss nun eine PIN gewählt und durch zweifache Eingabe bestätigt werden. Die PIN wird bei der Eingabe nicht angezeigt und kann nicht ausgedruckt werden. Anders als bei Anmelde-Passwörtern ist es nicht möglich, ein Initialpasswort vorzugeben, das vom Benutzer nach der ersten Anmeldung zu ändern ist. Da die PIN ausschließlich aus Ziffern besteht, ist es für Menschen schwierig, eine schwer erratbare PIN zu wählen. Wir empfehlen, stattdessen einen PIN-Generator zu verwenden. Der PIN-Generator muss eine gute Zufallsquelle verwenden und darf generierte PINs nicht speichern. Damit die PIN ausreichend sicher, aber dennoch merkbar ist, empfehlen wir eine Länge von sechs Ziffern.

Die PIN muss dem Benutzer in geeigneter Weise übergeben werden und sollte nicht aufbewahrt werden. Um dem Benutzer das Merken der PIN zu erleichtern, können deren Ziffern wie bei Telefonnummern in Paaren gruppiert werden (z.B. 32 71 63)

Wurde in den Gruppenrichtlinien die Betriebsart TPM+USB-Schlüssel gewählt, so muss ein leeres, mit einem VFAT-Dateisystem formatiertes USB-Speichermedium angeschlossen werden. Um die Wahrscheinlichkeit zu verringern, dass Benutzer das USB-Speichermedium zu anderen Zwecken verwenden, sollte ein USB-Speichermedium mit möglichst geringer Kapazität verwendet werden. Vorteilhaft ist es, wenn das USB-Speichermedium so gestaltet ist, dass es leicht am Schlüsselbund befestigt werden kann. Auf diese Weise kann erreicht werden, dass das USB-Speichermedium getrennt vom BitLocker-geschützten Gerät aufbewahrt wird.

Wiederherstellungsschlüssel oder -kennwort erzeugen

Falls in den Gruppenrichtlinien die Hinterlegung in einem AD-Server festgelegt wurde, so läuft dieser Prozess automatisch ab. Falls die Hinterlegung im AD fehlschlägt, etwa weil keine Netzwerkverbindung besteht, so erscheint eine Fehlermeldung. Das Problem muss behoben werden, bevor die Aktivierung von BitLocker abgeschlossen werden kann.

Falls kein AD-Server zur Schlüsselhinterlegung verwendet wird, müssen Wiederherstellungsschlüssel und Ausdrucke von Wiederherstellungskennwörtern manuell erstellt werden. Beides erfolgt über das selbe Dialogfenster. Um ein Wiederherstellungskennwort auszudrucken ist die Schaltfläche *»Kennwort drucken«* auszuwählen. Die Erstellung eines Wiederherstellungsschlüssels erfolgt über die irreführend benannte Schaltfläche *»Kennwort auf einem USB-Laufwerk speichern«*. Dabei wird sowohl ein Wiederherstellungsschlüssel als auch ein Wiederherstellungskennwort auf dem ausgewählten USB-Speichermedium abgelegt.

Verschlüsselung von Datenpartitionen

Ab Windows Vista SP1 bietet die Systemsteuerung im BitLocker-Fenster die Option, Datenpartitionen zu verschlüsseln. Alle vorhandenen Datenpartitionen werden dort unterhalb der Systempartition aufgelistet und können wie die Systempartition durch Anklicken verschlüsselt werden. Datenpartitionen können beim Systemstart automatisch entsperrt werden. Der Schlüssel der Datenpartition wird dabei auf der BitLocker-geschützten Systempartition abgelegt und ist somit vor Offline-Angriffen geschützt.

4.5 Auslieferung

Checkliste Auslieferung
Benutzer mit BitLocker vertraut machen, Sicheren Umgang mit System und Authentisierungsmerkmalen erläutern.
Merkblatt übergeben.
Authentisierungsmerkmal PIN oder USB-Schlüssel übergeben.
System übergeben (Abschluss der Verschlüsselung braucht nicht abgewartet zu werden.)

Bei der Übergabe eines BitLocker-geschützten Systems an seinen Nutzer sollten folgende Punkte erläutert werden:

1 Der Grund für den Einsatz von BitLocker
2 Die Verwendung des Authentisierungsmerkmals PIN oder USB-Schlüssel beim Systemstart
3 Der sichere Umgang mit dem Authentisierungsmerkmal
4 Verhalten bei Kompromittierung des Authentisierungsmerkmals
5 Mögliche Fehler und deren Ursachen (Insbesondere Fehleingabe der PIN und im Laufwerk befindliche CD-ROM)
6 Verbot von Modifikationen an der Hardware, dem BIOS und der Betriebssysteminstallation
7 Hinweis auf die Notwendigkeit einer aktuellen Datensicherung

Anhang A enthält jeweils ein Mustermerkblatt für PC- und Laptop-Benutzer, das diese Informationen kompakt zusammenfasst. Die Merkblätter sind als Vorlage für ein an die eigene Situation angepasstes Merkblatt gedacht.

Übergabe des Authentisierungsmerkmals

Die PIN sollte auf keinen Fall auf dem Merkblatt notiert werden, sondern auf einem separaten Blatt, das sofort nach dem Merken der PIN sicher zu vernichten ist.

Abschluss der Verschlüsselung

Die vollständige Verschlüsselung aller Sektoren von System- und Datenpartitionen kann je nach Größe und Geschwindigkeit der Festplatte mehr als eine Stunde dauern. Die Verschlüsselung läuft jedoch im Hintergrund ab und wird nach einem Neustart automatisch fortgesetzt. Es spricht daher nichts dagegen,

ein System an den Benutzer zu übergeben, bevor die Verschlüsselung abgeschlossen ist.

4.6 Betrieb

Checkliste Betrieb
Prozesse anpassen, die automatischen Neustart erfordern.
BitLocker bei Wartungsarbeiten berücksichtigen.
Online- statt Offline-Datensicherung verwenden, Sicherungskopien vor fremdem Zugriff schützen.
Vor dauerhaftem Benutzerwechsel neu verschlüsseln.

4.6.1 Kein automatischer Neustart des Systems

In größeren Netzwerken werden häufig Wartungsaufgaben auf den Einzelplatzsystemen zentral gesteuert und angestoßen. Dazu gehören die Installation von Software-Updates, die tägliche Datensicherung und die Inventarisierung von Hard- und Software.

Die empfohlenen BitLocker-Betriebsarten verlangen beim Systemstart die PIN-Eingabe oder den Anschluss des USB-Schlüssels. So geschützte Systeme können daher nicht ohne Benutzerinteraktion neu gestartet werden. Automatische Prozesse, die einen unbeaufsichtigten Neustart erfordern, können nicht vollständig durchgeführt werden.

Darüber hinaus empfehlen wir, BitLocker geschützte Systeme bei längerer Abwesenheit herunterzufahren oder in den Ruhezustand (suspend-to-**disk**) zu versetzen. Diese Empfehlung gilt insbesondere außerhalb der Arbeitszeit.

Zentralisierte Prozesse zur Wartung von Einzelplatzsystemen müssen daher gegebenenfalls angepasst werden:

- Anstoßen der Prozesse vom Einzelplatzsystem aus, wenn dieses eingeschaltet ist.
- Vermeidung von Neustarts

4.6.2 Änderungen an Hard- und Software

Checkliste Änderungen an Hard- und Software
Variante: Reaktivierung von BitLocker bei Bedarf nach Wartungsarbeiten:
- Sicherstellen, dass gültiges Widerherstellungskennwort oder Wiederherstellungsschlüssel vorhanden ist. - Wartungsarbeiten durchführen. - Falls Plattformvalidierung beeinflusst wurde, BitLocker vorübergehend deaktivieren, gleich im Anschluss wieder aktivieren. - Funktion der Plattformvalidierung prüfen.
Variante: Deaktivierung von BitLocker vor Wartungsarbeiten:
- BitLocker vorübergehend deaktivieren. - Wartungsarbeiten durchführen. - BitLocker aktivieren. - Funktion der Plattformvalidierung prüfen.

Die Installation von Software innerhalb des Betriebssystems (Anwendungsprogramme, Treiber für Peripheriegeräte) hat keinen Einfluss auf die BitLocker-Verschlüsselung. Das gleiche gilt für den Anschluss der meisten Peripheriegeräte. Grundsätzlich nicht betroffen sind BitLocker-verschlüsselte Datenpartitionen.

Bei folgenden Änderungen am System muss BitLocker berücksichtigt werden, da sie immer Einfluss auf die Plattformvalidierung während des Systemstarts haben:

- Update des System-BIOS
- Löschen des TPM
- Austausch der Hauptplatine bzw. Einbau der Festplatte in ein anderes System
- Update des Windows Vista-Betriebssystems das den Kernel oder Boot-Komponenten betrifft.

Folgende Änderungen können einen Einfluss auf die Plattformvalidierung haben:

- Einbau oder Anschluss von Hardware, von der ein Systemstart möglich ist. Dazu gehören interne und externe Speichermedien und Netzwerkkarten. Durch Abschalten des Systemstarts von diesen Geräten im System-BIOS können Probleme in der Regel vermieden werden

- Installation eines weiteren Betriebssystems (wird jedoch ohnehin nicht empfohlen)
- Änderungen am Bootsektor der Festplatte, an deren Partitionierung und am Windows-Bootmanager

Es gibt zwei Vorgehensweisen, um solche Wartungsarbeiten an einem BitLocker-geschützten System vorzunehmen:

1 **Reaktivierung bei Bedarf nach Wartungsarbeiten:** Wiederherstellung und Reaktivierung von BitLocker im Anschluss an die Wartungsarbeiten, falls diese sich auf die Plattformvalidierung ausgewirkt hat.
2 **Deaktivierung vor den Wartungsarbeiten:** Deaktivierung von BitLocker durch Anlegen eines Klartextschlüssels vor der Durchführung von Wartungsarbeiten, die mit hoher Wahrscheinlichkeit die Plattformvalidierung beeinflussen. Erneute Aktivierung nach Abschluss der Wartungsarbeiten.

Reaktivierung bei Bedarf nach Wartungsarbeiten

Diese Vorgehensweise wird in folgenden Fällen empfohlen:

- Wenn die Wartungsarbeiten von nicht vertrauenswürdigen Dritten durchgeführt werden und diese dafür keinen Zugriff auf das Betriebssystem benötigen. Dies ist in der Regel beim Austausch von defekten Hardware-Komponenten der Fall.
- Wenn Unbefugte während der Wartungsarbeiten Zugang zum System erlangen könnten.
- Wenn nicht davon auszugehen ist, dass eine Änderung die Plattformvalidierung beeinflusst bzw. wenn eine Änderung unerwartet die Plattformvalidierung beeinflusst hat.

Vor Änderungen, die nicht leicht rückgängig gemacht werden können, muss unbedingt sichergestellt werden, dass ein gültiger Wiederherstellungsschlüssel oder ein Wiederherstellungskennwort vorhanden ist.

Nach Durchführung der Wartungsarbeiten wird das System neu gestartet. Falls die Wartungsarbeiten Einfluss auf die Plattformvalidierung hatte, so erscheint beim Systemstart eine entsprechende Meldung. BitLocker fordert danach zum Anschluss des Wiederherstellungsschlüssels oder zur Eingabe des Wiederherstellungskennworts auf.

BitLocker muss in diesem Fall deaktiviert und neu aktiviert werden, um wieder wie vor den Wartungsarbeiten zu arbeiten. Dies geschieht auf der BitLocker-Seite der Systemsteuerung durch Auswahl von »*BitLocker deaktivieren*«. Im anschließenden Dialog ist der Punkt »*BitLocker-Laufwerksverschlüsselung deaktivieren*« auszuwählen. Die Deaktivierung ist in wenigen Sekunden abgeschlos-

sen. Gleich im Anschluss muss BitLocker wieder aktiviert werden. Dies geschieht in gleicher Weise auf der BitLocker-Seite der Systemsteuerung. (Diese muss unter Umständen nach der Deaktivierung durch Drücken von F5 aktualisiert werden.) Dadurch wird das BitLocker-Schlüsselmaterial im TPM mit dem neuen Plattformzustand verknüpft. Die korrekte Funktionsweise von BitLocker sollte im Anschluss durch einen Neustart des Systems überprüft werden.

Deaktivierung vor den Wartungsarbeiten

Diese Vorgehensweise wird nur dann empfohlen, wenn die folgenden Voraussetzungen erfüllt sind:

- Das System bleibt während des gesamten Zeitraums der Deaktivierung von BitLocker unter der Kontrolle einer vertrauenswürdigen Person. (Die Deaktivierung sollte so kurz wie möglich sein und das System sich in einem für Unbefugte unzugänglichen Raum befinden.)
- Die durchzuführenden Änderungen wirken sich zwingend auf die Plattformvalidierung aus.

BitLocker wird vor der Änderung für die Systempartition deaktiviert. Dies geschieht auf der BitLocker-Seite der Systemsteuerung durch Auswahl von *»BitLocker deaktivieren«*. Im anschließenden Dialog ist der Punkt *»BitLocker-Laufwerksverschlüsselung deaktivieren«* auszuwählen. Dadurch wird in den Metadaten des Volumes ein Klartextschlüssel angelegt mit dem die Plattformvalidierung sowie die Authentisierung außer Kraft gesetzt werden. In diesem Zustand kann das System auch dann noch ohne Wiederherstellungskennwort gestartet werden, wenn die Informationen zur Plattformvalidierung verändert wurden.

Sofort nach Abschluss der Wartungsarbeiten muss BitLocker wieder aktiviert werden. Dies geschieht ebenfalls auf der BitLocker-Seite der Systemsteuerung. Dadurch wird das BitLocker-Schlüsselmaterial im TPM mit dem neuen Plattformzustand verknüpft. Die korrekte Funktionsweise von BitLocker sollte im Anschluss durch einen Neustart des Systems überprüft werden.

4.6.3 Datensicherung

Bei der Datensicherung eines BitLocker-geschützten Volumes sind zwei zusätzliche Aspekte zu berücksichtigen:

1. Offline-Verfahren zur Erstellung der Datensicherung, die beispielsweise von einer selbstbootenden CD-ROM aus gestartet werden, funktionieren in der Regel nicht.
2. Online-Backups aus dem laufenden System sind unverschlüsselt, sofern das Backup-Programm keine eigene Verschlüsselung vornimmt.

Moderne Programme zur Offline-Datensicherung speichern aus Effizienzgründen nur diejenigen Teile eines Volumes, die tatsächlich Daten enthalten, bzw. die seit der letzten Sicherung verändert wurden. Dazu muss das Programm zur Datensicherung das Dateisystem des Volumes analysieren, was bei einem BitLocker-verschlüsselten Volume nicht möglich ist. Einfachere Programme, die ein 1:1-Abbild einer Partition oder Festplatte erstellen, sind auf Grund des anfallenden Datenvolumens für regelmäßige Datensicherungen unpraktikabel. Wird ein solches Verfahren verwendet, so ist es essentiell, dass ein Wiederherstellungs schlüssel oder -kennwort ebenfalls gesichert wird.

Online-Datensicherungen aus dem laufenden System sind nicht mit diesen Problemen behaftet, da der Client zur Datensicherung Zugriff auf die unverschlüsselten Daten hat. Dies impliziert jedoch, dass die Datensicherung ebenfalls unverschlüsselt ist. Hier sind zusätzliche Maßnahmen nötig, um sicherzustellen, dass die Vertraulichkeit der Datensicherung mindestens ebenso gut gewährleistet ist, wie die der Daten im BitLocker-verschlüsselten Volume. Das kann durch geeignete Verschlüsselung geschehen (was das Risiko der Nichtverfügbarkeit erhöht), oder durch physische Absicherung des Servers zur Datensicherung der Datensicherungsmedien.

Alle Versionen von Windows Vista, die BitLocker unterstützen, enthalten ein Programm zur Online-Datensicherung von einzelnen Dateien und ganzen Volumes. Die Datensicherung ist auch hier unverschlüsselt, worauf in einer Warnmeldung hingewiesen wird.

4.6.4 Wechsel des Benutzers

Beim Dauerhaften Wechsel des Benutzers eines Systems empfehlen wir aus Sicherheitsgründen die vollständige Neuverschlüsselung des BitLocker-geschützten Volumes, oder besser die Neuinstallation des kompletten Betriebssystems. Zur Neuverschlüsselung muss BitLocker deaktiviert und anschließend wieder aktiviert werden.

4.7 Notfälle

Checkliste Notfälle
Kompromittierte PINs, Kennwörter und Schlüssel sofort durch neue ersetzen.
Bei Diebstahl der Festplatte oder des Systems externe PINs, Kennwörter und Schlüssel vor fremdem Zugriff schützen.
Manipulierte Systeme nicht starten. Verschlüsseltes Volume als Datenvolume an vertrauenswürdigem System entschlüsseln.
Bei Festplattendefekten Abbild der verschlüsselten Partition erstellen. Keine Reparaturversuche mit nicht BitLocker-geeigneten Werkzeugen.

Beim Einsatz von BitLocker kann es zu verschiedenen Notfallsituationen kommen, in denen die Vertraulichkeit oder Verfügbarkeit der BitLocker-geschützten Daten gefährdet ist.

Die Vertraulichkeit ist dann gefährdet, wenn Unbefugte kurzzeitig Zugang zum verschlüsselten Volume und zu einem der dazugehörigen Authentisierungsmerkmale oder Schlüssel erhalten können.

Es kann aus verschiedenen Gründen dazu kommen, dass sich ein BitLocker-geschütztes System nicht mehr mit dem normalen Authentisierungsmerkmal starten lässt. Ursache können sowohl Benutzerfehler, Manipulation durch Dritte als auch Hardwaredefekte sein. Es hängt primär von der Fehlerursache ab, welche Maßnahme zu ergreifen ist. Tabelle 4 auf Seite 58 gibt einen Überblick über mögliche Ursachen und der Symptome.

Allgemeine Sicherheitsmaßnahmen bei der Anwendung von Wiederherstellungsschlüsseln und -kennwörtern

Soll einem Benutzer telefonisch ein Wiederherstellungskennwort übermittelt werden, so muss zuvor die Identität des Benutzers auf geeignete Weise überprüft werden.

Während der Verwendung des Wiederherstellungsschlüssels oder der Eingabe des Wiederherstellungskennworts sollte das System vom Netzwerk getrennt werden. Dadurch verringert sich das Risiko, dass Kennwort oder Schlüssel durch eine vorgetäuschte Eingabemaske ausgespäht und dem Angreifer direkt übermittelt werden.

Wenn der Verdacht besteht, dass ein System in böser Absicht manipuliert wurde, sollte die betroffene Systempartition nicht mehr gestartet, sondern nur noch als Datenpartition in einem vertrauenswürdigen System entsperrt werden.

Tabelle 4: Symptome und Ursachen möglicher Fehlfunktionen bei BitLocker-geschützten Systemen.

Meldung	Mögliche Ursache	Behebung
»Die Informationen zum Starten des Betriebssystems wurden seit dem Aktivieren von BitLocker geändert«	Geplante Änderung an der Hardware, z.B. BIOS-Aktualisierung	Mit Wiederherstellungsschlüssel oder -kennwort starten
	Geplante Änderung am Bootbereich (MBR) oder Bootmanager	BitLocker deaktivieren und erneut aktivieren
	Bootfähige CD-ROM oder USB-Speichermedium vorhanden	Medium entfernen und Neustart
	Veränderung am TPM, z. B. Löschung, Tausch oder Defekt des Mainboards	Mit Wiederherstellungsschlüssel oder -kennwort starten
		TPM neu initialisieren, BitLocker deaktivieren und erneut aktivieren
	Inkompatibles BIOS	BIOS-Aktualisierung
	Veränderung von Hardware oder Bootkomponenten durch Dritte	Plattform als nicht mehr vertrauenswürdig behandeln
»Es wurde zu oft eine falsche PIN eingegeben«	Korrekte PIN wurde vergessen oder verwechselt	Warten bis TPM wieder PIN annimmt oder Systemstart mit Wiederherstellungsschlüssel oder -kennwort
	Mutwillige Aktivierung der Sperre durch Fehleingaben	Wenn Sperre nicht rücksetzbar, TPM und BitLocker neu initialisieren
»Unerwarteter Fehler aufgetreten« beim Starten von Vista	Lesefehler bei einer der Bootkomponenten	Maßnahmen zur Datenrettung
	Manipulation an Bootkomponente vor Aktivierung von BitLocker	System als nicht mehr vertrauenswürdig behandeln
Lesefehler nach Start von Vista	Hardware-Defekt an Festplatte	Maßnahmen zur Datenrettung
	Änderung an verschlüsselten Datenbereichen	Gezielte Manipulation in Betracht ziehen

4.7.1 Benutzerfehler

Vergessen der PIN

Falls der berechtigte Benutzer sofort Zugriff auf das gesperrte System benötigt, kann dazu ein Wiederherstellungskennwort verwendet werden. Windows läuft danach wie gewohnt.

Bevor ein System mit Hilfe eines Wiederherstellungsschlüssels oder -kennworts für einen Benutzer entsperrt wird ist auf jeden Fall in geeigneter Weise die Identität des Benutzer und dessen Berechtigung zur Systembenutzung zu überprüfen. Die Identitätsprüfung bei telefonischer Übermittlung des Wiederherstellungskennworts ist schwierig. Möglichkeiten zur Absicherung sind das Tätigen eines Rückrufs an die bekannte Telefonnummer des Nutzers sowie die Abfrage von Informationen, die nur dem Benutzer persönlich bekannt sein sollten. Die Zuordnung von Systemen zu berechtigten Benutzern kann mit Hilfe einer Datenbank überprüft werden.

Die BitLocker PIN kann mit dem Kommandozeilenprogramm *manage-bde* neu gesetzt werden. Das Löschen der alten PIN erfolgt durch den Aufruf:

```
cscript.exe manage-bde.wsf -protectors -delete -t -TPMandPIN C:.
```

Die neue PIN wird durch:

```
cscript.exe manage-bde.wsf -protectors -add -TPMandPIN <neue-PIN> C:
```

angelegt. Abbildung 7 zeigt den gesamten Vorgang.

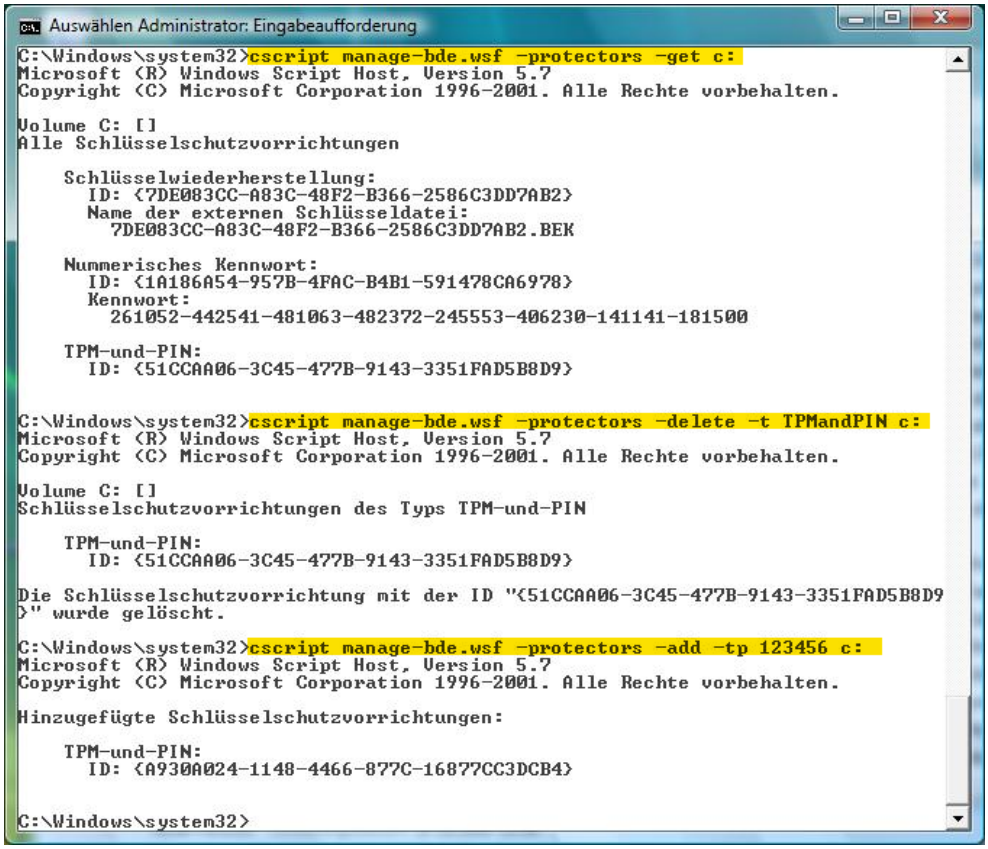
Zu häufige Fehleingabe der PIN

Um das Finden der korrekten PIN durch Ausprobieren zu verhindern, sperrt das TPM nach ca. 15 Fehleingaben die Eingabe weiterer PINs für eine mit jeder weiteren Fehleingabe zunehmenden Zeitspanne. Bei den TPM einiger Hersteller (unter anderem Infineon) bleibt diese Sperre auch nach einem Neustart aktiv. Die Sperre kann auch mutwillig ausgelöst worden sein, um dem Benutzer zu schaden.

Um diese Sperre aufzuheben, muss das TPM im BIOS oder in der TPM-Verwaltung unter Vista gelöscht und neu initialisiert werden. Der Vorgang entspricht der in Abschnitt 4.4.1 beschriebenen Ersteinrichtung des TPM.

Falls der berechtigte Benutzer sofort Zugriff auf das gesperrte System benötigt, kann dazu ein Wiederherstellungskennwort verwendet werden.

Abbildung 7:
Setzen einer neuen TPM-PIN mit *manage-bde*.



Beeinträchtigung der Plattformintegrität

Benutzer können unbeabsichtigt die Plattformintegrität beschädigen, wenn sie Veränderungen an der Hardware oder an Boot-Komponenten vornehmen. In diesem Fall ist zunächst zu klären, ob die Plattformintegrität durch eine leicht zu beseitigende Veränderung beeinträchtigt ist, etwa durch eine beim Systemstart eingelegte CD-ROM, ein U3-USB-Speichermedium[8] oder eine PCMCIA-Karte mit eigenem BIOS.

Falls die Änderung dauerhaft und erwünscht ist, etwa ein Update des System-BIOS, und der Benutzer vertrauenswürdig ist, so kann der BitLocker-Schlüssel

[8] USB-Speichermedien nach dem U3-Standard enthalten einen zweiten Speicherbereich, der dem System gegenüber wie ein externes CD-ROM-Laufwerk erscheint. Dort befinden sich Programme, die beim Anschließen des U3-USB-Speichermediums automatisch ausgeführt werden.

im TPM mit dem neuen Plattformzustand verknüpft werden. Dabei ist analog zu planmäßigen Wartungsarbeiten wie in Abschnitt 4.6.2 beschrieben zu verfahren.

4.7.2 Einwirkung Dritter

Kompromittierung von Authentisierungsmerkmalen

Unbefugte können auf verschiedenen Wegen Zugang zu einem Authentisierungsmerkmal erhalten:

- Diebstahl oder Fund verlorener USB-Schlüssel
- Kopieren von USB-Schlüsseln bei kurzzeitigem Zugriff, etwa wenn der USB-Schlüssel vom Benutzer an einen fremden Rechner angeschlossen wird.
- Einsicht in Notiz der PIN oder des Wiederherstellungskennworts
- Beobachtung der PIN-Eingabe
- Zugriff auf im Active Directory Server hinterlegte Schlüssel
- Zugriff auf Datensicherungen von Wiederherstellungsschlüsseln
- Social-Engineering
- Ausspähen der PIN durch Hardware-Keylogger

Wenn der Verdacht besteht, dass Unbefugte im Besitz eines Authentisierungsmerkmals sind, sollten die kompromittierten Schlüssel so schnell wie möglich durch neue ersetzt werden. Bis zu diesem Zeitpunkt muss das betroffene System besonders gut vor fremdem Zugriff geschützt werden.

Schlüssel und die PIN können mit dem Kommandozeilenprogramm *manage-bde* ersetzt werden.

Das Löschen der alten PIN erfolgt durch den Aufruf:

```
cscript.exe manage-bde.wsf -protectors -delete -t -TPMandPIN C:.
```

Die neue PIN wird durch:

```
cscript.exe manage-bde.wsf -protectors -add -TPMandPIN <neue PIN> C:
```

angelegt. Abbildung 7 zeigt den gesamten Vorgang. USB-Schlüssel, Wiederherstellungsschlüssel und -kennwörter werden auf die gleiche Weise ersetzt. Im Aufruf ist an Stelle von *-TPMandPIN* der entsprechende Typ und bei Schlüsseln deren Speicherort anzugeben. Hilfestellung hierzu liefert der Aufruf:

```
cscript.exe manage-bde.wsf -protectors -add -?.
```

Eine Person, die im Besitz eines Wiederherstellungsschlüssels oder -kennworts sowie einer Kopie der dazugehörigen Metadaten ist, kann das BitLocker-geschützte Volume durch Zurückkopieren der Metadaten auch noch nach einem Schlüsselwechsel entschlüsseln. Das gleiche gilt, falls die Person im Besitz einer Metadatenkopie mit Klartextschlüssel ist, d.h. Metadaten vom Zeitpunkt einer vorübergehenden BitLocker-Deaktivierung (siehe Abschnitt 4.6.2).

Falls der Verdacht besteht, dass Unbefugte im Besitz des Wiederherstellungsschlüssels oder -kennworts sind und für einen kurzen Zeitpunkt Zugriff auf die Festplatte des betroffenen Systems hatten, so muss das Volume vollständig neu verschlüsselt werden.

Diebstahl der Festplatte oder ihres Inhalts

Eine Entschlüsselung ist ohne das TPM und die vertrauenswürdige Plattform nur mit Hilfe eines Wiederherstellungsschlüssels oder -kennworts möglich. Falls eine Festplatte entwendet oder deren Inhalt von Unbefugten kopiert wird, so muss verhindert werden, dass die Täter sich die dazugehörigen Wiederherstellungsschlüssel oder -kennwörter beschaffen. Diese sollten deshalb möglichst vernichtet werden.

Diebstahl des kompletten Systems

Falls das vollständige System entwendet wurde, steht dem Dieb das TPM und die vertrauenswürdige Plattform zur Verfügung. Die Entschlüsselung des BitLocker-geschützten Volumes ist außer mit Wiederherstellungsschlüssel und -kennwort auch mit dem TPM-gebundenen Authentisierungsmerkmal möglich. Es muss verhindert werden, dass der Täter Zugriff darauf erlangen kann.

Verlorene oder gestohlene Laptops sind übrigens das Bedrohungsszenario, das nach Angaben von Microsoft die Motivation für den Einsatz von Bitlocker liefert [1].

Offline-Angriff gegen das System

Angreifer, die kurzzeitig Zugang zu einem BitLocker-geschützten System haben, können verschiedene fortgeschrittene Offline-Angriffe durchführen. Neben der Integrität der Hardware und der Boot-Komponenten könnte in sehr begrenztem Umfang auch die Integrität der verschlüsselten Daten geschädigt werden. Die Plattformvalidierung durch BitLocker verhindert nur, dass Schlüsselmaterial aus dem TPM freigegeben wird, falls Manipulationen an bestimmten Hardware- und Boot-Komponenten festgestellt werden.

Ein so manipuliertes System wäre nicht mehr vertrauenswürdig. Auf keinen Fall sollte das System mit einem Wiederherstellungsschlüssel oder -kennwort ge-

startet werden. Um für eine Datensicherung Zugriff auf die verschlüsselten Daten zu bekommen, sollte das Volume stattdessen vorsichtshalber als Datenpartition in einem vertrauenswürdigen System entsperrt werden.

Online-Angriff gegen das System

BitLocker bietet keinerlei Schutz gegen Online-Angriffe, also Manipulationen am entsperrten Volume im laufenden System. Solche Angriffe sind beispielsweise über das Netzwerk denkbar. Zum Schutz gegen Online-Angriffe können die üblichen Sicherheitsmaßnahmen wie sichere Systemkonfiguration, Firewall, Viren-Scanner, regelmäßige Datensicherung und richtiges Benutzerverhalten beitragen.

4.7.3 Hardwareschäden

In einer professionell betriebenen IT-Landschaft wird man in der Regel über ein funktionierendes Backup-Konzept verfügen und bei Hardwareschäden auf die letzte Sicherung zurückgreifen. Dennoch sind Situationen denkbar, in denen Daten von einer beschädigten Platte gerettet werden sollen.

Lesefehler der Festplatte

Um das Risiko eines Datenverlusts gering zu halten, sollte nicht weiter mit dem System gearbeitet werden.

BitLocker erschwert die Datenrettung und verhindert einige dabei übliche Vorgehensweisen. Ein BitLocker-geschütztes Volume enthält im verschlüsselten Zustand außer den Metadaten keine interpretierbaren Strukturen. Eine Erkennung und Rekonstruktion von Dateisystem- und Dateistrukturen ist daher nicht möglich. Reparaturwerkzeuge, die nicht auf BitLocker spezialisiert sind, dürfen nicht verwendet werden. Erstes Ziel der Datenrettung muss es sein, ein möglichst vollständiges Abbild des verschlüsselten Volumes auf einer zweiten Festplatte zu erstellen. Alle weiteren Arbeiten sind an Hand dieses Abbilds durchzuführen.

Als erste Maßnahme kann man versuchen, das Abbild des Volumes mit Hilfe eines Wiederherstellungsschlüssels oder -kennworts in einem zweiten Windows Vista System als Datenpartition zu entsperren. Falls dies nicht gelingt ist möglicherweise der erste Metadatenblock beschädigt. In diesem Fall kann ein von Microsoft erhältliches Wiederherstellungsprogramm (vgl. 2.7) verwendet werden. Es ist in der Lage, jede der drei Kopien der Metadaten oder alternativ ein Schlüsselpaket aus einem Active Directory Dienst zur Entschlüsselung zu verwenden. Alle entschlüsselbaren Sektoren des Volumes können so im Klartext auf eine weitere Festplatte geschrieben werden.

Beschädigung des TPM oder der vertrauenswürdigen Plattform

Falls die Hauptplatine mit dem TPM gewechselt werden muss, so kann wie in Abschnitt 4.6.2 beschrieben verfahren werden.

4.8 Außerbetriebnahme

Checkliste Außerbetriebnahme
Festplatte möglichst vollständig überschreiben.
Löschung der Metadaten alleine ist nur unter engen Vorraussetzungen ausreichend (keine Kopie der Metadaten vorhanden, Vernichtung aller Schlüssel).

Microsoft bewirbt BitLocker unter anderem damit, dass der Inhalt von Festplatten durch Löschen des in den Metadaten gespeicherten Schlüssels sehr viel schneller unlesbar gemacht werden kann, als durch das übliche mehrfache Überschreiben der gesamten Festplatte.

Es existieren jedoch verschiedene Szenarien, wie Metadaten wiederhergestellt werden können, etwa aus einem im AD gespeicherten Schlüsselpaket oder durch Widerherstellen einer Datensicherung.

Um ein sicheres Löschen der Daten zu gewährleisten empfehlen wir daher nach wie vor das Überschreiben der gesamten Festplatte inklusive der verschlüsselten Teile. Das bloße Löschen der Metadaten ist mit zu vielen Risiken und Einschränkungen verbunden und schützt daher zuverlässig nur vor Gelegenheitstätern, die etwa einen bei eBay ersteigerten Datenträger analysieren.

Kapitel 4
BitLocker im Einsatz

5 Alternativen und Ergänzungen

BitLocker ist weder die erste noch die einzige Möglichkeit, unter Windows Vista Daten zu verschlüsseln. Bereits seit Windows 2000 steht die Dateiverschlüsselung EFS zur Verfügung, die inzwischen einige Verbesserungen und Erweiterungen erfahren hat. Darüber hinaus ist eine breite Palette von freien und kommerziellen Produkten erhältlich. Eine vollständige Marktübersicht würde den Rahmen dieses Leitfadens sprengen und zudem schnell veralten. Wir beschränken uns daher darauf, mögliche Alternativen und Ergänzungen an zwei Beispielen zu erläutern. Die Wahl fiel auf das bereits erwähnte EFS, das den Anwendern von BitLocker stets zur Verfügung steht, sowie auf TrueCrypt[9] als Vertreter der Open-Source-Software. Beide Produkte sind insbesondere auch für solche Anwender interessant, die Windows-Versionen ohne BitLocker einsetzen.

5.1 Windows Encrypting File System (EFS)

Das EFS (*Encrypting File System*) ist eine Erweiterung des NTFS-Dateisystems von Microsoft und ist seit Windows 2000 fest in das Betriebssystem integriert. Im Gegensatz zu BitLocker verschlüsselt es keine ganzen Partitionen vollständig, sondern ausschließlich einzelne Dateien.

Die Aktivierung von EFS ist für den Anwender sehr einfach: Rechtsklick auf die zu verschlüsselnde Datei, innerhalb des Karteireiters *Allgemein* auf *Erweitert*, dann den Haken setzen bei *Inhalt verschlüsseln, um Daten zu schützen*. Installations- oder Konfigurationsarbeiten sind in diesem Fall nicht erforderlich.

Auch Ordner können auf diese Weise »verschlüsselt« werden. Das hat aber nur zur Folge, dass neu in diesem Ordner angelegte Dateien oder hineinkopierte Dateien künftig verschlüsselt werden. Optional kann die Verschlüsselung auch auf sämtliche bestehende Dateien und Unterordner sofort angewendet werden. Es handelt sich bei der Verschlüsselung von Ordnern also nur um das Setzen eines Datei-Attributes, das an Unterordner und Dateien weitervererbt wird. Dieses Attribut bedeutet nur, dass die Inhalte zu verschlüsseln sind. Ansonsten hat es keinen Einfluss. Sämtliche Metadaten (wie z.B. die Dateinamen) bleiben jedoch unverschlüsselt.

[9] http://www.truecrypt.org/

Jede Datei wird mit einem eigenen Datei-Schlüssel, dem sogenannten *File Encryption Key*, verschlüsselt. Dieser ist wiederum asymmetrisch mit dem öffentlichen Schlüssel des Benutzers verschlüsselt, der die Datei angelegt, kopiert oder verschlüsselt hat.

Ein Benutzer kann eine Datei auch für andere Personen verschlüsseln. Dies muss er aber für jede Datei und jeden Benutzer einzeln tun. Eine Datei kann nicht für bestimmte Gruppen verschlüsselt werden, sondern immer nur für einzelne Benutzer.

Die zum Entschlüsseln benötigten privaten Schlüssel sind in Zertifikaten gespeichert. Wo diese Zertifikate sich befinden, ist abhängig von der Lage der zu verschlüsselnden Dateien sowie von der Konfiguration des Windows-Netzwerks. Sie können im Benutzerverzeichnis, auf einem Profilserver, auf einem Dateiserver oder (ab Windows Vista) auf einer Smartcard liegen. Für den Benutzer spielt die Lage des Zertifikates beim Entschlüsseln normalerweise keine Rolle. Die Entschlüsselung geschieht automatisch, ohne dass ein gesondertes Eingreifen des Benutzers nötig ist. Die einzige Ausnahme ist die Verwendung einer Smartcard. In diesem Fall muss der Benutzer natürlich die Smartcard in das entsprechende Lesegerät schieben und die PIN eingeben.

Neben lokalen Dateien kann EFS auch solche auf Netzlaufwerken verschlüsseln. Um EFS-Verschlüsselung für Dateien auf Netzwerkfreigaben verwenden zu können oder um Dateien für mehrere Benutzer zu verschlüsseln, müssen die Zertifikate mit den öffentlichen Schlüsseln zentral verwaltet werden. Dafür muss im Netzwerk ein Zertifikatsserver installiert werden. Außerdem sollten für die EFS-Verschlüsselung auf Netzwerkfreigaben oder für mehrere Benutzer serverbasierte Profile verwendet werden, um größere Probleme zu vermeiden.

Um EFS auf einem Netzlaufwerk verwenden zu können, muss außerdem im Active-Directory für das Computerkonto des Servers die Option *»Computer für Delegierungszwecke vertrauen«* aktiviert werden. Ein Risiko, das dabei bleibt, ist die Tatsache, dass die Datenübertragung der Dateien im Netzwerk auch mit EFS nicht verschlüsselt ist.

EFS erlaubt keine Verschlüsselung von Betriebssystemdateien. Allerdings kann Windows Vista die Auslagerungsdatei mit Hilfe von EFS und einem bei jedem Systemstart zufällig gewählten Schlüssel verschlüsseln.

Um Datenverluste zu vermeiden, sollte ein Wiederherstellungsagent (Date Recovery Agent) eingerichtet werden. Das hat zur Folge, dass alle EFS-verschlüsselten Dateien nicht nur für den Benutzer, sondern gleichzeitig für den Wiederherstellungsagenten verschlüsselt werden.

5.2 TrueCrypt

TrueCrypt ist eine frei verfügbare, quelloffene Verschlüsselungssoftware für Windows und Linux, die als separates Programm installiert wird. Sie ist seit 2004 erhältlich und wird aktiv weiterentwickelt.

TrueCrypt erzeugt verschlüsselte Volumes, wie dies bei BitLocker auch der Fall ist. Diese Volumes sind auf einer vollständigen Partition (partitionsbasierte Volumes) oder als Datei (dateibasierte Volumes oder auch Container genannt) gespeichert. Im Gegensatz zu BitLocker schützt TrueCrypt aber nur Daten-Volumes. Die Betriebssystempartition hingegen kann TrueCrypt bislang nicht verschlüsseln.

Zur Authentisierung verwendet TrueCrypt alphanumerische Kennwörter und Schlüsseldateien. Dabei sind Ein- oder Zwei-Faktor-Authentisierungen realisierbar. Das heißt, man kann entweder ein Passwort oder eine Schlüsseldatei oder beides zum Authentisieren verwenden.

Für ein Volume kann jeweils nur ein einziger Authentisierungsmechanismus eingerichtet werden. Im Gegensatz zu BitLocker gibt es also keine Wiederherstellungsschlüssel oder -kennwörter, sondern ausschließlich die normale Nutzerauthentisierung für den alltäglichen Gebrauch.

Im Gegensatz zu BitLocker können TrueCrypt-Volumes im laufenden Betrieb beliebig geöffnet und geschlossen werden. Dadurch hat der Benutzer die Möglichkeit, einen TrueCrypt-Container nur dann offen zu halten, wenn er ihn gerade braucht. Es gibt zahlreiche Konfigurationsmöglichkeiten, mit denen eingestellt werden kann, wann ein TrueCrypt-Container automatisch wieder geschlossen wird, z.B. nach einer bestimmten Zeit der Inaktivität oder beim Aktivieren des Energiesparmodus oder des Ruhezustandes.

Vor dem Benutzen eines TrueCrypt-Containers muss dieser normalerweise manuell vom Benutzer geöffnet werden. Dabei gibt der Benutzer das Passwort ein und/oder wählt die Schlüsseldatei aus. Der Container kann dann wie ein normales Laufwerk verwendet werden. Das Öffnen von TrueCrypt-Containern kann aber auch automatisiert werden.

Wenn Anwendungsprogramme Dateien aus dem Container geöffnet haben und dieser (z.B. automatisch) geschlossen wird, kann es (z.B. beim Abspeichern) zu Fehlern führen, weil das TrueCrypt-Laufwerk nach dem Schließen des Containers nicht mehr verfügbar ist.

Wird TrueCrypt als Datei-Container verwendet, so kann eine Container-Datei auch auf einem Dateiserver gespeichert werden. Im Gegensatz zu BitLocker oder EFS ist in diesem Fall auch die Datenübertragung im Netzwerk verschlüs-

selt, da die Entschlüsselung erst auf dem Arbeitsplatzrechner stattfindet. Eine TrueCrypt-Datei auf einem Dateiserver kann auch für mehrere Benutzer zum Datenaustausch dienen, solange alle das Passwort kennen und/oder die Schlüsseldatei besitzen. Nachteilig ist aber, dass gleichzeitige Schreibzugriffe auf den selben TrueCrypt-Container immer nur von einem Benutzer durchgeführt werden können.

Im Februar 2008 ist die Version 5.0 von TrueCrypt erschienen. Sie bietet unter anderem die Möglichkeit, auch Windows-Systempartitionen zu verschlüsseln. Verbunden damit ist eine Pre-Boot-Authentisierung.

5.3 TrueCrypt und EFS als Ergänzung zu BitLocker

Differenzierte Zugriffskontrolle mit EFS

BitLocker ist nicht in der Lage, den Datenzugriff[10] auf Mehrbenutzersystemen auf einzelne Nutzer zu beschränken. Auf BitLocker-geschützten Volumes kann EFS diese Aufgabe übernehmen.

Für die Verschlüsselung von Daten auf gemeinsam genutzten Servern kann diese Fähigkeit eingeschränkt sinnvoll sein. Das ist insbesondere dann der Fall, wenn sich verschiedene Nutzer für einige Daten zusammenfinden (z.B. Projektdaten zu einem gemeinsamen Projekt mit bestimmten Projektteilnehmern). Aus Gründen der Handhabbarkeit ist dieser Einsatz allerdings nur dann empfehlenswert, wenn nur wenige Dateien für nur wenige Benutzer verschlüsselt werden müssen. Außerdem muss in diesem Fall ein Zertifikatsserver vorhanden sein, und es sollten serverbasierte Profile verwendet werden.

Eine andere sinnvolle Einsatzvariante ist die Verschlüsselung von Daten für einen einzelnen Nutzer auf einem Mehrbenutzersystem. In jedem Fall sollte bei der Nutzung von EFS ein Wiederherstellungsagent eingerichtet und verwendet werden, um vor ungewolltem Datenverlust zu schützen. Anders als bei BitLocker erfassen Online-Backups nicht automatisch die Klartextdaten.

Verschlüsselung von Daten-Volumes mit TrueCrypt

TrueCrypt kann als Ergänzung zu BitLocker eingesetzt werden, um Daten-Volumes zu verschlüsseln. Erst ab Service Pack 1 für Windows Vista soll BitLocker das selbst können (siehe auch Abschnitt 2.8). Die zurzeit bereits inoffiziell vorhandene Unterstützung ist noch nicht praxistauglich. TrueCrypt kann

[10] Bezogen auf die Durchsetzung von Zugriffsrechten mittels Verschlüsselung.

dieses Defizit ausgleichen. Umgekehrt deckt BitLocker gerade jene Gebiete ab, auf denen TrueCrypt noch Schwächen hat.

TrueCrypt-Dateicontainer eignen sich für kleinere Gruppen zum Datenaustausch. Hier ist vor allem von Vorteil, dass auch die Datenübertragung verschlüsselt ist. Für eine größere Zahl von Nutzern, die zeitgleich mit den enthaltenen Dateien arbeiten müssen, ist diese Lösung allerdings ungeeignet. Die Methode des Datenaustauschs ist dabei egal, Container können zum Beispiel auf einem Netzlaufwerk oder auf einem Memory-Stick abgelegt sein.

Gleichermaßen eignet sich TrueCrypt auch zu Verschlüsselung von Daten auf persönlichen externen Datenträgern, etwa persönlichen USB-Sticks oder externen Festplatten. Eine speziell dafür angepassten Funktion, der sogenannte *Traveller-Modus* bietet hier besondere Unterstützung. BitLocker bietet diese Funktion nicht.

5.4 TrueCrypt und EFS als Ersatz für BitLocker

Eine echte Alternative zu BitLocker ist derzeit weder EFS noch TrueCrypt.

EFS

EFS kann BitLocker nicht ersetzen. Hauptgrund ist, dass nur der Inhalt von Dateien verschlüsselt wird. Bereits die Existenz einer bestimmten Datei kann aber eine vertrauliche Information sein. Darüber hinaus kann ein Angreifer eine Datei trotz EFS gezielt löschen und durch eine unverschlüsselte ersetzen. Die fehlende Verschlüsselung der Betriebssystempartition erhöht zudem das Risiko unerwünschter Klartextkopien von im Original verschlüsselte Dateien. EFS ist also für mobile und stationäre Arbeitsplatzrechner als alleinige Verschlüsselungslösung nicht zu empfehlen.

Unter Umständen könnte der Einsatz von EFS sinnvoll erscheinen, wenn bereits eine PKI existiert, die Datenverschlüsselung in diese PKI integriert werden soll. In der Regel wird man in dieser Situation jedoch zu einem Produkt für die Disk- oder Volume-Verschlüsselung mit Smartcard-Unterstützung greifen.

TrueCrypt

Sollen allein Daten-Volumes verschlüsselt werden, so kann TrueCrypt ein brauchbarer Ersatz für BitLocker sein. Ähnlich wie bei EFS besteht aber auch dann wieder das Problem der unerwünschten Klartextkopien verschlüsselter Daten auf der Betriebssystempartition. Unter Windows Vista ist dieses Risiko beim Einsatz von TrueCrypt sogar noch höher, da TrueCrypt die Auslagerungsdatei nicht verschlüsseln kann.

Mit den geplanten Erweiterungen ab Version 5.0 könnte TrueCrypt zu einer in jeder Hinsicht ernstzunehmenden Alternative zu BitLocker heranwachsen. Als wesentlicher konzeptioneller Unterschied bliebe dann nur noch die in TrueCrypt fehlende TPM-Unterstützung übrig.

Tabelle 5: TrueCrypt und EFS als Ergänzung oder Alternative zu BitLocker

Verschlüsselungssoftware	Als Ergänzung zu BitLocker	Als Alternative zu BitLocker
EFS	Bedingt sinnvoll in Mehrbenutzerszenarien	In BitLocker-relevanten Szenarien kaum zu empfehlen
TrueCrypt	Zur zusätzlichen Verschlüsselung von Daten-Volumes geeignet	Geeignet, wenn *nur* Daten-Volumes verschlüsselt werden sollen
	Bedingt sinnvoll in Mehrbenutzerszenarien (als Datei-Container)	Bedingt sinnvoll in Mehrbenutzerszenarien (als Datei-Container)

Anhang A Mustermerkblatt für Benutzer

Benutzer sollten neben einer kurzen Einweisung ein Merkblatt mit Informationen und Verhaltensregeln zur korrekten Verwendung von BitLocker-geschützten Systemen erhalten. Wir haben zwei Mustermerkblätter erstellt, die als Vorlage für die Erstellung eines an die eigene Situation angepassten Merkblatts dienen sollen.

Das erste Merkblatt richtet sich an Benutzer, auf deren Laptop BitLocker in der Betriebsart TPM+PIN aktiviert wurde. Das zweite Merkblatt ist für Benutzer von Arbeitsplatzrechnern mit BitLocker in der Betriebsart TPM+USB-Schlüssel.

A.1 Merkblatt für Laptop-Benutzer

Auf Ihrem Laptop wurde BitLocker Drive Encryption installiert. BitLocker verschlüsselt alle auf der Festplatte C: gespeicherten Daten. Bei Verlust oder Diebstahl des Laptops ist es für Unbefugte sehr schwierig, die gespeicherten Daten zu lesen.

Was ändert sich für mich?

Beim Start, Neustart oder Aufwecken Ihres Laptops aus dem Ruhezustand fordert Sie BitLocker zur Eingabe der PIN auf, die Sie zusammen mit diesem Merkblatt erhalten haben. Prägen Sie sich diese PIN ein und vernichten sie dann die Notiz der PIN.

Geben Sie die PIN über die Tastatur ein und drücken sie Return.

Am weiteren Startvorgang und bei der Arbeit mit dem Laptop ändert sich für Sie nichts.

Was muss ich beachten?

- **Halten Sie ihre PIN geheim!** Schreiben Sie die PIN nicht auf. Geben Sie die PIN nicht weiter, auch nicht an Kollegen. Verwenden Sie die PIN nicht für weitere Zwecke, beispielsweise als Passwort. Achten Sie darauf, dass Sie bei der Eingabe der PIN nicht beobachtet werden.
- **Falls sie die PIN einmal vergessen sollten,** wenden Sie sich an unseren Helpdesk (Kontaktdaten stehen am Ende des Merkblatts). Versuchen Sie nicht, die korrekte PIN zu erraten. Nach insgesamt 15 Fehleingaben tritt sonst eine Sperre in Kraft. Machen Sie auf keinen Fall weitere Eingabeversuche, wenn die Meldung *»Es wurde zu oft eine falsche PIN eingegeben.«* erscheint.
- **Versetzen sie ihren Laptop in den Ruhezustand statt in den Energiesparmodus,** wenn Sie den Laptop aus den Augen lassen oder dessen Diebstahl möglich ist.

Welche Probleme können auftreten?

Bei Systemstart erscheint statt der Aufforderung zur PIN-Eingabe die **Fehlermeldung** *»Die Informationen zum Starten des Betriebssystems wurden seit dem Aktivieren von BitLocker geändert.«*

- Prüfen Sie, ob eine CD-ROM oder DVD-ROM eingelegt oder ein USB-Stick angeschlossen ist. Entfernen Sie das Medium und starten Sie den Laptop erneut.

- In allen anderen Fällen wenden Sie sich bitte an den Helpdesk.

Was muss ich tun wenn Unbefugte meine PIN erlangen?

- Wenn Sie den Verdacht haben, dass Unbefugte Kenntnis Ihrer PIN erlangt haben, so melden Sie das sofort dem Helpdesk!
- Verhindern Sie, dass sich Unbefugte Zugang zu Ihrem Laptop verschaffen. Schließen Sie Ihren Laptop ein. .

Helpdesk

Unseren Helpdesk erreichen Sie Montags bis Freitags rund um die Uhr unter der Telefonnummer …….. und unter der E-Mail-Adresse ……

A.2 Merkblatt für PC-Benutzer

Auf Ihrem PC wurde BitLocker Drive Encryption installiert. BitLocker verschlüsselt alle auf der Festplatte C: gespeicherten Daten. Bei Verlust oder Diebstahl des PC ist es für Unbefugte sehr schwierig, die gespeicherten Daten zu lesen.

Was ändert sich für mich?

Vor dem Start, Neustart oder Aufwecken ihres PC aus dem Ruhezustand müssen Sie den USB-Schlüssel, den Sie zusammen mit diesem Merkblatt erhalten haben, an Ihren PC anschließen. Sobald der USB-Schlüssel erkannt und ausgelesen wurde, werden Sie durch eine Bildschirmmeldung aufgefordert, das Schlüsselmedium zu entfernen. Ziehen Sie den USB-Schlüssel dann ab und bewahren Sie ihn an einem sicheren Ort auf.

Am weiteren Startvorgang und bei der Arbeit mit dem PC ändert sich für sie nichts.

Was muss ich beachten?

- **Bewahren Sie den USB-Schlüssel immer getrennt vom PC auf.** Schließen Sie den USB-Schlüssel erst beim Start des PC an und ziehen Sie ihn sofort danach ab. Tragen Sie den USB-Schlüssel sonst immer bei sich, z.B. an ihrem Schlüsselbund.
- **Verwenden Sie den USB-Schlüssel nicht für andere Zwecke**. Schließen Sie den USB-Schlüssel auf keinen Fall an andere Geräte als Ihren PC an. Speichern sie keine Daten darauf ab.

Welche Probleme können auftreten?

Bei Systemstart erscheint die Meldung *»Der BitLocker-Schlüssel ist erforderlich«* oder die **Fehlermeldung** *»Die Informationen zum Starten des Betriebssystems wurden seit dem Aktivieren von BitLocker geändert.«*

- Stellen Sie sicher, dass der USB-Schlüssel angeschlossen ist.
- Prüfen Sie, ob eine CD-ROM oder DVD-ROM eingelegt oder ein anderer USB-Stick angeschlossen ist. Entfernen Sie das Medium und starten Sie den PC erneut.
- In allen anderen Fällen wenden Sie sich bitte an den Helpdesk.

Was muss ich bei Verlust des USB-Schlüssels tun?

- Melden Sie den Verlust des USB-Schlüssels sofort dem Helpdesk!
- Verhindern Sie, dass sich Unbefugte Zugang zu Ihrem PC verschaffen. Schließen Sie Ihr Büro ab, auch wenn Sie es nur kurz verlassen.

Helpdesk

Unseren Helpdesk erreichen Sie Montags bis Freitags rund um die Uhr unter der Telefonnummer …….. und unter der E-Mail-Adresse …….

Anhang A
Mustermerkblatt für Benutzer

Glossar

Active Directory, AD	Verzeichnisdienst von Microsoft Windows zur zentralen Verwaltung von Identitäten.
Key Package, Schlüsselpaket	Datenpaket, das den mit einem Wiederherstellungskennwort verschlüsselten FVEK enthält. Kann bei der BitLocker-Aktivierung automatisch in einem Active Directory hinterlegt werden.
AES	Advanced Encryption Standard, der von Bitlocker verwendete Verschlüsselungsalgorithmus.
Authentisierungsmittel	In diesem Leitfaden: Sammelbegriff PIN, USB-Schlüssel, Wiederherstellungsschlüssel oder Wiederherstellungskennwörter. Von Microsoft auch Schlüsselschutzvorrichtung genannt.
BDE	BitLocker Drive Encryption, in diesem Leitfaden auch einfach BitLocker genannt.
Brute Force	Angriffstechnik gegen Passwörter und Schlüssel; der Angreifer probiert gezielt oder zufällig viele mögliche Werte aus.
CA	Certification Authority, Zertifizierungsstelle einer *PKI*.
CBC	Cipher Block Chaining, eine Betriebsart von Blockchiffren wie AES. CBC soll verhindern, dass aus identischen Klartextblöcken identische Chiffrate entstehen.
Daten-Volume	Alle Partitionen, die nicht System-Volume der laufenden oder zu startenden Instanz von Windows Vista sind.

Diffuser, Diffusor — Eine von Microsoft entwickelte Ergänzung zur Verschlüsselung. Der Diffuser bearbeitet Sektoren des Datenträgers und soll bekannte Schwächen des CBC-Modus beheben.

Dual-Boot, Dual-Boot-System — PC mit mehreren installierten Betriebssystemen, die sich mittels eines Bootmanagers abwechselnd starten lassen.

EFS — Encrypting File System, eine seit Windows 2000 verfügbare Verschlüsselungsfunktion für Dateiinhalte.

Energiesparmodus — → *Standby*

FIPS
FIPS 140-2
FIPS 197 — Federal Information Processing Standard, eine Reihe von Standards, die Lieferanten der US-amerikanischen Regierung einhalten müssen. FIPS 140-2 spezifiziert Anforderungen an Kryptomodule, FIPS 197 den Algorithmus AES.

Firewire — IEEE 1394.

FVEK — Full Volume Encryption Key. Aus diesem Schlüssel werden AES- und Sektorschlüssel abgeleitet.

IEEE 1394 — Eine serielle Busschnittstelle mit hoher Geschwindigkeit. Auch *Firewire*, *i.LINK* oder *DV* genannt.

Key Package — Ein verschlüsselter *FVEK*, der getrennt vom PC im *Active Directory* gespeichert werden kann. In Notfällen lassen sich damit Daten von beschädigten Volumes noch entschlüsseln.

Offline-Angriff — hier: Angriff auf den Datenträger ohne Mitwirkung des Betriebssystems, z.B. bei ausgeschaltetem PC.

Online-Angriff — hier: Angriff zur Laufzeit und unter Mitwirkung des Betriebssystems.

Partition — Organisationseinheit einer Festplatte. Entspricht unter Windows normalerweise einem Volume oder Laufwerk. In einem RAID-Verbund kann sich ein Volume aber auch über mehrere Partitionen erstrecken.

PIN	Personal Identification Number, ein Passwort, das i.d.R. nur aus Ziffern besteht.
PKI	Public-Key-Infrastruktur .
Replay	Hier: Überschreiben gespeicherter Datenblöcke (Sektoren) mit einer älteren Version desselben Blocks.
Ruhezustand, Suspend-to-Disk	Energiesparmodus, bei dem der Inhalt des Arbeitsspeichers auf die Festplatte gespeichert wird und so ohne Stromzufuhr erhalten bleibt.
Schlüsselschutzvorrichtung	Microsofts Sammelbezeichnung für Elemente der Schlüsselverwaltung: TPM, PIN, USB-Schlüssel, Wiederherstellungsmittel.
Sector Key, Sektorschlüssel	Ein zusätzlicher sektorabhängiger Schlüssel, der bei Verwendung des Diffusers in die Verschlüsselung einfließt.
Sektor	Datenblock auf einer Festplatte, kleinste Verwaltungseinheit für Speicherplatz auf dem Datenträger. Unter Vista zwischen 512 und 8192 Bytes groß.
Standby, Suspend-to-RAM	Energiesparmodus, bei dem nur der Arbeitsspeicher mit Strom versorgt wird.
System-Volume	Partition, von der Windows Vista startet, typischerweise Laufwerk C:.
TCG	Trusted Computing Group, das Standardisierungsgremium für die Trusted-Computing-Plattformen.
TCG-BIOS	Teil des System-BIOS, der u.a. für die Plattformvalidierung notwendig ist und der TCG-Spezifikation entsprechen muss.
TPM	Trusted Platform Module, Sicherheitschip in der Hardware eines PC und Kernbestandteil der Trusted-Computing-Plattform.
TrueCrypt	Eine Open-Source-Verschlüsselungssoftware. http://www.truecrypt.org

Trusted Computing	Eine Sicherheitstechnologie, die sich auf das TPM als Sicherheitsanker stützt.
Volume	Laufwerk unter Windows. Entspricht typischerweise einer Partition.
Volume-Schlüssel	→ *FVEK.*
Wiederherstellungskennwort	Eine 48-stellige Ziffernfolge, die einen 128-Bit-Schlüssel darstellt. Damit kann ein Volume unabhängig vom TPM entsperrt werden.
Wiederherstellungsschlüssel	Ein 256-Bit-Schlüssel, der für Notfälle gespeichert werden kann. Damit lassen sich Volumes unabhängig vom TPM entsperren.

Literatur

[1] Niels Ferguson: *AES-CBC + elephant diffuser, a disk encryption algorithm for Windows Vista.* http://www.microsoft.com/downloads/details.aspx?FamilyID=131dae03-39ae-48be-a8d6-8b0034c92555, 2006.

[2] Bundesamt für Sicherheit in der Informationstechnik: *IT-Grundschutz-Kataloge.* http://www.bsi.de/gshb/deutsch/, 2007.

[3] Brian Komar and Microsoft Corporation: *Microsoft Windows Server 2003 PKI and Certificate Security.* Microsoft Press, 2004.

[4] Microsoft: *Data Encryption Toolkit for Mobile PCs – Planning and Implementation Guide.* http://go.microsoft.com/fwlink/?LinkId=81666, Mai 2007, Version 1.0.

[5] Microsoft: *Data Encryption Toolkit for Mobile PCs – Security Analysis.* http://go.microsoft.com/fwlink/?LinkId=81666, April 2007, Version 1.0.

[6] Microsoft: How to use the BitLocker Recovery Password Viewer for Active Directory users and computers tool to view recovery passwords for Windows Vista. Knowledge Base article 928202, http://support.microsoft.com/kb/928202, Februar 2007.

[7] Microsoft: *How to use the BitLocker Repair Tool to help recover data from an encrypted volume in windows vista.* Knowledge base article 928201, http://support.microsoft.com/kb/928201, Februar 2007.

[8] Mark Minasi and Byron Hynes: *Administrating Windows Vista Security.* Wiley Publishing, Inc., Indianapolis, USA, 2007.

[9] Scott Moulton: *Data recovery whitepaper.* http://www.myharddrivedied.com/presentations_whitepaper.html, 2007.

[10] Microsoft TechNet: *Configuring Active Directory to back up Windows BitLocker Drive Encryption and trusted platform module recovery information.* http://technet2.microsoft.com/WindowsVista/en/library/3dbad515-5a32-4330-ad6f-d1fb6dfcdd411033.mspx?mfr=true.

[11] Bundesamt für Sicherheit in der Informationstechnik: *Trusted Computing. Informationen und Stellungnahmen zu aktuellen Entwicklungen im Bereich vertrauenswürdiger Plattformen.* http://www.bsi.de/sichere_plattformen/trustcomp/

[12] Microsoft: *Configuring Active Directory to Back up Windows BitLocker Drive Encryption and Trusted Platform Module Recovery Information.* http://www.microsoft.com/downloads/details.aspx?FamilyID=3A207915-DFC3-4579-90CD-86AC666F61D4&displaylang=en

[13] Bundesamt für Sicherheit in der Informationstechnik: *BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)*, Version 1.0, URL: http://www.bsi.de/literat/bsi_standard/standard_1001.pdf
[14] Microsoft TechNet: *BitLocker Drive Encryption.* URL: http://www.microsoft.com/technet/windowsvista/security/bitlockr.mspx