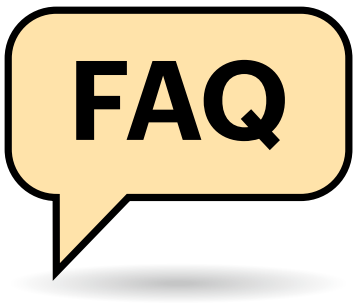


BitLocker

Die in Windows enthaltene Laufwerksverschlüsselung führt hin und wieder zu Verwirrung, Ärger und Beratungsbedarf. Hier beantworten wir die wichtigsten Fragen.

Von Jan Schüßler

BitLocker ohne Zutun aktiv

Nach einem BIOS-Update konnte mein Rechner mit Windows 11 Home neulich nicht mehr booten, es kam nur die Aufforderung, den Wiederherstellungsschlüssel für die BitLocker-Verschlüsselung einzugeben. Ich habe aber keinen, denn ich habe BitLocker nie aktiviert. Was nun?

Vermutlich haben Sie einen, wissen es nur nicht. Denn BitLocker steckt technisch auch in der Home-Edition von Windows, darf dort nur nicht so heißen. Stattdessen nennt Microsoft die Funktion dort „Geräteverschlüsselung“. Um sie zu nutzen, muss der Rechner ein paar Hardwarestandards erfüllen. Wir erleben immer wieder Systeme, bei denen die Verschlüsselung fürs Systemlaufwerk nach einer sauberen Neuinstallation sofort aktiv ist.

Das ist einer der Gründe, warum Microsoft Ihnen bei der Ersteinrichtung so penetrant ein Microsoft-Konto aufs Auge drücken will: Sobald Sie sich mit einem solchen an Windows 10 oder 11 anmelden, landet der Wiederherstellungsschlüssel automatisch in Ihrem Konto – unter account.microsoft.com/devices/recoverykey können Sie ihn auslesen.

Wiederherstellungsschlüssel ins Microsoft-Konto?

Einen Wiederherstellungsschlüssel im Microsoft-Konto zu speichern erscheint mir unter Datenschutz- und Sicherheitsaspekten völlig grotesk. Wer tut sowas bei vollem Bewusstsein?

Tatsächlich ist dieses Verfahren rational nachvollziehbar. Die Geräteverschlüsselung in Windows Home ist eine Funktion für die breite Masse, also für Menschen, die sich mit Verschlüsselung nicht auseinandersetzen wollen oder können. Für die ist es allemal sinnvoller, eine Verschlüsselung zu haben, zu der Microsoft einen Hintereingang kennt, als komplett ohne Verschlüsselung herumzulaufen. Bedenken Sie: Um mit einem Wiederherstellungsschlüssel überhaupt etwas anfangen zu können, muss ein Angreifer Ihren Rechner in seinem Besitz haben.

Ein Sicherheitsrisiko besteht in Extremfällen, und zwar dann, wenn jemand es ganz gezielt auf Ihre Daten abgesehen hat – und zu hohem Aufwand bereit ist, um sie zu erlangen. Der Angreifer müsste dafür erstens an den Schlüssel herankommen, was er entweder durch einen Einbruch in Ihr Microsoft-Konto schaffen kann (ein guter Grund für Zwei-Faktor-Authentifizierung), oder wenn es sich beim Angreifer um eine Ermittlungsbehörde handelt, die Microsoft zwingen kann, den Schlüssel herauszugeben. Und zweitens muss der Angreifer Ihren Rechner in die Finger bekommen, sprich: stehlen.

Sofern Sie ein so hochpreisiges Ziel sind, dass ein solcher Angriff realistisch ist, ist der Wiederherstellungsschlüssel im Microsoft-Konto tatsächlich ein Risiko – dann wäre es aber ohnehin grob fahrlässig, so zu verfahren. Für die allermeisten Windows-Nutzer ist dieses Szenario aber nicht relevant, sondern eher das Risiko, ein Notebook mit allerhand Dokumenten und Fotos in der Bahn zu verlieren. Und dann ist es gut zu wissen, dass ein Finder nichts auslesen kann.

BitLocker-Zustand anzeigen

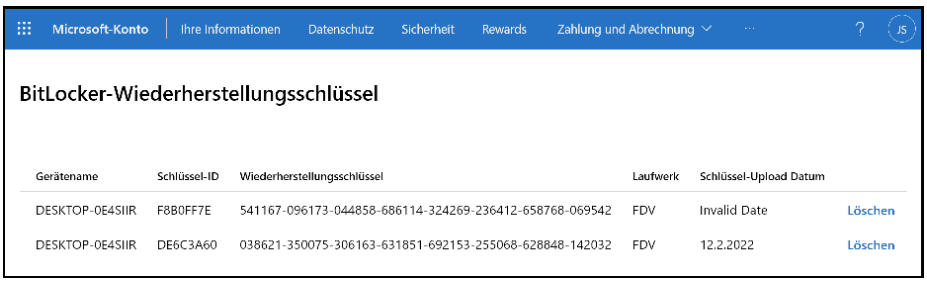
Kann ich mir irgendwie anzeigen lassen, ob ein Laufwerk verschlüsselt ist, und wenn ja, mit weiteren Details? Vor allem unter Windows Home, wo die BitLocker-Verwaltung weder in der Systemsteuerung noch in den Einstellungen zu finden ist?

Dafür gibt es das Kommandozeilentool manage-bde.exe – auch in Home-Editionen. Um den Verschlüsselungszustand aller Laufwerke anzuzeigen, öffnen Sie ein Terminal mit Administratorrechten, etwa via Windows-Taste+X. Der Befehl `manage-bde -status` zeigt Details zur Verschlüsselung jedes angeschlossenen Laufwerks an. Damit können Sie auch im Handumdrehen prüfen, ob Ihr Systemlaufwerk verschlüsselt ist: In der Zeile „BitLocker-Version“ meldet das Tool bei unverschlüsselten Laufwerken „Kein“, ansonsten eine Versionsnummer (meist 2.0).

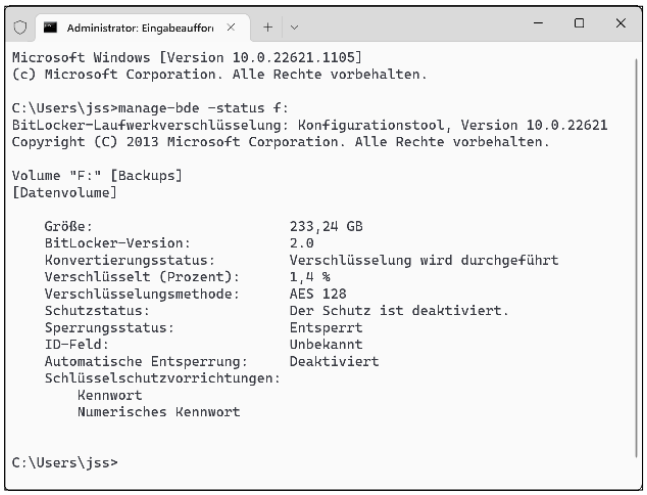
„Geräteverschlüsselung“ – sinnvoll oder nicht?

Empfehlen Sie, die Geräteverschlüsselung in Windows 10 oder 11 Home zu nutzen?

Wir empfehlen, eine Verschlüsselung zu nutzen, vor allem, wenn es um mo-



Der Wiederherstellungsschlüssel im Microsoft-Konto ist nur in Sonderfällen ein Problem – und kann im Zweifelsfall ein rettender Notnagel sein.



Per Eingabeaufforderung lesen Sie im Handumdrehen aus, ob die Verschlüsselung aktiv ist, welcher Algorithmus zum Einsatz kommt und Ähnliches.

bile Geräte geht, die schnell abhandenkommen oder bei einem Wohnungseinbruch gestohlen werden können. Es muss nicht zwingend die Geräteverschlüsselung sein, denn gerade diese Sparvariante von BitLocker lässt sich gar nicht konfigurieren, sondern nur ein- oder ausschalten, und sie funktioniert auch nicht für externe Datenträger. Teilen Sie Ihre System-SSD auf mehrere Partitionen auf, werden zwar alle durch die Geräteverschlüsselung geschützt, aber auch alle beim Systemstart automatisch entsperrt.

Wenn Sie also etwa USB-Medien schützen oder ein internes Laufwerk D: per Kennworteingabe entsperren wollen, sollten Sie die Geräteverschlüsselung abschalten und stattdessen ein flexibleres Tool wie VeraCrypt einsetzen. Das einzige, was Microsoft auf der Home-Edition mit USB-Medien erlaubt, ist das Verwenden bereits verschlüsselter Datenträger.

BitLocker unter Home ausschalten

Laut dem vorigen Tipp ist das Systemlaufwerk meines Windows 10 Home schon verschlüsselt, aber ich möchte es lieber mit VeraCrypt verschlüsseln. Wie werde ich die Microsoft-Verschlüsselung los?

Da das BitLocker-Verwaltungsmodul der Systemsteuerung in Ihrer Home-Edition fehlt, schauen Sie zunächst im Bereich „Geräteverschlüsselung“ in der Einstellungen-App nach, ob Sie die Funktion dort direkt abschalten können. Auf Windows 10 liegt das Menü unter „Update & Sicherheit“, auf Windows 11 unter „Datenschutz und Sicherheit“.

Fehlt die Schaltfläche, oder behauptet Windows, die Verschlüsselung sei mangels Microsoft-Konto nicht scharf geschaltet, können Sie die Entschlüsselung auch erzwingen – in einem Terminal mit Administratorrechten per `manage-bde -off c:`. Je nach Laufwerksgröße und -geschwindigkeit kann das ein paar Minuten oder auch ein, zwei Stunden dauern. Wie weit die Entschlüsselung vorangeschritten ist, können Sie mit dem zuvor genannten Statusbefehl auslesen: Sie ist abgeschlossen, sobald der Wert in der Zeile „Verschlüsselt (Prozent)“ auf 0,0 steht.

BitLocker in Home per Kommandozeile?

Wenn das Tool manage-bde.exe auch in Windows Home enthalten ist und bloß ein paar Konfigurationsmenüs fehlen, warum nicht BitLocker unter Home einfach per Kommandozeile einrichten?

Leider fehlt mehr als nur die Menüs: Kommandozeilenschalter für manage-bde.exe, die Sie zum Erstellen und Verwalten von BitLocker bräuchten, verweigert das Tool unter Home mit einem Hinweis auf fehlende Unterstützung in Ihrer Edition.

Dass Microsoft in Home-Editionen nicht wenigstens die BitLocker-Einrichtung für USB-Medien erlaubt, wirkt im Jahr 2023 einigermaßen absurd – die Fähigkeit, ein portables Laufwerk vor fremden Blicken zu schützen, sollte zu den Grundfunktionen eines PC-Betriebssystems gehören. Der Schalter `-off` ist neben `-status` übrigens einer der wenigen, die auch mit der Home-Edition funktionieren.

Sicher unterwegs?

Reicht es im Hinblick auf Diebstahlschutz und ähnliches, einfach BitLocker einzuschalten, oder muss ich mehr beachten?

Sie müssen sich bei Windows per Kennwort, PIN oder ähnlichem anmelden. Haben Sie ein lokales Benutzerkonto, das ohne Kennwort direkt in den Desktop bootet, bringt Ihnen die Verschlüsselung nichts – jedenfalls nicht, solange das Systemlaufwerk beim Booten automatisch per Trusted Platform Module (TPM) entsperrt wird. Sie müssten dann zusätzlich ein Bootkennwort oder einen Schlüssel-Stick einrichten (siehe auch folgender Tipp).

BitLocker konfigurieren

Gibt es Dinge, die ich einstellen sollte, bevor ich Windows meine Laufwerke verschlüsseln lasse?

Hier gilt wieder einmal die Universalantwort: kommt darauf an! Jede Menge Optionen finden Sie im Gruppenrichtlinien-Editor im Ordner „Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/BitLocker-Laufwerkverschlüsselung“. Wenn Sie BitLocker zum Beispiel auf einem PC ohne Trusted Platform Module (TPM) einrichten wollen, müssen Sie im Unterordner „Betriebssystemlaufwerke“ die Richtlinie „Zusätzliche Authentifizierung beim Start anfordern“ aktivieren (eine weitere Konfiguration ist nicht nötig). Zum Systemstart brauchen Sie ein Kennwort oder einen USB-Stick mit einer Schlüsseldatei.

Ganz Vorsichtige finden zudem mit den Richtlinien zum „Verschlüsselungsmethode und Verschlüsselungsstärke für Laufwerk auswählen“ eine Möglichkeit, 256 Bit lange Schlüssel statt den voreingestellten 128-bittigen zu verwenden. Damit potenziert man die Zeit, die ein erfolgreicher Brute-Force-Angriff auf die Verschlüsselung bräuchte, doch der Sicherheitsgewinn ist Stand heute sehr marginal: Auch bei 128 Bit wären mit zurzeit verfügbarer Rechenleistung Millionen oder gar Milliarden Jahre erforderlich. Ansonsten sind viele der BitLocker-Optionen vor allem fürs Verschlüsselungsmanagement in Firmenumgebungen gedacht. *(jss@ct.de)*