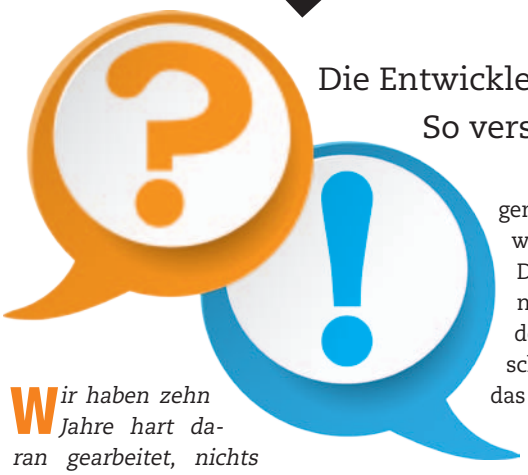
SICHER VERSCHLÜSSELN

FAQ: Truecrypt



Die Entwickler haben hingeschmissen. Truecrypt gibt es nicht mehr. So verschlüsseln Sie künftig Ihre Daten sicher. ■ WOLF HOSBACH

Wir haben zehn Jahre hart daran gearbeitet, nichts hält ewig“, entschuldigt David, einer der anonymen Entwickler des Verschlüsselungsprogramms Truecrypt, das Ende des Projekts (**bit.ly/1u54Msb**). „*Warnung: Truecrypt zu verwenden ist nicht sicher und kann unbehobene Sicherheitsprobleme enthalten*“, steht auf der Homepage. Nach dem Ende von XP, sei kein Verschlüsselungsprogramm mehr nötig, da Windows ab 7 die Funktion Bitlocker enthält.

Ist Truecrypt jetzt unsicher?

Die Frage ist derzeit schwer zu beantworten, denn es gibt außer der entsprechenden Vermutung auf der Truecrypt-Homepage keinen Hinweis auf eine Lücke (abgesehen von einem schon bekannten Angriff auf aktuell geöffnete Container. Schließen Sie daher Container immer, wenn Sie sie nicht mehr verwenden). Experten vermuten, dass der Hinweis auf der Tatsache beruht, dass das Tool nun verwaist ist und daher zwangsläufig auf Dauer unsicher wird. Alle verwendeten Algorithmen und Verfahren gelten als sehr sicher, Fehler könnten aber in der Implementierung liegen. Derzeit prüft eine Gruppe von Entwicklern den Code (**opencryptoaudit.org**). Dieses sogenannte Audit hat bislang noch keine gravierenden Lücken gefunden, die Prüfung aber noch nicht abgeschlossen. Die Gruppe hat angekündigt, das Verfahren weiterzuführen.

Soll ich Truecrypt weiter verwenden?

Derzeit ja. Aber achten Sie auf die Ergebnisse des Audits. Wenn diese negativ sind, sollten Sie wechseln. Außerdem sollten Sie sich auf Dauer ein neues Programm suchen, wenn keiner sich findet, der Truecrypt weiterentwickelt. Denn bei einem brachliegenden Projekt werden auch kleinere Fehler nicht mehr bereinigt.

Soll ich dem Rat der Entwickler folgen und Bitlocker verwenden?

Bitlocker ist eine Windows-Komponente, die ganz ähnlich arbeitet wie Truecrypt. Allerdings verschlüsselt es nur ganze Festplatten, sodass es beispielsweise nicht möglich ist, einen Container auf einen anderen Rechner zu übertragen, um ihn dort zu öffnen. Auch eine mobile oder Linux-Nutzung verschlüsselter Daten ist nicht möglich. Derselbe Angriff auf eine geöffnete Partition wie bei Truecrypt ist auch bei Bitlocker möglich. Außerdem besteht theoretisch die Gefahr, dass es eine Backdoor geben könnte, denn die Quellen des Programms sind nicht offengelegt. Konkrete Hinweise darauf existieren nicht. Für Windows-Anwender ist Bitlocker insgesamt eine gute Wahl.

Wie sicher sind die Alternativen?

Bekannte Verschlüsselungsprogramme sind beispielsweise Steganos Safe oder Archicrypt. Bei beiden sind keine Lücken oder Backdoors bekannt. Da sie nicht Open Source sind, besteht hier ein Restrisiko, das für Privatanwender jedoch gering ist. Zum Verschlüsseln einzelner Dateien eignet sich auch GnuPG/Gpg4win, das wiederum Open Source ist **www.gpg4win.de**.

Gibt es eine NSA-Backdoor?

Eine Verschwörungstheorie besagt, dass die Entwickler sich zurückgezogen haben, weil sie nicht mit der NSA kooperieren wollen. Darauf gibt es keinen belastbaren Hinweis. Die Audit-Gruppe würde außerdem eine Backdoor finden.

Wie geht es weiter mit Truecrypt?

Auch das ist derzeit schwer abzuschätzen. Aus dem Kreis der Audit-Gruppe gibt es Stimmen, die Truecrypt als Fork weiterführen wollen. Der oben zitierte Truecrypt-Entwicker rät davon ab, da seiner Meinung nach, der Code für Fremde zu undurchschaubar ist. Dennoch wäre es schade, wenn der Versuch nicht unternommen würde. Denn mit dem endgültigen Ende von Truecrypt würde die Welt ein vertrauenswürdiges und zuverlässiges Verschlüsselungsprogramm verlieren. **tr**

Bitlocker statt Truecrypt: Die Truecrypt-Homepage enthält nur noch eine Anleitung zum Umstieg.

Sicher mit Open Source: Zum Verschlüsseln einzelner Dateien lässt sich Gpg4win einsetzen.