IT-SYSTEME

Die Qual der Wahl bei Festplattenverschlüsselung

Wer Wert auf Datensicherheit legt, verschlüsselt sensible Daten. Egal ob E-Mails, einzelne Dateien oder ganze Festplatten. Gerade wenn es um letzteres geht scheiden sich jedoch die Geister. Die einen setzen auf Software kommerzieller Anbieter wie **BestCrypt** oder **BitLocker**. Andere bevorzugen Open-Source-Software und schätzen deren Transparenz und unabhängige Entwickler-Gemeinde.

Mit diesem Blogbeitrag gebe ich einen Einstieg in die Datei- und Festplattenverschlüsselung mit Open-Source-Software.

Das quelloffene, kostenfreie und plattformübergreifende Verschlüsselungstool **TrueCrypt** erfreute sich lange großer Beliebtheit. Einziges Manko war seinerzeit die Tatsache, dass Teile des ansich offenen Quellcodes, auch aufgrund ihrer Historie, mit unterschiedlichen Urheberrechten verknüpft waren. Zwar wurden diese unterschiedlichen Lizenzen zu einem Lizenz-Packet gebündelt um rechtliche Klarheit zu schaffen, jedoch war TrueCrypt nie offiziell eine „frei Software" im Sinne der „Open Source Initiative".

Im Mai 2014 kam jedoch der große Knall: Ein plötzlicher Rückzug der anonymen Entwickler. Auf der Homepage prangt seither nur noch die Warnung, dass Truecrypt möglicherweise unsicher wäre und man doch auf das Windows-eigene BitLocker umsteigen solle. Weitere Stellungnahmen blieben aus. Die Netzgemeinde war in Aufruhr, Gerüchte und

Verschwörungstheorien machten die Runde. Kann man dieser Software noch vertrauen? Wie sicher ist sie wirklich?

Ein Audit des „Open Crypto Audit Project" brachte Gewissheit. Nur relativ kleine Sicherheitslücken kamen zum Vorschein. Auch zwei später gefundene Schwachstellen greifen nur bei explizitem Zugriff auf den Computer und geöffnete Dateien. Damit können viele Nutzer leben und so erfreut sich selbst heute noch die letzte Version, TrueCrypt 7.1a, großer Verbreitung.

Doch wie steht es um die Weiterentwicklung? Gibt es inzwischen, fast zwei Jahre nach dem Ende von Truecrypt, brauchbare Alternativen?

Ja, die gibt es in der Tat! Zum einen wäre **DiskCryptor** zu nennen. Ein einfach zu bedienendes reines Windows-Tool. Auch wenn das Tool ursprünglich TrueCrypt-Code enthielt, ist es leider nicht (mehr) TrueCrypt-kompatibel. Zudem ist die jüngste Version dieses Tools schon über anderthalb Jahre alt und somit unwesentlich aktueller als die letzte TrueCrypt Version.

Wer Wert auf Kompatibilität mit TrueCrypt legt, sollte einen Blick auf die Erben von TrueCrypt werfen. Inzwischen haben sich drei Projekte mit unterschiedlichem Fokus herauskristallisiert.

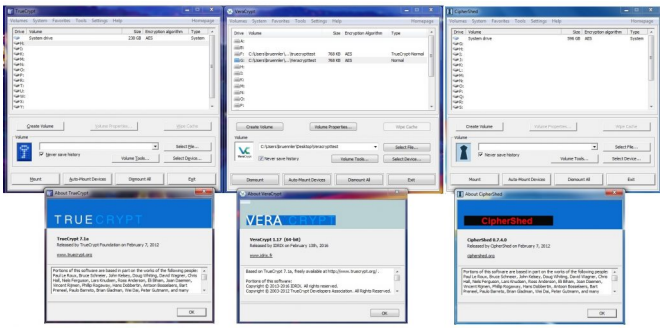
Der am wenigsten bekannte ist **GostCrypt** und setzt auf einen anderen Verschlüsselungsalgorithmus als sein Stammvater. Statt des im angloamerikanischen Raum weit verbreiteten AES- wird der ursprünglich von der UDSSR entwickelte GOST-Chiffre verwendet. Für 2016 ist eine CSPN-Zertifizierung (First Level Security Certification) in Frankreich geplant. Die aktuell herunterladbare Version ist jedoch auch schon über ein Jahr alt.

Der direkte TrueCrypt-Nachfolger **TCNext** ging irgendwann im Projekt **CipherShed** auf. Man wollte weg von allem, was mit dem unter TrueCrypt herrschenden Lizenz-Chaos zu tun hatte. Das Hosting erfolgt nun in der Schweiz, die Entwickler sind nicht anonym und der Name erinnert auch nicht mehr an den ehemals beliebten Vorgänger. Aktuell schreiben die Entwickler sukzessive den Quellcode um. Damit soll zum einen die Abwärtskompatibilität zu TrueCrypt gewahrt bleiben, zum anderen kann der dann völlig neue Code unter einer anerkannten Open-Source-Lizenz stehen. Auch wenn diese Arbeiten noch nicht abgeschlossen sind, kann bereits eine funktionsfähige Vorabversion 0.7.4 heruntergeladen und genutzt werden. Seinen Status als offizieller TrueCrypt-Nachfolger unterstreicht das Tool dadurch, dass nicht nur das „Look-and-feel" dem von TrueCrypt entspricht, sondern auch dass

während einer Installation von ChipherShed, bestehende TrueCrypt Installationen erkannt und aktualisiert werden. Eine Parallelinstallation zu TrueCrypt ist nicht möglich.

Am weitesten fortgeschritten ist das Projekt **VeraCrypt**, das aktuell in der Version 1.17 vorliegt. Der Fokus der französischen Entwickler liegt weniger auf dem Lizenzmodell, sondern auf einer konsequenten Weiterentwicklung des TrueCrypt-Codes. So ist man zum einen abwärtskompatibel, hat jedoch auch ein eigenes, verbessertes Format für Verschlüsselungscontainer entwickelt. Laut Aussage der Entwickler wurden außerdem die bisher in TrueCrypt entdeckten Schwachstellen geschlossen. Äußerlich unterscheidet sich VeraCrypt nur wenig von seinem „Vorfahr". Das Tool lässt sich jedoch problemlos parallel zu TrueCrypt (und CipherShed) installieren.

Welches der Tools man verwenden möchte ist sicherlich Geschmacksache. Die Ansätze sind jedenfalls vielversprechend. Die Zukunft wird zeigen, ob eines dieser Projekte die gleiche Stellung wie seinerzeit TrueCrypt erreichen wird. Die Probleme der Verschlüsselung von Systempartitionen unter UEFI/GPT sind bei allen Open-Source-Tools noch nicht gelöst. Hier haben die kommerziellen Tools wie BitLocker und Co. weiterhin die Nase vorne. Zumindest CipherShed und VeraCrypt haben diese Funktionalität jedoch auf ihrer Roadmap und CipherShed weißt explizit darauf hin, dass man aktuell an dieser Thematik arbeitet. Es bleibt also spannend.



Veröffentlicht am Mittwoch, 06.04.2016

AUTOR
Oliver Brünnler

Vielen Dank für Ihr Interesse.
Weitere Blog Beiträge finden Sie unter adiccon.de