idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Fraunhofer-Institut für Sichere Informationstechnologie SIT
Oliver Küch
12/10/2020
http://idw-online.de/en/news759746

Research results, Scientific Publications
Information technology
transregional, national

VeraCrypt mit leichten Mängeln

In der kostenlosen Open-Source-Verschlüsselungssoftware VeraCrypt wurden keine gravierenden Sicherheitslücken gefunden, allerdings gibt es Verbesserungsbedarf bei der Entwicklungspraxis und der Codequalität. Das ist das Ergebnis einer Sicherheitsanalyse der Expertinnen und Experten des Fraunhofer-Instituts für Sichere Informationstechnologie SIT in Darmstadt, die im Auftrag des Bundesamts für Sicherheit in der Informationstechnik BSI durchgeführt wurde. Die vollständigen Ergebnisse der Analyse sind in einer Studie zusammengefasst, die von der Webseite des BSI heruntergeladen werden kann: https://www.bsi.bund.de/DE/Publikationen/Studien/VeraCrypt/veracrypt.html.

Die beliebte Open-Source-Software VeraCrypt ermöglicht die Verschlüsselung von Festplatten sowie die Erstellung von verschlüsselten Containern, die Daten beinhalten. So können Daten auf einem Gerät vor fremdem Zugriff geschützt und auch sicher online verschickt werden, per E-Mail, über Dropbox oder ähnliches. „Diese Grundfunktionalitäten haben in keinem unserer Tests signifikante Sicherheitsprobleme gezeigt“, erklärt Dr. Steven Arzt, Leiter der Abteilung Sichere Softwareentwicklung am Fraunhofer SIT. Auch in den verwendeten VeraCrypt-Verschlüsselungsalgorithmen hatten die Forscher keine Schwachstellen gefunden.

Probleme in der Programmierpraxis

Allerdings bemängeln die Fraunhofer-Forscher die sehr fehleranfällige Art und Weise des Codierens, weil etablierte Praktiken und Richtlinien für die Entwicklung sicherer Software nicht berücksichtigt wurden. Der VeraCrypt-Code ist dadurch schlecht wartbar, wodurch gravierende Fehler in der Zukunft nicht ausgeschlossen werden können. „Wir empfehlen dem VeraCrypt-Projekt, bei der Implementierung von Verschlüsselungsfunktionen auf anerkannte und zuverlässige Open-Source-Bibliotheken umzusteigen, statt eigenen Krypto-Code zu entwickeln“, nennt Steven Arzt als Beispiel. Für den privaten Gebrauch sei VeraCrypt aktuell zwar sehr gut nutzbar, wenn im Zweifel auch flexibel auf eine andere Lösung gewechselt werden kann. Für den großflächigen Einsatz im Unternehmen sollte man allerdings die langfristige Entwicklerperspektive berücksichtigen, da hier ein möglicherweise notwendiger Wechsel mit hohem Aufwand verbunden ist. In jedem Fall empfehlen die Fraunhofer-Experten die Verwendung starker Passwörter.

Schutz vor Datendiebstahl

VeraCrypt biete vor allem dann einen guten Schutz, wenn Daten offline auf verschlüsselten Laufwerken gelagert werden, etwa auf einer Festplatte oder einem USB-Stick, so Steven Arzt. VeraCrypt schütze auch verschlüsselte Daten auf abgeschalteten Laptops, wenn diese gestohlen werden oder bei der Online-Übermittlung verschlüsselter Daten. VeraCrypt schützt aber prinzipbedingt nicht vor Angriffen auf ein laufendes System mit geöffnetem VeraCrypt-Container.

Das Fraunhofer SIT hat die Ergebnisse der Analyse vor ihrer Veröffentlichung dem Hauptentwickler des VeraCrypt-Projekts mitgeteilt. Einige der Empfehlungen der Fraunhofer-Forscher sind bereits in die aktuelle Version von

VeraCrypt eingeflossen.

Nachfolgeprojekt von TrueCrypt

VeraCrypt ist der Nachfolger des bekannten Projekts TrueCrypt, einer Verschlüsselungssoftware, deren Entwicklung 2014 plötzlich eingestellt wurde. VeraCrypt hat den größten Teil des Quellcodes von TrueCrypt übernommen und weist bis heute viele Ähnlichkeiten mit dem älteren Projekt auf. Das Fraunhofer SIT hatte 2015 – ebenfalls im Auftrag des BSI – bereits eine Sicherheitsanalyse von TrueCrypt durchgeführt. Die in TrueCrypt bekannten kryptografischen Mängel wurden mit dem Nachfolgeprojekt VeraCrypt größtenteils beseitigt. Die zuvor bereits bekannten Probleme in der Codequalität bestehen allerdings weiterhin.

Ergebnisse der VeraCrypt-Analyse: https://www.bsi.bund.de/DE/Publikationen/Studien/VeraCrypt/veracrypt.html

Ergebnisse der TrueCrypt-Analyse: https://www.bsi.bund.de/DE/Publikationen/Studien/TrueCrypt/truecrypt.html

Mehr zur Abteilung Secure Software Engineering: https://www.sit.fraunhofer.de/de/secureengineering/

contact for scientific information:
Dr. Steven Arzt

Original publication:
https://www.bsi.bund.de/DE/Publikationen/Studien/VeraCrypt/veracrypt.html