Martin Rost, Christian Krause

Relativer Vertraulichkeitsschutz mit TrueCrypt

Sollte man TrueCrypt nutzen, wenn Dateien gesichert vertraulich zu speichern sind? Diese Frage stellt sich mit neuem Druck seit Ende Mai 2014, als eine Meldung auf der Webseite der TrueCrypt Foundation überraschend die Einstellung der Pflege des Programms verkündete. Bislang war TrueCrypt nicht negativ aufgefallen, im Unterschied zu anderen Programmen mit vergleichbaren Funktionszusagen. Wir versuchen eine differenzierte Antwort zu geben, allerdings nicht durch eine Bewertung der von TrueCrypt verwendeten Kryptotechnik, sondern durch eine pragmatische Einschätzung möglicher Angreifer auf TrueCrypt-Container.

1 Einleitung

Auf der TrueCrypt-Webseite von sourceforge fand sich im Mai 2014 neben der Aufkündigung der weiteren Entwicklung auch die Empfehlung, anstelle von TrueCrypt Bitlocker zu nutzen. Fürsorglich wurde gleich eine Anleitung zur Konfiguration des Microsoft-Programms beigelegt. Die Diskussion über die Bedeutung dieser Aktion war kontrovers: Wurden die Entwickler unter Druck gesetzt, ihre Software aufzugeben, um die Nutzer in die Arme der NSA zu treiben? Oder sollten alle das nur denken, wo doch in Wirklichkeit TrueCrypt selbst eine Hintertür hat, die bloß noch nicht gefunden wurde? Tatsächlich wusste (und weiß) niemand, was von den Ansagen der TrueCrypt-Entwickler zu halten ist.[1] Ironischerweise trifft diese Unsicherheit hier ausgerechnet ein OpenSource-Projekt. Offenbar ist freier Quellcode alleine noch kein Indikator oder gar Garant für Vertrauenswürdigkeit. Als weitere Alternativen zu TrueCrypt werden gegenwärtig VeraCrypt oder das im Unix-Umfeld schon länger bekannte tcplay aufgeführt.

Seit den Snowden Leaks im Sommer 2013 stellt sich ganz generell die Frage nach der Sicherheit bzw. der Vertrauenswürdigkeit bislang etablierter Kryptotechniken. Ist die Verschlüsselung, wie sie von vielen Applikationen geboten wird, obsolet - man denke konkret etwa an 7zip oder an WPA2 der WLAN-Router oder an SSL im Browser oder Mailprogramm oder an VPN? Wird die Sicherheit, die bspw. gnupg zur Verschlüsselung von E-Mails bietet, überschätzt? Wie steht es um die Sicherung der Vertraulichkeit auch von Kommunikations- bzw. Metadaten durch JAP, Jondos, TOR? Wieviel Vertrauenswürdigkeit darf einem Steganografieprogramm wie F5 zugebilligt werden? Kurz: Woran können Verantwortliche in Organisationen und Privatnutzer, denen an Selbstdatenschutz gelegen ist, erkennen, dass die eingesetzte Software sicher und vertrauenswürdig ist?

Selbst wenn die Kryptoalgorithmen wissenschaftlich beurteilt weiterhin Schutz bieten, so sind die Programmiersprachen bzw. Libraries, die BIOS- und Bootmechanismen der Rechner, die CPUs, GPUs oder anderen Hardware-Komponenten, in denen Krypto-Algorithmen implementiert sind, sicherheitstechnisch objektiv vollständig intransparent. Sie sind für niemanden, der strukturell Vertrauenswürdigkeit beansprucht, tatsächlich prüffähig und insofern per se nicht vertrauenswürdig.[2] Wir wissen, dass die NSA Kryptostandards unterwandert hat[3]. Am TrueCrypt-Fall wird deutlich, dass auf den Prüfstand nicht nur Software und Hardware in all ihren Einzelheiten gehört, sondern auch jede Organisation, die Techniken standardisiert und Techniken im Namen der Allgemeinheit stellvertretend für andere prüft. Angesichts der schieren Menge von zu prüfenden Details und des Innovationstakts der Technik erscheint die Idee ei-

1 Die Diskussion um TrueCrypt lässt sich im lesenswerten Wikipedia-Artikel zu TrueCrypt nachvollziehen.

Martin Rost

Mitarbeiter im Technikreferat des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD, Kiel)

E-Mail: martin.rost@datenschutzzentrum.de

Christian Krause

Mitarbeiter im Technikreferat des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD, Kiel)

E-Mail: ULD38@datenschutzzentrum.de

2 Und zugleich gilt es, trotzdem derartige Analysen durchzuführen (vgl. Weber 2015). Andere Untersuchungen kamen zum Ergebnis: „In TrueCrypt 7.1a stecken keine Hintertüren" (vgl. iSEC Partners 2015).

3 Vgl. hierzu die Geschichte des Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG), http://de.wikipedia.org/wiki/Dual_EC_DRBG .

ner vollumfänglichen Prüfbarkeit, und damit einer Beherrschbarkeit sozusagen von einem Punkt aus, utopisch. Niemand ist in der Lage, das gesamte Setup tatsächlich zu überblicken und zu beurteilen. Jeder punktuelle Experte muss sich an einem bestimmten Punkt der Bearbeitung dieser Frage auf die Angaben anderer Experten verlassen und benutzt dabei implizit ein Angriffs- oder Vertrauensmodell. Das sind alles keine neuen Einsichten, nur wird aus unserer Sicht viel zu wenig über die Schlussfolgerungen daraus gesprochen.

Dass die Überprüfung von Sicherheitseigenschaften letztlich nicht möglich ist und man deshalb rein logisch zum Schluss kommen muss, dass es keine beurteilbare Sicherheit gibt, darf nicht zum Schluss führen, auf die Nutzung von Kryptotechniken zu verzichten. Es gilt, sich pragmatisch in der Unsicherheit einzurichten. Denn ein Verzicht des Aufbaus von Hürden erleichterte erst Recht die Aktivitäten der an den Daten interessierten Kriminellen. Aber vor allem erleichterte ein Verzicht die Zugriffe der sich zunehmend weniger an das Datenschutzrecht haltenden Unternehmen sowie der permanent am Rande der Legalität agierenden Sicherheitsbehörden und der faktisch unkontrolliert agierenden Geheimdienste.

Auch wenn die NSA vielleicht die gesamte technische Infrastruktur vom Telefon bis zum Toaster unterwandert haben sollte, kann Kryptotechnik durchaus Schutz vor Angreifern unterhalb des Niveaus von Geheimdiensten bieten. Auf der Ebene möglicher Alltags-Angreifer bzw. im unmittelbaren Kontext eines Nutzers bieten bspw. die Verschlüsselung von Word- oder pdf-Dokumenten oder eine Standard-De-Mail einen relativ ausreichenden Vertraulichkeitsschutz. Zugleich besteht kein Zweifel daran, dass die Nutzung von De-Mail weder vor unbefugten Zugriffen von IT-Herstellern, noch den Providern und staatlichen Behörden schützt.

2 Kriterien

Für die Risikoanalyse von TrueCrypt ziehen wir folgende Komponenten heran:

- Die sechs elementaren *Schutzziele*, mit denen die Anforderungen des Datenschutzrechts vollständig operationalisiert werden von dem Moment an, an dem eine gültige Rechtsgrundlage vorliegt, die das Verbot mit Erlaubnisvorbehalt im BDSG bzw. in den LDSG für ein personenbezogenes Verfahren punktuell aufhebt. Diese Schutz- bzw. Gewährleistungsziele lauten: Schutz der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit.
- Operationalisierung von Erforderlichkeits- und Angemessenheitsabwägungen durch drei *Schutzbedarfsabstufungen* „normal", „hoch" und „sehr hoch" in methodischer Anlehnung an den IT-Grundschutz des BSI. Allerdings mit der bedeutsamen Änderung, dass der primäre Schutz datenschutzrechtlich den Betroffenen gilt und nicht primär den Geschäftsprozessen einer Organisation.[4]
- Beachtung der *Verfahrenskomponenten* Daten, IT-System und Prozesse.
- Einen Katalog mit typischen *Angreifermotiven*. Diesen Katalog entnehmen wir der soziologischen Systemtheorie, die vier gesellschaftliche Funktionssysteme ausweist, die Organisationen mit strukturellen Motiven aufladen (vgl. Rost 2013).

Dieser Kriterienkatalog der Risikoanalyse orientiert sich an dem Standard-Datenschutzmodell (SDM) dessen Handbuch in der V.0.8 von der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) im Oktober 2014 verabschiedet wurde.[5]

Mit organisierten Angriffen auf Personen ist immer dann zu rechnen, wenn sich mit auswertbaren personenbezogenen Daten Geld verdienen lässt, wenn Macht politisch gesichert und rechtlich legitimiert werden soll oder wenn neues Wissen über Personen und soziale Prozesse verschafft werden kann. Aus Datenschutzsicht gilt deshalb methodisch, dass grundsätzlich jede Organisation als ein Angreifer auf die Grundrechte von Personen aufzufassen ist und sich diese Sichtweise eben nicht auf Hacker, im Streit ausgeschiedene Mitarbeiter oder auf Geheimdienste verengen darf. Jede Organisation sammelt heute Daten „ihrer" Bürger, Kunden, Patienten, Nutzer, Mitglieder, Zwangsinsassen und Mitarbeiter mit dem Ziel, eigene operative Risiken zu minimieren bzw. Risiken auf Personen als strukturell schwächere Risikonehmer abzuwälzen - gänzlich unbeeindruckt vom Verbot mit Erlaubnisvorbehalt.

Zudem sind die klassischen Randbedingungen für Angriffe zu beachten. Dazu zählt der Zugriff auf Ressourcen wie Techniken, Geld und Kompetenz sowie Zeit seitens der Angreifer. Zur Beurteilung der Risiken von Angriffen zählt aber auch, ob Angreifer dem Risiko von Prüfungen durch externe, unabhängige Stellen ausgesetzt sind. Zu beachten ist ferner, ob es ein Rechtssystem gibt, an das sich Betroffene aussichtsreich als Fallback wenden können, damit etwaige Schäden nachträglich behoben werden können. Dass es ein rechtliches Auffangsystem grundsätzlich gibt, ist jedenfalls der Kern eines jeden rechtstaatlichen Versprechens. Im nationalen Rahmen mag die Gerichtsbarkeit grundsätzlich noch funktionieren. Die Verlässlichkeit des EU-Rahmens ist angesichts insbesondere englischer Sonderwege unklar. Gegen amerikanische, russische, chinesische Hersteller bzw. Unternehmen, deren Aktivitäten das Internet bis in die kognitiven Prozesse und Körper jeder einzelnen Person hineinträgt, und erst Recht gegen die Geheimdienste dieser Welt hat realistisch derzeit niemand eine hinreichende Chance auf Intervention. Angreifermodelle auf Geschäftsprozesse von Organisationen sowie auf Personen werden typischerweise als Use-Cases modelliert und diese als wesentliche Komponente von Risikoanalysen beurteilt. Methodisch müssen Use-Cases immer dann herangezogen werden, wenn als notwendig zu beachtende Randbedingungen stark variieren können oder für eine Untersuchung unbekannt sind.

4 Daraus folgt, dass auch die in der Regel datenschutzrechtlich grundsätzlich zu begrüßenden Maßnahmen des IT-Grundschutzes den normativen Anforderungen des Datenschutzrechts zu folgen haben.

5 Die DSK hat den Autoren des SDM-Handbuches auferlegt, wegen der noch gegebenen Vorläufigkeit des Handbuchers die Herausgabe des Handbuches auf Experten zu beschränken. Der bislang fehlende Referenz-Maßnahmenkatalog des Handbuches soll bis zum Herbst 2015 vorliegen. Das SDM der DSK entspricht in den wesentlichen Aspekten der Vorstellung des SDM in der DuD 2012/06 (vgl. Rost 2012). Bei absehbar berechtigtem Bedarf an sofortiger Einsichtnahme in den aktuellen Stand des SDM wenden Sie sich bitte an Ihren Landesdatenschutzbeauftragten bzw. an die BfDI, Kontaktadressen unter www.datenschutz.de/institutionen/adressen/

Abbildung 1 | Typisierung von Angreifern und Bedrohungsszenarien

Angreifer	*Interesse an Daten*	*Technische Möglichkeiten*	*Prüfbarkeit / Sanktionierbarkeit*	*Kann Verschlüsselungstechnik Betroffene schützen?*
Freunde, Nachbarn, Kollegen, ScriptKiddies				Ja
Im gewerblichen Umfeld: Firmen-Konkurrenz			 im Inland	Ja
Arbeitgeber und dessen IT			 im Inland	Nein, da IT nicht vom Nutzer kontrolliert wird
Medizin-/ Sozialforschungsinstitute			 im Inland	Ja
IT-Dienstleister, Provider, Cloud-Betreiber			 im Inland	Ja, bei clientseitiger Verschlüsselung
Social Web			Im Inland ja, faktisch Nein	Ja, bei clientseitiger Verschlüsselung
Polizei, Staatsanwaltschaft, Verfassungsschutz			 im Inland	Bedingt
IT-Hersteller zentraler Komponenten (Compiler, Libraries, Betriebssystem)	 (abhängig vom Geschäftsmodell)			Nein
Nachrichtendienste (ND)				Nein

3 Angreifertypisierung

Will man nun eine Risikoabschätzung für TrueCrypt vornehmen, so gilt es, zunächst mögliche Angreifer auf Vertraulichkeit auszumachen. Abhängig von deren technischen Möglichkeiten und Motivationen lassen sich dann Aussagen zum Schutzniveau bzw. der Brauchbarkeit von TrueCrypt im konkreten Fall machen.

a) *Als stärkste, nicht abwehrbare Angreifer müssen IT-Hersteller und Geheimdienste angesehen werden.* Die Hersteller kontrollieren den Entstehungsprozess der eingesetzten Infrastruktur und können potentiell jedes System unterminieren. IT-Hersteller haben – abhängig vom jeweiligen Geschäftsmodell – unterschiedlich großes Interesse an personenbezogenen Daten. So betreiben reine Hardwareherstelller vermutlich keine Auswertung von Kundendaten, ihr Interesse an solchen Daten ist eher gering. Unternehmen wie bspw. Apple oder Google hingegen verknüpfen eben solche Auswertungen mit Herstellung und Vertrieb von Hard- und Software. Hier ist die Nutzung von Daten Teil des Geschäftsmodells und dient gleichermaßen der Monetarisierung wie der Entwicklung und Bereitstellung von Dienstleistungen.

Der gleiche Einflussumfang gilt für die Geheimdiente, die zwar vermutlich keinen unmittelbaren Zugriff auf die Herstellungsprozesse haben, dafür jedoch über insgesamt nicht kalkulierbare Ressourcen verfügen, sowohl personell als auch finanziell. Hinzu kommt bei ihnen ein exorbitantes Interesse an personenbezogenen Daten. Vor diesen Angreifern schützt eine Software wie TrueCrypt nicht. Wenn TrueCrypt keine direkten Sicherheitslücken aufweist, könnten diese Angreifer andere Wege finden, die Software anzugreifen (Hardware-Manipulation, unterminierte Krypto-Standards oder manipulierte Betriebssysteme). Und weil der Staat ein Gewaltmonopol besitzt bzw. zuletzt noch auf Militär zugreifen kann, kann sich der Staat immer Zugriff auf Daten verschaffen. Wenn TrueCrypt unbeabsichtigte Sicherheitslücken aufweist, könnten Geheimdienste diese als Zero-Day-Exploits nutzen. Wenn TrueCrypt beabsichtigte Sicherheitslücken enthält, sind Geheimdienste mit großer Wahrscheinlichkeit Veranlasser und Nutzer derselben.

b) Ausgestattet mit weniger Ressourcen als Geheimdienste und nicht am Herstellungsprozess beteiligt, gibt es eine Reihe *von mittelstarken Angreifern* auf Vertraulichkeit. *Social Web-Anbieter* beispielsweise zeichnen sich sowohl durch großen Datenhunger als auch umfassende technische Möglichkeiten aus. *IT-Dienstleister* bzw. *Provider* hingegen haben zwar als Betreiber von Teilen der Infrastruktur große technische Möglichkeiten, sind jedoch in der Regel weniger an den vertraulichen Inhaltsdaten ihrer Kunden interessiert. *Konkurrenz-Firmen* im gewerblichen Umfeld können mitunter ebenfalls erhebliche technische Ressourcen aufwenden, ihr Interesse an Daten kann im Einzelfall ebenfalls sehr hoch sein.

Vor diesen Angreifern kann eine Software wie TrueCrypt durchaus schützen, sofern keine bekannten, direkt verwertbaren Sicherheitslücken vorliegen. Wenn TrueCrypt unbeabsichtigte Sicherheitslücken aufweist, könnten bspw. Konkurrenz-Unternehmen Zero-Day-Exploits auf dem Schwarzmarkt einkaufen und nutzen. Dies setzt vermutlich große finanzielle Mittel sowie einen hohen Aufwand für die Beobachtung entsprechender Insiderkreise voraus. Wenn TrueCrypt beabsichtigt eingebaute Sicherheitslücken enthält, hat dieser Typ von Angreifer vermutlich keine Kenntnis darüber, schließlich waren sie nicht Veranlasser dieser Lücken.

Eine Sonderform von Angreifern stellen Arbeitgeber dar. Da sie die IT für ihre Mitarbeiter stellen und gleichzeitig ein großes Interesse an den Daten derselben haben, ist ein Schutz hier unmöglich, da der Mitarbeiter stets nicht vertrauenswürdige Hard- und Software nutzt. Der Arbeitgeber könnte sämtliche Schutzmechanismen aushebeln.

c) *Als schwache Angreifer auf TrueCrypt-Container stufen wir individuelle Hacker ein.* Einzelpersonen haben zwar oftmals ein großes Interesse an Informationen zu Personen ihres Umfelds, wobei vor allem Neugierde anzunehmen ist. Da die technischen Mittel hier vergleichsweise gering sind, bietet eine Software wie TrueCrypt ausreichenden Schutz. Wenn TrueCrypt keine direkten Sicherheitslücken hat, schützt es vor diesem Angreifertypus. Wenn TrueCrypt unbeabsichtigte Sicherheitslücken oder auch beabsichtigte Sicherheitslücken aufweist, schützt es trotzdem vor diesem Angreifertypus, weil dieser nicht in der Lage ist, diese Lücken zu nutzen. Natürlich kann es hier Ausnahmefälle geben, wenn besonders findige Hacker agieren. Das dürfte etwa die

Situation in den 80er und 90er Jahren gewesen sein, die das vorherrschende Bild, wem gegenüber der Schutz zu gelten hat, lange Zeit beherrschte.

Was folgt aus diesen noch groben Überlegungen oberhalb der reinen Experten-Diskurse bzgl. der kryptografischen Sicherheit? Für normalen Schutzbedarf kann man die Nutzung von TrueCrypt-v7.1a weiterhin empfehlen, solange sich die Faktenlage in Bezug auf etwaige Schwachstellen nicht ändert. Bei hohem Schutzbedarf von Daten, wobei hoher Schutzbedarf aus Datenschutzperspektive formuliert dann vorliegt, wenn Personen von Leistungen von Organisationen abhängig sind und sich Personen ohne diese nicht mehr helfen können, müssen Organisationen parallel zur Nutzung von TrueCrypt organisatorische Schutzmaßnahmen als Auffangmechanismen vorsehen. Wird TrueCrypt bspw. in einem Rechenzentrums- oder Cloudumfeld eingesetzt, kann der Diensteanbieter dem Nutzer Protokolle zuschicken über jeden Speicherzugriff auf den von TrueCrypt genutzten Speicherbereich. Das bietet keinen unmittelbaren Vertraulichkeitsschutz, hilft aber unberechtigte Zugriffe aufzuklären. Natürlich kann diese Maßnahme sehr leicht unterwandert werden. Es besteht aber eine Chance, dass ein solches Unterwandern zumindest im Nachhinein erkennbar wird, und dass dann ein solches Unternehmen als nicht vertrauenswürdig eingestuft wird, das falsche Auskünfte erteilt hat. Allerdings muss dann noch ein funktionierendes Rechtssystem oder zumindest eine Publizistik existieren, die einen solchen Diensteanbieter unter Rechenschaftsdruck setzt. Das entspricht der Funktion eines internationalen Gerichtshofs, der es ermöglicht, dass Kriegsverbrechen zumindest im Nachhinein verfolgt bzw. sanktioniert werden. Bei sehr hohem Schutzbedarf bzgl. der Vertraulichkeit von Daten, wenn also die Existenz von Personen durch Organisationen bedroht ist, sollten zusätzlich zum Einsatz von TrueCrypt und Protokollierungsmechanismen weitere Programme aus unterschiedlichen Quellen, in unterschiedlichen Programmiersprachen von unterschiedlichen Herstellern aus unterschiedlichen Ländern geschrieben kombiniert werden.

4 Fazit

Aus der Erkenntnis nicht garantierbarer Sicherheit folgt die Notwendigkeit, sich in eben jener Unsicherheit einzurichten. Fatalistische oder naive Sichtweisen sind in diesem Kontext nicht hilfreich. Nachvollziehbar gelingen kann das Arrangieren mit der Unsicherheit nur durch Analyse von Angriffsszenarien und entsprechend abgestimmten Schutzmaßnahmen.

TrueCrypt-v7.1a sollte bei normalem Schutzbedarf weiterhin eingesetzt werden; die grundsätzlich bestehenden Unwägbarkeiten der Alternativen sind nicht geringer – unabhängig vom Angreiferszenario. Sofern höherer Schutzbedarf besteht, sollten zusätzliche Vorkehrungen zur Sicherung der Vertraulichkeit getroffen werden. Es ist rational davon auszugehen, dass sich Hersteller zentraler IT-Komponenten (CPU, Compiler, Libraries) auf Datencontainer Zugriff verschaffen können. Und das bedeutet, dass sich der Gewaltmonopolist Staat wiederum an diese Hersteller halten kann, sobald die eigenen technischen Möglichkeiten erschöpft sind.

Literatur

iSEC Partners, 2015: *TrueCrypt Security Assessment*, https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf .

Rost, Martin, 2012: *Standardisierte Datenschutzmodellierung*; in: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 433-438.

Rost, Martin, 2013: *Zur Soziologie des Datenschutzes*; in: DuD - Datenschutz und Datensicherheit, 37. Jahrgang, Heft 2: 85-91.

Weber, Damian, 2015: *Alles ist geknackt ...alles? Nein!*; in: heise Security News vom 09.01.2015; http://www.heise.de/security/artikel/SSH-SSL-IPsec-alles-kaputt-kann-das-weg-2514013.html .