# Verschlüsselungssoftware gesucht

## Beitrag von „Super-Lion“ vom 5. Juli 2014 17:12

Hallo zusammen,

welche Verschlüsselungssoftware verwendet Ihr?
Bei uns am Seminar verwendet man Drag 'n' Crypt zum Verschlüsseln der Seminarberichte, wenn diese per E-Mail verschickt werden.

Kennt jemand True Crypt? Wenn ja, wie ist es? Wofür verwendet Ihr es.

Danke und viele Grüße
Super-Lion

---

## Beitrag von „Herr Rau“ vom 5. Juli 2014 17:49

Um Mails zu verschlüsseln: das Thunderbird-Plugin Enigmail, das auf OpenPGP basiert.
Material auf der Festplatte: TrueCrypt.
Wenn ich mal für jemanden etwas verschlüsseln muss, der kein PGP verwendet, nehme ich das Packprogramm 7zip, das ist eh mein Standard-Packprogramm. Kommt aber selten vor.

TrueCrypt: Für alle wichtigen Sachen, speziell mein Mail- und Browser-Profil und mein Passwort-Aufbewahrungsprogramm. Einige wenige Schülerdaten.

Bis ich das hier geschrieben habe, hat sicher schon jemand anderes die Geschichte von TrueCrypt erzählt. 

---

## Beitrag von „Bonzo21“ vom 5. Juli 2014 17:52

Hallo,
ich verwende axcrypt, wohl so ähnlich wie dein Programm. gut daran ist, dass ich pro Arbeitssitzung nur einmal das Passwort eingeben muss, alle verschlüsselten Dateien werden dann ohne Nachfrage geöffnet. Mir ist das wichtig, weil ich viel mit verschlüsselten Dateien arbeite, da immer das PW einzugeben ist nervig.

Meinen ganzen Krempel hab ich in der Cloud bei Wuala - End to end-Verschlüsselung!
Truecrypt verschlüsselt nicht einzelne Dateien, sondern legt einen Container an, in den dann die Dateien gelegt werden. Das Programm wird aber nicht weiterentwickelt. Außerdem benötigt es Admin-Rechte, ich kann also meine Stick-Dateien nicht an jedem Rechner öffnen (mit Axcrypt-portable geht das).
Ciao

---

## Beitrag von „Hawkeye“ vom 5. Juli 2014 18:05

Ich benutze seit einiger Zeit Boxcryptor in der Unlimited Personal Version, weil ich nicht so viel Zeit habe, mich einzulesen und einzufrickeln. Verschlüsselt halt meine Cloud(s), inklusive NAS-Daten, die ich mobil erreichen möchte.

Mein MacBook ist mit Hausmitteln verschlüsselt.

Meine Passworte landen in 1Password, das ich auf allen Geräten verwende.

Das mit der Mailverschlüsselung wollte ich demnächst mal angehen. Ich suche nur einen zum Testen :D.

---

## Beitrag von „Herr Rau“ vom 5. Juli 2014 18:46

> Zitat von Hawkeye
>
> Das mit der Mailverschlüsselung wollte ich demnächst mal angehen. Ich suche nur einen zum Testen

Wer mir eine verschlüsselte Mail schicken möchte, braucht meinen öffentlichen Schlüssel dazu, den hänge ich mal unten an. (Es gibt natürlich keine Garantie, dass nicht jemand diesen Schlüssel manipuliert und durch den eines anderen ersetzt hat, der sich zwischen den Sender und mich hängt und die Mails abfängt und liest, bevor er sie weiterleitet. Notfalls mich anrufen und Schlüssel vergleichen, das eindeutige Original habe ja ich.)

---

## Beitrag von „Hawkeye“ vom 5. Juli 2014 21:33

Obwohl ich das nicht ganz verstehe: Ich schicke meinen öffentlichen Schlüssel über Email. Das heißt, dieser kann doch, da nicht verschlüsselt, auch von allen möglichen Leuten eingesackt werden, um dann damit meine Emails zu lesen, auch wenn sie verschlüsselt sind.

Oder muss dafür mein geheimer Schlüssel passen?

---

## Beitrag von „Herr Rau“ vom 5. Juli 2014 21:54

> Zitat von Hawkeye
>
> Oder muss dafür mein geheimer Schlüssel passen?

Richtig. Ich habe das mal in einem Blogeintrag (http://www.herr-rau.de/wordpress/2013...bei-e-mails.htm) zu erklären versucht, das war aber prä-Snowden und ist immer noch viel zu technisch.

Deinen öffentlichen Schlüssel kann jeder wissen, deshalb kannst du ihn auch per Mail verschicken und auf deine Webseite stellen. Bei den bekannteren "("symmetrischen") Verschlüsselungsverfahren ist es so, dass man einen Schlüssel zum Verschlüsseln braucht und im Prinzip den gleichen, nur quasi andersherum, zum Entschlüsseln. Wer den Verschlüsselungscode kennt (alle Zeichen um eins nach rechts schieben), der kann auch leicht den Entschlüsselungscode (alle Zeichen wieder um eins nach links schieben) herausbringen.
Bei asymmetrischen Verschlüsselungsverfahren hilft dir der Verschlüsselungsschlüssel aber gar nichts, wenn es ums Entschlüsseln geht. Deswegen kann auch jeder eine Mail an mich verschlüsseln (mit dem öffentlichen, frei zugänglichen Schlüsselteil), aber nur ich kann sie entschlüsseln (mit meinem privaten Entschlüsselungsteil).

(Für Fortschreitenden: Ich kann die Nachricht aber auch mit meinem privaten Schlüssel signieren, und nur wenn mein dir ja bekannter öffentlicher Schlüsselteil dazu passt, dann weißt du, dass die Mail garantiert von mir stammt.)

---

## Beitrag von „Hawkeye“ vom 5. Juli 2014 22:20

Und für alle Anfänger: Für OS X gibt es die GPG-Tools / GPG-Suite, die Apple Mail umrüsten und diese Schlüssel erzeugen.

Bedeutet eine geringe Schwelle zum Einstieg.

https://gpgtools.org/gpgsuite.html

Uns spätestens jetzt erscheinen wir doch auf dem Bildschirm von irgendeinem, oder?

---

## Beitrag von „*Eichhoernchen*“ vom 6. Juli 2014 17:23

Wir haben von der Schule alle einen Stick mit truecrypt bekommen. Allerdings meine ich vor ein paar Wochen mal gelesen zu haben, das soll auch nicht mehr sicher sein. ICh hatte leider einen Vorfall damit, dass er kurzfristig den verschlüsselten Ordner nicht gefunden hatte und ich dachte alle Daten seien futsch. Nachdem ich die Gutachten erneut verbesser hatte, war der Ordner auf einmal wieder da

---

## Beitrag von „pintman“ vom 6. Juli 2014 17:32

Mit der alten Version von TrueCrypt kannst du noch arbeiten. Die neue Version ist im Moment zweifelhaft.

http://www.heise.de/newsticker/mel...er-2211037.html

---

## Beitrag von „Hawkeye“ vom 7. Juli 2014 07:14

http://pb21.de/2014/07/im-pra...rschluesselung/

Noch zum Thema.