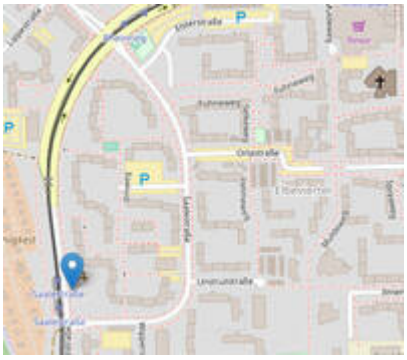
Veranstaltung, Krypto-Party, KP.2018.2

Krypto-Party [KP.2018.2]

Am: **2018-02-21 ab 18:00 Uhr** machen wir eine Krypto-Party!

Anfahrt / Adresse:

Im Nachbarschaftszentrum / Haus der Talente, Elbestr. 45 (Tram 3, Haltestelle: Saalestr.) Anfahrt:



Programm:

DRAFT 🔧 Fix Me!

LUKS / on Laptop / on Stick Passwortmanager Cryfs vs. encfs Veracrypt Verschlüsselte Verzeichnisse, auch für USB SSH / SSH-Keys handling

? TLS

Wir informieren worum es überhaupt geht und warum das Thema Verschlüsselung wichtig ist. Vorstellung der benötigten Software zum sicheren Email Versand. Austauschen und signieren vorhandener Schlüssel. Erzeugen neuer Schlüssel. Erste Schritte/Einweisung, und die Beantwortung eurer Fragen und nette Gespräche.

Da wir das Ganze zum ersten Mal machen, wird sicher einiges nicht optimal sein, wir bitten um Nachsicht.

Zusätzlich gibt es folgende Kurzvorträge:

- 18:30 Uhr: Marius: Warum GPG?
- 19:15 Uhr: Franke: GPG in der Praxis, Email-Verschlüsselung in Thunderbird mit Enigmail
- 20:00 Uhr: Marius, Franke: Forum / Eure Fragen, unsere Antworten

Sowie Speis' und Trank.

Was ist eine Krypto-Party (KP)?

Auf einer KP werden digitale Schlüssel signiert und/oder erzeugt mit denen sich dann der Email-Verkehr und Daten verschlüsseln lassen. Desweiteren wird über die Techniken und deren Anwendung informiert. Z.B.: wie man Email-Verschlüsselung benutzt, was das Web_of_Trust [WOT] ist, oder wie das Ganze überhaupt funktioniert.

Das 'Party' bezieht sich auf das turbulente Treiben und darauf, dass es auch oft einen Party ähnlichen Charakter hat und/oder mit einem Begleitprogamm versehen ist.

Public-Private-Key in Kürze

Das Programm GPG verwaltet ein Public-Private-Key Verschlüsselungsverfahren. Das heißt, dass zum Verschlüsseln von Nachrichten keine geheimen Informationen nötig sind. Jeder GPG-Nutzer erstellt ein Schlüsselpaar, das aus zwei Teilen besteht: Dem privaten Schlüssel und dem öffentlichen Schlüssel. Daneben gibt es noch eine Reihe von weiteren Helferprogrammen.

Dabei kann man sich den privaten Schlüssel als richtigen Schlüssel und den öffentlichen als das dazugehörige Schloss vorstellen. Anstatt nun einfach eine Email zu versenden - was in etwa wie eine Postkarte ist, macht GPG nun einen Umschlag darum der durch das Schloss verschlossen wird. Somit ist sichergestellt, dass nur noch der Besitzer des richtigen Schlüssels das Schloss entsperren und den Umschlag wieder öffnen kann. Die Schlösser (öffentlichen Schlüssel) können so beliebig verbreitet werden, damit einem auch Fremde sichere (verschüsselte) Nachrichten schicken können.

Umgekehrt besteht auch die Funktion unterschriebene (signierte) Nachrichten zu verifizieren. Dabei wird mit dem Private Key signiert und dies kann jeder der den Public Key hat, einfach überprüfen. So kann Bob sicherstellen das die Nachricht auch tatsächlich und unverändert von Alice kommt.

Das Web_of_Trust - also Netz des Vertrauens - kann einem Hinweise geben, ob man dem Schlüssel einer fremden Person vertrauen kann. Dazu kann jeder andere Schlüssel mit seinem Private Key unterschreiben - (!) was man nur tut wenn man sich sehr sicher ist (Ausweis geprüft?), das die zum Schlüssel gehörende Person auch die richtige ist; im Grunde verbürgt man sich dafür. Diese Unterschriften können - wie schon die öffentlichen Schlüssel - verteilt werden, damit jeder diese nutzen kann. So kann beispielsweise Bob darauf vertrauen, das der Key wirklich zu Maria gehört, wenn der von Alice unterschrieben ist; welcher Bob ja vertraut.

Mehr Informationen und Erklärungen dann auf der Party…

Teilnahmebedingungen:

Interessierte können sich per Voranmeldung registrieren oder einfach vorbeikommen.

Mitzubringen sind:

- Ein USB-Stick, mit/bez. für euren (neuen) digitalen Schlüssel
  - Wenn Ihr schon einen Schlüssel habt, reicht auch ein Zettel mit der Email-Adresse und dem dazugehörigem Key-ID nebst Fingerprint. Die Keys werden dann am nächsten Tag unterschrieben und zugesandt. Eine Ausgabe erzeugt Ihr z.B. mit folgendem Befehl:

```
gpg –fingerprint <Euer_Name|KEY_ID>

# Es werden nur folgende Informationen benötigt, Beispiel:

pub   1024D/12345678 2000-01-01
Schl.-Fingerabdruck = FFFF 1111 2222 BBBB AAAA  4444 5555 6666
7777 8888
uid       [ foobar] Dein Name (2000-01-01) <deine@email.tld>
... ggf. weitere Emails dazu
```

```
uid       [ foobar] Dein Name2 (2000-01-01)
<deine_anderen@emails.tld>
```

- Euren Ausweis, weil nur verifizierte Schlüssel unterschrieben werden.
- Evtl. euren Laptop um Thunderbird passend einzurichten, Schlüssel zu generieren, etc..

Wir freuen uns schon auf euren Besuch! 😀

Voranmeldungen:

Es wäre nett wenn ihr eine Voranmeldung abgeben würdet, damit wir ungefähr wissen mit wie vielen Leuten wir rechnen müssen. Vielen Dank!

Voranmeldung zum KP.2018.2
Dein Vor- und Nachname * Deine Email-Addy: * Anmerkungen: * Und nun 'anmelden' in dieses Feld schreiben! *
Bitte übertragen Sie die Buchstaben in das Eingabefeld. O Z T J K Dieses Feld bitte leer lassen
Voranmeldung absenden

Veranstalter:

Veranstalter ist die Braunschweiger - Linux-User-Group (kurz BS-LUG) und Freiwillige, unterstützt von FKN-Systems und dem Haus der Talente. Der Eintritt zur Veranstaltung ist frei.

Medien zum IP

- Plakat - Ankündigung: 

/ bs-lug_-_kp.2018.2.plakat.20180108.pdf

- Postcards - Ankündigung: 

/ bs-lug_-_kp.2018.2.plakat_postcards.20180108.pdf

Pressemitteilung

From:
https://bs-lug.de/ - **BS-LUG**

Permanent link:
https://bs-lug.de/activitys/2018/20180221_kp_cryptoparty/start?rev=1580924589

Last update: **2020-02-05 18:43**