

# Verschlüsselungsworkshop

Idee: Verschlüsselungsworkshop für Interessierte da das Thema gerade dank PRISM und TEMPORA wieder sehr aktuell ist.

Es folgt die - stichwortartige - Sammlung von Themenbereichen und Inhalten die man in einem Verschlüsselungsworkshop ansprechen kann oder sollte. Die eigentlichen Themen müssen noch weiter ausgearbeitet werden, und die endgültige Auswahl der Themen gegebenenfalls jeweils an den konkreten Vortrag bzw das Publikum angepasst werden.

## Durchführung/Planung

Passwort Sicherheit: Auf Flyer von Asta/c't verweisen. - Beispiele(konkret) warum sich verschlüsseln lohnt

Theoretischer Teil(max: 1h, eher 30min)

- Allgemeine Einführung Asymmetrisch / Symmetrische Verschlüsselung / Cäsar/Rot13 (Nerdgirl)
- Metadaten(Stu)

Hierbei Erwähnen: Komfort vs Sicherheit und Spenden für Tools & Diszipliniertes Verhalten Erwähnen

Praktischer Teil(~3h)

1. PGP/Enigmal + Thunderbird (sand)
2. Tor + httpseverywhere (Amnethyst)
3. OTR/Jabber (ands)
4. Dropbox/boxcryptor (stu)

Organisation

- Hand-Out erstellen
- Warpzone Vorlage für Präsentationen erstellen(Libreoffice o.ä.) (laura / phryk)
- Flyer erstellen
- Doodle für nächsten Termin (stu)
- Folien und ähnliches im git einchecken

Das Git findet sich unter [gitolite@warpzone.ms:cryptoworkshop](mailto:gitolite@warpzone.ms:cryptoworkshop)

Idee

- Thema an Schulen bringen

## Aufbau

- Theoretischer Teil unterteilt in (allgemeine) Einführung und die verschiedenen Bereiche. Jeder Teil sollte weit verbreitete Software vorstellen, auf möglicherweise vorhandene Probleme

hinweisen und möglichst eine sichere Alternative vorstellen.

- Praktischer Teil: Hilfe beim Installieren von ausgewählten Programmen.
- Anpassen der Themenbereiche während des Vortrags (Umfragen wer etwas nutzt) oder auch schon vorher (z.B: Vortrag an Uni; mehr SozialeNetze/Cloud/IM, BürgerNetz, mehr Email etc.)

## Allgemeiner Teil

- Zitate von Snowden/Manning etc.
- Beispiel, um zu zeigen wie man in den Fokus geraten kann: unkommentiert nach Begriffen suchen -> „Fehl“schlüsse sammeln -> Erläutern weshalb/wonach man wirklich suchte
- Schocken: z.B: Mitschneiden von unverschlüsselten Mails per Wireshark, Ethercap mitlaufen lassen, <https://en.wikipedia.org/wiki/Firesheep>
- Plausible Deniability(Truecrypt/OTR(?)/..)
- Asynchrone/Synchrone Verschlüsselung
- Bestandsdatenauskunft s. [heise](#)

## Kommunikation

### Email

- PGP / Enigmail (Dezentral) - including: Keysigning-party Quellen für Anleitung: [Metronaut](#)
- MIME (selbe Problem wie bei SSL)
- negativ Beispiel: DE-Mail - keine Ende-to-Ende Verschlüsselung
- Anonymer Briefkasten?

### Instant Messaging

- Jabber / OTR
- Whatsap / Alternativen(Threma?)

### VOIP

- Skype [Vorsicht beim Skypen - Microsoft liest mit](#)
- Alternativen?

### anonyme Kommunikation

- toter USB „Briefkasten“

## Soziale Netze

- Facebook
- G+

- Twitter
- Grundsatzfrage: Klar machen was man online stellt. Bewusst alles (an solchen Orten) öffentlich stellen.
- Beispiel: (Deutsches) Au-Pair wird an Amerikanischer Grenze nach Hause geschickt nach (schwarz)Arbeit Verabredung über Facebook
- Alternativen? Eher nicht

## Cloud(Services)

- Dropbox etc.
- Boxencrypter/TrueCrypt o.ä.
- selber hosten? → Private Cloud z.b. owncloud o.ä.? nur kurz
- Schnittstelle zum Anzapfen direkt eingebaut → Beispiel M\$

## Metadaten

- Implikationen?
- Beispiel: Malte Spitz → Handy-Bewegungsdaten siehe [Netzpolitik](#) und [Zeit.de Visualisierung Artikel wie CIA Agent mithilfe von MetaDaten geschnappt werden](#)
- Vermeidung quasi nicht möglich

## WWW/Surfen

- TOR
- VPN/Proxy
- CCC Anonymiser(Name? Ähnlich TOR? → Stuc fragen)

## Passwörter

- Datenbank/Keepass
- Auswahl des Passworts/Wie Merken?/Was ist ein sicheres Passwort?/Nie dasselbe Passwort auf mehreren Seiten nutzen!
- Artikel in der c't [Passwort Schutz für jeden](#)

## Ausführung: physische Sicherheit

- Schlüssel
- Keylogger
- Vollverschlüsselung
- ...

# Quellen

- [Cryptoparty Handbuch](#) und [Flyer](#) als Mögliche Quelle via ML sowie <http://www.cryptoparty.in/index> auch gut [Security in a box](#)
- Software: [Übersicht von Software und freien alternativen](#) sowie [Suche nach alternativen zu bekannter Software](#)

From:

<http://wiki.warpzone.ms/> - **warpzone**

Permanent link:

<http://wiki.warpzone.ms/projekte:verschluesselungsworkshop?rev=1405436703>

Last update: **01.03.2017**

