CryptoParty

in Erlangen

12. Juli 2014

Diese Checkliste soll euch einen groben Leitfaden für verschiedene Themengebiete geben. Alle empfohlene Software haben wir heute für euch unter `http://172.16.100.10/crypto` gesammelt. Wir werden zu jedem Thema kleine Gruppen bilden, in denen wir die Software gemeinsam einrichten und praktisch ausprobieren, diese Checkliste soll euch primär einen groben Überblick geben.

E-Mail-Verschlüsselung mit GnuPG (GPG, OpenPGP)

- □ Für Windows: GPG4Win installieren: `https://www.gpg4win.de/`
  GPG4Win enthält die Verschlüsselungssoftware GnuPG
- □ Für Mac OS X: GPGTools (GPG Suite): `https://gpgtools.org/`
- □ Für Linux: gnupg und Mailprogramm installieren
- □ Mailprogramm einrichten:
  Damit ihr GnuPG im Alltag bequem verwenden könnt, müsst ihr ein Mailprogramm verwenden. Manchmal benötigt dieser ein Plugin, um Verschlüsselungsunterstützung nachzurüsten. Für Windows gibt es viele Möglichkeiten:
  - Thunderbird `http://www.mozilla.org/de/thunderbird/` → Enigmail (`https://www.enigmail.net/home/index.php`
  - Outlook → das Plugin in GPG4Win enthalten
  - Claws Mail → Benötigt kein Plugin
  - andere Mailprogramme: (Windows Mail, Webmail, ...): Häufig schwierig

  Falls ihr noch kein Mailprogramm eingerichtet habt, empfehlen wir Thunderbird.
- □ Schlüssel erzeugen:
  - 4096 Bit Schlüssellänge
  - Ablaufdatum sinnvoll (kann jederzeit verlängert werden)
- □ Eventuell: Schlüssel auf einen Keyserver hochladen
- □ Wichtig: GPG signiert nur den Inhalt einer Mail, nicht den Betreff!

Benutzung von Tor Wenn ihr Tor verwenden wollt, empfiehlt es sich sehr, das Tor-Browser-Bundle (`https://www.torproject.org/projects/torbrowser.html.en`) zu installieren. Es enthält einen Browser, der bereits fertig eingerichtet ist, Tor zum Zugriff auf das Internet benutzt und so konfiguriert ist, eure Privatsphäre zu schützen.

Tails Tails (**T**he **a**mnesic **i**ncognito **l**ive **s**ystem, `https://tails.boum.org/`) ist ein Betriebssystem, das ihr von einer CD oder einem USB-Stick starten könnt und das keine Spuren auf eurem System hinterlässt. Es enthält alle Software, die ihr benötigt, um sicher kommunizieren zu können (z. B. Tor, GPG, ...). Wir haben mehrere USB-Sticks und ein paar CDs mit Tails, so dass ihr Tails direkt ausprobieren könnt.

Passwortverwaltung Wenn ihr Wert auf sichere Internetnutzung legt, ist eine sinnvolle Passwortnutzung unumgänglich. Unsichere oder wiederverwendete Passwörter sind eines der größten Sicherheitsprobleme. Das bedeutet, dass ihr Passwörter auf keinen Fall wiederverwendet und wenn möglich zufällig erstellt.

Es gibt Programme, die euch dabei unterstützen, da sich niemand für jede Seite ein eigenes Passwort merken kann.

- Eine beliebte Wahl ist KeePass2 (Windows: `http://keepass.info/download.html`) und KeePassX (Linux, Windows, Android: `http://www.keepassx.org/`).
- Auch die in vielen Browsern integrierten Passwortverwaltungen sind sinnvoll, haben aber den massiven Nachteil, dass sie meistens keine Passwörter generieren können und deshalb dazu verleiten, weiterhin unsichere Passwörter zu verwenden.