Aufteilung der Teilnehmer

Die Teilnehmer sollten so sortiert werden, dass Leute mit gleicher Konfiguration nebeneinander sitzen, also

- Windows-Nutzer, Mac-Nutzer und Linux-Nutzer
- Thunderbird-Nutzer und Apple-Mail-Nutzer

Wenn man dann immer noch die Auswahl hat, bietet es sich an, möglichst einen versierten Computernutzer neben einen oder zwei andere zu setzen. Außerdem sollte man gleich zu Beginn klären, welche Teilnehmer Ambitionen haben, die Technik später anderen beizubringen, damit diejenigen das, was an ihrem eigenen Rechner passiert ist, danach bei anderen Teilnehmern machen – erst unter Aufsicht, danach alleine. Das dürfte auch Zeit sparen.

Softwareverteilung

Insbesondere bei größeren Teilnehmerzahlen bzw. einem ungünstigen Teilnehmer-Helfer-Verhältnis bietet es sich an, schon vor Beginn den eintreffenden Teilnehmern, die einen USB-Stick dabei haben, die Software (usw.) darauf zu kopieren, weil das schneller geht, als mit Sticks rumzugehen und von dort auf die Rechner zu kopieren.

Vorbereitung

Oft haben sich nicht alle . Die Teilnehmer sollten deshalb zu Beginn daran erinnert werden, was benötigt wird, damit sie sich darum kümmern, bevor die entsprechenden Daten oder Entscheidungen benötigt werden.

ggf. kurzer Einführungsvortrag

Wenn die verfügbare Zeit unkritisch ist, kann es eine kurze Kryptografie-Einführung geben. Das ist aber nicht immer sinnvoll. Es kostet auf jeden Fall Zeit, ist nicht leicht verständlich und hilft für den Praxisteil erfahrungsgemäß nur wenig, verbraucht aber einen Teil der begrenzten Aufnahmekapazität der Teilnehmer.

Auf jeden Fall sollte etwas zu dem Sicherheitsniveau gesagt werden, das den Teilnehmern geboten wird, und was in dem Zusammenhang zu beachten ist (Systemsicherheit).

Umfang der Erklärungen

Als Dozent hat man verständlicherweise einen starken Drang, das zu erklären, was man gerade macht. Das erhöht sicherlich den Nutzen für die Teilnehmer beträchtlich, verbraucht aber in der Praxis unglaublich viel Zeit. Etwas am Beamer mit Erklärung vorzumachen und auf die Teilnehmer zu warten, dauert zumeist länger, als es kommentarlos schnell selber an allen Rechnern einzurichten. Die schnelle Variante bietet sich vor allem bei denen an, die nicht planen, anderen dabei zu helfen, sondern es nur selber benutzen wollen. Wenn die Teilnehmer einen XMPP-Supportzugang haben, ist der Verlust auch weniger schlimm. Wenn am Ende Zeit übrig ist, kann man immer noch erklären. Da das Interesse der Teilnehmer meist primär auf OpenPGP gerichtet ist, sollte man eher das mit Erklärung am Beamer machen (wobei ein XMPP-Supportraum hilfreich ist) und den XMPP-Teil, der vor allem Hilfsmittel ist, zügig durchziehen.

XMPP-OTR (Pidgin/Adium)

Zunächst wird den Teilnehmern Pidgin (plus OTR; Windows / Linux) bzw. Adium (Mac) installiert. Das ist einfacher und schneller erledigt als der OpenPGP-Teil. Die Teilnehmer lernen dort, in einem einfacheren Kontext, was Fingerprints sind, haben schnell ein Erfolgserlebnis, sind beschäftigt und bekommen für später einen Support-Account als Kontakt. Außerdem können sie darüber später ihre OpenPGP-Fingerprints austauschen.

Wenn jemand einen Mailaccount bei einem Anbieter hat, der XMPP direkt mit zur Verfügung stellt (z.B. GMX, web.de, Google), dann bekommt er erst mal dort einen Account, ansonsten bei einem der kostenlosen Anbieter.

Erzeugung der Offline-Hauptschlüssel

Haben sie Zertifikate / Fingerprints (aus sicherer Quelle!) dabei, die gleich signiert werden sollen?

Vorbereitung der sicheren Systeme: Nicht vergessen, vor dem Booten die Netzwerkverbindung zu kappen!

Anbieten, gleich zwei Schlüssel zu erzeugen: einen Alltagsschlüssel und einen Hochsicherheits-Schlüssel.

Mailclient-Einrichtung (Enigmail)

- Schlüssel importieren (oder über die Schlüsselverwaltung(!) erzeugen)
- Enigmail (o.Ä.) konfigurieren
- Schlüssel auf den Keyserver hochladen
- Hinzufügen von Kontakten üben
- Crypto-Werbung in die Textsignatur
- Nachbereitungsseite zeigen und als Bookmark anlegen

Fingerprintzettel

Wenn die verfügbare Zeit es erlaubt und ein Drucker verfügbar ist, sollten den Teilnehmern Fingerprintzettel (PDF) ausgedruckt werden – weil die meisten es sonst sowieso nicht machen.