Strategien der Krypto-Qualifizierung

- Was ist der aktuelle Stand?
- Ansätze zur Verbesserung
- Was ist zu vermitteln?
- technischer Änderungsbedarf

www.openpgp-schulungen.de
www.crypto-fuer-alle.de

Strategien der Krypto-Qualifizierung

- Was ist der aktuelle Stand?
- Ansätze zur Verbesserung
- Was ist zu vermitteln?
- technischer Änderungsbedarf

der quantitative Erfolg

- Damit sich die Qualität des deutschen Internet merklich ändert, brauchen wir in spätestens 10 Jahren 10 Millionen Nutzer von Kryptografie.
- Das heißt für Berlin: 50.000 neue Nutzer pro Jahr. Nutzer, nicht bloß Schulungsteilnehmer!
- Die Realität 2013: <500 Schulungsteilnehmer
- www.cryptoparty.in/location

Warum ändert sich nichts?

- Henne-Ei-Problem der einzelnen User: keine Krypto-Kontakte → Teilnahmehemmung und Verluste nach der Schulung
- Nur solche Teilnhmer, die sich eigenständig entschieden haben, etwas zu ändern
- Kein Bedrohungsgefühl, wenn man zu den 99% gehört
- Kein flächendeckendes Schulungsangebot

Strategien der Krypto-Qualifizierung

- Was ist der aktuelle Stand?
- Ansätze zur Verbesserung
- Was ist zu vermitteln?
- technischer Änderungsbedarf

Was muss passieren?

- Wie werden wir zwei Größenordnungen besser?
  - Sichtbarkeit des Themas **im Alltag**
  - Bestehende Gruppen schulen
    - besser für die Teilnehmer
    - Verstetigung der Schulung in der Organisation
  - Gruppenzwang statt Überzeugung
  - Vernetzung der Lernenden (Verluste minimieren)

Sichtbarkeit des Themas

- www.crypto-fuer-alle.de/wishlist/sichtbarkeit/
- alle sind gefordert, Personen & Organisationen
  - insbesondere die Schulungsteilnehmer
- Links (Web, E-Mails, kryptotaugliche Software):
  - Informationen: www.openpgp-schulungen.de/fuer/alle/
  - Schulungsangebote: www.cryptoparty.in/location#germany
  - Förderung: www.openpgp-schulungen.de/fuer/unterstuetzer/
- ein Symbol

ein Symbol für IT-Sicherheit

- www.crypto-fuer-alle.de/wishlist/mitmach-symbol/
- sehr allgemein: „Ich kümmere mich aktiv um meine digitale Sicherheit!“

bestehende Gruppen

- Hochschulen
  - Erstsemester! (Gruppenzwang)
  - Es geht los: krypto.mi.fu-berlin.de/
  - www.openpgp-schulungen.de/fuer/hochschulen/
- Schulen
  - www.openpgp-schulungen.de/fuer/schulen/
  - www.openpgp-schulungen.de/erfahrungen/schulen/
- Unternehmen, Vereine

Strategien der Krypto-Qualifizierung

- Was ist der aktuelle Stand?
- Ansätze zur Verbesserung
- Was ist zu vermitteln?
- technischer Änderungsbedarf

typisches Szenario

- Einsteigerniveau (unsichere Hauptschlüssel)
- alles soll schön einfach sein → kaum Sensibilisierung für die übergeordneten Strukturen der Sicherheitsproblematik
- Cryptoparty-Teilnehmer
  - bereiten sich nicht auf die Veranstaltung vor
  - Entwickeln sie sich danach weiter?

Warum ist das ein Problem?

Bruce Schneier:
„Security is a process, not a product.“

- Die Sicherheit, die man unterm Strich hat, kommt zu
  - 10% aus der verwendeten Technik
  - 60% daraus, dass man (immer!) weiß, was man tut
  - 30% aus der Disziplin, das Wissen zu beachten

Einfachheit vs. Sicherheit

- Das Thema hat eine hohe Komplexität.
- Die kann man nicht verstecken, nur ignorieren.
- Gefahr: Illusion von Sicherheit
- Software kann dem User nicht das Verständnis dessen abnehmen, was er tut. Nicht heute; nicht, ohne ihn zu entmündigen.

Was braucht die Masse?

- Es ist **nicht** sinnvoll, alles zu verschlüsseln.
- Alle müssen verschlüsseln **können.**
- Metadaten-Vermeidung meistens unnötig
- Monopolisierung vermeiden (Threema)
- verinnerlichen: Einfache Lösungen bieten nur begrenzte Sicherheit
- einen Entwicklungspfad fürs Krypto-Lernen

Was ist als Einstieg sinnvoll?

- Neulinge müssen weder Softwareeinrichtung noch Schlüsselerzeugung verstehen
  - kann also auch kompliziert sein
- Sie sollten Technik bekommen, an der sie wachsen können
  - Fehlendes Verständnis ist nicht schlimm, wenn daraus kein Sicherheitsrisiko erwächst
- Schulungsempfehlung (OpenPGP & XMPP):
  - www.openpgp-schulungen.de/inhalte/einrichtung/materialien/

„Das ist zu kompliziert“

- Kryptografie ist in brauchbarer Anwendung nicht komplizierter als die Erstellung eines Serienbriefs.
- Sie erscheint nur kompliziert, weil die Leute ohne Vorwissen mit so viel Neuem konfrontiert werden.
- Mögliche Lösung: gestreckte Schulungen (Schule, Uni, online): zwei Wochen lang 5–15 Minuten pro Tag. Wenig lernen, gleich üben.

Strategien der Krypto-Qualifizierung

- Was ist der aktuelle Stand?
- Ansätze zur Verbesserung
- Was ist zu vermitteln?
- technischer Änderungsbedarf

Alptraum Standardsoftware

- Enigmail
  - Standardeinstellung: allen Schlüsseln vertrauen
- GPGTools
  - keine Anzeige des Fingerprints beim Signieren von Schlüsseln
- Die großen Erfolge der Vereinfachung?
- GnuPG zeigt die Zertifizierungsqualität nicht an.
- Kein GUI kann Offline-Hauptschlüssel.

Sicherheitslevel und Transparenz

- www.crypto-fuer-alle.de/wishlist/securitylevel/
- Die Anforderungen schwanken extrem; sogar beim selben User. Die Technik muss dem Rechnung tragen.
- Sicherheit ist nur mit Transparenz des Sicherheitsniveaus sinnvoll möglich.
- Das heißt: mehrere Schlüssel für dieselbe Adresse

einheitliche Einteilung

- nutzbar für
  - die Bewertung der Schlüsselsicherheit
  - die Bewertung der Systemsicherheit
  - die Bewertung der Authentizität von Zertifikaten
  - die Bewertung der User (Konfiguration)
- Unsichere Schlüssel / Systeme oder kaum verifizierte Schlüssel sind nicht automatisch schlecht, sondern müssen zur Situation passen. Transparenz für alle Beteiligten!

Danke fürs Zuhören

- www.openpgp-schulungen.de/fuer/unterstuetzer/
- www.crypto-fuer-alle.de/wishlist/
- Machen Sie was! Es gibt keine Ausreden!