CryptoParty

Verschlüsselung und Passwortschutz zum Schutz der Privatsphäre

CryptoParty

CampusGrün Hamburg

Uni Hamburg

CryptoParty

Motivation 1

Betroffen sind z.B.:

- Bürgerinnen und Bürger
- Unternehmen
- Organisationen
- verschiedene Berufsgruppen

Gefährdet sind z.B.:

- das Recht auf informationelle Selbstbestimmung
- das Post- und Fernmeldegeheimnis
- die Pressefreiheit
- das Betriebs- oder Geschäftsgeheimnis

CryptoParty

Konsequenz

- Wir verschlüsseln unsere Daten
  - E-Mails auf dem Weg durchs Internet
  - Daten in der Cloud
  - Webseitenzugriffe
  - Chats.

- Verschlüsselung darf kein Verdächtigkeitskriterium sein. Deswegen grundsätzlich verschlüsseln!

CryptoParty

Motivation 3

Verlust von Sicherheit durch Fehler im Umgang mit Passwörtern.

- zu kurze Passwörter
- leicht zu erratende Passwörter
- wenn andere unsere Zugangspasswörter nicht vertraulich behandeln.

CryptoParty

Grundlagen von Verschlüsselung

Verschlüsselung kann dafür sorgen, dass Daten

- gegenüber Dritten geheim bleiben
- unverändert / echt sind
- erkennbar tatsächlich von einer bestimmten Person/Organisation stammen

CryptoParty

Einsatzzwecke und Grenzen von Verschlüsselung

Verschlüsselung kann Inhalte sichern. Z.B.
- auf Datenträgern
- in E-Mails oder Chats

Verschlüsselung schützt oft nicht vor dem Sammeln von Metainformationen bzw. Verkehrsdaten.

Verschlüsselung ist wirkungslos, wenn
- auf Eurem Gerät ein Trojaner /Virus ist..
- Ihr an einem fremden Computer z.B. im Internet-Cafe sitzt.

CryptoParty

Was macht Verschlüsselung schwierig?

- auf ein gemeinsame Technik einigen
- Programme dafür installieren
- Authentizität herstellen
  (wissen, dass man wirklich mit Hans und nicht mit der NSA verschlüsselt kommuniziert)
  => Fingerabdruckvergleich
- Schlüssel austauschen

CryptoParty

Wir erkunden heute gemeinsam

- Sicherer Umgang mit Passwörtern
- E-Mail-Verschlüsselung mit GnuPG und Enigmail

… man kann noch mehr tun

… heute Abend reicht die Zeit dazu nicht

CryptoParty

Organisatorisches

Bitte diejenigen mit gleichem System zusammensetzen,

- dann könnt Ihr einander behilflich sein,
- oder jemand von uns kann Euch gemeinsam helfen.

Links zu Software-Downloads und unsere E-Mail-Adresse

- http://Mafiasi.de/CG-CryptoParty

CryptoParty

1. Symmetrische Verschlüsselung

Alle, die im Besitz des Schlüssels sind, können Inhalte verschlüsseln und entschlüsseln.

- Zur Veranschaulichung: Alle, die den Schlüssel zu einer Tür haben können diese öffnen und im Raum dahinter Dinge hinterlegen oder sie herausnehmen.
- Password-Speicher, KeePass (machen wir noch)
- Beispielsweise Festplattenverschlüsselung verwendet dieses symmetrische Verfahren.

CryptoParty

2. Asymmetrische Verschlüsselung

- Es gibt zwei Schlüssel (Schlüsselpaar)
  - Den öffentlichen Schlüssel (verschlüsseln)
  - Den privaten Schlüssel (entschlüsseln)
- Nur der Inhaber eines privaten Schlüssels, kann die mit dem zugehörigen öffentlichen Schlüssel verschlüsselten Inhalte entschlüsseln.
- Veranschaulichung: Ein öffentlich angebrachter Briefkasten, in den jeder Inhalte einwerfen kann, kann nur von seiner Besitzerin geöffnet werden.
- Beispielsweise E-Mail-Verschlüsselung verwendet (vorwiegend) dieses asymmetrisches Verfahren.

CryptoParty

Folien-Lizenz

Autoren: Moritz Duge, Jens-Uwe Möller, Patrick Hanft,
Otfried Hilbert