GPG-Signaturen überprüfen

Eigentlich sollte man niemals Dateien aus dem Internet herunterladen und einfach auf dem eigenen Computer installieren. Linux-Nutzer*innen sollten immer die Paketverwaltung ihres Betriebssystems benutzen, die sicherstellt dass die installierten Pakete vertrauenswürdig sind.

Manchmal ist das aber nicht möglich, zum Beispiel wenn man Windows verwendet. Besonders für sicherheitskritische Software, wie den Tor Browser oder die Passwortverwaltung KeePassXC ist es üblich, die Installations-Datei mit einer digitalen Signatur zu versehen. Dadurch können andere überprüfen, ob die Datei die sie heruntergeladen haben auch tatsächlich der*dem Entwickler*in der Software stammt und keien Schadsoftware beinhaltet.

Für die Überprüfung einer Signatur musst du GnuPG (Gnu Privacy Guard) installiert haben. Auf Linux-Systemen ist GnuPG vorinstalliert. Windows-Nutzer*innen müssen vorher GPG4Win installieren, für Mac gibt es die GPG-Suite

1. Schritt: Datei und Signatur besorgen

Lade zunächst Datei und Signatur herunter und **speichere sie im selben Verzeichnis ab**. Eine Signatur-Datei hat immer denselben Namen wie die ursprüngliche Datei mit dem Zusatz „.sig“ oder „.gpg“. Die Signatur-Datei zu einer Datei namens *Tor_Browser.exe* heißt dann etwa *Tor_Browser.exe.sig*

2. Schritt: Signatur überprüfen

2.1 Überprüfung mit grafischer Oberfläche

Es gibt für GnuPG verschiedene grafische Frontends, die es dir ersparen Befehle ins Terminal einzugeben.

Windows

Bei der Installation von GPG4Win wirst du gefragt, ob du Kleopatra oder GnuPrivacyAssistend als grafische Oberfläche mitinstallieren möchtest. *Kleopatra* ist wesentlich benutzer*innenfreundlicher und erweitert das Kontext-Menü (Rechtsklick-Menü) deines Dateibrowsers um die wichtigsten GPG-Funktionen.

Du kannst nun einfach das Verzeichnis öffnen, die Signatur-Datei mit Rechtsklick auswählen und „Entschlüsseln/Überprüfen“ auswählen.

Weiter unter Schritt 3.

Linux

Linux kannst du Kleopatra oder Seahorse verwenden.

Kleopatra

- integriert sich sehr gut in Kubuntu und andere KDE Desktops.
- installiere dafür das Paket `kleopatra`

Seahorse

- integriert sich sehr gut in die Desktop-Umgebungen GNOME (dem Standard-Desktop von Ubuntu), MATE und Cinnamon.
- Installiere dafür Paket `Seahorse` und die zugehörige Erweiterung für deinen Filebrowser, `seahorse-nautilus` (GNOME), `nemo-seahorse` (Cinnamon) `caja-seahorse` (MATE)

Nachdem du das passende Programm installiert hast, kannst du das Verzeichnis öffnen in dem die Dateien liegen und mit Rechtsklick auf die Signatur-Datei die Signatur überprüfen.

Weiter unter Schritt 3.

MacOs

Bei der Installation der GPG-Suite wird eine grafisches Oberfläche mitinstalliert. Du kannst im Filebrowser die Signatur-Datei im Kontext-Menü (Rechtsklick) auswählen und die Signatur überprüfen.

Weiter unter Schritt 3.

2.2 Überprüfung mit Terminal

Öffne das Terminal und bewege dich mit **cd** in das Verzeichnis, in dem die Datei lieg die du überprüfen willst.

```
cd /Pfad/zur/Datei/
```

Mit ls kannst du überprüfen, welche Dateien im Verzeichnis liegen (und wie genau sie heißen)

```
ls
```

Der Output des Terminals könnte nun sein: **Dateiname.exe Dateiname.exe.sig**

Jetzt kannst du die Dateien mit GnuPG (gpg) überprüfen. Der kurze Befehl dafür ist `gpg –verify`. Weil gpg aber den öffentlichen Schlüssel der Unterzeichnerin benötigt, würde es eine Fehlermeldung herausgeben dass es den öffentlichen Schlüssel nicht auf deinem Computer gefunden hat. Als zusätzliche Option kannst du deswegen –auto-key-retrieve angeben. Dadurch wird gpg die Identität der Unterzeichnerin aus der Signatur ablesen, deren Öffentlichen Schlüssel herunterladen und die Dateien überprüfen. Wichtig ist nur, dass im Anschluss daran **erst** die Signatur, und **danach** die Datei selber angegeben werden:

```
gpg  --verify  --auto-key-retrieve  Dateiname.exe.sig  Dateiname.exe
```

3. Schritt: Fingerprint überprüfen

Die Antwort von GPG sollte etwa so aussehen:

```
gpg: Good signature from "Irgendeine Identität <user@mail.org>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: AAAA BBBB CCCC DDDD EEEE  FFFF GGGG HHHH IIII
```

Wichtig ist der Teil **Good signature from…**

Die Warnung kannst du ignorieren, das bedeuet nur das der Öffentliche Key bisher nicht von dir als *vertrauenswürdig* signiert wurde.

Aber ob diese Person auch wirklich die richtige ist, musst du selber herausfinden.Dazu schaust du auf der Webseite dieser Person nach, ob der Fingerprint `AAAA BBBB CCCC DDDD EEEE FFFF GGGG HHHH IIII` auch tatsächlich ihr gehört. Wenn es sich um Software handelt Du kannst den Fingerprint auch in verschiedene Suchmaschinen tippen, und gucken ob es vertrauenswürdige Seiten gibt die diesen Fingerprint mit derjenigen Person assoziieren.

Revision #1
Created 21 July 2023 05:58:05 by Hermann
Updated 21 July 2023 05:58:53 by Hermann