Inhaltsverzeichnis

Datenschutz & Kommunikationssicherheit

Der Text entstand auf Basis einer Mail von Nac zu diesem Thema.

Bei unserem 3. Netzwerktreffen war auch Sicherheit und Anonymität ein Thema, welches einige Teilnehmer beschäftigte.

Man kann sich recht gut und vor allem einfach schützen. Grundsätzlich stellt sich zu allererst die Frage: **Vor was möchte ich mich schützen?** Einzelpersonen, Geheimdienste, Staaten oder aber Firmen wie Facebook, Google & Co.?

Die Verteidigung sieht meistens recht gleich aus - sie beginnt im Kopf.

- Achtet darauf, wem ihr welche Daten von euch oder anderen preisgebt.
- Bei der Weitergabe von Daten Dritter ist stets das Einverständnis einzuholen!
- Sensibilität und gesundes Mißtrauen sind beim Datenschutz und bei der Datensicherheit angebracht, hängen aber auch vom Wissen und Erfahrungsschatz des Einzelnen ab.

Die meisten Messenger (wie WhatsApp, Viper, Line, ...) sind Vorzeigebeispiele, wie es nicht sein sollte. Diese APPs scannen beispielsweise die Kontaktdaten und übertragen alle Inhalte zu eigenen Servern. Für sicher in Bezug auf Datenschutz halten wir folgende Messenger APPs:

- XMPP / Jabber (nac`s Favorit: https://de.wikipedia.org/wiki/Extensible_Messaging_and_Presence_Protocol)

- Clients für alle gängigen Plattformen (Windows, Linux, OS X, Android, iOS, Windows Phone, etc.)
- Anleitung folgt noch
- DeltaChat https://delta.chat/de/
- Im Prinzip ist es ein E-Mail Client (wie Thunderbird) nur eben auf Instant Messanging ausgelegt. Ich konnte es bisher noch nicht ausgiebig testen, es sieht jedoch sehr gut erst einmal aus. Man kann damit problemlos seine eigene E-Mail Adresse nutzen.
- Mumble Sprachkommunikation, frei https://de.wikipedia.org/wiki/Mumble
- https://palava.tv/ Auch wenn keine App, so dennoch in jedem gängigen Browser nutzbar, Entwickler aus Dresden, freie Software

Um anonym zu bleiben - auch wenn eine Mailadresse oder Telefonnummer öffentlich wird - ist ein Pseudonym hilfreich. Dieses sollte keinen Bezug zu einem selbst haben.

Vertraut man seiner Hardware, so gilt es die Software zu sichern. Grundsätzlich ist es ratsam alle Geräte, sofern möglich, zu verschlüsseln. Hierzu kann man bspw. bei Smartphones, Tablets, Notebooks sowie PCs die Festplatte verschlüsseln. Das hat zur Folge, dass die Daten auf dem jeweiligen Gerät nicht einfach „geklaut“ werden können. Sollte es also mal dazu kommen, dass ein Notebook entwendet wird, so ist das Risiko für die darauf gespeicherten Daten wesentlich geringer, wenn die Festplatte verschlüsselt war. Festplatten Verschlüsselung ist mittlerweile auf allen gängigen Geräten und Betriebssystemen möglich.

Solltet ihr dem Datenschutz eine sehr hohe Priorität einräumen, ist der Umstieg auf Linux / BSD empfehlenswert. Ein Vorteil ist, dass es für Linux sowohl kommerziellen Support (z.B. bei unserem Kooperationspartner Datenkollektiv) als auch Community Support gibt.

Community Support in Dresden

- lug - Linux User Group Dresden http://lug-dd.schlittermann.de/
- Chaos Computer Club Dresden (c3d2) https://c3d2.de/space.html
- FSFW Sprechstunde in der Slub https://wiki.fsfw-dresden.de/doku.php/doku/sprechstunde

Unser Netzwerk kommuniziert größtenteils über Mailinglisten. Diese Mailinglisten sind administriert und moderiert. Die einzelnen Mailadressen dahinter sind für Außenstehende nicht einsehbar. Die Sicherheit würde erhöht durch Verschlüsselung der Kommunikationswege - ein Mitlesen Dritter könnte so ausgeschlossen werden. Eine Möglichkeit dafür ist die E-Mail Verschlüsselung durch GnuPG.

Sie ist mittlerweile recht einfach zu handhaben und eignet sich daher auch für nicht technik-affine Menschen. Eine Anleitung findet ihr hier:

https://wiki.fsfw-dresden.de/doku.php/doku/software/gpg/anleitungen_zu_pgp

Sicheres Surfen: Grundsätzlich empfielt sich freie Software.

Firefox hat sich als Browser bewährt. Mit folgenden PlugIns ist er als gut geschützt einzustufen:

- HTTPS Everywhere
- NoScript
- Adblock Plus
  - würde ich aufgrund von kommerzialisierung nicht empfehlen. (nac)
- uBlockOrigin (ein toller, freier Adblocker)
- Better Privacy (Vernichtet alle Cookies nach beenden von Firefox)

Folgende Einstellungen bei Firefox empfehlen wir, um den Datenschutz zu erhöhen:

- Passwörter niemals speichern
- Cookies können immer gelöscht werden

Hier könnt ihr die Sicherheit eures Browser`s testen: https://panopticlick.eff.org/

Eine recht einfache Möglichkeit anonym zu surfen, ist ein s.g. „virtuelles privates Netzwerk“; kurz VPN. Das konventionelle VPN bezeichnet ein virtuelles privates (in sich geschlossenes) Kommunikationsnetz. Mit Tor und dem dazu gehörigen Browser lässt sich das recht unkompliziert umsetzen: https://www.torproject.org/

Grundsätzlich bleibt festzuhalten: Es gibt keine absolute Sicherheit!