Privatsphäre im Internet „Cryptoparty“

Wer will meine Daten haben und warum?

- *Firmen* wollen ihre Daten haben um Ihnen noch mehr Produkte verkaufen zu können, Ihnen gezielt Werbung nach Ihren Interessen zu zeigen. Es gibt wieder andere Firmen die mit Ihren Daten handeln und an Werbetreibende verkaufen. Im Bankensektor wird mit solchen Daten entschieden wie Teuer ihr Kredit wird und ob Sie überhaupt einen bekommen.

- *Kriminelle* wollen ihre Daten haben um auf ihre Kosten ein zu kaufen, um mit ihrem guten Namen Menschen zu bestehlen und zu bedrohen oder um mit ihrem Computer Mist zu machen - zum Beispiel Spam zu verschicken.

- *Staaten* wollen ihre Daten haben um Sie zu kontrollieren. Wissen ist Macht. Mit diesen Daten wird Entschieden wohin sie Reisen können, ob Sie als Beamter arbeiten dürfen. Es gilt die Logik der Angst: Wer harmlos aussieht hat seine terroristischen Absichten nur gut versteckt. Nichts zu Verbergen haben gibt es nicht.

Wo fallen überall Datenspuren an?

Datenspuren fallen immer dann an, wenn Daten weiter gegeben werden. Im Internet werden Daten von Hand zu Hand weiter gereicht. Stellen Sie sich eine Postkarte vor, die sie in der Briefkasten werfen. Jemand leert den Briefkasten, jemand sortiert die Briefe nach Postleitzahl, jemand fährt die Brief ins Verteilungszentrum, jemand Holt den Brief aus dem Verteilungszentrum ab, jemand bringt den Brief zur Adresse. Alle diese Personen können Ihre Postkarte lesen, ohne das Sie oder Empfängerin bzw. Empfänger etwas davon merken können. Im Internet funktioniert das ähnlich.

Wie kann man seine Daten schützen?

Sicherheit ist kein Programm, dass man sich einmal Installiert sondern eine Verhaltensweise.

Generelle Hinweise

- Datenmissbrauch und -Verlust kommt vor. Rechne damit!
- Daten kommen leicht ins Internet rein, nur sehr schwer wieder raus
- Informiere dich über Zusammenhänge! (Webdienste,Verknüpfungen,Finanzierung)
  - Wer ist das Produkt wer ist der Kunde => Folge dem Geld
- Datenhaufen trennen!
  - Unterschiedliche Namen verwenden
  - Konten auch mal löschen und ein Neues eröffnen

Passwörter

Gute Passwörter sind vor allem *lang*.
„Kartoffel42++++++++++++“ ist besser als „Ü+Cb§n,-9@js4“

Für jeden Dienst ein eigenes Passwort!

Damit man sich nicht alles Merken muss kann man Passwortverwaltungsprogramme wie **KeePassX** verwenden.

Freie Software

Nur Software bei der Quellcode, das Kochrezept für das Programm, öffentlich ist kann man Vertrauen. Firmen können einem viel Versprechen, aber leider müssen sie tun was der Staat ihnen sagt. Bei freier Software können viele Menschen Sicherheitslücken suchen. Das ist keine Garantie für Sicherheit aber ein sehr gutes Zeichen.

Daten verschlüsseln

Truecrypt ist ein gutes Programm um Daten zu verschlüsseln.

E-mail verschlüsseln

Dazu verwenden wir **PGP** bzw die Open Source Variante **GPG.**

Unter **Windows**: GPG4Win + Thunderbird + Enigmail

bei **MacOSX:** GPG Tools installieren und mit Mail zusammen verwenden

unter **Linux:** über die Paketverwaltung GPG installieren dazu Thunderbird mit Enigmail.

Tarnkappe im Internet

Tor ist eine freie Software, die dafür sorgt, dass man wie mit einer Maske in Internet unterwegs ist.

Weitere Informationen

Anleitungen für die hier erwähnte Software kann man leicht im Internet finden.

Video dieser Präsentation: https://www.youtube.com/watch?v=ESirhqNEvxo

Umfassendes Handbuch: http://www.privacy-handbuch.de/

Umfassendes Handbuch in Englischer Sprache:
https://www.cryptoparty.in/documentation/handbook

Überblick über Software-Alternativen: https://prism-break.org/de/