Datenschutz in Selbsthilfe

- Worum gehts?
- Die eigene Maschine
- Die eigenen Daten
- Netzwerke

Wichtige Unterscheidung:

- Abwehr von gezielten Angriffen oder
- Datenhygiene

Die goldene Regel: Nutzt euer Hirn.

Die eigene Maschine I

Viele Programme werden zur „Sicherheit“ auf dem Rechner empfohlen. Viele davon haben eher die Wirksamkeit von Kameraüberwachung.

- Virenchecker
- Personal Firewalls
- Filternde Proxies
- Verschlüsselungsprogramme

Grundsatz: Kein Programm ersetzt Nachdenken

Die eigene Maschine II

Sinnvolle Maßnahmen zur Sicherung der eigenen Maschine:

- Updates einspielen
- „Aktive“ Inhalte wann immer möglich ausschalten.
- Automatiken wann immer möglich ausschalten
- Im Zweifel die hässlichere Darstellung wählen
- Keine HTML-Mail
- Keine Office-Dokumente verschicken
- Cookies und Referrer kontrollieren
- Hardware-Router

Eigene Daten: Verschlüsselung

Für eure eigenen Daten lohnt sich unter Umständen eine lokale Verschlüsselung. Die Verschlüsselungsfunktionen der üblichen Office-Pakete sind meistens Quatsch.

Ihr könnt mit PGP und gnupg einzelne Dateien verschlüsseln, das kommerzielle PGP kommt mit einem Programm zur Verschlüsselung einer ganzen Partition.

Klar ist, dass ihr den Schlüssel (das „Passwort“) besser nicht auf den Rechner klebt...

Eigene Daten: Formate

Verwendet, wann immer möglich, schlichten Plain Text (notepad erzeugt sowas, für Tabellen kommt z.B. csv in Frage). Nur dabei wisst ihr wirklich, was der Rechner speichert bzw. überträgt.

In Office-Dateien werden regelmäßig Metadaten gespeichert, die Rückschlüsse auf die AutorInnen der Dateien zulassen.

Wenn ihr unbedingt formatierten Kram austauschen wollt, nehmt PDF oder HTML o.ä., in der größten Not RTF und guckt mit einem Editor nach, was euer Programm dort so reinschreibt.

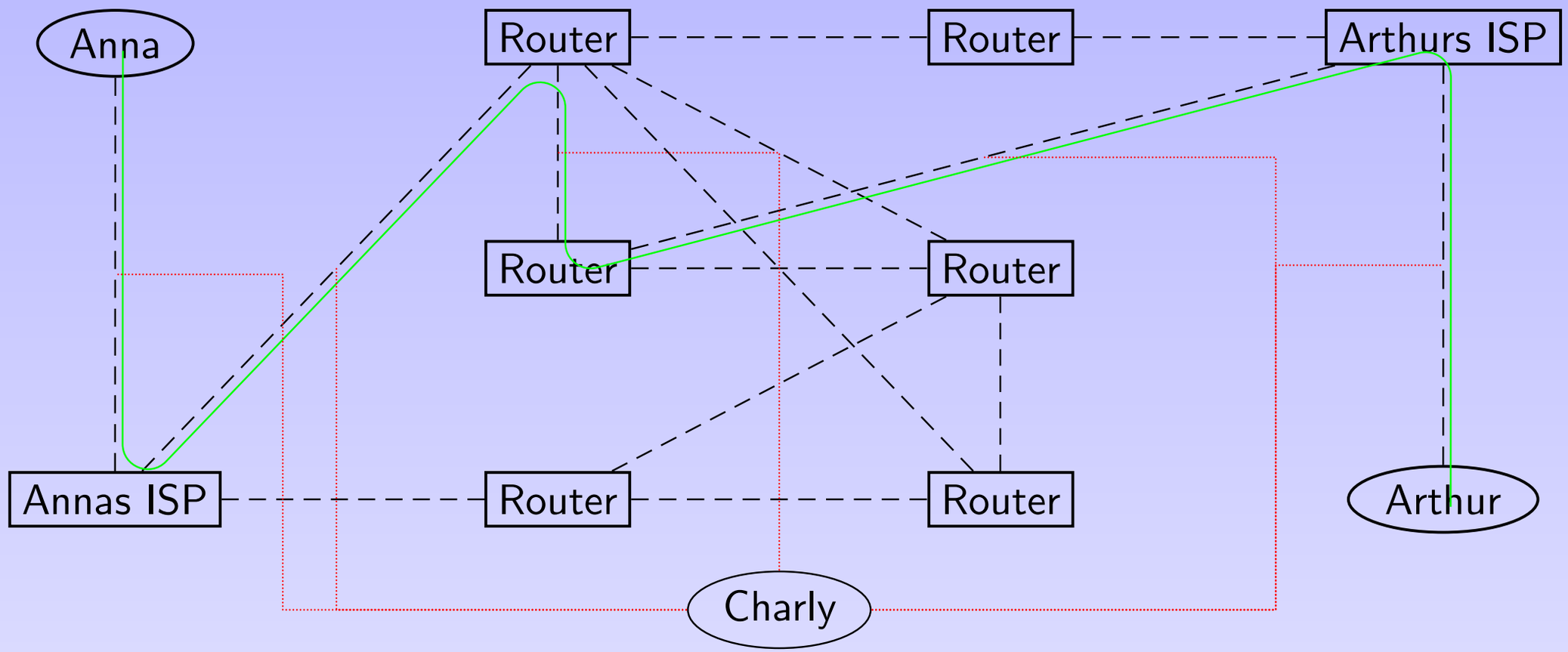
Eigene Daten: Spuren

Euer Rechner speichert häufig, was ihr so tut – welche Webseiten ihr besucht, welche Programme ihr gestartetet, was ihr in Formulare eingetragen habt.

Seid euch bewusst, dass diese Daten existieren und ausgewertet werden, wenn eure Kiste beschlagnahmt wird. Versucht, sie regelmäßig zu löschen.

Wenn ihr selbst Kram ins Netz stellt, tut das, wo ihr wisst, dass die Leute verantwortlich mit Logs umgehen. Nadir ist ein guter Tipp.

Das Netz



Das Netz besteht aus vielen Teilen, zwischen denen Router Pakete verschieben.

Vorratsdatenspeicherung

Bei der Vorratsdatenspeicherung werden die Kommunikationsdaten aller NutzerInnen flächendeckend für mindestens sechs Monate gespeichert.

Vorläufig sollen diese Daten nur für rückwirkende personenbezogene Anfragen verwendet werden.

Richtig spannend werden diese Daten aber erst, wenn auf ihnen Data Mining betrieben wird.

Gespeichert werden nach der gegenwärtigen EU-Richtline Mail- und VoIP-Verbinungen, wobei die Definition im Gesetz eher seltsam gehalten ist.

Verschlüsselung am Netz

Verschlüsselung ist sinnvoll, weil sie der Staatsgewalt den Zugang zu Kommunikationsinhalten jedenfalls um Größenordnungen erschwert.

- Für Mail: PGP
- Fürs Web: https
- (Anonymizing Proxies)
- Weitere Einzelprotokolle
- Für alles: Tor

Zum Abschluss

Überwachung in erster Linie ein politisches Problem und sollte politisch bekämpft werden.

Trotz allem: Keine Panik!

Wer sich Arbeit sparen möchte: Es ist gar nicht so dumm, den eigenen Rechnner nicht ans Netz zu hängen, alle eigenen Daten auf einem USB-Stick zu halten und bei Bedarf ins Internetcafe zu gehen.

Weitere Infos und Links auf http://www.datenschmutz.de

Links zu sinnvollen Programmen:
http://www.argh-it.de/crypto/