**Raffael Rittmeier**

# How To FIfF

## Teil 2: Initiativen und Arbeitsgruppen, -kreise, -kringel, -punkte

In Teil 1 von *How To FIfF* habe ich die FIfF-Regionalgruppen beschrieben. Inhaltliche Themen haben aber in der Regel keine regionalen Grenzen. In Arbeitskreisen oder Arbeitsgruppen schließen sich deshalb Menschen überregional zusammen, die sich zu einem bestimmten Themengebiet austauschen und dazu arbeiten möchten. So soll sich die inhaltliche Arbeit des FIfF gestalten – im Idealfall. Gibt es keine Arbeitsgruppen, dann bleibt die Arbeit an Einzelnen hängen, nicht selten aus dem Vorstand. Da der Vorstand die vielfältigen Themen nicht allein bearbeiten kann (und soll), sei hiermit auf die Wichtigkeit der Arbeitskreise und -gruppen hingewiesen. Die Ziele und die Organisationsform eines AK oder einer AG können sehr unterschiedlich sein. Häufig gibt es auf den Jahrestagungen Impulse zur Gründung einer kontinuierlichen AG. Wichtig sind die Kommunikation und Öffentlichkeitsarbeit, schließlich sollen Andere sich anschließen oder später auf die erarbeiteten Ergebnisse aufbauen können. Die Ergebnisse können auf der Webseite *fiff.de* und in der FIfF Kommunikation veröffentlicht werden. Eventuell kommen so viele Informationen zusammen, dass eine eigene Broschüre veröffentlicht werden kann (wie zuletzt die zweite Broschüre zur elektronischen Gesundheitskarte: *fiff.de/egk*). Zur Unterstützung der Arbeit und Kommunikation können Mailinglisten eingerichtet und das Wiki genutzt werden *(wiki.fiff.de)*. Die Geschäftsstelle und der Vorstand stehen bereit Interessierte zu unterstützen. Dafür haben wir folgende Themengebiete zusammengefasst und verantwortliche Kontaktpersonen benannt:

- Arbeit
- Datenschutz, Überwachung, Kontrolle
- Frieden
- Bildung, Gesundheit, Soziales, Umwelt
- Gender
- Informationsgesellschaft, IT-Politik, IT-Recht
- IT-Sicherheit, Verletzlichkeit
- Verantwortung von InformatikerInnen, „Informatik und Gesellschaft“ in der Lehre

Den Kontakt kann unsere Geschäftsstelle herstellen: *fiff@fiff.de.*

**Der Kommentar**

# Staatlicher Hausfriedensbruch

*Es ist ungeheuerlich! Unser Grundgesetz, geschaffen nach den Erfahrungen einer Diktatur und mühevoll verteidigt vom Verfassungsgericht, kann uns Bürgerinnen und Bürger nicht mehr vor Eingriffen des Staates schützen. Nicht gegen einen bayrischen Innenminister mit der unerschütterlichen Gewissheit, dass nichts an diesem Trojaner grundrechtsverletzend sei. Nicht gegen Sicherheitsbehörden, die beschaffen, was Software-Buden produzieren, ohne sich einen Teufel darum zu scheren, wie und von wem ihre Produkte eingesetzt werden. Wissen sie alle nicht, was sie tun? Oder machen sie, was sie wollen?*

Wir danken Euch aus tiefstem Herzen, liebe HacktivistInnen vom Chaos Computer Club, die getan haben, was ein BSI hätte tun sollen, oder irgendeine andere staatliche Organisation! Was sind das nur für Institutionen, die entweder so inkompetent und dumm oder so zynisch sind, dass sie wie ein Elefant im Porzellanladen über Bürgerrechte hinweg trampeln und dann die verdutzte Unschuld markieren?

Compliance und ähnliche Symbolbegriffe, Gesetze und Verordnungen, all das soll uns einreden, ein fürsorglicher Staat kümmere sich um Sicherheit und Wohlergehen seiner Bürger. Die Realität sieht anders aus, wie der CCC feststellen musste: „Aufgrund von groben Design- und Implementierungsfehlern entstehen außerdem eklatante Sicherheitslücken in den infiltrierten Rechnern, die auch Dritte ausnutzen können.“ Es wäre lächerlich, wenn es nicht so traurig wäre: Da öffnen unsere staatlichen Beschützer ausländischen Diensten oder dem organisierten Verbrechen mit einem Danaergeschenk an die nichtsahnenden Bundesbürger die Hintertüren auf deren Rechner. Und wir müssen hoffen, dass es *nur* deutsche Sicherheitsbehörden sind, die sich auf den infizierten PCs tummeln.

Wir fordern, dass unseren Verfassungsrichtern anderes übrig bleibt, als in ohnmächtigem Zorn ihre roten Roben zusammenzuknüllen und in die Ecke zu schmeißen ... Quellen-TKÜ, das ist Sicherheitsbehörden in außergewöhnlichen Fällen erlaubt: Ja, sie dürfen notfalls und gemäß den Vorgaben des Verfassungsgerichts die verschlüsselte Kommunikation gefährlicher Personen abhören.

Aber sie dürfen unter keinen Umständen die Rechner ihrer *Untertanen* durchschnüffeln und manipulieren! Egal, ob sie ihren eigenen Dilettantismus oder die Gefährdung der öffentlichen Sicherheit oder ähnliche Ausreden dafür ins Feld führen! Schon gar nicht dürfen sie Daten und Code-Zeilen in die USA umleiten und dort einem nochmals erhöhten Risiko aussetzen. Das ist verboten, die Gesetzesbrecher sind sie!

*Dagmar Boedicker*