BÜPF und NDG

Stellungnahme der Arbeitsgruppe “Privacy” in der Fachgruppe Informatik und Gesellschaft der Schweizer Informatikgesellschaft (SI)

Kontakt: Dr. Andreas Geppert (geppert@acm.org)

1 Einleitung

In der Schweiz wurden neue Gesetze durch das Parlament verabschiedet, die in die Privatsphäre und andere Grundrechte der Schweizer BürgerInnen eingreifen. Das Nachrichtendienstgesetz (NDG) definiert die Aufgaben des Nachrichtendienstes des Bundes [1] inklusive der Überwachung der grenzüberschreitenden Kommunikation (Kabelaufklärung). Das Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs (BÜPF) regelt Vorratsdatenspeicherung und andere Überwachungsmassnahmen [2] im Inland. Die SI und ihre Mitglieder sind von diesen Gesetzen nicht nur als (Stimm-)BürgerInnen betroffen, sondern auch als InformatikerInnen gefordert, Stellung zu beziehen und mit ihrer Expertise MitbürgerInnen zu informieren. Im folgenden Text fassen wir zusammen, warum die Arbeitsgruppe „Privacy“ beide Gesetze für zu massive, nicht verhältnissmässige Eingriffe in die Grund- und Menschenrechte hält.

2 Grundlagen

Überwachungsmassnahmen sind immer Eingriffe in die Privatsphäre und andere Grundrechte, wie sie in der Schweizer Verfassung festgehalten sind. Folgende Prinzipien helfen uns bei der Analyse, ob diese Eingriffe noch akzeptabel und verhältnismässig sind:

- professionelle Ethikrichtlinien (von SI [4], ACM [5] und anderen Informatikverbänden);
- Grundsätze zur Evaluation von Überwachungsmassnahmen, die von der Electronic Frontier Foundation und anderen Organisationen erarbeitet wurden [3];
- ein Expertengutachten der NSA-Praktiken zuhanden von Präsident Obama [6]

3 Schlüsse

Der Staat soll die Sicherheit seiner BürgerInnen so weit wie möglich garantieren. Sicherheit bedeutet einerseits Schutz vor Terror und Kriminalität, jedoch auch persönliche Sicherheit – den Schutz der Privatsphäre. Unserem Dafürhalten nach stellen beide Gesetze, NDG und BÜPF, unverhältnissmässige Eingriffe in die Privatsphäre und andere Grundrechte dar:

- Vorratsdatenspeicherung und Kabelaufklärung sind **verdachtsunabhängig** und stellen alle BürgerInnen unter **Generalverdacht**;
- Sowohl durch Sammeln der Verbindungsdaten (Metadaten) als auch durch Kabelaufklärung erhält der Staat ein vollständiges und äusserst detailliertes Bild seiner BürgerInnen; der „**gläserne Bürger**“ wird Realität (s. Fichenaffäre);
- Nicht nur aus der Schweiz, sondern auch aus anderen Ländern ist bekannt, dass

Terrorismusabwehr oft als „Türöffner“ für Datensammlungen und Überwachung dient. Behörden können dann der Versuchung, die bereits vorhandenen Daten für **weitere Zwecke** zu verwenden, nicht widerstehen (s. Literatursammlung der Arbeitsgruppe);

- Das Abhören mittels Staatstrojanern nutzt Schwachstellen aus, anstatt diese zu schliessen – dies bringt InformatikerInnen in einen **unlösbaren Konflikt** mit ihren Ethikcodes. Die verwendeten Schwachstellen können natürlich nicht nur von den inländischen und demokratisch legitimierten Behörden, sondern auch von denen autoritärer Regimes oder gar kriminellen Akteuren ausgenutzt werden;
- Abhörmassnahmen sind **intransparent**, und Erfahrungen aus der Schweiz und dem Ausland (USA, UK, Deutschland) zeigen, dass Überwachungsapparate **nicht kompetent und effektiv beaufsichtigt** werden können und schnell ein Eigenleben entwickeln.
- Schliesslich wird der Kreis der Organisationen, die Metadaten liefern (müssen), massiv ausgeweitet auf alle Anbieter von jeglichen Kommunikationsdiensten – diese Erweiterung ist **nicht** praktikabel und wird die Schweizer IKT-Wirtschaft finanziell belasten.

Strafverfolgungsbehörden müssen in der Lage sein, einzelne Personen oder Organisationen im Rahmen von Strafverfahren mit richterlichem Beschluss gezielt zu überwachen. **Verdachtslose** und **ungezielte Überwachung** aller BürgerInnen ist jedoch ein massiver und nicht verhältnismässiger Eingriff in die Grundrechte, insbesondere der Privatsphäre. Massnahmen wie Staatstrojaner verschlechtern die Sicherheit, gefährden die Demokratie und schwächen die Schweizer IKT-Wirtschaft.

Aus diesen Gründen schlagen wir dem SI-Präsidium folgendes vor:

- den SI-Mitgliedern zu empfehlen, beim Referendum das NDG abzulehnen;
- den SI-Mitgliedern zu empfehlen, das Referendum gegen das BÜPF zu unterschreiben.

4 Literaturhinweise

1. Nachrichtendienstgesetz. Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (zugegriffen am 25.2.2016)
2. Überwachung des Fernmeldeverkehrs (zugegriffen am 25.2.2016)
3. International Principles on the Application of Human Rights to Communications Surveillance. Necessary and Proportionate, May 2014
4. Ethik-Richtlinien der SI
5. ACM Code of Ethics and Professional Conduct
6. R.A. Clarke, M.J. Morell, G.R. Stone, C.R. Sunstein, P. Swire (eds.): Liberty and Security in a Changing World. Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies, December 2013