Kritik an der BÜPF-Revision (Botschaft vom 27. Februar 2013)

Digitale Gesellschaft
www.digitale-gesellschaft.ch

27. April 2013

1 Eingangsbemerkung

Anders als in der Botschaft versprochen, wird mit der vorgeschlagenen Revision die Überwachung stark ausgeweitet. Wurde bis anhin bei den Post- und Fernmeldedienstanbieter angesetzt, sollen nun beide Enden der Kommunikation mit einbezogen werden: Auf dem Benutzer-Computer per GovWare und auf der Server-Seite durch Ausweitung des Geltungsbereichs auf sämtliche Diensteanbieter. Zusätzlich soll die Dauer der Vorratsdatenspeicherung verdoppelt werden.

Als Digitale Gesellschaft fühlen wir uns der kritischen, digitalen Zivilgesellschaft verpflichtet und möchten im Folgenden auf die wichtigsten betroffenen Gesetzesartikel hinweisen.

Eine Zusammenfassung[1], wie auch eine ausführliche Stellungnahme[2] können auf der Website der Digitalen Gesellschaft gefunden werden.

Vom EJPD wurde 2012 zudem eine Studie zu den Kosten der Fernmeldeüberwachung[3] veröffentlicht.

[1] http://www.digitale-gesellschaft.ch/2013/04/21/bupf-revision-kommt-in-den-standerat/

[2] http://www.digitale-gesellschaft.ch/uploads/2013/04/stellungnahme_20130420.pdf

[3] http://www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/berisc-ejpd-fda-pda-d.pdf

2 Kritische Bemerkungen zu einzelnen Artikeln

2.1 Persönlicher Geltungsbereich

Geltend Art. 1 Abs. 2 BÜPF
Entwurf Art. 2 BÜPF

Geltend:

- Internet-Anbieterinnen (Access Provider)

Neu:

- Anbieterinnen von Fernmeldediensten (Access Provider)
- Anbieterinnen von Diensten, die sich auf Fernmeldedienste stützen und eine Einweg- oder Mehrwegkommunikation ermöglichen (Anbieterinnen abgeleiteter Kommunikationsdienste)
  - E-Mail-Anbieterinnen, Chat- und Forenbetreiber (auch Privatpersonen und Vereine)
  - Hostingprovider (auch Privatpersonen und Vereine)
- Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen
  - Hotels, Spitäler, Schulen, Bibliotheken, Internet-Cafés
  - Privatpersonen (die bspw. ihr WLAN mit dem Nachbarn teilen)

Aufgrund des Territorialitätsprinzips kann allerdings auch das neue Gesetz genau jene ausländischen Anbieterinnen abgeleiteter Kommunikationsdienste nicht umfassen, die heute diese Märkte dominieren!

2.2 Identifikation der Täterschaft bei Straftaten über das Internet

Geltend Art. 14 Abs. 4 BÜPF
Entwurf Art. 22 BÜPF

Bei Verdacht einer Straftat via Internet müssen (sämtliche vorliegenden) Angaben (bspw. aus der Vorratsdatenspeicherung) zur Identifikation geliefert werden:

- ohne Einschränkung durch einen Deliktskatalog
- ohne Richtervorbehalt
- ohne Einschränkung auf die Speicherdauer der Vorratsdatenspeicherung

Weiterführende Links [4] [5]

[4] http://www.reko-inum.ch/de/display_file.php?fname=114010669724120&query=
[5] http://jumpcgi.bger.ch/cgi-bin/JumpCGI?id=22.01.2013_1B_481/2012

Der Bundesrat bestimmt

- welche Angaben von den Access Provider erhoben werden müssen
- welche Anbieterinnen abgeleiteter Kommunikationsdienste welche Angaben erheben müssen

2.3 Pflichten bei der Überwachung des Fernmeldeverkehrs

Geltend Art. 15 BÜPF
Entwurf Art. 26, 27 und 29 BÜPF

Anbieterinnen abgeleiteter Kommunikationsdienste müssen

- eine Überwachung dulden
- unverzüglich Zugang zu ihren Anlagen gewähren
- die für die Überwachung notwendigen Auskünfte erteilen
- die ihnen zur Verfügung stehenden Randdaten liefern

Der Bundesrat unterstellt alle oder einen Teil dieser Anbieterinnen, die Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten, allen oder einem Teil der generellen Überwachungspflichten (inkl. der Vorratsdatenspeicherung).

Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen, müssen ebenfalls

- eine Überwachung dulden
- unverzüglich Zugang zu ihren Anlagen gewähren
- die für die Überwachung notwendigen Auskünfte erteilen
- die ihnen zur Verfügung stehenden Randdaten liefern

2.4 Vorratsdatenspeicherung

Geltend Art. 15 Abs. 3 BÜPF
Entwurf Art. 26 Abs. 5 BÜPF

- Ausweitung der Speicherdauer von 6 auf 12 Monate
- Die Daten werden nicht "aufbewahrt" sondern von den Providern erhoben.
- Wieso die Dauer nicht ausreicht, wird in der Botschaft nicht weiter erläutert.
- Es fehlt eine Begründung, wieso die Vorratsdatenspeicherung "zur Bekämpfung der Kriminalität unerlässlich" sei.

- Eine Studie des Max-Planck-Instituts[6] kommt zum gegenteiligen Schluss.
- Ein Grundrechtseingriff ist ohne Nachweis der Verhältnismässigkeit jedoch nicht zulässig.

2.5 Neue Pflichten und Strafbestimmungen

Für Anbieterinnen von Fernmeldediensten

- Dem Dienst ÜPF müssen Informationen über aktuelle und geplante Dienstleistungen mitgeteilt werden (Art. 25 BÜPF)
- Der Dienst ÜPF kann Qualitätskontrollen anordnen (Art. 33 BÜPF)
- Er kann eine Konzession entziehen (Art. 41 Abs. 2 BÜPF)

Für alle vom persönlichen Geltungsbereich betroffenen

- Die Missachtung einer Verfügungen kann mit bis zu 100'000.- bestraft werden (Art. 39 BÜPF)
- Eine Überwachungsanordnung kann zwar angefochten werden (Art. 42)
  - jedoch nicht bezüglich den Voraussetzungen einer Überwachungsanordnung
  - und einer Beschwerde fällt keine aufschiebende Wirkung zu

3 IMSI-Catcher

Aktuell keine Gesetzesgrundlage
Entwurf Art. 269bis StPO

Nicht nur das zu überwachende Mobiltelefon bucht sich via IMSI-Catcher in das Mobilfunknetz ein, sondern alle Geräte im Empfangsbereich. Dadurch ist es der Polizei auch möglich herauszufinden, wer sich aktuell mit eingeschaltetem Handy im Umkreis befindet.

4 GovWare, d.h. Trojaner Federal

Aktuell keine Gesetzesgrundlage, mit viel Interpretation Art. 280 & 281 StPO
Entwurf Art. Art. 269ter StPO

- Keine technische Beschränkung auf Daten aus einem laufenden Telekommunikationsvorgang
- Weit gefasster Deliktskatalog[7]

[6] http://vds.brauchts.net/MPI_VDS_Studie.pdf
[7] http://www.steigerlegal.ch/2013/03/04/umfangreicher-straftatenkatalog-fuer-bundestrojaner/

Einige offene Fragen:

- Wie kommt der Bundestrojaner auf das System?
- Darf sie sich die Polizei eine Sicherheitslücke auf dem Schwarz-Markt beschaffen?
- Darf beim Einsatz eine vorhandene AntiViren-Software deaktiviert werden?
- Wie wird der ursprüngliche Zustand nach Abschluss der Überwachung wieder hergestellt?
- Wie wird sichergestellt, dass nur die Kommunikation von der tatsächlich zu überwachenden Person (beim Teilen eines PCs) aufgezeichnet wird?
- Ab wann kann bspw. bei E-Mails von Kommunikation gesprochen werden? Ist eine strickte Trennung von Inhalts- und Kommunikationsverschlüsselung vorgesehen?
- Die Aufzeichnung eines Video-Chats ist immer auch eine Wohnraumüberwachung.
- Wie wird die nötige Beweissicherheit für die Verwendung vor Gericht auf einem fremden und entfernten System gewährleistet?