



Bundesamt für Justiz
Direktionsbereich Strafrecht
Bundesrain 20
3003 Bern

Bern, den 18. August 2010

Vernehmlassung zur Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

Sehr geehrte Damen und Herren

Swiss Police ICT, Trägerin des Schweizer Polizei Informatik Kongress' SPIK, nimmt zum Vorentwurf zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) wie folgt Stellung:

1. Allgemeines & Hauptvorteil

Wir *begrüssen* die vorgesehene Revision, bringt sie doch *grosse Fortschritte* mit sich. Der wichtigste ist aus unserer Sicht, dass das BÜPF den *neuen Kommunikationstechnologien angepasst* wird.

Im vorliegenden Entwurf zur Revision des BÜPF sind jedoch zu viele Punkte noch nicht geklärt und bedürfen einer Überarbeitung, um rechtsstaatlichen Prinzipien zu genügen: Der erheblichste Mangel der Vorlage ist, dass der Überwachungsdienst *gleichzeitig normativ und exekutiv* tätig sein soll. Er sollte aber generell weisungsungebunden sein und wohl mit Konzessions- und Aufsichtsbehörden, nicht aber mit Strafverfolgungsbehörden zusammenarbeiten. Unseres Erachtens wird hier zu viel vermengt, was ordnungspolitisch nicht zusammengehört.

Trotz der grundsätzlich richtigen Stossrichtung plädieren wir daher für eine grundsätzliche Überarbeitung der Vorlage.

2. Vorteile

- Der Hauptvorteil der Vorlage ist, dass das BÜPF den neuen Kommunikationstechnologien angepasst wird, so dass neben den reinen Internet-Zugangs-Providern im engeren Sinne neu auch die Anbieter weiterer IT-Kommunikationsdienste, die keinen eigentlichen Internet-Zugang ermöglichen, unter das BÜPF fallen, wie z.B. Hosting Provider und Anbieter von Mail- und Chatdiensten.
- Dass die Kommunikationsdaten neu 12 statt 6 Monate aufbewahrt werden, ist angesichts der globalen Netzwerke und der Zeit, die es dauern kann, bis ein möglicher Straftatbestand entdeckt wird, sehr sinnvoll.
- Die zentrale Lagerung der Daten ist gegenüber der heutigen dezentralen Praxis ein eindeutiger Fortschritt: Dies aus technischen Gründen als auch unter dem Aspekt der Kontrollierbarkeit des Umgangs mit den Daten und der fristgerechten Löschung. Zudem soll diese Lösung mithelfen, Kosten im Überwachungsprozess zu senken.
- Dass die Fernmeldediensteanbieter (FDA) verpflichtet werden, im Bedarfsfall bei der Platzierung (in keinsten Weise aber bei der Entwicklung) eines so genannten Trojaners zu helfen, wird von SPIK begrüsst. Angesichts des technologischen Fortschritts auch der Cyber-Kriminellen – Stichworte sind Anonymisierung, Verschleierung und Verschlüsselung – ist der Trojaner bisweilen die *ultima ratio*. Sein Einsatz ist im Übrigen klar geregelt und an strenge Voraussetzungen geknüpft. Dass die Firmen, welche von den Möglichkeiten der neuen Technologien geschäftlich profitieren, angehalten werden, im Bedarfsfall zu Aufklärung des Missbrauchs eben dieser Technologien beizutragen, scheint uns schlüssig.

3. Kritikpunkte (namentlich Art. 3, 15, 18)

- Unser Haupteinwand richtet sich gegen den Art. 3, „Überwachungsdienst“. Dieser soll laut Abs 2 „weisungsungebunden“ sein, was seiner Funktion als technischer Dienstleister der Polizei im Überwachungsfall widerspricht: Er befolgt dann die Weisungen der Strafverfolgungsbehörden. (Die Prüfung, „ob die Überwachung eine gemäss dem anwendbaren Recht überwachungsfähige Straftat betrifft und von der zuständigen Behörde angeordnet wurde“ (Art. 15 a) kann auch nur formell sein, nicht aber materiell.) Allerdings muss der Dienst laut Art. 3 Abs. 3 wohl mit Konzessions- und Aufsichtsbehörden, interessanterweise aber nicht mit Strafverfolgungsbehörden zusammenarbeiten.

Nun ist dieser Dienst, der die Überwachung erbringt, gleichzeitig die normsetzende Behörde: Laut Art 18 zertifiziert er „Anbieterinnen von Fernmeldediensten auf deren Kosten, dass sie Überwachungen wirksam durchzuführen imstande sind“. Dass ein und derselbe Dienst als Empfänger von Anordnungen der Strafverfolgungsbehörden agiert und gleichzeitig selbständig und die Normen des Vollzugs soll setzen und zertifizieren können, ist unseres Erachtens befremdlich – insbesondere, da offenbar niemand den weisungsungebundenen Dienst kontrolliert.

Unseres Erachtens ist der Dienst zweizuteilen: Die Ausführung der von den Strafverfolgungsbehörden angeordneten Zwangsmassnahme „Überwachung“ nach einer formellen Prüfung sowie der Betrieb des zentralen Systems und die Pflege der dort lagernden Daten nach recht und Gesetz gehören in eine Hand, Normierung, Zertifizierung und Kontrolle des ausführenden Überwachungsdienstes und seines Systems in eine andere. Letztere Instanz soll durchaus weisungsungebunden sein und im Dialog mit den FDAs Standards setzen, erstere hingegen sei ein kontrolliertes ausführendes Organ der Strafverfolgung.

- Ein weiterer Einwand betrifft die klare Definition der Pflichten der FDA (Art 19. ff). Die entsprechenden Richtlinien sind bekanntermassen schon zu lange pendent; ohne ein klares Regelwerk aber ist eine Zertifizierung der FDA ebenso wenig möglich wie eine nachvollziehbare Kosten-Diskussion. Rechtssicherheit heisst auch, dass alle an einem System beteiligten genau wissen, was von ihnen wann verlangt wird. Dieser Punkt ist zwingend *vor der parlamentarischen Behandlung* des Geschäftes zu regeln. Dabei ist darauf zu achten, dass die Regeln nicht einseitig von der Ausführenden Behörde erlassen werden.

Es würde uns sehr freuen, wenn Sie unsere Hinweise berücksichtigen könnten.

Mit freundlichen Grüssen,

Rolf Nägeli



Vorstand SPIC I
Leiter AG Cybercrime

Mark A. Saxer



Geschnattstunrer SPIC I

Der **Verein Swiss Police ICT** bezweckt die regelmässige Durchführung von Informatik- und Kommunikations- (ICT-) Fachveranstaltungen für die Polizei und Ihre Partner – namentlich zu nennen ist der Schweizer Polizei Informatik Kongress SPIK (www.spik.ch) – sowie die Förderung von Aktivitäten zur Bekämpfung der Computer- und Internetkriminalität. Im **politischen Beirat** sitzen die Nationalrätinnen Corina Eichenberger (FDP, AG), Edith Graf-Litscher (SP, TG), Barbara Schmid-Federer (CVP, ZH), Regierungsrat Hans-Jürg Käser (FDP, BE) und Beat Hensler (Kdt Kapo LU). **Präsident** ist Martin Gächter (Chef Kommandodienste Kapo SG).