Swico
Hardturmstrasse 103
CH-8005 Zürich

Tel. +41 44 446 90 90
www.swico.ch
info@swico.ch

Swico zum Referendum gegen das BÜPF

Das von den eidgenössischen Räten am 18. März 2016 verabschiedete „Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs“ BÜPF ist primär auf die Begehren der Strafverfolgungsbehörden ausgerichtet und wird daher in der Politik kontrovers diskutiert, wobei vor allem der Schutz der Bürgerrechte thematisiert wird. Allerdings weist das Gesetz auch aus Sicht der ICT-Branche zahlreiche Mängel auf:

Kritische Punkte aus Sicht der ICT-Anbieter

Wirkungslosigkeit: Eine der wichtigsten und aufwändigsten Massnahmen im BÜPF ist die Vorratsdatenspeicherung. In der Praxis sind zahlreiche Methoden bekannt, wie sie von Kriminellen leicht umschifft werden kann und in der Literatur wurde mehrfach belegt, dass sie per Saldo die Wirksamkeit der Strafverfolgung nicht messbar erhöht. Es ist daher nicht sinnvoll, die Wirtschaft mit dem entsprechenden umfangreichen Überwachungsauftrag zu belasten.

Diskriminierung: In der Kumulation bilden die massiven Pflichten, welche das BÜPF den Schweizer ICT-Anbietern auferlegt, eine Diskriminierung gegenüber Firmen, welche in der Schweiz Kunden akquirieren, aber hier keinen Geschäftssitz haben – wie es in einer globalisierten und zunehmend digitalisierten Welt immer mehr der Fall ist. Auch in dieser Beziehung verletzt das BÜPF das Verhältnismässigkeitsprinzip.

Innovationsfeindlichkeit: Das BÜPF sieht allen Ernstes vor, dass Schweizer Firmen neue Produkte mit Kommunikationsfähigkeiten sechs Monate vor Lancierung den Behörden vorzulegen haben: Im Zeitalter von internationalem Wettbewerb und „Minimum viable products“ ein absoluter Innovationskiller. Damit werden in Zukunft in unserem Land sicher keine neuen Produkte mehr entwickelt. Insbesondere auch die Gaming-Industrie wird in Zukunft einen weiten Bogen um die Schweiz machen.

Gefährdung der Netzsicherheit: Staatstrojaner müssen via „Backdoor“ auf die Zielgeräte eingeschleust werden. Damit werden diese jedoch auch für jede andere Schadsoftware verwundbar und somit zu regelrechten Virenschleudern, was sich nicht nur auf die betroffenen Geräte auswirkt, sondern auch die Netzstabilität beeinträchtigt und die Datensicherheit bei allen Netznutzern gefährdet. Der Einsatz von Staatstrojanern ist eine Einladung zum Aufbau von Bot-Netzen und zu organisierter Internet-Kriminalität.

Überrissene Mitwirkungspflichten: Das BÜPF verlangt von den ICT-Anbietern nicht nur die Duldung von Überwachungsmassnahmen (was ja gerechtfertigt und notwendig ist), sondern auferlegt ihnen auch die Pflicht, sich auf Vorrat als „Überwacher“ vom Bund zertifizieren zu lassen (!) und einen automatischen Zugriff des Bundes auf ihre Systeme einzurichten. Verschlüsselungen müssen entfernt werden. ICT-Anbieter haben keine echte Kontrolle mehr darüber, was bei ihnen passiert. Insbesondere können sie damit ihren Kunden gegenüber auch keine entsprechenden Garantien mehr abgeben.

Uferloser Adressatenkreis: Vom Smart-TV-Anbieter zum Betreiber eines WLAN in einer WG, vom Krankenhaus zum Gaming-Startup: Der Staat darf so gut wie jedes Unternehmen und jede Organisation zwingen, aktiv Drittpersonen auszuforschen, und verbietet gleichzeitig mit

saftigen Strafen, dies zu kommunizieren („Gag order“). Insbesondere ICT-Anbieter werden gezwungen, ihre Kunden aktiv auszuspionieren, was der Reputation und dem Verkaufserfolg abträglich ist, sobald es bekannt wird – was ja unweigerlich passieren wird.

Interner Sicherheitsaufwand: Der interne Sicherheitsaufwand vieler ICT-Anbieter nimmt mit dem BÜPF massiv zu und erfordert den Aufbau aufwändiger Strukturen. So werden zum Beispiel Access-Provider gehalten, rund um die Uhr auf Abruf für Aufträge des Bundes zur Verfügung zu stehen, was wohl vielen der kleineren Anbietern aus Kostengründen das Genick brechen wird.

Gefährdung Datenstandort: Die massive Aufrüstung des Überwachungsapparats macht die bisher als sicheren Standort für die Datenspeicherung interessante Schweiz unattraktiv und wird damit das Business der spezialisierten Anbieter in diesem Bereich stark beeinträchtigen.

Fehlende Rechtsmittel: ICT-Anbieter können sich wenn überhaupt erst nachträglich gegen Anordnungen der Behörden wehren, selbst wenn dadurch ihre Systeme gefährdet werden oder ihre Geschäftstätigkeit beeinträchtigt wird. Die Geheimhaltungsinteressen des Staates haben Vorrang, so dass es so gut wie unmöglich sein wird, für finanzielle Schäden entschädigt zu werden, welche aufgrund von Überwachungsmassnahmen gegen Dritte herrühren (von den immer möglichen Reputationsschäden gar nicht zu reden).

Fehlende Transparenz: Es gibt keinerlei Verpflichtung im Gesetz, die Wirksamkeit der Massnahmen zu prüfen, statistisch auszuwerten und offenzulegen. Damit gibt es keine Möglichkeit, unwirksame Vorgehensweise zu identifizieren und auszusetzen, welche die ICT-Anbieter übermässig belasten, aber nichts bringen.

Deshalb unterstützt Swico das Referendum

Die Strafverfolgungsbehörden müssen ihr Arsenal weiter entwickeln, um dem technischen Fortschritt zu folgen und auf neue Formen der Kriminalität zu reagieren. Der Ausbau des Instrumentariums für die Überwachung muss sich jedoch an den Kriterien der Notwendigkeit, der Wirksamkeit, der Verhältnismässigkeit und der demokratischen Kontrolle orientieren. Wie oben ausgeführt weist das BÜPF in jedem dieser vier Bereiche gravierende Mängel auf, welche insbesondere die ICT-Anbieter stark tangieren, teilweise sogar existenziell gefährden.

Aufgrund dieser Beurteilung hat der Vorstand des ICT-Anbieter-Verbands Swico einstimmig beschlossen, die Unterschriftensammlung für das Referendum gegen das BÜPF zu unterstützen.

18.3.16 /hh