Einschreiben
Bundesamt für Justiz
Direktionsbereich Strafrecht
Bundesrain 20
3003 Bern

Mittwoch, 18. August 2010

Totalrevision des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs – Vernehmlassungsantwort

Sehr geehrte Damen und Herren

Wir lassen Ihnen hiermit unsere Antwort auf die Vernehmlassung zur Totalrevision des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs zukommen.

Die Information Security Sociey Switzerland (ISSS) ist mit ihren über 750 Mitgliedern, darunter 100 Kollektivmitgliedern, führende Fachorganisation der Schweiz auf dem Gebiet von Schutz und Sicherheit der Informationssysteme. Die ISSS wurde 1993 als Verein unter dem früheren Namen FGSec gegründet und ist Mitglied von ICTswitzerland sowie offzieller Security Fachpartner von SwissICT.

Unsere Stellungnahme basiert auf zahlreichen Beiträgen unserer ISSS-Mitglieder, welche täglich mit Informationssicherheit in ihrem Beruf zu tun haben. Die Beiträge wurden ihm Rahmen einer Special Interest Group „Revision BÜPF“ von unserem Rechtsexperten lic. iur. Beat Lehmann konsolidiert.

Wir hoffen, dass wir mit unserer detaillierten Vernehmlassungantwort einen direkten Beitrag zur Förderung der Informationssicherheit in unserem Lande leisten können und danken Ihnen für die Berücksichtigung unserer Anträge.

1. Allgemeines

1.1 Die Revision wird mit den modernen Formen der Computerkriminalität begründet. In unserer Antwort zur Vernehmlassung vom 30. Juni 2009 zum Beitritt der Schweiz zum Übereinkommen des Europarates über die Cyberkriminalität (ECC), verfügbar unter https://www.isss.ch/fileadmin/publ/sigccc/ECC-Vernehmlassung-ISSS.pdf, haben wir eingehend dargelegt, dass unser auf der Informationstechnologie der 80er Jahre ausgerichtete Schweizer Strafrecht in der Erfassung der betreffenden Tatbestände zwar die bescheidenen Anforderungen der ECC erfüllt, in wichtigen Punkten jedoch der internationalen Entwicklung hinterher hinkt. Diesbezüglich besteht tatsächlich ein erheblicher Anpassungsbedarf.

1.2 Andererseits verfügt die Schweiz mit dem bestehenden BÜPF vom 6.10.2000 und der Bestimmungen von Art. 269ff der Schweizerischen Strafprozessordnung vom 5. Oktober 2007 (die gemäss Vernehmlassungsentwurf, obwohl noch nicht in Kraft getreten, bereits wieder geändert werden soll) über ein gut ausgebautes Instrumentarium zur Überwachung des Post- und Fernmeldeverkehrs, und es sind keine Umstände bekannt geworden oder im Begleitbericht schlüssig nachgewiesen, welche einen Ausbau der Überwachungsmittel und Verfahren in dem von der Revision vorgeschlagenen Umfang erfordern würden.

1.3 Den Interessen unseres Gemeinwesens und seiner Bürger wäre somit nach hier vertretener Auffassung wirkungsvoller durch den Ausbau des strafrechtlichen Schutzdispositivs vor den aktuellen Bedrohungen der Cyberkriminalität gedient als durch die Erweiterung des im internationalen Vergleich bereits sehr weitreichenden Überwachungssystems. Dabei ist zu berücksichtigen, dass viele Anbieter von Fernmeldediensten und die Infrastruktur für die elektronische Kommunikation in einem erheblichen Umfange mangels territorialer Anbindung an unser Land von der schweizerischen Gesetzgebung gar nicht erfasst werden, sodass mit dem revidierten BÜPF zwar im Inland eine umfassende Überwachungsordnung geschaffen wird, welche aber von den wirklich gefährlichen, international agierenden Tätern im Bereich Terrorismus, Menschenhandel, Korruption und andere Wirtschaftsdelikte relativ einfach umgangen werden kann.

1.4 Die Überwachung des Post- und Fernmeldeverkehrs betrifft ein elementares, durch die Bundesverfassung (Art. 13 Abs. 1 BV) gewährleistetes Grundrecht: Die Vertraulichkeit der privaten Kommunikation. Die im Gesetzesentwurf vorgesehene starke Erweiterung der Mittel und Verfahren zur Überwachung privater Kommunikation sollte daher durch einen entsprechenden Ausbau des Instrumentariums zur Kontrolle der gesetzes-konformen Anwendung dieser Mittel und Verfahren ausgeglichen werden.

1.5 Ziel der Gesetzgebung zur Bekämpfung der Cyberkriminalität sollte sein, den Schutz und die Sicherheit der Informationen zu erhöhen. Diesbezüglich wurde von unseren Mitgliedern festgestellt, dass die Einführung der geheimen Online-Überwachung, die Entwicklung und der Einsatz von Spähprogrammen (“Bundes-Trojaner“) und die Pflicht der Fernmelde- und Internet-Dienstanbieterinnen zur Entfernung der von ihnen angebrachten Vorrichtungen zur Wahrung der Vertraulichkeit privater Kommunikation zu einer erheblichen Minderung des Schutzes und der Sicherheit der Internet-kommunikation führen dürfte, die sich nachteilig auf den Wirtschaftsstandort Schweiz auswirken kann.

1.6 Besonders kritisch wird von unseren Mitgliedern die im Gesetz nicht weiter spezifizierte Ausdehnung der durch die Revision des BÜPF vorgesehenen vielfältigen und neuerdings mit Strafe bedrohten Überwachungs-Pflichten auf sämtliche Anbieterinnen von Telekommunikations- und Internet-Dienstleistungen erachtet. Dabei wird als

rechtsstaatlich höchst bedenklich die vorgesehene Übertragung der Durchführung der Überwachungsmassnahmen an die Anbieterinnen von Fernmelde- und Internet-Dienstleistungen betrachtet, d.h. das “Outsourcing“ staatlicher Tätigkeit in einem besonders heiklen Bereich an privatrechtlich organisierte Organisationen.

1.7 In diesem Zusammenhang ist noch besonders die auf aufwändigen organisatorischen und technischen Auflagen hinzuweisen, welchen die mit diesen Überwachungsmass-nahmen betrauten Organisationen unterworfen sein sollen, wie z.B. die Zertifizierungs-pflicht, die verlängerte Aufbewahrung von Verbindungsdaten, die Triage bzw. das Ausfiltern von Datenflüssen. Dass die DienstanbieterInnen nach den Vorstellungen des Gesetzgebers die Kosten dieser organisatorischen und technischen Massnahmen selber zu tragen haben, widerspricht nach hier vertretener Auffassung anerkannten Grundsätzen der Beteiligung Privater an einem gegen Dritte geführten Strafverfahren (vgl. die Entschädigung von Zeugen und Sachverständigen).

1.8 Darüber hinaus birgt die Überwälzung der Kosten für die Überwachung des elektronischen Kommunikations- und Internetverkehrs die nahe liegende Gefahr in sich, dass die zur Anordnung von Überwachungsmassnahmen ermächtigten Behörden von den ihnen neuerdings unentgeltlich zur Verfügung gestellten Mittel in einem Umfang Gebrauch machen, der durch das Gesetz nicht vorgesehen ist. Denn das revidierte BÜPF enthält weder eine externe institutionelle Kontrolle des “Zentralen Dienstes“ mit seinen erheblich erweiterten Kompetenzen, noch Rechtsmittel für die mit Überwachungsbegehren der Behörde konfrontierten DienstanbieterInnen.

2. Stellungnahme zu einzelnen Bestimmungen des Vorentwurfs

Art. 2 Abs. 1 Bst. b / 31 RevE – Persönlicher Geltungsbereich

Die Überwachung des Post- und Fernmeldeverkehrs soll im Auftrag des bereits bestehenden Überwachungsdienstes des Bundes (“Zentraler Dienst“) ausgeführt werden durch

a) die **Anbieterinnen von Post- und Fernmeldediensten**, einschliesslich jene Internet-Anbieterinnen (“ISP“), die ihre Tätigkeit berufsmässig ausüben, sowie durch

b) (natürliche und juristische) Personen, die berufsmässig für die Fernmeldedienst-anbieterinnen und ISP Kommunikationsdaten verwalten, an Dritte Kommunikations-daten weiterleiten oder die dafür notwendige Infrastruktur zur Verfügung stellen.

In Bezug auf die mit Überwachungsaufgaben betreuten Personen stellt sich die Frage, auf welche Stellen, welche Dienstleistungen im Zusammenhang mit dem Internet anbieten, das BÜPF in Zukunft ausgedehnt werden soll. Im Begleitbericht werden unter diesem Titel erwähnt: Reine Service-Provider, Web Hoster und Hosting Provider, Anbieterinnen von E-Mail und Mailbox-Diensten, von Speicherplatz oder von externer Daten-Aufbewahrung.

Dies bedeutet, dass in Zukunft alle natürlichen und juristischen Personen, die nicht für sich selber, sondern für Dritte, analoge und digitale Kommunikationsdaten bearbeiten, der Über-

wachungspflicht unterstellt sein sollen. Da praktisch bei jedem einzelnen Kommunikationsvorgang eine Mehrzahl von Dienstanbietern mit der Erfassung, Zwischenspeicherung und Weiterleitung der Daten befasst sind, führt die sehr allgemeine Umschreibung des RevE zu einer schwer absehbaren Ausdehnung des persönlichen Geltungsbereiches.

Darunter können auch Kommunikationsdienstleistungen in verbundenen Unternehmen fallen, das Angebot von Archivierungslösungen oder von Informations-Datenbanken, professionelle Dienstleistungen zur Datensicherung ("Managed Security Services"), Betreiberinnen von Informationsdiensten und -Plattformen aller Art (Yahoo, Google, Twitter, Facebook, Blogs) oder von elektronischen Marktplätzen (wie eBay oder Ricardo): Denn in allen diesen Erscheinungsformen der Informationsgesellschaft werden auf einer dafür geschaffenen Infrastruktur Kommunikationsdaten erfasst, weitergeleitet und gespeichert.

Nach dem Konzept des RevE BÜPF setzt die Erfüllung dieser Überwachungspflicht aufwändige organisatorische und technische Vorkehrungen voraus, welche die privaten Überwachungsorgane auf eigene Kosten zu entwickeln und zu betreiben haben (Art. 20-26 RevE), und die Verletzung der Überwachungspflicht durch diese unterstellten Organe ist darüber hinaus nach Art. 31 RevE mit Strafe bedroht, was bei einer derart unklaren Umschreibung des persönlichen Geltungsbereiches gegen das Legalitätsprinzip von Art. 1 StGB verstösst.

Aus diesen Überlegungen ergibt sich, dass der persönliche Geltungsbereich entweder durch eine Anpassung von Art. 2 RevE, oder durch Ausführungsbestimmungen in einer dafür vorgesehenen Verordnung auf jene Organisationen zu beschränken ist, welche geschäftsmässig Kommunikationsdienstleistungen für Dritte erbringen, wie in Art. 2 der Verordnung über Fernmeldedienste umschrieben.

Art. 6 / 33 RevE - Zentraler Dienst / Aufsicht / institutionelle Kontrolle

Der Bund betreibt durch den "Zentralen Dienst" ein Informationssystem zur Verarbeitung (d.h. Erfassung, Speicherung, Aufbewahrung und Gewährung des Online-Zugriffs) der durch die Überwachung des Fernmeldeverkehrs gewonnen Daten (Kommunikations- und Inhaltsdaten des Fernmelde- und Internet-Verkehrs der überwachten Personen).

Im Begleitbericht wird hervorgehoben, dass die Schaffung eines zentralen Systems unter dem Gesichtspunkt des Datenschutzes und der Wahrung der Grundrechte einen Fortschritt bilde, weil die Daten damit besser kontrolliert und geschützt werden können. Diesbezüglich enthält der Gesetzesentwurf die Bestimmung in Art. 33, dass der Zentrale Dienst über die Einhaltung der Gesetzgebung betreffend die Überwachung des Post- und Fernmeldeverkehrs wacht.

Andererseits schafft ein solches zentrales System mit der langfristigen Speicherung sämtlicher in der Schweiz aus den verschiedensten Gründen (nicht nur bei der Verfolgung qualifizierter Delikte) erfassten Daten aus dem privaten Kommunikationsverkehr aber auch offensichtliche Probleme für den Schutz der Grundrechte, der Privatsphäre und die Gefahr des Missbrauchs und verlangt nach hier vertretener Auffassung zwingend eine Kontrolle durch eine

unabhängige Instanz, wie z.B. den Eidgenössischen Datenschutzbeauftragten, welche die Interessen der Betroffenen zu wahren hat.

Die im RevE zur Verfolgung von Tatbeständen der Cyberkriminalität vorgesehene ausserordentlich weitgehende Ausdehnung der Überwachung des gesamten analogen und digitalen Kommunikationsverkehrs verlangt im demokratischen Rechtsstaat zwingend eine institutionelle Kontrolle - dies auch im Interesse der mit der Überwachung betrauten Stellen selbst (es sei in diesem Zusammenhang an frühere und aktuelle sog. “Fichen-Affären“ erinnert).

Art. 11 RevE - kontrollierte Aufbewahrung und Vernichtung der Daten

Die Daten über den Kommunikationsverkehr der überwachten Personen sollen im Informationssystem des Zentralen Dienstes während sehr lange Dauer von 5 bis 30 (sic!) Jahren gespeichert bleiben, wobei die Aufbewahrungsdauer durch unbestimmte Begriffe wie “so lange es für das verfolgte Ziel erforderlich ist“ bestimmt wird.

Darüber hinaus kann die mit dem Verfahren befasste Behörde vom zentralen Dienst die Herausgabe der Daten (in elektronischer Form) nach Ablauf der Aufbewahrungsdauer im zentralen System verlangen, ohne dass im BÜPF bestimmt ist, zu welchem Zweck und wie lange die ersuchende Behörde die Daten dann weiterhin nutzen darf.

Diesbezüglich ist das Gesetz zwingend durch Regeln über die Bestimmung der Aufbewahrungsfrist im Einzelfall, die Voraussetzungen und Pflichten sowie das Vorgehen für die unverzügliche Vernichtung der für die Zwecke der Überwachung nicht mehr benötigten gespeicherten Daten, sowie die Kontrolle der tatsächlichen Löschung zu ergänzen.

Wie bereits an anderer Stelle erwähnt führt der RevE zwar im Interesse des Schutzes des Gemeinwesens, von Gesellschaft und Wirtschaft vor dem Missbrauch der Kommunikationsinfrastruktur der Informationsgesellschaft durch kriminelle Organisationen zu einer damit einhergehenden ausserordentlich weitgehenden Ausdehnung der Überwachung der gesamten Informationstätigkeit, hat jedoch bisher vernachlässigt, dass aus fundamentalen rechtsstaatlichen Überlegungen diese Kompetenzen der Überwachungsorgane durch institutionelle Normen und Kontrollen geregelt und einer unabhängigen Kontrolle zu unterstellen sind.

Art. 18 RevE - Zertifizierung

In Zukunft soll die Eignung der Anbieterinnen von Fernmeldediensten zur “wirksamen Durchführung von Überwachungsmassnahmen“ auf deren eigene Kosten durch den Zentralen Dienst auf der Grundlage einer Zertifizierung bescheinigt werden.

Dazu ist zunächst festzuhalten, dass der Gegenstand und die Verfahren der Zertifizierung sehr unbestimmt formuliert sind und sich die grundsätzliche Frage stellt, ob sich die Eignung

einer Dienstanbieterin zur gesetzeskonformen Durchführung der Überwachung überhaupt in einem Zertifizierungsverfahren feststellen lässt.

Auch ist nicht klar, ob sich auch Internet Service Provider (ISP) und die in Art. 2 Abs. 1 (b) RevE genannten weiteren Provider zertifizieren lassen müssen. Aufgrund des fast unübersehbaren Kreises solcher Provider wäre damit der Aufbau eines kostspieligen Zertifizierungsapparates von sehr zweifelhaftem tatsächlichen Wert verbunden.

RevE passim – Kostentragungspflicht der Dienstanbieterinnen

Hinzuweisen ist auch auf die wesentliche Änderung im rev BÜPF, dass die privaten Personen, welche mit der Durchführung der Überwachung betraut werden, dafür keine Entschädigung mehr erhalten, wie dies unter Art. 16 des geltenden BÜPF noch vorgesehen war. Wie bereits erwähnt verstösst diese Regelung gegen bisher anerkannte Grundsätze über die Beteiligung Privater als Zeugen, Sachverständigen und Gehilfen der Strafverfolgungsbehörden im rechtsstaatlichen Strafverfahren.

Zusammen mit den an die privaten Provider delegierten erweiterten Aufgabe und die immer komplexer werdenden Überwachungsmassnahmen im elektronischen Kommunikationsverkehr dürfte das rev. BÜPF daher eine nicht unerhebliche Belastung der Diensteanbieterinnen mit sich bringen. Der Hinweis im Begleitbericht, dass die zusätzlichen Kosten nur eine verhältnismässig geringfügige Belastung des Umsatzes (sic!) der Fernmeldedienstanbieter und ISP nach sich ziehen dürfte, erscheint für die professionell tätigen Mitglieder der ISSS etwas lebensfremd, da Mehrkosten in der Höhe von Umsatzprozenten auf jeden Fall viele vorwiegend kleinere Dienstanbieterinnen mit tiefer Bruttomarge in den Ruin treiben würden.

Art. 20 Abs. 3 und Art. 22 RevE – Identifizierung der Internet-Benützer

Wie schon aus den Ausführungen im Begleitbericht abgeleitet werden kann, würde die Einführung einer Pflicht der Fernmeldedienstanbieter zur persönlichen Identifikation jedes einzelnen Teilnehmers am digitalen Kommunikationsverkehr und bei der Nutzung des Internet vor praktisch unlösbare Aufgaben stellen, weil die Möglichkeit, sich z.B. über ein Wi-Fi-Netzwerk oder über öffentlich zugänglichen Stationen (in Hotels, Restaurants, Bibliotheken usw.) Zugang zum Internet zu beschaffen, zu den nicht rückgängig zu machenden Errungenschaften der Informationsgesellschaft gehören.

Es ist aus der Sicht der ISSS undenkbar, dass sich in der Schweiz – im Unterschied zum Rest der Welt – jeder Benützer, der eine Verbindung zum Internet jerstellt, zuerst durch ein Identifikationsmittel (wie die SuisseID) gegenüber dem System ausweisen und identifizieren müsste - ganz abgesehen, dass solche technischen Identifikationsmittel von kriminellen Elementen voraussichtlich umgangen werden können.

Gegenstand und Umfang der Teilnehmeridentifikation sind daher nach den heutigen und voraussehbaren künftigen Formen der Nutzung der digitalen Kommunikation und des Internets anzupassen und zu konkretisieren.

Art. 21 Abs. 2 RevE – Verzugslose Datenlieferung

Die Mitglieder der ISSS betrachten insbesondere die vorbehaltlose und unbeschränkte Verpflichtung der Lieferung von Informationen über den Fermeldeverkehr überwachter Personen in Echtzeit als ausserordentlich weitgehend: Sie kann die Dienstanbieterin zur Entwicklung und Bereitstellung umfangreicher organisatorischer und technischer Massnahen zwingen, welche die Dienstanbieter nach dem RevE auf eigene Kosten bereit zu stellen haben.

Art. 21 Abs. 2 Rev E - Entfernung von Verschlüsselungen

Nach dem RevE BÜPF müssen Fernmeldedienstanbieter und ISP müssen im Rahmen von Überwachungsverfahren die von ihnen angebrachte Verschlüsselungen an Daten vor deren Weiterleitung an den zentralen Dienst entfernen.

Die “Entschlüsselung“ bezieht sich offenbar auch auf die offen zu legenden Telekommunikationsdaten nach Art. 14 und 20 RevE, d.h. auf einen sehr weiten Bereich der Fernmelde- und Internet Überwachung.

Die Offenlegung gesicherter elektronischer Kommunikation durch die Dienstanbieter ist ein in qualifizierten Fällen wohl notwendiger, aber äusserst weitgehender Eingriff in das verfassungsmässig garantierte Fernmeldegeheimnis. Es ist davon auszugehen, dass Fernmeldedienstanbieterinnen und ISP ihre Kunden nach Inkrafttreten des RevE aufgrund ihrer gesetzlichen Treue- und Sorgfaltspflicht ihre Kunden darüber aufklären müssen, dass die verwendete Verschlüsselung im Rahmen eines Überwachungsverfahrens nach BÜPF aufgehoben werden kann.

Die Auswirkungen der in Art. 21 Abs. 2 RevE vorgesehenen vorbehaltlosen Offenlegungspflicht auf die schweizerische IT Landschaft ist schwierig abzuschätzen. Es ist durchaus möglich, dass Anwender, welche auf die Wahrung der Geschäfts- und Berufsgeheimnisses besonders angewiesen sind (Forschungseinrichtungen, Banken, Anwälte, Medizinalpersonen) in Zukunft auf die von Dienstanbietern angebotenen geschützten Kommunikationsverfahren verzichten und für ihre Bedürfnisse auf proprietäre “peer-to-peer“ Verschlüsselungen ausweichen werden. Das gleiche würden - leider – vor allem auch jene Kreise tun, die ihre kriminellen Aktivitäten vor dem Zugriff der Behörden schützen wollen.

Für die ISSS, deren Mitglieder sich für einen hohen Stand der Vertraulichkeit und Sicherheit der Daten in der elektronischen Kommunikation einsetzen, bedeutet die neue Bestimmung über die Offenlegung verschlüsselter Informationen einen schwerwiegenden Eingriff in einen wesentlichen Bereich der Informationsgesellschaft.

Die Offenlegung der von Dienstanbietern angebrachten Verschlüsselung zum Schutz der elektronischen Kommunikation ihrer Kunden sollte daher auf bestimmte, im Gesetz klar umschriebene Fälle beschränkt werden, und es sollte ein Verfahren vorgesehen werden, in welchem die Dienstanbieter die Interessen ihrer Kunden an geschützter Kommunikation vor der Offenlegung der Schlüssel geltend machen und einer richterlichen Entscheidung zuführen können.

Art. 21.3 - Pflicht zur Filterung / Triage von Datenbeständen und Datenflüssen

Auf Verlangen des zentralen Dienstes sind die Fernmeldedienstanbieter und ISP verpflichtet, dem Zentralen Dienst nur einen bezeichneten Typ oder bestimmte Typen von Daten aus dem Datenstrom zu liefern.

Eine solche Aussonderung der gewünschten Daten aus dem ungefilterten Datenstrom kann zu einem sehr erheblichen Triage-Aufwand führen, der von den Fernmeldedienstanbietern und ISP zu tragen ist; sie müssen auch die entsprechenden Triage-Systeme und Verfahren entwickeln.

Es ist Pflicht des ISSS, an dieser Stelle warnend darauf hinzuweisen, dass die Entwicklung solcher Filtrierungs- und Triage-Systeme leider auch die Wirkung haben kann, die Ausforschung von Datenbestände und Datenflüsse durch Unberechtigte zu erleichtern und daher den Stand der Informationssicherheit in unserem Lande beeinträchtigen kann.

Nach hier vertretener Auffassung sollten solche Analyse- und Filtrierungs-Programme daher nur in qualifizierten Einzelfällen, aufgrund richterlicher Anordnung angeordnet werden dürfen: Die generelle Bereitstellung solcher Werkzeuge zur Analyse von Datenbeständen und Datenflüsse schafft ein erhebliches zusätzliches Risiko für die Gewährleistung des Informationsschutzes.

Art. 21.4 – Entwicklung und Einsatz von Spionageprogrammen

Fernmeldedienstanbieterinnen und ISP sind verpflichtet, dem zentralen Dienst bei der Überwachung zu unterstützen, für welche Informatikprogramme nach Art. 270bis StPO zum Abfangen und Lesen von Daten erforderlich sind

Der neue Art. 270bis StGB schafft die Möglichkeit des Einsatzes von Spionageprogrammen (“Bundes-Trojaner“). Dass der Einsatz Spionage-Programm zur verdeckten Online-Durchsuchung von informationsverarbeitenden Systemen schwerwiegende grundrechtliche Bedenken erweckt, sollte seit dem Entscheid des deutschen Bundesverfassungsgerichtes vom 27. Februar 2008 - 1 BvR 370/07 / 1 BvR 595/07 auch für den Gesetzgeber in der Schweiz offenkundig sein.

Es ist im RevE nicht klar geregelt, ob die Fernmeldedienstanbieterinnen und ISP im Auftrag des Zentralen Dienstes selber solche Spionageprogrammen entwickeln und einsetzen müssen, oder ob sie nur die Infrastruktur, Methoden und Verfahren für den Einsatz der vom Dienst entwickelten "Bundes-Trojaner" bereit stellen müssen. Auf jeden Fall erscheint die Zusammenarbeit des Zentralen Dienstes mit den Fernmeldedienstanbieterinnen und ISP in bezug auf den Einsatz von "Bundes-Trojanern", einem Untersuchungsmittel von verfassungsrechtlich höchst zweifelhafter Art, als ein ganz kritischer Regelungsbereich des revidierten BÜPF.

Dazu ist aus der spezifischen Sicht der Mitglieder der ISSS ergänzend anzubringen, dass die unter dem RevE vorgesehene bzw. zulässige Entwicklung und Verwendung der sonst mit krimineller Strafe bedrohten Spionageprogrammen zur Ausforschung von Datenbeständen und Datenflüssen geeignet sein wird, das in der Schweiz erreichte Niveau von Datenschutz und Informationssicherheit erheblich zu beeinträchtigen.

Art. 21 RevE – Auswirkungen auf Schutz und Sicherheit der Informationen

Wie bereits erwähnt können die verschiedenen in Art. 21 RevE vorgesehenen neuen Pflichten der Dienstanbieter zur Erfassung und Speicherung von Informationen über die digitale Kommunikation, wie namentlich die Bereitschaft zur verzugslosen Herausgabe von Informationen, die vorbereitete Entfernung der Verschlüsselung der Informationen, Entwicklung und Bereitstellung von Spionageprogramme, zu einer ganz erheblichen Schwächung des von den Mitgliedern der ISSS aktiv geförderten Dispositivs der umfassenden Sicherung von Informationen in unserem Land führen.

Es stellt sich in diesem Zusammenhang aus der Sicht der Mitglieder der ISSS die Frage, ob es sich aufgrund der nicht zu bestreitenden mögliche Nutzung der Informations- und Kommunikationsmittel durch Unbefugte zur Vorbereitung und Durchführung rechtswidriger Handlungen wirklich rechtfertigt, eine derart weitgehende Schwächung des im Interesse des weit überwiegenden Anteils berechtigter Anwender erzielten Standes von Informationsschutz und Informatiksicherheit der Schweiz in Kauf zu nehmen.

Sollten die vom BÜPF vorgesehen Massnahmen unverändert realisiert werden, wäre nach hier gestützt auf die Meinung unabhängiger Experten vertretenen Auffassung die Weitergabe von Daten aus geschützten Wirtschaftszweigen an unberechtigte Empfänger, einschliesslich Behörden im Ausland, erheblich einfacher als heute: Denn die Daten wären ja dann umfassend geordnet archiviert, unverzüglich abrufbar, mit Hilfe von Durchsuchungs- und Filterungsmöglichkeiten sortierbar, und mit der vorbereiteten Aufhebung der Verschlüsselung für unerlaubte Zwecke unmittelbar verwendbar.

Es stellt sich somit folgende Frage: Soll der nicht zuletzt durch die Mitglieder der ISSS aufgebaut hohe Stand des Informationsschutzes in unserem Land auf dem Altar der erleichterten Ermittlung und Verfolgung möglicher Straftäter geopfert werden? Das ist letztlich

eine politische Frage, welche durch die Vertreter von Bevölkerung und Wirtschaft im Parlament entschieden werden muss.

Art. 23/31 RevE – Verlängerte Aufbewahrung der Kommunikationsdaten

Die Kommunikationsdaten (nicht die Inhaltsdaten) über den Fernmeldeverkehr sind von den Fernmeldedienstanbieterinnen und ISP neu während zwölf Monaten aufzubewahren. Die vorsätzliche Verletzung dieser Aufbewahrungspflicht ist neu mit Strafe bedroht.

Diese Bestimmung bringt für die Fernmeldedienstanbieterinnen und ISP zweifellos einen gewissen zusätzlichen Aufwand. Aus dem Begleitbericht ergibt sich keine schlüssige Begründung für die Verdoppelung der Aufbewahrungsdauer.

Die Vorratsdatenspeicherung ist ein Eingriff in das grundrechtlich geschützte Telekommunikationsgeheimnis. Die sich aus der Änderung der Gesetzgebung ergebende sehr grossen Datenmengen schaffen mögliche Gefährdungen für die Individuen und die Unternehmen: Denn nach den Grundsätzen des Persönlichkeits- und Datenschutzes sind personenbezogene Angaben – und darum dürfte es sich nach der Rechtsprechung auch bei den Verbindungsdaten handeln – unverzüglich zu vernichten, wenn für deren Aufbewahrung kein zwingender Grund mehr besteht.

Allenfalls könnte das Gesetz daher so angepasst werden, dass der Zentrale Dienst im Einzelfall anordnen kann, dass ein Dienstanbieter die Verbindungsdaten betreffend einen oder mehrere bestimmte Teilnehmende am Kommunikationsverkehr länger, bis maximal 12 Monate aufzubewahren hat.

Art. 25 RevE - Informationen über Technologien und Dienste

Fernmeldedienstanbieterinnen und ISP müssen den zentralen Dienst auf dessen Anfrage jederzeit ausführlich über die Art und Merkmale von Technologien und Diensten unterrichten, welche sie der Öffentlichkeit zur Verfügung gestellt haben oder stellen werden.

Abgesehen von dem durch diesen Art. 25 geschaffen zusätzlichen Aufwand ist auf das Risiko der Preisgabe von Geschäfts- und Betriebsgeheimnissen der Fernmeldedienstanbieterinnen und ISP beim Vollzug einer solchen Anfrage des zentralen Dienstes hinzuweisen.

Aus der Mitte der ISSS wird dazu aufmerksam gemacht, dass die hier angesprochenen “Technologien“ sich in einem Grossteil der Fälle im Besitz ausländischer Unternehmen befinden werden. Es ist mehr als zweifelhaft, ob die internationalen Anbieter der Informations- und Kommunikationstechnologie ohne weiteres bereit sein werden, dem Zentralen Dienst der Schweiz ihre geheimen Technologien herauszugeben, auch wenn der zentrale Dienst darüber eine strafbewehrte Anordnung nach Art. 31 RevE erlässt.

Diese Bestimmung könnte somit für den Wirtschaftsstandort Schweiz ganz erhebliche Probleme hervorrufen und Retorsionsmassnahmen auslösen bzw. dazu führen, dass die

Inhaber der Technologie ihrer aktuellen Systeme und Verfahren aufgrund der möglichen Preisgabegefahr in der Schweiz nicht mehr einsetzen. Damit würde der Informationsgesellschaft Schweiz ein echter Bärendienst erwiesen.

Eine derartige Verpflichtung der Inhaber von Informationstechnologie müsste nach Auffassung der ISSS international abgestimmt werden und kann bis zu einem entsprechenden internationalen Abkommen nur von Fall zu Fall, aufgrund einer Übereinkunft des zentralen Dienstes mit dem Inhaber der Technologie umgesetzt werden. Wir sind überzeugt, dass sich die Inhaber der Technologie im Einzelfall einer begründeten Offenbarung bestimmter konkreter Technologien und Verfahren nicht widersetzen werden.

Art. 34 RevE – Rechtsschutz

In diesem Zusammenhang wurde von unseren Mitgliedern insbesondere auch darauf hingewiesen, dass es für die Dienstanbieter kein Verfahren gibt, eine vom Zentralen Dienst angeordnete Überwachung (einschliesslich Offenlegung der Verschlüsselung, Einrichtung und Einbau von Spionage-Programmen, Triage der Datenbestände und Datenflüsse nach Art. 21 Abs. 21 Abs. 2 – 21 Abs. 4 RevE) in Frage zu stellen, d.h. in einem rechtsförmigen Verfahren durch eine richterliche Behörde überprüfen zu lassen.

Dabei vertreten wir die Meinung, dass ein Dienstanbieterin in Anlehnung an die vorgeschlagenen Fassung von Art. 34 RevE zwar die Anordnung einer Überwachung als solche und deren Verhältnismässigkeit nicht in Frage und einer richterlichen Überprüfung unterstellen kann, wohl dagegen die von der Zentralen Behörde angeordneten Einzelmassnahmen, wie Umfange der Triagemassnahmen, Einsatz von Spionageprogrammen, Offenbarung bestimmter Technologien und Verfahren: Hier müsste im Einzelfall eine einvernehmliche Regelung bzw. ein gerichtlicher Entscheid angestrebt werden.

Zusammenfassung

Die Information Security Society Switzerland (ISSS) als Organisation, welche das Ziel der Förderung der Sicherheit der Informations- und Kommunikationstechnologie in der Schweiz verfolgt, unterstützt die Bestrebungen, welche den Strafverfolgungsbehörden die Mittel zur wirkungsvollen Bekämpfung der modernen Formen der Cyber-Kriminalität verschaffen. Diesbezüglich sollten jedoch nicht nur der Strafprozess und das BÜPF, sondern insbesondere auch verschiedene durch die technische Entwicklung durch das StGB nicht mehr genügend erfassten Tatbestände angepasst werden.

Bei der Erweiterung der Mittel und Verfahren zur Überwachung der digitalen Kommunikation und der Nutzung des Internets darf jedoch nicht ausser Acht gelassen werden, dass damit den Strafverfolgungsbehörden äusserst wirkungsvolle Instrumente zur geheimen Überwachung der privaten und durch Art. 13 BV geschützten Kommunikation von Personen, Unternehmen und Verwaltungsstellen zur Verfügung gestellt werden

Die Forderung zur persönlichen Identifizierung der Teilnehmenden am Kommunikationsverkehr und der Internetnutzer, die integrierte langfristige Speicherung aller Daten aus der elektronischen Überwachung in einem grossen zentralen System (mit den dadurch geschaffenen Auswertungsmöglichkeiten) und der vorgesehene Einsatz von Spionageprogrammen ruft jedoch zwingend nach adäquat ausgelegten Kontrollvorkehrungen durch eine unabhängige fachkundige Kontrollinstanz wie z.B. der Eidgenössische Datenschutzbeauftragte: Nicht nur die Spiesse der Strafverfolgungsbehörden und der Cyber-Kriminellen sollten gleich lang sein, sondern auch die Spiesse der Behörde und der in ihrer Privatsphäre und ihrer grundrechtlich geschützten Kommunikation betroffenen Bürger.

Es ist ein besonderes Anliegen der ISSS, den Gesetzgeber auf die zu wenig beachteten Risiken für den Informationsschutz und die Informatiksicherheit in der Schweiz hinzuweisen, welche namentlich durch die nach RevE BÜPF verlangte generelle Pflicht zur Aufhebung der von Anbietern zum Schutz der Kommunikation der Teilnehmenden angebrachten Verschlüsselungen, die Vorkehrungen zur Filterung und Triage der Datenflüsse, der durch das RevE BÜPF geförderte Einsatz von Spionageprogrammen und die geforderte Offenbarung geheimer Technologien hervorgerufen werden

Darüber hinaus dürfte die im RevE BÜPF vorgesehene Übertragung der organisatorisch-technischen Überwachungsmassnahmen und der verschiedenen damit verbundenen zusätzlichen Aufgaben vom Gemeinwesen auf die Fernmeldedienstanbieter und ISPs, wie z.B. die neu geschaffene Zertifizierungspflicht, die Qualitätskontrolle, die Verdoppelung der Aufbewahrungsdauer der Randdaten, die Identifizierung aller Internetnutzer an öffentlich zugänglichen Orten wie Hotels, Schulen, Restaurants, die Entfernung von privaten Schlüsseln, die Triage der bei der Überwachung erfassten Daten usw. eine nicht unerhebliche zusätzliche Belastung der Privatwirtschaft nach sich ziehen, welche den allgemein anerkannten Grundsätzen für die Beteiligung Privater am Strafverfahren widersprechen.

Wenn die ISSS somit auch grundsätzlich die Zweckmässigkeit der Revision des BÜPF anerkennt und den vorliegenden Entwurf als Schritt in die zutreffende Richtung erachtet, so muss doch festgehalten werden, dass der Gesetzesentwurf, gerade auch unter dem Gerichtspunkt des Informationsschutzes und der Informatiksicherheit, mit derart gravierenden Mängeln behaftet ist, dass er in verschiedenen Punkten grundlegend überarbeitet werden sollte.

Mit freundlichen Grüssen

Dr. Thomas Dübendorfer
Präsident
Information Security Society Switzerland ISSS
president@isss.ch
www.isss.ch

lic. iur. Beat Lehmann
Koordinator
ISSS Special Interest Group
“Revision BÜPF”