ISSS NewsFlash August 2010



Editorial

Neue Partnerschaften, Revision BÜPF und SIGs

Die ISSS hat neue Partnerschaften geschlossen, die Ihnen neu auch Rabatte auf Bücher und Software bieten. Für KMUs führen wir mit dem SKV aktuell eine Spezialaktion durch.

Unsere neu gegründete SIG „SuisseID – benefits and risks for e-Commerce“ ist mit 21 Mitgliedern sehr erfolgreich gestartet und weitere spannende SIGs stehen in den Startlöchern. Noch können Sie sich dazu anmelden.

Im Focus dieser Ausgabe drucken wir die per 18.8.2010 beim Bundesamt für Justiz eingereichten Stellungnahmen von ISSS und von David Rosenthal zur umfangreichen Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), welche u.a. Staatstrojaner zu legitimieren plante, im Volltext ab.

Im Rahmen der geplanten Portraitletters können auch Sie als Security Professional im ISSS NewsFlash zu Wort kommen, und das erst noch mit professioneller Unterstützung durch einen Journalisten. Bei Interesse melden Sie sich direkt bei newsflash@isss.ch.

Dr. Thomas Dübendorfer
Präsident, ISSS
president@isss.ch

Highlights in dieser Ausgabe

ISSS:

- Thali AG neuer Partner von ISSS - Spezialkonditionen auf Software und Bücher
- ISSS Mitglieder stellen sich vor im ISSS NewsFlash
- Spezialangebot von ISSS für Mitglieder im Schweizerischem KMU Verband SKV
- Fachpartnerschaft mit ASIS
- STZ interviewt ISSS-Vorstand

SIGs: Erfolgreicher Start und weitere Gründungen geplant

Focus: Revision BÜPF

- Stellungnahme der ISSS
- Stellungnahme von David Rosenthal

Review: Security Lunch in Lausanne

Agenda:

- Partnerevents: hashdays workshops, ISSE
- ISSS Security Events
  - ISSS Secuity Lunches: „SuisseID - erste Erfahrungen aus der Praxis“ und „Cloud Computing - was ist aus rechtlicher Sicht zu beachten?“
  - Yubikey als Geschenk

Information Security Society Switzerland

ISSS

Thali AG neuer Partner von ISSS - Spezialkonditionen auf Software und Bücher

Seit August 2010 ist die Thali AG neuer Partner von ISSS. Dadurch erhalten alle ISSS-Mitglieder Spezialkonditionen bei der Thali AG (www.thali.ch) mit Rabatt auf Bücher, Spiele, Puzzles (je 15%), Software, Tinte, Toner (je 10%) und Updates (5%). Das Angebot umfasst u.a. Microsoft Software und O'Reilly Bücher.

Details zum Vorgehen für den Erhalt des Rabatts finden Sie wie immer in unserem ISSS Mitgliederbereich auf http://www.isss.ch/mitgliederbereich/.

ISSS Mitglieder stellen sich vor im ISSS NewsFlash

Durch die geplante Einführung von „Portraitletters" im ISSS NewsFlash zu Security Professionals, die bei ISSS Mitglied sind, wollen wir der ISSS ein persönlicheres Gesicht geben. Was bewegt unsere Mitglieder, die täglich mit Information Security zu tun haben? Wo liegen die Herausforderungen? Als Basis des Portraitsletters dient ein Telefoninterview, woraus ein von der ISSS beauftragter Journalist den Text frü den ISSS NewsFlash verfasst. Das portraitierte Mitglied erhält den Text zum Gegenlesen für die Druckfreigabe. Haben wir Ihr Interesse geweckt? Wenn Sie auch portraitiert werden wollen, schreiben Sie an newsflash@isss.ch,.

Spezialangebot von ISSS für Mitglieder im Schweizerischem KMU Verband SKV

Die ISSS durfte am 27.7.2010 ihr 100. Firmenmitglied begrüssen und möchte ganz bewusst auch vermehrt KMUs ansprechen und entsprechend sind wir seit August 2010 ein Partnerverband des Schweizerischen KMU Verbands (SKV). Zu dieser Partnerschaft gehört auch, dass sich Mitglieder des SKVs, die ISSS als Firmenmitglied beitreten, ein Spezialangebot erhalten:

- Sie müssen für das laufende Jahr 2010 keinen Mitgliederbeitrag bezahlen.
- Sie erhalten zudem einen Gratiseintritt für einen Vertreter Ihrer Firma zu unserer grössten Tagung, der Berner Tagung für Informationssicherheit zum Thema "Unbegrenzte Mobilität - Chancen und Risiken (dies entspricht einem Gegenwert von CHF 240).

Das Spezialangebot ist gültig bis 1. November 2010 für Firmen des SKVs, die sich als Neumitglieder bei ISSS anmelden. Alles weitere auf https://www.isss.ch/kmu/.

Fachpartnerschaft mit ASIS

Das ASIS International Chapter 160 Switzerland ist im August 2010 mit ISSS eine Partnerschaft eingegangen. Dadurch gelten für ISSS-Mitglieder an Veranstaltungen vom ASIS International Chapter 160 Switzerland ab sofort die ASIS-Mitgliedertarife. Zudem ist der Besuch von zwei Fachreferaten inkl. Apéro kostenlos pro ISSS-Mitglied. Für den Besuch von mehr als zwei Fachreferaten wird eine ASIS-Mitgliedschaft vorausgesetzt. Details zu den ASIS-Veranstaltungen und zum Vorgehen bei der Anmeldung für den Erhalt der Spezialkonditionen finden Sie im ISSS Mitgliederbereich auf http://www.isss.ch/mitgliederbereich/. Der nächste ASIS-Anlass ist das ASIS-Fachmeeting mit einem Referat zu "Cybercrime" von Dr. Thomas Dübendorfer am 7.9.2010 von 16:30 - 18:30 im WIDDER Hotel in Zürich mit anschliessendem Apero und ist für ISSS-Mitglieder kostenlos. Eine Anmeldung beim ASIS Vice Chairman asis@bcswitzerland.com ist erforderlich.

STZ interviewt ISSS-Vorstand

Ein Interview mit Dr. Lukas Ruf zu "Stabilität Internet" und eines mit Bernhard Tellenbach zu "Hacking" erscheint in der Zeitschrift STZ von Swiss Engineering zum Schwerpunkt "IT Sicherheit". Beide sind Mitglied im ISSS-Vorstand.

SIGs: Erfolgreicher Start und weitere Gründungen geplant

SIG "SuisseID – benefits and risks for e-Commerce" offiziell gestartet

Unter der Leitung von Anthony Thorn (anthony.thorn@isss.ch) wurde diese SIG mit dem Kick-Off Meeting vom 12.7.2010 offiziell gegründet. Die SIG hat 21 (!) Mitglieder, welche die Chancen und Risiken bezüglich des Einsatzes der SuisseID untersuchen und Empfehlungen für die Nutzung der SuisseID durch natürliche Personen (insbesondere aus Bürger-, Mitarbeiter- und Konsumentensicht) erstellen.

Innerhalb dieser SIG existieren zwei Untergruppen:

- Chancen, Risiken und Massnahmen
- Konsumentenschutz

Weitere Gründungen geplant

Die folgenden drei SIGs, die sich in Gründung befinden, suchen noch Mitglieder.

Social Media als Informationsquelle: Möglichkeiten und Gefahren

Informationssicherheit in 10 Jahren

Computerkriminalität und Schadprogramme

Bis 12.9.2010 können Sie sich noch für diese SIGs anmelden. Sie finden sämtliche Informationen zu den SIGs in Gründung auch auf http://www.isss.ch/aktivitaeten/.

Aktuelle SIGs für ISSS-Mitglieder

Special Interest Groups in Gründung

- **SIG Social Media als Informationsquelle: Möglichkeiten und Gefahren**
  Leitung: Anton Heer
  anton.heer(at)isss.ch
  Detailbeschreibung zu dieser SIG: PDF

  Interessierte Mitglieder melden sich bitte bis 12.09.2010 per E-Mail bei Anton Heer.
  Inhaltliche Fragen richten Sie ebenfalls bitte direkt an Herrn Heer.

- **SIG Informationssicherheit in 10 Jahren**
  Leitung: Rolph Haefelinger
  rolph.haefelfinger(at)isss.ch
  Detailbeschreibung zu dieser SIG: PDF

  Interessierte Mitglieder melden sich bitte bis 12.09.2010 per E-Mail bei Rolph Haefelfinger.
  Inhaltliche Fragen richten Sie ebenfalls bitte direkt an Herrn Haefelfinger.

- **SIG Computerkriminalität und Schadprogramme**
  Leitung: Marc Furner
  mark.furner(at)isss.ch
  Detailbeschreibung zu dieser SIG: PDF

  Interessierte Mitglieder melden sich bitte bis 12.09.2010 per E-Mail bei Marc Furner. Inhaltliche Fragen richten Sie ebenfalls bitte direkt an Herrn Furner.

Aktuelle Special Interest Groups

- **SIG SuisseID – benefits and risks for e-Commerce**
  (sig-sid, Leitung Anthony Thorn, Gründung 12.7.2010, Status: aktiv)

  Innerhalb dieser SIG existieren zwei Untergruppen:
  - Chancen, Risiken und Massnahmen
  - Konsumentenschutz

  Die originale Ausschreibung zu dieser SIG ist als PDF verfügbar.

- **SIG Revision BÜPF**
  (sig-buepf, Leitung Beat Lehman, Gründung: 22.6.2010, Status: aktiv)
  Resultat: Detaillierte Stellungnahme der ISSS zur Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). Eingereicht ans Bundesamt für Justiz per 18.8.2010.

- **SIG Cybercrime Convention "ECC Arbeitskreis"**
  (sig-scc, Leitung Beat Lehman, Gründung: 16.4.2009, Status: aktiv, Kick-off meeting am 19.5.2009)
  Resultat: Detaillierte Stellungnahme zum Nachvollzug der European Cybercrime Convention in der Schweiz und Artikel "Rechtshilfe gegen Kriminalität im Internet" in der NZZ am Sonntag vom 25.10.2009.

- **SIG Secure Information Exchange**
  (sig-sie, Leitung Martin Sibler, Gründung: 15.3.2009, Status: aktiv)
  Ziele:

  Weitere Infos zu dieser SIG finden Sie unter http://www.sgrp.ch/securex

Focus: Revision BÜPF – Stellungnahme der ISSS

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

Die ISSS Special Interest Group „Revision BÜPF" bestehend aus zahlreichen ISSS-Mitgliedern, Vertretern des ISSS-Vorstandes, dem ISSS-Präsidenten und weiteren Experten haben unter Leitung von ISSS-Vorstandsmitglied Beat Lehmann in einer Rekordzeit von sieben Wochen trotz Sommerferien unter Einbezug des Berichts zur BÜPF-Revision eine detaillierte Stellungnahme zur Vorlage der BÜPF-Revision erarbeitet. Die Stellungnahme ist hier im Originaltext abgedruckt wie per 18.8.2010 ans Bundesamt für Justiz eingereicht. Bei Fragen wenden Sie sich bitte direkt an beat.lehmann@isss.ch.

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 gesetzeskonformen 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 Internetkommunikation 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 Überwachungsmassnahmen betrauten Organisationen unterworfen sein sollen, wie z.B. die Zertifizierungspflicht, 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 Fernmeldedienstanbieterinnen und ISP Kommunikationsdaten verwalten, an Dritte Kommunikationsdaten 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 Überwachungspflicht 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 organisatorischtechnischen 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, ISSS

lic. iur. Beat Lehmann, Koordinator „SIG Revision BÜPF“

Focus: Revision BÜPF – Stellungnahme von David Rosenthal

Totalrevision des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (Vernehmlassung)

Folgender Text gibt den Brief von David Rosenthal vom 18.8.2010 an den Direktionsbereich Strafrecht im Bundesamt für Justiz in Bern wieder. Wir danken dem Autor für die Genehmigung für den Abdruck.

Sehr geehrte Damen und Herren

Ich erlaube mir, im Rahmen der Vernehmlassung zum Vorentwurf einer Totalrevision des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (**VE-BÜPF**) Stellung zu nehmen.

Ich beschränke mich dabei bewusst auf einige wenige grundsätzliche Punkte im Fernmeldebereich, die nach meiner persönlichen Meinung und Erfahrung aus meiner Praxis sehr problematisch sind und in dieser Form nicht umgesetzt werden sollten.

Dies betrifft vor allem die geplante Erweiterung des Anwendungsbereichs des BÜPF sowie gewisse Pflichten, die den Anbietern im Anwendungsbereich des BÜPF neu auferlegt werden sollen.

Art. 2 Abs. 1 Bst. b VE-BÜPF

Grundsätzliches

Der Geltungsbereich des BÜPF soll durch Art. 2 Abs. 1 Bst. b VE-BÜPF erklärtermassen stark ausgeweitet werden. Nicht mehr nur Fernmeldedienstanbieter werden erfasst, sondern praktisch jedes Unternehmen, das in irgendeiner Weise "beruflich" mit "Kommunikationsdaten" zu tun hat.

Die Motivation einer solchen Erweiterung ist klar; es ist aus Sicht der Strafverfolgungsbehörden natürlich interessant, ohne weitere Kosten und jederzeit (auch in Echtzeit) auf alle und jegliche Daten zugreifen zu können, die sich irgendwo in der "digitalen Welt" bewegen. Dies gesetzlich festzuschreiben ist jedoch unverhältnismässig, schiesst weit über den Zweck des BÜPF hinaus und ist in der Praxis so gar nicht umzusetzen, geschweige denn auf Kosten der Wirtschaft.

Keine echte Verbesserung der Situation

Bis anhin erfasst das BÜPF nur die meldepflichtigen Fernmeldedienstanbieter im Sinne des FMG (**FDA**). Dies sollte auch weiterhin so bleiben, denn der Sinn und Zweck des BÜPF ist im Telekombereich einzig die Überwachung des Fernmeldeverkehrs. In der Praxis stellt dies nach all meinen Erfahrungen auch kein wirkliches Problem dar, das sich durch die angedachte Erweiterung lösen liesse.

Erstens wird das Ziel, bestimmte Anbieter, wie etwa Betreiber reiner E-Mail-Plattformen wie GMX, Hotmail oder Gmail, neu zu erfassen, schon aus praktischen Gründen nicht erreicht werden können. Diese Betreiber können heute in der Tat nicht unter das BÜPF fallen, weil sie keine FDA sind. Sie werden jedoch auch in Zukunft nicht unter das BÜPF fallen, da sie sich erfahrungsgemäss alle im Ausland befinden und dort das BÜPF keine Anwendung findet (in der Schweiz sind höchstens Schwestergesellschaften angesiedelt, die mit dem Betrieb der betreffenden Diensten nichts zu tun haben; so ist das zum Beispiel bei Google). Genau hier liegen auch die praktischen rechtlichen Probleme in der Praxis, nicht beim zu engen persönlichen Geltungsbereich des BÜPF. Denn die Straftäter, denen es auf den Schutz der Anonymität ankommt, wählen erfahrungsgemäss bewusst ausländische Anbieter.

Zweitens kooperieren diese Anbieter in aller Regel trotz allem freiwillig mit den hiesigen Behörden (etwa, wo es um die Identifikation von Straftätern geht), d.h. die nötigen Ermittlungen können *de facto* durchgeführt werden.

Drittens löst die angedachte Erweiterung das Problem, dass der Endbenutzer seine Kommunikation bzw. seine Daten möglicherweise verschlüsselt (Skype-Problematik) und seinem Internet-Anbieter (ob FDA i.S. des Gesetzes oder nicht) seinen Schlüssel nicht anvertrauen wird, nicht. Diese Problematik ist es ja auch, die zum Wunsch der Strafverfolger geführt hat, sog. Trojaner einzusetzen, also das "Abhören" vom Netz (bzw. Server des Anbieters) auf das Gerät des Endbenutzers zu verlagern. Sie zeigt aber auch, dass ein Aufrüsten auf Seiten der Anbieter nichts bringen wird.

Viertens ist darauf hinzuweisen, dass dort, wo eine Straftat unter Einsatz des Internets (oder auch sonst) begangen wurde und ein Anbieter über für die Behörden relevante Beweise verfügt, dieser diese auch nach bestehendem Recht nicht ohne Weiteres vernichten oder zurückhalten darf, da er sich sonst der Begünstigung im Sinne von Art. 305 StGB strafbar machen könnte. Eine entsprechende Kasuistik im "Offline"-Bereich existiert seit Jahren; seit kurzem gibt es Gerichtspraxis auch betreffend Internet-

Anbietern (vgl. Entscheid des BGer vom 8. Januar 2010, 6B_766|2009, wenngleich dieser Fall aus anderen Gründen zweifelhaft ist). Somit besteht bezüglich dem Grundanliegen nicht nur kein praktischer, sondern auch kein gesetzgeberischer Bedarf.

Fünftens darf nicht vergessen werden, warum es das BÜPF überhaupt gibt. Der Grund hierfür ist u.a., dass FDA unter dem Fernmeldegeheimnis stehen und daher gesetzlich geregelt sein muss, wann und wie sie Informationen, die eben diesem Berufsgeheimnis unterstehen, herausgegeben werden müssen. Dies sollte nämlich unter sehr engen Voraussetzungen möglich sein. Das bedeutet aber auch, dass es systemwidrig wäre, das BÜPF nun über den Kreis eben jener FDA hinaus auch auf andere Personen auszudehnen, die nicht dem Fernmeldegeheimnis unterstehen. Die anderen Anbieter, die erfasst werden sollen, werden diesem höchstens ausnahmsweise unterliegen. Ihre Unterlagen sind somit auch unter Verwendung der herkömmlichen strafprozessualen Mitteln zugänglich. Es gibt schon deshalb gar keinen Grund, solche Anbieter ebenfalls dem BÜPF zu unterstellen. Tut man es doch, wird die Aufgabe der Strafverfolgungsbehörden möglicherweise sogar erschwert, da diesfalls ohne Weiteres vertreten werden könnte, dass durch die Regelung in einem Spezialgesetz alle anderen allgemeinen Regelungen betr. Herausgabe von Unterlagen, Erteilung von Auskünften oder Beschlagnahmungen mitunter nicht mehr gelten können. Zwar wäre das neue BÜPF so wie derzeit angedacht sehr weitgehend, doch auch dieses hätte seine Grenzen und bietet in verschiedener Hinsicht weniger Spielraum als das allgemeine Strafprozessrecht. Überdies sind die im BÜPF vorgesehenen Verfahren komplizierter und aufwändiger. Der VE-BÜPF sorgt durch Art. 5 zudem dafür, dass selbst Informationen, die sonst nicht dem Fernmeldegeheimnis unterliegen würden, dies kraft des BÜPF trotzdem tun. Somit würde den Strafverfolgungsbehörden letztlich ein Bärendienst erwiesen werden.

Es droht beträchtlicher Flurschaden

Die angedachte Erweiterung des Anwendungsbereichs wird somit keine wirkliche Verbesserung bringen, sorgt aber ohne Not für einen beträchtlichen Flurschaden und eine Verunsicherung bei all jenen Anbietern, die neu erfasst würden und selbstverständlich bestrebt sein würden, sich gesetzeskonform zu verhalten – mit entsprechenden Kostenfolgen durch technische Massnahmen, Berater und weitere Aufwendungen, die plötzlich nötig werden (z.B. ständig erreichbare Personen, etc.). Denn mit der bestehenden Formulierung müssten je nach Interpretation plötzlich zahlreiche weitere Unternehmen (und auch natürliche Personen) in der Schweiz im Wesentlichen dieselben Pflichten erfüllen müssen, wie bisher nur FDA.

Dies ist schon deshalb problematisch, weil all diejenigen Pflichten, welche diese Personen zu erfüllen hätten, auf FDA zugeschnitten sind und deshalb überhaupt nicht klar ist, wie diese sie erfüllen könnten, geschweige denn, welcher Aufwand (auch auf Seiten der Behörden) damit verbunden wäre, diese Anbieter anzubinden und zu überwachen. Das wird deutlich, wenn vor Augen geführt wird, welche weiteren Unternehmen aufgrund der Formulierung von Art. 2 Abs. 1 Bst. b VE-BÜPF erfasst werden können.

Dies wäre(n) beispielsweise

– *jeder* Betreiber einer Website, der irgendeine Funktion verfügt, mit der Personen einander Mitteilungen zukommen lassen können, so z.B. die gängigen Medienwebsites, mit denen andere Personen via E-Mail über interessante Berichte informiert werden können. Einerseits betreiben sie entweder Mailserver für Dritte selbst bzw. haben ihn an einen solchen eines FDA angebunden, andrerseits übertragen sie bei jedem Übermittlungsvorgang E-Mails von Dritten an den Mailserver des Empfängers. Es kann ohne Weiteres vertreten werden, dass dies somit Unternehmen sind, die berufsmässig an Dritte Kommunikationsdaten weiterleiten bzw. die dafür nötige Infrastruktur zur Verfügung stellen. Der Bericht zum VE-BÜPF (der **Bericht**) spricht auf S. 17 ausdrücklich davon, Anbieter von *"elektronischen Postdiensten"* zu erfassen. Doch selbst wenn entgegen dem Bericht Art. 2 Abs. 1 Bst. b VE-BÜPF so gelesen oder angepasst würde, dass diese Anbieter "für" einen FDA handeln müssten, könnte mit guten Gründen vertreten werden, dass sie erfasst sind, weil sie selbst auf die Kooperation von FDA angewiesen sind, um ihre diesbezüglichen Maildienste zu realisieren;

– unzählige Hosting-Provider, also z.B. auch solche, die E-Commerce-Plattformen anbieten, wie etwa eBay oder Ricardo und jede Firma, die es auf ihrer Website Dritten erlaubt, irgendwelche Kommentare kund zu tun (z.B. in einem Gästebuch oder einem Blog). Denn auch sie leiten letztlich Kommunikationsdaten (z.B. den Inhalt einer Verkaufsanzeige) an Dritte (die Besucher) weiter bzw. stellen die dafür nötige Infrastruktur zur Verfügung. Der Bericht spricht auch hier auf S. 17 offen davon, dass reine *"Hosting-Provider"* erfasst werden

sollen. Auch alle elektronischen Medien, die Leserbriefe oder Anzeigen im Internet veröffentlichen, sind nach heutigem Verständnis Hosting-Provider und sollen offenbar erfasst werden;

All diese Unternehmen müssten somit enorme Infrastrukturen aufbauen, um die nach VE-BÜPF vorgesehenen Pflichten erfüllen zu können (und zwar auf eigene Kosten). Zweifellos ist es für eine Strafverfolgungsbehörde verlockend, in alle und jegliche Vorgänge im Internet jederzeit Einblick erhalten zu können. Dies kann und soll jedoch nicht Zweck des BÜPF sein, das lediglich der Überwachung der Telekommunikation und nicht aller Teile der "digitalen" Welt dient (was schon aus dem Titel des Erlasses hervorgeht). Schon heute ist es den Strafverfolgungsbehörden möglich, den Internet-Verkehr von Personen auf der Übermittlungsstrecke weitgehend zu überwachen. Warum – um es überspitzt zu formulieren – nun auch noch mit hohen Kosten eine Live-Direktschaltung in das Innere eines jeden öffentlichen Webservers auf dem Territorium der Schweiz aufgebaut werden soll und zwar möglichst auf Vorrat, sodass die Behörde sich jederzeit unbemerkt einklinken und beobachten kann, ist unverständlich. Jedenfalls ist es unverhältnismässig, weil dies nicht nur mit erheblichen Kosten, sondern auch mit erheblichen Sicherheitsrisiken[1] (wurden hier überhaupt je Abklärungen von Fachleuten vorgenommen?) verbunden wäre, von Fragen zum Schutz der Privatsphäre ganz abgesehen. Es ist mir jedenfalls kein westliches Land bekannt, welches das Internet derart weitgehend überwachen möchte wie dies der VE-BÜPF im Ergebnis vorsieht. Dem mag man zwar entgegenhalten, dass dies nicht beabsichtigt sei, doch ein Gesetz zu schaffen, das dies vorsieht, mit dem Versprechen, es nicht so anzuwenden, stellt keine saubere Gesetzgebung dar.

– Betreiber von internen Fernmeldenetzen und Hauszentralen, die zwar in Abs. 2 separat aufgeführt sind, aufgrund die Formulierung in Art. 2 Abs. 1 Bst. b VE-BÜPF aber ebenfalls erfasst sein können, denn sie stellen die zur Weiterleitung von Kommunikationsdaten an Dritte erforderliche Infrastruktur bereit. Selbst wenn dem entgegengehalten würde, dass damit der Verkehr der Unternehmen selbst nicht gemeint ist, könnten trotzdem zahlreiche Unternehmen erfasst sein, nämlich solche, die ihren Mitarbeitern erlauben, private Telefongespräche zu führen oder E-Mails zu versenden oder Unternehmen, die innerhalb von Firmengruppen als IT- und Telecom-Service-Center auftreten und in dieser Funktion für andere Gruppengesellschaften Fernmeldedienstleistungen erbringen (was immer häufiger vorkommt). Diese Sichtweise ist keineswegs absurd; in Deutschland gilt sie als Stand der Lehre, dies mit der Folge, dass Unternehmen auch bezüglich der privaten E-Mails ihrer Mitarbeiter dem Fernmeldegeheimnis unterstehen. Auch hier sind die Konsequenzen der Erweiterung des persönlichen Anwendungsbereichs des BÜPF völlig unverhältnismässig. Aus genau diesem Grund hat der Gesetzgeber in Art. 2 FDV für gruppeninterne FDA ausdrücklich klargestellt, dass sie *keine* FDA sind, obwohl sie solche Dienste technisch gesehen erbringen. Mit der Revision droht diese sinnvolle Regelung ohne jede Not unterlaufen zu werden.

– Firmen, die Dienstleistungen im Netzwerksicherheitsbereich anbieten (z.B. Managed Security Services), in dem sie z.B. Netzwerke von Firmen überwachen und verwalten (z.B. durch den Betrieb von Firewalls). Sie könnten ebenfalls erfasst sein, denn es könnte vertreten werden, dass sie z.B. mit der Bereitstellung eines Firewalls (einem Gerät zum Schutz vor Hackerangriffen, durch welches sämtlicher ein- und ausgehender Datenverkehr eines Betriebs führt) beruflich die notwendige Infrastruktur zur Verfügung stellen, damit Kommunikationsdaten an Dritte weitergeleitet werden können. Sie sind heute aber keine FDA, da sie quasi "innerhalb der Mauern" ihrer Kunden an der Übermittlung beteiligt sind und nicht Standorte miteinander verbinden. Hier zeigt sich ebenfalls, wie absurd die Erwei-

[1] Eine Überwachung in der vorgeschriebenen Art und Weise ist nur möglich, wenn die betreffenden Server-Anwendungen über entsprechende Schnittstellen verfügen. In der Fernmeldeindustrie sind diese über Jahre entwickelt worden und einigermassen standardisiert. In dem Bereich, den der VE-BÜPF nun erfassen will, ist dies nicht der Fall. Hier plant die Schweiz einen Alleingang. Es müssen somit "Bastel"-Lösungen" realisiert bzw. Sonderlösung entwickelt werden, denn es soll nicht genügen, auf Anfrage lediglich jene Protokolle herauszugeben, die noch verfügbar sind. Eine Überwachung soll gem. Art. 21 Abs. 2 und 3 VE-BÜPF den gesamten Fernmeldeverkehr einer Person (also alles, was der Webserver empfängt oder sendet) wenn möglich in Echtzeit an die Behörde liefern. Hierzu müsste in bisher gut geschützte Abläufe eingegriffen werden, was wiederum nur durch Aufbrechen der bestehenden Sicherheitsmassnahmen möglich wäre. Das wiederum schwächt das betreffende Gesamtsystem, da, anders als im Fernmeldebereich, die besagten Systeme nicht für solche Überwachungsmassnahmen konzipiert sind. Es erscheint mir unabkömmlich, dass diese Problembereiche vor einer Kodifizierung durch Experten überprüft werden.

terung wäre: Die in Art. 21 Abs. 4 und Art. 25 VE-BÜPF vorgesehenen Pflichten können dazu führen, dass diese Unternehmen plötzlich gezwungen werden könnten, ihre eigenen Kunden im Auftrag der Behörden auszuspionieren, indem sie ihre Kenntnisse über deren Sicherheitsmassnahmen, die sie Kraft ihrer Stellung haben (über die aber FDA nicht verfügen würden) preisgeben müssten. Diesen Unternehmen wird durch eine Unterstellung unter das BÜPF faktisch die Geschäftsgrundlage entzogen, denn kaum jemand würde eine Firma mit der Sicherstellung seiner Netzwerksicherheit beauftragen, wenn er weiss, dass diese Firma verpflichtet ist, den Behörden jederzeit heimlich Zugriff auf das Unternehmensnetz zu gewährleisten und zwar in einer Art und Weise, wie es die Firma selbst nicht tun muss. Diesem Schaden muss dem Nutzen der Übung entgegengehalten werden: Er ist praktisch Null, denn die Zielpersonen, um die es geht, werden sich durch Einbezug ausländischer Produkte und Anbieter zu schützen wissen und wer es nicht weiss, kann auch heute schon erfasst werden.

– Firmen, die Netzwerk-Hard- oder Software in der Schweiz verkaufen, da sie FDA bzw. auch anderen Unternehmen zweifellos notwendige Infrastruktur zur Verfügung stellen, indem sie solche verkaufen oder vermieten. Dass sie über diese nach dem Verkauf oder der Vermietung keinen ordentlichen Zugriff mehr auf die Systeme haben, ändert nichts an ihrer Verpflichtung – und sei es nur, dass eines Tages jemand auf die Idee kommen könnte, von ihnen gestützt auf Art. 21 Abs. 4 VE-BÜPF Hintertüren in ihre Systeme einbauen zu lassen oder zusätzlich gestützt auf Art. 25 VE-BÜPF die Offenlegung von streng geheimen Informationen, wie z.B. Verschlüsselungscodes oder Systemschwächen in Verschlüsselungs- und Netzwerksystemen, zu verlangen. Abgesehen von den enormen Sicherheitsrisiken, die dies schaffen würde, würde die Vertrauenswürdigkeit eines ganzen Industriezweigs massiv untergraben. Genau das ist in den USA geschehen: Es wird heute vielerorts nicht mehr US-Produkten vertraut, weil befürchtet wird, dass US-Behörden über Hintertüren verfügen, die die Vertraulichkeit der Kommunikation untergraben. Obwohl dies stets dementiert wird, bleibt der Generalverdacht bestehen. Die Schweiz droht hier noch einen Schritt weiter zu gehen: Sie will dies sogar gesetzlich und für jeden nachvollziehbar festschreiben, und dies ohne Not und ohne jeden nachhaltigen Nutzen, denn die Stellen, gegen welche sich die Massnahmen richten, werden kurzerhand auf andere Produkte ausweichen. Es trifft somit auch hier die Falschen.

Diese Beispiele zeigen meines Erachtens, dass die Erweiterung des Anwendungsbereichs des BÜPF und die Folgen nicht wirklich durchdacht worden sind. Selbst der verwendete Schlüsselbegriff der "Kommunikationsdaten" ist nicht definiert. So schafft die Erweiterung wesentlich mehr Probleme als sie lösen kann. Selbst wenn sie nicht so gemeint sein mag (wofür aber keine Anhaltspunkte zu erkennen sind), birgt sie das Potenzial für erhebliche Rechtsunsicherheiten in der Wirtschaft, was letztlich vor allem jenen Unternehmen schadet (und kostet), die sich rechtskonform verhalten wollen und im Zweifel mehr tun, als wirklich nötig wäre, um unter keinen Umständen im ersten Pilotprozess wegen Missachtung des BÜPF bestraft zu werden. Dieser Faktor darf in der Schweiz, wo Unternehmen ein sehr hohes Compliance-Verständnis haben, nicht unterschätzt werden. Dass diese Befürchtung berechtigt ist, belegt eine Aktion des Informatik Service Center ISC-EJPD vom Juli dieses Jahres, in welcher zahlreiche Betriebe, die auch nur entfernt etwas mit Telekommunikation zu tun haben, brieflich über ihre angeblichen *"Pflichten als Fernmeldedienstanbieterin[nen]"* informiert wurden. Ob es sich bei den betreffenden Betrieben tatsächlich um FDA handelte, wurde nicht geprüft oder in aufgeworfen. Der Brief sorgte verständlicherweise für erhebliche Verwirrung und Verunsicherung in der Branche, denn etliche Unternehmen waren keine FDA.

In diesem Zusammenhang ist auch zu erwähnen, dass gemäss Bericht Internetcafés oder Cybercafés sowie alle Arten von Schulen, Hotels, Restaurants und Privatpersonen, welche beispielsweise drahtlose Netzwerke ihren Kunden oder Dritten zur Verfügung stellen, nicht erfasst sein sollen. Das ist vernünftig, doch entspricht dies nicht der Formulierung von Art. 2 Abs. 1 Bst. b VE-BÜPF. Es ist überdies nicht wirklich nachvollziehbar, warum ein Internetcafé keine Überwachungsmassnahmen durchführen soll, die Betreiber von Websites, welche die Besucher der Internetcafés anwählen, hingegen schon. Diese sind nicht nur sehr viel zahlreicher sondern auch viel weiter "weg" vom Zielobjekt und sehr viel weniger in der Lage, die betreffende Person zu identifizieren. Ihnen soll aber genau diese Pflicht auferlegt werden (Art. 22 VE-BÜPF).

Zu erwähnen ist schliesslich auch, dass selbst der Fall des "Outsourcings" der Erbringung von Fernmeldediensten durch eine FDA an Dritte normalerweise keine Probleme

verursacht. Entweder wird der Dritte selbst zur FDA (Reseller von Fernmeldediensten sind schon heute erfasst, auch wenn sie dies nicht realisieren mögen) oder das Outsourcing ändert an der Möglichkeit der Überwachung nichts. Denn ungeachtet eines Outsourcings einzelner oder vieler Aufgaben einer FDA an einen Dienstleister bleibt der FDA verpflichtet, die Überwachung sicherzustellen. Im Falle eines Outsourcings tut er dies nicht mittels Weisung an seine Arbeitnehmer, sondern einer Weisung an den bzw. vertraglichen Vereinbarung mit dem Outsourcing-Provider. Somit ist aus diesem Grund die Erweiterung von Art. 2 Abs. 1 Bst. b VE-BÜPF nicht erforderlich.

Ich rate daher dringend dazu, die Erweiterung in Art. 2 Abs. 1 Bst. b VE-BÜPF fallen zu lassen, sie zumindest aber grundlegend umzugestalten, so dass sie selbst bei weiter Auslegung tatsächlich nur jene erfasst, die es treffen soll.

Weitere problematische Punkte

Der VE-BÜPF enthält noch diverse weitere Punkte, die aus meiner Sicht sehr kritisch sind und in der Praxis zu Unsicherheiten und Problemen führen werden oder schlichtweg unverhältnismässig sind. Hier nur drei Punkte:

– **Identifizierung von Internet-Benutzern** (Art. 22 VE-BÜPF): Diese Bestimmung ist unsinnig, so wünschenswert das angestrebte Ergebnis (kein anonymes Surfen mehr, totale Kontrolle des Internet-Zugangs) für den einen oder anderen möglicherweise sein mag. Niemand würde von einem Telefonanbieter verlangen, dass er Massnahmen trifft festzustellen, *wer* einen bestimmten Telefonanschluss benutzt. Verlangt wird höchstens die Identifikation des *Inhabers* des Anschlusses. Dies geschieht bei Internet-Anschlüssen ohnehin und stellt in der Praxis kein Problem dar, ausser bei offenen drahtlosen Netzwerken und Internetcafés, die aber gerade nicht erfasst sein sollen. Diese aber sollen gemäss Bericht gerade keine Überwachungen durchführen müssen und unterliegen daher auch nicht Art. 22 VE-BÜPF. Somit zielt die Norm am Problem vorbei bzw. ist gar nicht vernünftig zu realisieren;

– **Unterstützung beim Einsatz von Spionageprogrammen** (Art. 21 Abs. 4 VE-BÜPF): Diese Programme sind schon an sich problematisch und sehr umstritten. Die Anbieter nun noch zwingen zu wollen, die Behörden beim "Hacken" in die Systeme von Kunden und Dritter in jeder erdenklichen Form zu unterstützen, ohne dass das Gesetz irgendwelche klaren Leitlinien aufstellt, geht aus meiner Sicht zu weit und ist auch nicht erforderlich. Es untergräbt, wie oben dargestellt, auch das Vertrauen einer ganzen Industrie und schafft Sicherheitsrisiken, die letztlich der ganzen (rechtsschaffenden) Wirtschaft schaden;

– **Entschädigungen** (Art. 30 VE-BÜPF): Der Bericht vertritt auf S. 10 die Kostentragung durch die erfassten Anbieter mit dem Argument, eine Entschädigung sei im Strafrecht systemwidrig. Das ist falsch. Auch das Beispiel mit der Edition der Banken hinkt. Vorliegend geht es nicht einfach wie im Fall einer Edition bei einer Bank darum, dass gewisse Unterlagen, über welche die Anbietern verfügen, so herausgegeben werden müssen, wie sie eben vorliegen (verlangt wird bei den Banken in der Regel einzig, dass diese als Papierkopie in "gut lesbarer Form" herauszugeben sind). Hier geht es darum, dass die Anbieter einen erheblichen Zusatzaufwand betreiben sollen, um es den Behörden zu ermöglichen, die Daten in der von ihnen gewünschten Form und auf die von ihnen gewünschte Art und Weise zu erhalten, möglichst im Direktzugriff und möglichst in Echtzeit. Es gibt keine Bank in der Schweiz, die den Behörden auch nur ansatzweise einen derart weitgehenden und aufwändigen Zugang zu ihren Daten geben muss, wie die Anbieter unter dem BÜPF dies tun sollen. Es würde ausserhalb des BÜPF auch niemand auf die Idee kommen, eine derart weitgehende Mitwirkung an einer Strafverfolgung entschädigungslos zu verlangen. Entschädigungen für Fachexperten, die von einer Behörde für Ermittlungen beigezogen werden, sind die Regel und nicht die Ausnahme.

Insgesamt erscheint mir der VE-BÜPF nicht ausgereift und besonders bezüglich der Erweiterung des persönlichen Anwendungsbereichs als sehr problematisch und in seinen Konsequenzen zu wenig durchdacht. Ich hoffe, mit diesen Ausführungen etwas zur Vorlage beigetragen zu haben und stehe für weitere Fragen und Diskussionen gerne zur Verfügung.

Freundliche Grüsse

David Rosenthal

Konsulent für Informations- und Telekommunikationsrecht in einer Zürcher Anwaltskanzlei und Lehrbeauftragter der Universität Basel und ETH Zürich.

Review: Security Lunch in Lausanne

Security Lunch in Lausanne

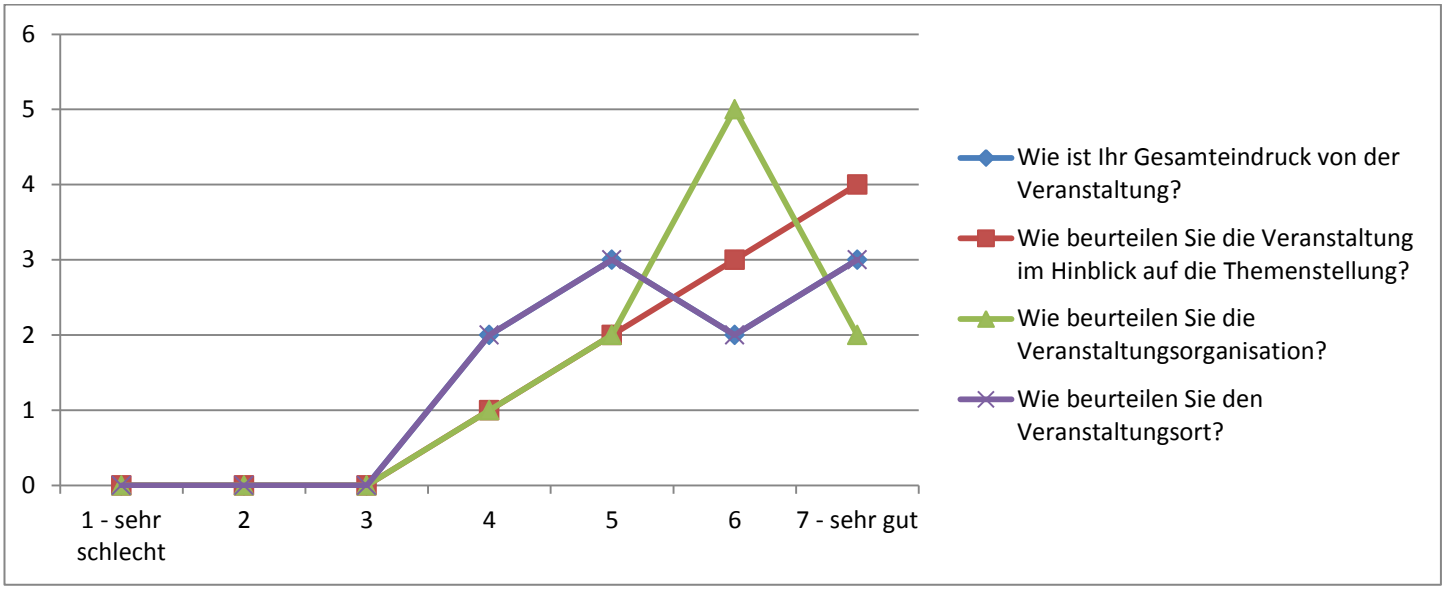
Mit Ed Gelbstein konnten wir einen bekannten Speaker gewinnen für unseren ersten Security Lunch in Lausanne. Dieser fand am 28.6.2010 statt und war mit 19 Besuchern sehr gut besucht.

Seinen Vortrag **„The Rise (and Fall) of the CISO - How the CISO Role is Evolving"** finden Sie auch als Video auf ISSSview.

Die Slides finden Sie ebenfalls online:

https://www.isss.ch/veranstaltungen/2010/security-lunch-2010-06-28/

Aufgrund der positiven Erfahrung mit Security Lunches in der Welschschweiz planen wir weitere Events dort.



Grafik: Feedbackauswertung zum Security Lunch in Lausanne.

Information Security Society Switzerland

Partner Events: News

hashdays Workshops in Luzern

Ort: Radisson Blu, Luzern, Datum: 3.-4. November 2010, Sprache: Englisch
Preis: ISSS-Members zahlen bei Anmeldung mit Rabattcode "ISSSNWSL" bis **31. August 2010** nur CHF 425.- (statt 700.-) pro Management-Session und CHF 2040.- (statt 2600.-) pro technischen Workshop

Infos & Anmeldung: http://www.hashdays.ch/

Exclusive Management Sessions on the Cyber Threat Landscape Facing Companies

In two separately bookable half-day Management Sessions (morning/afternoon Nov 4), the current and future threat landscape for companies is highlighted exclusively for the benefit of an interested management audience. The cyber threat landscape is compiled by top speakers presenting their latest research results at the hashdays conference. A moderator with management experience will bridge the gap between the technical experts and the interested audience. The audience is not asked to disclose any company specifics.

Protecting from GSM attacks

In this workshop (Nov 3/4) Harald Welte, Karsten Nohl and David Burgess revisit the basics of GSM, SS7, and OTA before discussing control and trust mechanisms. It will become apparent that technology providers and attackers can invade GSM users' location and communication privacy in multiple ways. The workshop is targeted at GSM users concerned with the confidentiality of their information and location. The class provides technical and organizational protection strategies for minimizing the attack surface and mitigating the risks of the telecom infrastructure.

Exploit Laboratory

Saumil Shah brings to you an action packed class (Nov 3/4) teaching the art of exploitation from scratch. We start with insights into system architecture, process execution, operating systems and error conditions. We then accelerate to using debuggers, reproducing reliable error conditions and exploit writing. Most of the class time is spent working on exercises that cover both the Linux and Windows, illustrating stack overflows, heap overflows and memory overwrites. The class is delivered in a down-to-earth, learn-by-example methodology.

Security Conference ISSE 2010 in Berlin

The ISSE 2010 (www.isse.eu.com) will take place in Berlin, Germany on 5-7 October 2010.

This year, ISSE is joining forces with the GI-SICHERHEIT conference, a long established event run by the German Informatics Society (Gesellschaft für Informatik, GI). Delegates will learn about new initiatives on a Pan European scale with an unrivalled opportunity to choose each day from six different security tracks including exclusive insights into the new German Identity card scheme launching in November 2010.

To view the exceptional conference programme in detail, please click here. Session titles include: ‘The eID Function of the New German Identity Card (nPA); Security Properties and Infrastructure Components’.

Book your delegate place NOW to claim your early booking discount!

Early booking discounts are available until **7th September** (with special rates for EEMA / TeleTrusT / GI members), please visit www.isse.eu.com. ISSS Members use booking code "ISSE10GI" to get the same discount as GI members.

Kind Regards,

Roger Dean
Executive Director, EEMA

Information Security Society Switzerland

Agenda: Partner Events mit Rabatt für ISSS Mitglieder

Nächste Security Events unserer Partner

Programm und Anmeldung unter: https://www.isss.ch/veranstaltungen/aktuell/

Datum	Zeit	Veranstalter	Titel und Details	Ort
Di, 31.08.2010	09:00 - 17:30	privatim	**15th Symposium on Privacy and Security 2010 "Fischen im Datenmeer"** 20% ISSS-Rabatt ("Mitglied von ISSS" ankreuzen und ISSS-Mitgliedsnummer unter Bemerkungen angeben)	Zürich
Mo, 06.09.2010	09:00 - 16:45	Swiss E-Voting Competence Center	**Swiss E-Voting Workshop 2010: State-of-the-Art E-Voting Systems**	Fribourg
Di, 07.09.2010	16:30 - 18:30	ASIS	**ASIS Fachmeeting: "Cybercrime"** Referent: Thomas Dübendorfer. Die Teilnahme ist für ISSS Mitglieder gratis.	Zürich, Hotel Widder
Do, 09.09.2010	08:30 - 17:00	Compass Security AG	**Compass Event 2010 - iPhone, Laptop & Co. unter Beschuss** 20% Rabatt für ISSS Mitglieder	Rapperswil
Di, 14.09.2010	09:00 - 17:00	IBCOL	**Praktiker-Fachtagung „IT Risk Management & BCM“** Anmeldeschluss: Freitag, 13. August 2010. 15% Rabatt für ISSS Mitglieder. 15% Rabatt für Frühbucher bis 15. Juli 2010.	Zürich
Mi - Sa, 03.11.-06.11.2010	ganztags	DEFCON	**Hashdays Security & Risk Conference (#days)** ISSS Mitglieder erhalten den "reduced delegate" Tarif (255.- statt 300.- CHF) bei Anmeldung bis 31.08.2010.	Luzern

Nächste Security Kurse unserer Partner

Programm und Anmeldung unter: https://www.isss.ch/veranstaltungen/kurse/

Mo - Fr, 06.09. - 10.09.2010	ganztags	ROMAN Consulting & Engineering	**Security Fachkurs: "Check Point Security Administrator R70 (CCSA R70)"** ISSS-Mitglieder zahlen CHF 3868.- statt CHF 4550.- (15% Rabatt)	Zürich
Mo - Fr, 27.09. - 01.10.2010	ganztags	ROMAN Consulting & Engineering	**Security Fachkurs: "EC-Council: Disaster Recovery and Business Continuity (EDRP)"** ISSS-Mitglieder zahlen CHF 4760.- statt CHF 5600.- (15% Rabatt)	Zürich
Di - Mi, 23.11. - 24.11.2010	8:30 - 17:00	Plattner Beratung und Schulung	**Kompaktkurs "Internet (In)Security Exposed" - Internetgefahren verstehen und Webapplikationen richtig schützen in Theorie und Praxis.** ISSS-Mitglieder zahlen CHF 1840.- statt CHF 2300.- (20% Rabatt). Frühbucherrabatt bis 1.10.2010.	Zürich

Beachten Sie bitte auch die Agenda mit wissenschaftlichen Konferenzen:
https://www.isss.ch/veranstaltungen/wiss-konferenzen/

Agenda: Hinweise zu ISSS Security Events

ISSS Secuity Lunch: „SuisseID - erste Erfahrungen aus der Praxis“

Am 31.8.2010 über Mittag 12:00 – 14:00 wird Herr Daniel Messerli, Leiter Bereich Information Security und Risk Management, ERGONOMICS, in Bern zur SuisseID referieren. Anmeldungen werden noch bis 28.8.2010 über die ISSS-Website entgegengenommen: https://www.isss.ch/veranstaltungen/2010/security-lunch-2010-08-31/

Zum Inhalt: Eine technische Standardlösung für effiziente eGovernment-Prozesse, vertrauenswürdige eCommerce-Transaktionen und sichere Zugangskontrollen - erfüllt SuisseID dies alles? Seit einem halben Jahr sorgt die SuisseID für Aufbruchstimmung in der Schweizer IT-Landschaft. Digitaler Identitätsnachweis, qualifizierte Signatur - das soll die SuisseID ab Mai 2010 als Gesamtsystem vereinen. Erste Erfahrungen aus der Praxis.

ISSS Security Lunch „Cloud Computing - was ist aus rechtlicher Sicht zu beachten?“

Am 9.9.2010 wir über Mittag 12:00 - 14:00 in Luzern Frau Maria Winkler, mag. iur., IT&Law Consulting, zu Cloud Computing referieren. Der Anmeldeschluss ist am 6. September 2010, 12:00.

Zum Inhalt: Mit dem Bezug von IT-Dienstleistungen aus der „Cloud“ erhoffen sich die Unternehmen grosse Einsparungen. Den Vorteilen des Cloud Computings stehen einige rechtliche Risiken gegenüber, welche bei der Verhandlung und Ausgestaltung des Vertrages mit dem Anbieter soweit als möglich reduziert werden sollten. Im Rahmen der Veranstaltung werden die zu berücksichtigenden rechtlichen Aspekte und allfällige Lösungsmöglichkeiten aufgezeigt.

Anmeldung online auf: https://www.isss.ch/veranstaltungen/2010/security-lunch-2010-09-09/

Yubikey als Geschenk am Abendseminar „Innovative Alternativen zum Passwort“ vom 26.10.2010

Die Teilnehmenden des kostenlosen Abendseminars von ISSS und ISACA zum Thema „Innovative Alternativen zum Passwort“ vom 26.10.2010 von 17:30 - 21:30 (inkl. Apéro) in Zürich werden alle einen Yubikey als Geschenk erhalten. Dieser kann über die Plattform der clavid AG auch als OpenID eingesetzt werden. Die Platzzahl am Anlass ist beschränkt und eine online Anmeldung ist erforderlich:

Programm und Anmeldung: https://www.isss.ch/veranstaltungen/2010/alternativen-zum-passwort/.

Information Security Society Switzerland

Agenda: Events der Information Security Society Switzerland

Nächste ISSS Fachtagungen

26.10.2010	17:30 – 21:30	**ISSS/ISACA Abendseminar:** **„Innovative Alternativen zum Passwort“** (inkl. Apéro, kostenloser Eintritt, Anmeldung erforderlich, ein Yubikey als Geschenk für jeden Teilnehmenden, Platz begrenzt)	Zürich
25.11.2010	13:15 – 18:30	**13. Berner Tagung für Informationssicherheit:** **„Unbegrenzte Mobilität - Chancen und Risiken“** (Anmeldung)	Bern

Nächste ISSS Security Lunches

Eintritt kostenlos, auch für Nichtmitglieder; Essen wird zu Selbskosten vom Restaurant vor Ort in bar eingezogen; Anmeldung erforderlich.

31.08.2010	12:00 – 14:00	**SuisseID - erste Erfahrungen aus der Praxis**	Bern
09.09.2010	12:00 – 14:00	**Cloud Computing - was ist aus rechtlicher Sicht zu beachten?**	Luzern
06.10.2010	12:00 – 14:00	**Kostengünstige Identifizierung bisher nicht erkannter Sicherheitslücken mit Threat Modeling, Static Analysis und Fuzzing**	Zürich
28.01.2011	12:00 - 14:00	**Wirksames Informationssicherheitsmanagement für KMU**	Zürich

Vollständige Agenda mit Links zu Programm und Anmeldung: **www.isss.ch**

Impressum
Information Security Society Switzerland
Wasserwerkgasse 37
3000 Bern 13
newsflash@isss.ch
Tel. +41 31 311 5300
Auflage: Nur elektronische Auslieferung.
Versand als PDF per Email an alle ISSS-Mitglieder und Publikation auf http://www.isss.ch/