

Informatik Service Center – ISC EJPD
Dienst Überwachung Post- und Fernmeldeverkehr
Bereich Recht und Controlling
z.Hd. Patrik Schöpf <patrik.schoepf@isc-ejpd.admin.ch>
3003 Bern

VÜPF – Anhörung zu den vorgeschlagenen Änderungen: Stellungnahme des Chaos Computer Clubs Zürich (CCCZH)

Zürich, den 15. Juli 2011

Sehr geehrte Damen,
sehr geehrte Herren.

Der Chaos Computer Club Zürich, kurz CCCZH¹, möchte hiermit Stellung zu den geplanten Änderungen der „*Verordnung über die Überwachung des Post- und Fernmeldeverkehrs*“ (VÜPF) beziehen.

Dem Namen nach soll die VÜPF die Überwachung des *persönlichen* Nachrichtenverkehrs einer verdächtigen Person nach genehmigter Anordnung durch zuständige Stellen regeln. Dabei wird gewollt der Eindruck vermittelt, dass es hierbei nur um die *direkte und persönliche Kommunikation einer Person* geht, die einer Straftat verdächtigt und deren Kommunikation deshalb auf Anordnung hin kontrolliert, archiviert und ausgewertet werden darf.

Auch wenn die zur Zeit gültige Fassung der VÜPF dieser Interpretation durch die sogenannte rückwirkende Überwachung mit der Vorgabe einer verdachts-unabhängigen und langfristigen Speicherung von Kommunikationsdaten in Bezug auf Email-Austausch und (Mobil-)Telefonie schon erheblich zuwiderläuft, öffnen die vorgeschlagenen Änderungen durch ihre unklare und unbestimmte Formulierung – vor allem im *Abschnitt 6: Überwachung des Internets* – einer Protokollierung sämtlicher Internetnutzungen aller Anwender in der Schweiz Tür und Tor. Dem Vorsatz, zu einer transparenteren Überwachungs-Praxis beizutragen und mehr Rechtssicherheit auch für involvierte Firmen wie Internet-Service-Provider (ISP) zu bieten, tragen die vorgeschlagenen Änderungen aus unserer Sicht in keiner Weise Rechnung.

1 Siehe auch: <http://ccczh.ch>

Für den Chaos Computer Clubs Zürich (CCCZH), der sich den Idealen der informationellen Selbstbestimmung verpflichtet fühlt, ist diese Entwicklung deshalb bedenklich und konsequent abzulehnen.

In den nachfolgenden Abschnitten werden die einzelnen Kritikpunkte an den vorgeschlagenen Änderungen der VÜPF näher ausgeführt. Basierend auf der Kern-Kompetenz des CCCZH, die technischen und politischen Entwicklungen in der digitalen Welt zu begleiten, liegt der Schwerpunkt der Kritik in den Regelungen zum *Abschnitt 6: Überwachung des Internets*. Kritische Anmerkungen zu anderen Abschnitten der Verordnung sind in einem eigenen Kapitel zusammen gefasst.

Abschnitt 6: Überwachung des Internets

Art. 23 Überwachungsanordnung

Internet-Anbieterin

In **Art. 23 Bst. f** wird in der Überwachungsanordnung auf die involvierte *Internet-Anbieterin* verwiesen, die in die Überwachung eingebunden und für die Übermittlung der Informationen an die überwachende Stelle zuständig ist. Nach Glossar ist unter einer *Internet-Anbieterin* im Sinne des VÜPF eine Firma zu verstehen, die *kommunikations-basierte IP-Dienstleistungen im Sinne des Fernmeldeverkehrs (fernmeldetechnische Übertragungen)* wie zum Beispiel VoIP (Internet-Telefonie) oder Email anbietet und deshalb unter die Regelungen und Anordnungen der VÜPF fällt, ohne selbst Internet-Zugangsanbieterin sein zu müssen.

Diese Definition geht von der Annahme aus, dass für einen Dienst (z.B. VoIP) auch nur eine Internet-Anbieterin *zuständig* ist, über die der Dienst abgewickelt wird und die daher auch in der Lage ist, die geforderten Informationen an die überwachende Stelle zu übermitteln.

Auf Grund der technischen Abläufe zum Beispiel bei einer VoIP-Kommunikation (SIP für den Verzeichnisdienst und RTP für die Nutzdatenübertragung) ist dies aber in der Regel nicht der Fall: Die VoIP-Anbieterin verwaltet nur die Benutzerkonten und stellt einen Verzeichnisdienst (ähnlich einem Telefonbuch) zur Verfügung; ob ein VoIP-Gespräch nach einem Lookup (Nachschlagen im Verzeichnis) auch wirklich stattfindet, wann es beginnt und wie lange es dauert oder gar welchen Inhalt das Gespräch hat, kann die VoIP-Anbieterin technisch nicht bestimmen und daher auch nicht übermitteln, da die Daten mittels RTP *an ihr vorbei* übertragen werden (ähnlich dem Datentransport in einen P2P-Netzwerk wie z.B. Torrent).

Eine Überwachung von VoIP-Gesprächen erfordert daher sowohl die koordinierte Überwachung zwischen der VoIP-Anbieterin (SIP) und dem Internet-Zugangsanbieter (RTP) (im Falle einer Echtzeitüberwachung) als auch weitergehenden technischen Aufwand (D/SPI, *Deep/Stateful Packet Inspection*) bei einer Überwachung/Protokollierung/Archivierung des gesamten Internet-Verkehrs aller Nutzer beim Internet-Zugangsanbieter (rückwirkende Überwachung). Die sich daraus

ergebende Totalüberwachung beim Internet-Zugang ist aus Sicht des CCCZH konsequent abzulehnen, da sie Privatsphäre und informationelle Selbstbestimmung verletzt.

Ähnliche Massnahmen einer Totalüberwachung wären auch notwendig, wenn zu überwachende Personen VoIP- und/oder Email-Dienste bei ausländischen Anbietern nutzen. Da sich die erwünschten Überwachungsdaten auch in diesem Fall nur durch aufwendige Analyse des gesamten Internetverkehrs am Internet-Zugang ermitteln lassen, ist auch dies aus Sicht des CCCZH konsequent abzulehnen.

Adressierungselemente

In **Art. 23 Bst. g** wird festgelegt, dass die Überwachungsanordnung bestimmte technische Adressierungselemente wie zum Beispiel MAC-Adressen, IMSI- und IMEI-Nummern enthalten sollte. Im Glossar der Verordnung wird in Bezug auf diese Adressierungselemente der Eindruck erweckt, als wären diese Elemente unveränderbare und damit identifizierende Merkmale der verwendeten Kommunikations-Endgeräte wie Computer und Handy und somit ihrer Benutzer.

Tatsächlich lassen sich diese Werte aber mit vorhandenem technischen Know-How und vertretbarem Aufwand auf der heute gängigen Hardware verändern.^{2 3 4} Damit ist die Gefahr gegeben, dass verdächtige Kriminelle diese Adressierungselemente absichtlich verändern, um ihre Kommunikation verschleiern und damit gewollt oder ungewollt *unbeteiligte und unschuldige Dritte* in den Verdacht einer Straftat bringen und zum Ziel einer Überwachung werden lassen, da ISPs nach diesen Angaben Kommunikations- und Inhaltsdaten filtern, sammeln und an die überwachende Behörde weiterleiten.

Fall-Szenario: MAC-Adressen sind z.B. im Falle einer WiFi-Verbindung mit einem offenen WLAN-Hotspot (z.B. einem *Access Point* (AP) in einem Hotel) das einzig zu Verfügung stehende Adressierungselement, um ein Endgerät und damit einen Nutzer zu identifizieren. Wird in einem solchen Fall das Netz zur Begehung von Straftaten verwendet (z.B. Kinderpornographie), kann aus der IP-Adresse des AP-Betreibers und dessen Logdateien bestenfalls die MAC-Adresse des Endgeräts ermittelt werden. Wird daraufhin durch eine Überwachungsanordnung der gesamte zukünftige WiFi-Verkehr überwacht, der von dieser MAC-Adresse aus geführt wird, können dabei wie oben beschrieben die Persönlichkeitsrechte unschuldiger Dritter verletzt werden. Dies ist aus Sicht des CCCZH konsequent abzulehnen.

Art. 24 Überwachbare Internetzugänge und Anwendungen

Überwachbare Internet-Zugänge

In **Art. 24 Abs. 1 Bst. f** werden explizit Zugänge über OSI Schicht 3 erwähnt. Dies ist

2 **MAC-Adresse ändern:** siehe z.B. <http://www.mydigitallife.info/how-to-change-or-spoof-mac-address-in-windows-xp-vista-server-20032008-mac-os-x-unix-and-linux/>

3 **IMEI ändern auf iPhone4:** siehe z.B. <http://www.iclarified.com/entry/comments.php?enid=657>

4 **IMSI ändern auf SIM-Karte:** siehe z.B. <http://www.nowsms.com/discus/messages/1/42197.html>

technisch redundant, da unter **Art. 24 Abs. 1 Bst. e** bereits Zugänge nach OSI Schicht 2 erwähnt sind und OSI Schicht 3 notwendigerweise OSI Schicht 2 voraussetzt.

Das explizite Aufführen von OSI Schicht 3 wäre nur verständlich, wenn damit auch Internet-Verkehr, dessen *physikalischer Zugang nicht in der Schweiz stattfindet*, ebenfalls unter die Regelungen des VÜPF fallen soll. Dies würde aber bedeuten, dass auch Angehörige fremder Staaten von den Massnahmen der Vorratsdatenspeicherung (rückwirkende Überwachung) betroffen sein können und dass die Schweiz damit das Territorialitätsprinzip verletzt. Dies ist aus Sicht des CCCZH konsequent abzulehnen.

Überwachbare Internet-Anwendungen

In **Art. 24 Abs. 2 Bst. b** wird aufgeführt, dass zu den überwachbaren Anwendungen im Internet sogenannte Multimedia-Dienste gehören.

Entgegen den Erklärungen des erläuternden Berichtes⁵ zu den geplanten Änderungen an der VÜPF, der unter dieser Kategorie nur explizit Internettelefonie-Systeme wie Skype aufführt, besagt das allgemeine Verständnis von Multimedia aber etwas viel umfassenderes⁶: „Der Begriff Multimedia bezeichnet Inhalte und Werke, die aus mehreren, meist digitalen Medien bestehen: Text, Fotografie, Grafik, Animation, Audio und Video.“

Nach dieser Definition ist *jede Webseite im Internet oder jeder andere über das Internet angebotene Dienst* ein Multimedia-Dienst und der Zugriff auf diese Inhalte kann nach VÜPF auch überwacht werden. Da hier rückwirkende Überwachung nicht explizit ausgenommen ist, kann jeder ISP dazu verpflichtet werden, *alle besuchten URLs aller seiner Internet-Kunden zu protokollieren*, zu archivieren und auf Verlangen an die überwachenden Behörden auszuhändigen.

Art. 24a Überwachungstypen (Echtzeit)

Totalüberwachung

In **Art. 24a Bst. a** wird die vollständige Weitergabe aller Daten, die über einen überwachten Anschluss übermittelt werden, zu einem erlaubten Überwachungstyp erklärt.

Diese Totalüberwachung steht in direktem Widerspruch zu den Ausführungen in **Art. 24 Abs. 2 Bst. b**, der die überwachbaren Anwendungen definiert, einschränkt und keine Ausnahmen festlegt. Es liegt nur dann kein Widerspruch vor, wenn unsere Einwände gegen die unklare Formulierung „Multimedia-Dienst“ als generischer Internet-Traffic hier genauso verstanden werden.

Adressierungselemente

In **Art. 24b Bst. b Zif. 5** wird ebenfalls auf die Protokollierung und Weitergabe von Adressierungselementen wie MAC-Adresse, IMSI- oder IMEI-Nummer verwiesen.

5 http://www.bfm.admin.ch/content/dam/data/pressemitteilung/2011/2011-06-08/110608_ber-de.pdf

6 Zitiert nach Wikipedia: <http://de.wikipedia.org/wiki/Multimedia>

Die zum **Art. 23 Bst. g** vorgetragenen Einwände (leichte Manipulierbarkeit dieser Informationen und damit einhergehende Kompromittierung unschuldiger Dritter) sind hier ebenfalls gültig.

Inhalt der Kommunikation

In **Art. 24a Bst. c** wird die Überwachung und Weitergabe des Inhaltes in Bezug auf eine überwachte Anwendung nach **Art. 24 Abs. 2** festgeschrieben.

Durch die unklare Definition des Begriffes „Multimedia-Dienst“ in **Art. 24 Abs. 2 Bst. b** kann dies dazu führen, dass der Inhalt der gesamten Internet-Nutzung überwacht werden kann und dann eine identische Situation wie **Art. 24a Bst. a** (Totalüberwachung) bedeutet. Dies ist aus Sicht des CCCZH konsequent abzulehnen.

Art. 24b Überwachungstypen (rückwirkend)

Rückwirkende Überwachung basiert auf der verdachtsunabhängigen Speicherung der Kommunikationsdaten aller Internet-Nutzer durch die Internet-Service-Provider (ISPs). Die Verordnung verpflichtet ISPs, die Kommunikationsdaten aller Kunden *ohne genehmigte Anordnung oder eines begründeten Straftatverdachtes* über einen Zeitraum von mindestens sechs Monaten zu archivieren und auf Verlangen den zuständigen Behörden auszuhändigen.

An dieser Stelle kann nur die schon in Bezug auf **Art. 24 Abs. 2 Bst. b** geäußerte Kritik wiederholt werden: durch die unklare Formulierung des Begriffes „Multimedia-Dienst“ kann nach geplanter VÜPF jeder ISP dazu verpflichtet werden, *alle besuchten URLs aller seiner Internet-Kunden zu protokollieren*, zu archivieren und auf Verlangen an die überwachenden Behörden auszuhändigen. Diese Form der Vorratsdatenspeicherung halten wir mit den Grundsätzen der informationellen Selbstbestimmung für unvereinbar.

Zudem sind die ISPs für die Vertraulichkeit der gespeicherten Daten verantwortlich. Zahllose Fälle von Datendiebstahl durch interne oder externe Verursacher haben immer wieder deutlich gezeigt, dass Firmen dieser Verantwortung nicht oder nur ungenügend nachkommen können. Der kommerzielle Nutzen der Kommunikationsdaten sollte in diesem Zusammenhang nicht unterschätzt werden – nicht nur für Firmen im IT/TK-Umfeld.

Art. 25 Durchführung der Überwachung

Berufsgeheimnisträger

In **Art. 25 Abs. 2** wird die widerrechtliche Speicherung von Kommunikationsdaten und -inhalten für den Fall erzwungen, dass die Überwachung einer bestimmten Person auf Grund ihres Berufsstandes ohne besondere Ausnahmegenehmigung nicht möglich ist und diese Ausnahmegenehmigung nicht vorliegt.

Die Formulierung, „der Dienst zeichnet die Daten auf und benachrichtigt die Genehmigungsbehörde“ schreibt einen nicht zumutbaren Zustand für die betroffene

Person und den ISP fest, der die Daten an den Dienst liefern muss. Es wird an keiner Stelle darauf verwiesen, in welchem Zeitraum die nachträgliche Genehmigung zu erteilen ist noch was mit den Daten (und daraus vielleicht schon gewonnener Kenntnisse) passiert, wenn die Genehmigung nicht erteilt wird.

Ausserordentliche Überwachung

In **Art. 25 Abs. 5** wird auf „Überwachungsmassnahmen, die nicht explizit in dieser Verordnung aufgeführt sind“ verwiesen. In diesem Fall wird der gesamte „Fernmeldeverkehr der überwachten Person in Echtzeit und permanent zum Verarbeitungszentrum übertragen“. Nähere Modalitäten dieser Überwachungsform werden in den Änderungen nicht beschrieben, sondern „vom Dienst geregelt“.

In den Erklärungen des erläuternden Berichtes⁷ zu den geplanten Änderungen an der VÜPF wird hier mit der „in Anlehnung an die jahrelange durch Gerichte gestützte Praxis“ argumentiert. Wenn tatsächlich Gerichte heute schon Überwachungsmassnahmen verfügen, die nicht durch die VÜPF abgedeckt sind, stellt sich uns die Frage, auf welcher gesetzlichen Grundlage diese Anordnungen erlassen werden und warum es dann überhaupt Regelungen für Echtzeit-Überwachungen durch eine VÜPF braucht?

Art. 27 Auskünfte über Internet-Teilnehmerinnen und -Teilnehmer

In **Art. 27 Abs. 1** werden die ISPs verpflichtet, dem Dienst verdachtsunabhängig und ohne weitere Anordnungen oder Genehmigungen Informationen über ihre Internet-Kunden auszuhändigen.

Aus unserer Sicht kann eine solche Anfrage nur nach Genehmigung durch eine zuständige Behörde zulässig sein. Die Informationen, die der Dienst von den ISPs im Rahmen dieser Verordnung einfordern darf, können sehr schnell die Privatsphäre von Personen berühren, die als unbeteiligte Dritte nicht legitimes Ziel einer Überwachungsmassnahme sind oder werden dürfen.

Kritik zu Artikeln in anderen Abschnitten

Art. 8 Verarbeitungszentrum

Datensicherheit

Die VÜPF sieht vor, dass der zuständige Dienst im EJPD ein Verarbeitungszentrum für die Daten aus der Überwachung des Fernmeldeverkehrs einrichtet. Die im Zentrum archivierten Daten werden rund um die Uhr denjenigen Behörden zugänglich gemacht, die als Empfängerinnen der Überwachungsdaten vorgesehen sind.

Eine zentrale Speicherung der durch Überwachung gewonnen sensiblen Daten ist aus Sicht des CCCZH indiskutabel, da jedes System für internen oder externen Verlust von Daten anfällig ist, der weder durch technische noch organisatorische Massnahmen

⁷ http://www.bfm.admin.ch/content/dam/data/pressemitteilung/2011/2011-06-08/110608_ber-de.pdf

vollständig verhindert werden kann (siehe dazu auch Anmerkungen zum **Art. 24b**).

Einsicht in nicht-öffentliche Verzeichnisse

Der Dienst führt schliesslich für die Strafverfolgungsbehörde ein System zur Vermittlung von Auskunftgesuchen über Fernmeldeanschlüsse ein. Dieses System wird besonders die Erteilung von Auskünften über Anschlüsse ermöglichen, die in den öffentlichen Verzeichnissen der Fernmeldeanbieter nicht zu finden sind (siehe auch **Art. 27**).

Dies gilt es aus Sicht des CCCZH konsequent abzulehnen. Es ist nicht nachvollziehbar zu erkennen, welche vermuteten Straftaten eine Einsichtnahme in diese Informationen und somit einen massiven Eingriff in die Privatsphäre rechtfertigen, d.h. ob beispielsweise ein einfacher Verdacht auf Steuerbetrug dafür ausreicht.

Art. 9 Datensicherheit

Nach **Art.9 Abs. 2** sind die Anbieterinnen von Kommunikationsdienstleistungen bei den Anordnungen zur Überwachung für die Datensicherheit der Überwachungsdaten bis zur Übergabe an den Dienst selbst verantwortlich.

Die zu **Art. 24b** geäusserte Kritik, dass keine technische oder organisatorische Massnahme den Verlust der Daten vollständig verhindern kann, gilt hier ohne Einschränkung.

Da zusätzlich nach **Art. 2 Abs. 2 Bst. c** des Datenschutzgesetzes⁸ der Datenschutz für die Daten aus einer Überwachung nicht anwendbar ist, wird die nicht-intentionale Nutzung der Daten durch den Anbieter (zum Beispiel für eigene kommerzielle Interessen) nicht explizit ausgeschlossen. Dies ist aus Sicht des CCCZH konsequent abzulehnen.

Art. 17 Abs. 2 Berufsgeheimnisträger

Die zum **Art. 25 Abs. 2** geäusserte Kritik gilt auch für die entsprechenden Artikel in Bezug auf (Festnetz- und Mobil-)Telefonie. Interessanterweise gilt die Regelung, den speziellen Schutz der Kommunikation von Berufsgeheimnisträger bei einer Überwachung ohne spezielle Genehmigung zu ignorieren, nicht für den (physikalischen) Postverkehr.

Abschliessende Betrachtungen

Abschliessend ist aus Sicht des CCCZH folgendes festzustellen:

1. Bei der **Echtzeitüberwachung** kann *ohne Einschränkung*, d.h. ohne an die konkreten Vorgaben dieser Verordnung oder des zugrunde liegenden Bundesgesetzes gebunden zu sein, der gesamte Telefonie- und Internetverkehr einer verdächtigen Person auf Anordnung überwacht und gespeichert werden (**Art. 25 Abs. 5**). Dieses Vorgehen unterliegt dabei offensichtlich *keiner Kontrolle* durch

unabhängige Stellen, sondern obliegt allein der genehmigenden Behörde bzw. dem zuständigen Dienst beim EJPD. Auch die Regelungen zur *Überwachung von Berufsgeheimnisträgern ohne spezielle Genehmigung* ist unserer Meinung nach eine untragbare Regelung (**Art. 25 Abs. 2**). Dies mit einer „jahrelangen Praxis“ zu rechtfertigen, scheint aus Sicht des CCCZH fragwürdig und ist deshalb insgesamt konsequent abzulehnen.

2. Bei der **rückwirkenden Überwachung (Vorratsdatenspeicherung)** wird durch unpräzise Formulierungen (**Art. 24**) einer *Totalüberwachung* aller Internetnutzer durch *Protokollierung aller Internet-Aktivitäten* bei Dienste-Anbieterinnen Tür und Tor geöffnet. Die sich dadurch zwangsläufig ergebende Profilerstellung und der unkontrollierbaren Nebennutzung dieser Informationen ist aus Sicht des CCCZH mit der informationellen Selbstbestimmung nicht zu vereinbaren und deshalb konsequent abzulehnen.

Für die Beachtung unserer Kritikpunkte danken wir Ihnen bestens.

Mit freundlichen Grüßen,

Bernd Fix, i.A.d. Chaos Computer Clubs Zürich