Positionspapier der ISPA
zur verdachtsunabhängigen Speicherung von Verkehrs- und Standortdaten (Data Retention)

Management Summary:

Die ISPA, der Verband der österreichischen Internet Service Provider bezieht zur Data Retention Richtlinie (RL 2006/24/EG vom 15. März 2006) und deren anstehenden Umsetzung in das österreichische Recht folgende Position:

Unverhältnismäßige Grundrechtseingriffe

Den Strafverfolgungsbehörden müssen aus Sicht der ISPA effiziente Mittel zur Ermittlung, Feststellung und Verfolgung von schweren Straftaten zur Verfügung stehen. Allerdings müssen die mit solchen Maßnahmen verbundenen Grundrechtseingriffe so gering wie möglich gehalten werden. Die in der Data Retention Richtlinie vorgesehene verpflichtende verdachtsunabhängige Speicherung von Verkehrs- und Standortdaten (Vorratsdatenspeicherung, Data Retention) stellt jedoch gegenüber der geltenden Rechtslage in Österreich einen grundlegenden Paradigmenwechsel dar: Strafverfolgungsbehörden können zur Zeit ausschließlich auf Daten zurückgreifen, die bei Betreibern deshalb vorhanden sind, weil er sie für seine Geschäftstätigkeit braucht. Die Daten sind – sofern keine Einwilligung des Betroffenen zu einer weiteren Verwendung vorliegt – nach Beendigung der Verbindung oder dann, wenn sie nicht mehr für die Verrechnung relevant sind, ausnahmslos zu löschen oder zu anonymisieren. In der Data Retention Richtlinie ist demgegenüber vorgesehen, dass Verkehrs- und Standortdaten ausschließlich zum Zweck der Strafverfolgung gespeichert werden, ohne dass sie für den Betreiber irgendeinen wirtschaftlichen Zweck hätten. Die ISPA hegt große Bedenken, sowohl hinsichtlich der Effizienz der ins Auge gefassten Maßnahmen im Hinblick auf die in der Richtlinie genannten Ziele der Bekämpfung schwerer Straftaten und des Terrorismus, als auch im Bezug auf das Ausmaß der Eingriffe in grundrechtliche Positionen.

Technische Vorgaben der Richtlinie unklar und daher nicht umsetzbar

Die Data Retention Richtlinie sieht für Internet Service Provider (ISPs) die Vorratsspeicherung diverser Daten im Bereich der elektronischen Kommunikation vor. Das betrifft insbesondere den Internetzugang, den E-Mail-Verkehr und die Internet-Telefonie. Im Bereich Internetzugang erscheint eine direkte Umsetzung der Richtlinie realistisch. Vor allem in den Bereichen E-Mail und Internet-Telefonie bestehen jedoch noch weitgehende Unklarheiten sowohl für die Sicherheitsbehörden als auch die Internet Service Provider, deren Klärung intensive Untersuchungen erfordert, bevor eine sinnvolle Umsetzung der Richtlinie möglich ist. Die Durchführung und Dokumentation dieser Untersuchungen ist das Ziel einer Studie am Institut für Distributed and Multimedia Systems der Fakultät für Informatik der Universität Wien. Keinesfalls darf der in der Richtlinie vorgegebene Grundsatz der Verhältnismäßigkeit verletzt werden, wonach hinsichtlich Daten, die von einem Betreiber nicht erzeugt oder verarbeitet werden, keine Speicherpflicht besteht.

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

Vorschläge für die Umsetzung für den Bereich Internet

- *Umsetzungsfrist*: Österreich hat die Möglichkeit in Anspruch genommen, die Umsetzung der Regelungen im Bezug auf Internet-Zugang, Internet-Telefonie und Internet-Email bis 15. März 2009 aufzuschieben. Die Frist sollte ausgenützt werden, um im Zusammenwirken aller Betroffenen (Strafverfolgungsbehörden, Betreiber und Kunden) eine die Grundrechte möglichst wenig einschränkende, wirtschaftlich verträgliche aber möglichst effiziente Umsetzung zu gewährleisten und nationale (vgl. neuer ETSI-Standard bei der Überwachung) und internationale Erfahrungswerte im Zusammenhang mit der Vorratsdatenspeicherung zu verwerten.
- *Keine zentrale Speicherung der gesammelten Daten:* Die gesammelten Daten dürfen ausschließlich beim Provider, bei dem sie anfallen, gespeichert werden. Eine zentrale Speicherung für die Daten aller Betreiber würde eine enormes Missbrauchspotential mit sich bringen.
- *Zugriff auf die gesammelten Daten*: Wesentlich ist, dass zum Schutz der Privatsphäre und der personenbezogenen Daten der Bürger gewährleistet ist, dass auf die gesammelten Daten nur auf richterlichen Befehl und zur Verfolgung schwerer Straftaten (Verbrechen, also Vorsatzdelikte, die mit lebenslanger oder mit mehr als dreijähriger Freiheitsstrafe bedroht sind) zugegriffen wird, und dass Dritte, insbesondere Private, keinesfalls Zugriff auf die Daten erhalten.
- *Kosten*: Bei der Vorratsdatenspeicherung handelt es sich um eine Maßnahme, die ausschließlich der Strafverfolgung, also zur Erfüllung einer staatlichen Aufgabe dient. Die zu speichernden Daten haben für die Betreiber keinerlei wirtschaftlichen Wert. Den Betreibern sind daher sowohl die laufenden als auch die Einrichtungskosten der Speicherung und Bereitstellung der Daten zeitnahe mit der technischen Umsetzung zu ersetzen.
- *Speicherdauer:* Studien haben gezeigt, dass sich – soweit Verkehrs- und Standortdaten für Ermittlungszwecke überhaupt gebraucht werden – 95% der Anfragen von Ermittlungsbehörden auf Vorfälle beziehen, die weniger als 6 Monate zurückliegen. Die Speicherdauer darf daher keinesfalls länger als 6 Monate sein, um die Eingriffe in die Privatsphäre der Bürger und deren Grundrecht auf Schutz ihrer personenbezogenen Daten so gering wie möglich zu halten.
- *Datenkategorien:* Im Zusammenhang mit den zahlreichen technischen Unklarheiten sollte bereits in den gesetzlichen Bestimmungen auf die jeweiligen „wirtschaftlichen und technischen Gegebenheiten und Möglichkeiten“ Bedacht genommen werden. Beispiele hierfür sind in den telekommunikationsrechtlichen Bestimmungen hinlänglich bekannt (z.B. § 22 TKG 2003, § 3 Abs 3 ÜVO).

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

Zu den Fragestellungen im Detail:

I. Juristische Fragen

1.) Effizienz

Die ISPA bezweifelt, dass die in der Richtlinie vorgesehenen Maßnahmen überhaupt geeignet sind, das Ziel der Richtlinie, nämlich die Erleichterung der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, zu erreichen. Zum einen sind nur Anbieter *öffentlich zugänglicher* elektronischer Kommunikationsdienste oder Betreiber eines *öffentlichen* Kommunikationsnetzes zur Vorratsdatenspeicherung verpflichtet, andererseits sind von diesen ausschließlich Verkehrs- und Standortdaten im Bezug auf bestimmte Dienste (Telefonie, Internet-Access, VoIP, Email) zu speichern. Jedem, der sich der Speicherung seiner Daten entziehen will, ist dies leicht möglich , indem er etwa mit von der Speicherpflicht nicht umfassten Diensten wie Instant Messaging kommuniziert, einen eigenen Mailserver einrichtet oder anonyme Accounts verwendet (hier werden zwar unter Umständen Verkehrsdaten gespeichert, können aber keiner Person zugeordnet werden). Eine weitere Ausweitung der Speicherpflichten würde dem ebenfalls nicht abhelfen, weil allein die nach dieser Richtlinie anfallenden Datenmengen so gewaltig sind, dass bezweifelt werden muss, dass sie überhaupt für die Verbrechensbekämpfung eingesetzt werden können. Darüber hinaus besteht jederzeit die Möglichkeit, sich eines außerhalb der EU tätigen Providers zu bedienen. Zusammenfassend kann gesagt werden, dass diejenigen, die etwas zu verbergen haben, der Data Retention leicht ausweichen können und überwiegend nur Kommunikationsprozesse unbescholtener Bürger aufgezeichnet werden. Viele datenschutzbewusste Bürger werden daher wohl ebenfalls zu Providern außerhalb der EU wechseln, was negative Folgen für die europäische Internetwirtschaft haben würde.

2.) Eingriff in Grundrechte

Die Data Retention führt dazu, dass Verkehrs- und Standortdaten im Zusammenhang mit Kommunikationsvorgängen aller Bürger, unabhängig von einem konkreten Anlass, insbesondere ohne konkrete Verdachtsmomente, gespeichert werden müssen. So ist etwa auch denkbar, dass aufgrund der gespeicherten Daten umfassende Bewegungs- und Verhaltensprofile erstellt werden können. Dies stellt einen massiven Eingriff in fundamentale Freiheitsrechte, insbesondere in das Recht auf Achtung des Privat- und Familienlebens (Art 8 MRK), das Kommunikations- bzw. Fernmeldegeheimnis (Art 10a StGG) sowie das Grundrecht auf Datenschutz (§ 1 DSG 2000), dar. Einschränkungen dieser Grundrechte sind aber nur unter sehr engen Bedingungen zulässig. Gemäß Art 8 Abs 2 MRK darf nur dann in das Grundrecht auf Achtung des Privat- und Familienlebens eingegriffen werden, wenn die Maßnahme in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutze der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig und verhältnismäßig ist. Der Europäische Gerichtshof für Menschenrechte[1] hat festgestellt, dass die Notwendigkeit und Verhältnismäßigkeit in ihrer ganzen Tragweite nachgewiesen werden muss.

[1] Urteil des EGMR vom 22. Oktober 1981 in der Rechtssache Dudgeon, A45, Nr. 7525

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

Entgegen der Beteuerung in Erwägungsgrund 22 sind die Voraussetzungen für den Grundrechtseingriff durch die Data Retention-Richtlinie jedoch nicht erfüllt. Die Vorratsdatenspeicherung wird zwar in Erwägungsgrund 9 als für die Bekämpfung von Terrorismus und organisierter Kriminalität notwendig bezeichnet. Es wird aber nicht nachgewiesen, dass mit weniger eingriffsintensive Maßnahmen, wie etwa einer anlassbezogene Datenspeicherung (Data Preservation, data freeze), wie sie auch die Cybercrime Convention des Europarates vorsieht, dieses Ziel nicht ebenfalls erreicht werden kann. Aufgrund der schon angesprochenen Möglichkeiten des Ausweichens auf nicht von der Data Retention betroffenen Kommunikationswege ist klar, dass in erster Linie Daten unbescholtener Bürger gesammelt werden. Gerade deren Daten sind aber für die Strafverfolgung gar nicht notwendig.

Im Bezug auf die von Art 8 MRK geforderte Verhältnismäßigkeit ist festzustellen, dass der Ausgleich zwischen dem Interesse an einer effizienten Strafverfolgung gegenüber dem Interesse der Bürger auf Schutz ihrer Privatsphäre gänzlich fehlt. Wenn in die Rechte aller, vor allem auch unbescholtener, Bürger eingegriffen wird und die Maßnahmen hinsichtlich der verfolgten Ziele der Ermittlung, Feststellung und Verfolgung von schweren Straftaten ineffizient sind, ist der Eingriff in die Grundrechte unverhältnismäßig und somit unzulässig.

Gerade bei elektronischen Nachrichten zeigt sich ein – technisch nicht trennbares – Verschmelzen von Inhalts- und Verkehrsdaten, welches zwangsläufig zu einem Verstoß gegen das Verbot der Verarbeitung von Inhaltsdaten führt. Im Zweifel muss von einer Speicherpflicht bereits bei der gesetzlichen Umsetzung abgesehen werden.

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

II. Technische Fragen

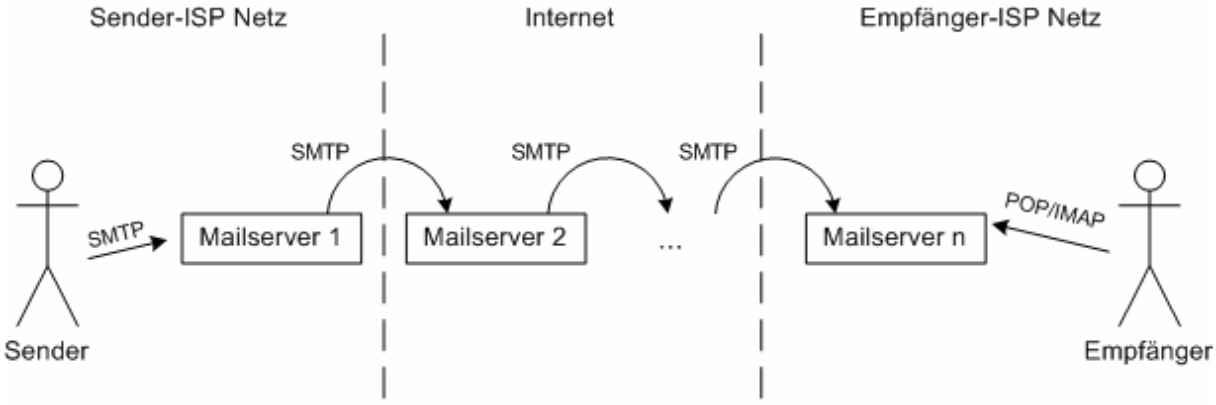
1.) Allgemeines

Diverse Methoden zur Verschlüsselung der Kommunikation, welche die Sicherheit im Internet erhöhen soll, können bei dem Versuch, Verkehrsdaten zu erfassen, zu Problemen führen. Im Idealfall sind bei verschlüsselter Kommunikation nur die beiden Endpunkte in der Lage, entsprechende Informationen bereitzustellen. Der ISP stellt oft nur die Infrastruktur für eine Datenübertragung zur Verfügung, und nicht notwendigerweise auch die Dienste, die auf der Basis dieser Infrastruktur genutzt werden (ein wichtiger Unterschied zum ebenfalls in der EU-Richtlinie abgedeckten Telefoniebereich!). Daher kann es schwierig bis unmöglich sein, relevante Verkehrsdaten zu erfassen.

2.) E- Mail

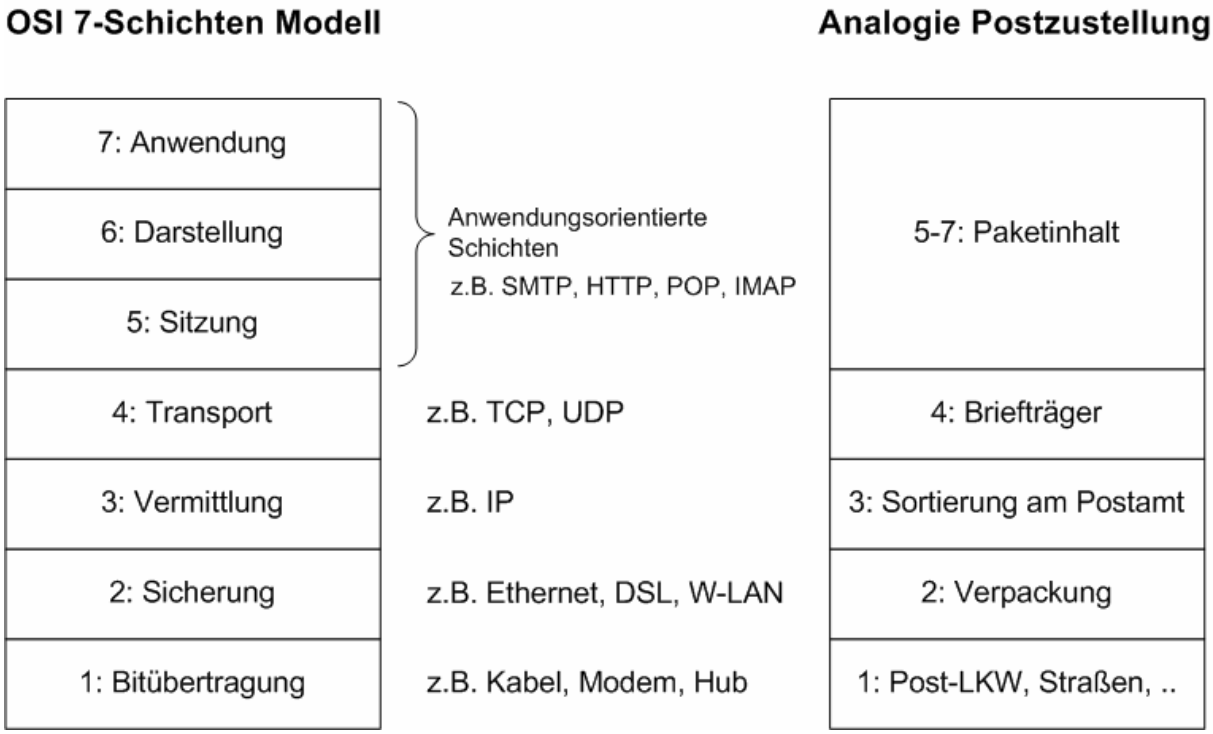
Im Kontext des E-Mail-Verkehrs wird jedem Benutzer, der an einer Kommunikation teilnimmt, zumindest eine E-Mail-Adresse zugewiesen. Die Übergabe der E-Mails im Internet vom Sender an den ersten Mailserver bzw. von einem Mailserver an den nächsten wird durch das Simple Mail Transfer Protocol (SMTP) geregelt.

Die vorliegende EU-Richtlinie fordert von den Internet Service Providern die Identifizierung der Teilnehmer einer Kommunikation, ungeachtet dessen ob eine E-Mail das Netz des Providers verlässt oder in diesem ankommt. Hinsichtlich der Daten über Absender und Empfänger, die dem Provider in jedem der beiden Fälle zur Verfügung stehen, ist diese Unterscheidung jedoch eine sehr wichtige. Ein Grund dafür liegt in der Struktur des Internets. Während bei anderen Diensten, wie zum Beispiel im Bereich der Telefonie, das zugrunde liegende Netzwerk und die Dienste, oft vom selben Betreiber angeboten werden, ist dies im Internet nicht so. Hier wird prinzipiell der Zugang zum Netz angeboten, jedoch ist das Internet selbst dann für alle Nutzer praktisch gleich und jeder Dienst von jedem Anbieter kann durch praktisch jeden Kunden genutzt werden. Wie man in der folgenden Graphik sieht, erfolgt die Kommunikation per E-Mail bzw. im Internet generell, nicht nur über eine Stelle. Vielmehr durchlaufen die Informationseinheiten des Internets, Pakete genannt, verschiedene Netze und Server , die von verschiedenen Anbietern betrieben werden. Details dazu, wie die gezeigten Protokolle SMTP, POP und IMAP oder die Arbeitsweise eines Mailservers, werden in den nachfolgenden Absätzen beschrieben.



address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

Das Open Systems Interconnection (OSI) Reference Model, oft OSI 7-Schichten Modell genannt, gliedert die verschiedenen Komponenten und Protokolle, die benötigt werden, um elektronische Kommunikation in einem Netzwerk wie dem Internet zu ermöglichen, in 7 Schichten. Zum leichteren Verständnis enthält die folgende Grafik sowohl das 7 Schichten Modell, als auch einen Vergleich, wie diese Schichten im Kontext einer klassischen Postzustellung interpretiert werden könnten.



Da es im Kontext dieser Richtlinie um Verkehrsdaten und nicht um Inhaltsdaten geht, sind für die Internet Service Provider die ersten vier Schichten in vollem Ausmaß, wobei die Schichten drei und vier die im Internet eher interessanten Verkehrsdaten festlegen, und eingeschränkt die Schicht fünf, interessant.

3.) Voice over IP

Voice over IP ist ein Sammelbegriff für alle Techniken, Hard- oder nur Software, um Sprache in IP Pakete einzubetten und zu übertragen. Hier existieren einige verschiedene Ansätze und Protokolle, verpackt in Hardware oder Software-Lösungen. Manche der Protokolle sind standardisiert, manche proprietär. Die Identifikation der Teilnehmer und Nachverfolgung eines Internet-Telefonie-Gesprächs kann aus der Sicht des ISPs aufgrund von Verschlüsselung und unterschiedlichen Protokollen sehr komplex sein.

Damit die Introspektion für den ISP gegeben ist, muss das Protokoll offen gelegt sein, weil der Inhalt der Pakete sonst nicht verstanden werden kann. Zwei größere Ansätze zur Standardisierung und Vereinheitlichung der VoIP Kommunikation sind das Session Initiation Protocol (SIP) und die von Google entwickelte Erweiterung "Jingle" für das Jabber-Protokoll. Weiters werden auch die Protokolle der H.323-Empfehlung genutzt, etwa von Microsoft Netmeeting .

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

Skype[2] beispielsweise, eines der bekanntesten VoIP-Programme, benutzt ein proprietäres Protokoll mit verschlüsselten Paketen und komplexen Routingalgorithmen, um die Anonymität seiner Nutzer zu wahren und die vorhandenen Leitungen bestmöglich zu nutzen. Da die Pakete zwischen zwei Teilnehmern eines Gespräches über den jeweils vom System als besten angenommenen Pfad geroutet werden[3], der nicht für jedes Paket gleich sein muss, und zusätzlich verschlüsselt sind, wäre es für den ISP doppelt schwer die Teilnehmer eines Gesprächs zu identifizieren. Zum einen kann er nicht wissen wo das aktuelle Paket noch hingeroutet werden wird und zum anderen kann er den Inhalt des Pakets, der vielleicht Aufschluss über die Teilnehmer geben würde, nicht betrachten, weil dieser verschlüsselt ist.

Neben Skype existieren unter anderem Google Talk[4], das zwar ein offen gelegtes Protokoll benutzt, jedoch Verschlüsselung in naher Zukunft angekündigt hat[5], oder Team Speak[6], das für die Online-Spieler Community optimiert ist und ein proprietäres Protokoll verwendet. Oder auch Windows Live Messenger[7] der ein teilweise offen gelegtes Protokoll verwendet, und Yahoo! Messenger[8], mit bekanntem Protokoll.

4.) Kommentare zu einzelnen Textstellen der Richtlinie

- Ad Art 5 Abs 1 lit. a Z 2 – Identifizierung der Quelle

i) Benutzerkennung
Betreffend Internet-E-Mail soll zur Identifizierung des Urhebers einer Nachricht die "zugewiesene Benutzerkennung" gespeichert werden. Für, in das Netz des Providers eingehende, E-Mails steht dafür nur die Headerinformation, sowie die Adresse, an welche die Nachricht zugestellt werden soll, zur Verfügung.

Da die Daten, die in den Header einer Nachricht geschrieben werden vom E-Mail Programm des Benutzers (Mail User Agent / MUA) mehr oder weniger frei gewählt werden können, sind sie nur bedingt als Quelle für Verkehrsdaten geeignet. Prinzipiell stellt sich bei den Headern einer E-Mail die Frage ob die darin enthaltenen Informationen generell als Inhaltsdaten oder Verkehrsdaten gelten, weil sie zum einen Trace-Felder und zum anderen Daten, wie z.B. den Betreff, enthalten. Eine genauere technische Untersuchung dieser Frage wird in der angesprochenen Studie durchgeführt werden.

Die einzige authentische Information, die im allgemeinen garantiert verfügbar ist, ist einerseits die Empfängeradresse und andererseits der Name des Servers, welcher die Nachricht übergibt.

[2] http://www.skype.com/
[3] http://www.skype.com/products/explained.html
[4] http://www.google.com/talk/
[5] http://www.google.com/talk/about.html
[6] http://www.teamspeak-systems.de/
[7] http://get.live.com/messenger/overview
[8] http://messenger.yahoo.com/

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

Laut MessageLabs[9] lag der weltweite Anteil von Spam am gesamten E-Mail-Aufkommen im Oktober 2006 bei fast 70% und andere Schätzungen liegen noch deutlich höher. Aus naheliegenden Gründen ist hier anzunehmen, dass in diesen Fällen nicht die wahre Absenderadresse, sondern eine fiktive oder fremde angegeben wurde, die daher keinerlei Auskunft über die wahre Identität der Quelle gibt.

Ein weiterer problematischer Aspekt an der Erfassung und Speicherung der Verkehrsdaten sind die diversen Freemail-Provider, die ihren Benutzern ein Web-Interface zur Verfügung stellen, um die allgegenwärtige Verwaltung der E-Mails per Browser zu ermöglichen. In diesem Fall werden also die E-Mails nicht von einem Mail-Client per SMTP an den Mailserver (Mail Transfer Agent, MTA) übergeben, sondern ein Webserver, zu dem sich der Benutzer per Hypertext Protocol (HTTP) verbindet, interagiert hier mit dem Mailserver. Da die Verkehrsdaten, wie z.B. E-Mail Adressen, in diesem Fall in HTTP Pakete eingebettet sind, gelten sie als Inhalt der Kommunikation und dürfen daher nicht mehr vom Provider gespeichert werden. E-Mails, die über Webmail-Provider verschickt oder empfangen werden, gehen daher in gewissem Sinn am ISP vorbei und sind für diesen nicht direkt fassbar. Nachrichten von Freemail Providern können nur dann erfasst werden, wenn die Nachrichten an einen ISP geschickt werden, welcher die Verkehrsdaten aufzeichnet (wie zuvor erwähnt sind dann der Adressat und der sendende Server bekannt), bzw. wenn der Freemail Provider sich in der EU befindet und daher seinen eigenen (in diesem Fall ausgehenden) E-Mail Traffic speichern muss.

Ein ähnliches Problem stellt sich bei IP Tunneln, wie sie bei Virtual Private Networks (VPNs) gebraucht werden. IP Tunnel sind logische Verbindungen zwischen zwei Rechnern über ein anderes Netzwerk, wie zum Beispiel dem Internet. Im Falle von VPNs werden verschlüsselte Verbindungen zwischen bestimmten Rechnern über das Internet hergestellt, um einer bestimmten Gruppe an Benutzern sichere Kommunikation über ein prinzipiell öffentliches Netz zu ermöglichen. Alle SMTP Nachrichten, die – verschlüsselt oder nicht - über so einen Tunnel gehen, sind eingebettet in andere Protokolle und zählen daher, wie oben erwähnt, als Inhalt einer Kommunikation und dürfen nicht mehr vom Provider gespeichert werden.

ii) Benutzerkennung & Rufnummer der Nachricht
Prinzipiell stellt sich hier die Frage, ob wirklich die "Benutzerkennung" und "Rufnummer" der Nachrichten gemeint sind, weil weder das eine noch das andere Bezeichnungen für die Kennungen einer Nachricht sind, sondern Bezeichnungen für Teilnehmer einer Kommunikation sind und leicht missverstanden werden können.

iii) Name und Anschrift des Teilnehmers
Bei jedem "Hop", d.h. jedem SMTP-Server, den eine E-Mail im Rahmen ihres Weges vom Absender zum Empfänger durchläuft, muss nach RFC 2821[10] eine sogenannte "Received"-Zeile in der Mail hinterlassen werden, die normalerweise angibt, von wem die E-Mail entgegengenommen wurde und welches Protokoll verwendet wurde.

Zwar sind die Mailserver laut Standard dazu verpflichtet eine Received-Zeile in den Headern zu vermerken und es wird ihnen verboten bereits vorhandene Einträge zu modifizieren oder zu löschen. Jedoch wird es ihnen auch verboten eine E-Mail aufgrund der Trace-Informationen, wie z.B. den Received-Einträgen, zu verwerfen. Damit könnten prinzipiell

[9] http://www.messagelabs.co.uk/
[10] http://tools.ietf.org/html/rfc2821#page-26

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

gefälschte oder gar keine Informationen in diesen Trace-Feldern vermerkt sein und trotzdem würde diese E-Mail zugestellt werden.

Zusätzlich sind die enthaltenen Informationen, z. B. IP-Adressen, und auch das Format, mit Ausnahme der Zeitangabe, frei wählbar. Es ergibt sich durch diese Vorgangsweise auch die Unsicherheit der Zeitangaben, weil nicht alle Mailserver zeitsynchronisiert sind.

Auch ist es möglich, und wird von Spam-Quellen praktiziert, diese Information zu verfälschen, indem z.B. der erste, von einem Spammer kontrollierte, SMTP-Server in der Kette einen erfundenen "Received"-Eintrag hinzufügt. Damit muss diese Ansammlung an Einträgen nicht zwingend den wahren Weg einer E-Mail vom Absender zum Empfänger repräsentieren. Da man davon ausgehen kann, dass die Mailserver der ISPs ordnungsgemäß konfiguriert sind, sind die Received-Zeilen vertrauenswürdig erst ab jenem Punkt, an dem die Mail an einen Mailserver des Providers übergeben wurde.

Außerdem ist es möglich, mit Anonymisierungs-Diensten wie z.B. Anonymizer[11] den Zusammenhang zwischen IP-Adresse und Absender zu verschleiern. Hier wird eine Stelle zwischengeschalten, die den Absender mimt. Damit sieht die Kommunikation, wenn man die SMTP Nachrichten betrachtet, aus wie Anon.-Dienst - Empfänger und der wahre Absender der Nachricht bleibt hinter dem Anonymisierungs-Dienst verborgen.

Die Quelle einer E-Mail Nachricht kann der ISP eindeutig ausmachen, wenn einer seiner registrierten Kunden eine Nachricht über dessen SMTP Server verschickt. In diesem Fall ist es dem Provider möglich den Absender über die Authentifizierung am SMTP Server oder über die zum jeweiligen Zeitpunkt zugewiesene IP-Adresse zu identifizieren.

Aber selbst bei diesen E-Mails, die per SMTP von einem Kunden des Providers ausgeschickt werden, lässt sich eine Zuordnung zu einer bestimmten Identität eines Absenders nicht mit völliger Sicherheit vornehmen. Die E-Mail könnte durch ein offenes Mail-Relay, d.h., einen wahllos annehmenden und zustellenden SMTP Server, das am Computer des Benutzers eingerichtet ist, versandt worden sein. Als offene Mail-Relays können auch schlecht konfigurierte oder von Unautorisierten absichtlich platzierte Mailserver fungieren. Eine aktuelle Problematik in diesem Kontext sind Bot-Netze: Computer, die ohne Wissen des Besitzers über bekannte Sicherheitslücken (z. B. im Betriebssystem) mit Hintertüren versehen wurden und, zu riesigen Netzwerken organisiert, das tun, was Ihnen über verschlüsselte Kanäle aufgetragen wird; z. B. E-Mails versenden.

- Art 5 Abs 1 lit. b Z 2 – Identifizierung des Adressaten

Das "RCPT TO"-Feld im SMTP-Dialog, das den Empfänger einer E-Mail angibt, dient als Grundlage für die Zustellung und kann damit nicht manipuliert werden, ohne zu bewirken, dass die Nachricht, ausschließlich oder zusätzlich, jemand anderem zugestellt wird.

Wird eine E-Mail aus dem Netz eines ISP in ein anderes Netz gesandt, so kennt der ISP nur die E-Mail-Adresse des Empfängers. Es ist ihm im Allgemeinen *nicht möglich*, aus dieser auf die laut Richtlinie zu speichernden Informationen Name und Anschrift des Empfängers zu schließen. Andererseits kann der Internet Service Provider im Fall einer in sein Netz

[11] http://www.anonymizer.com

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

eingehenden E-Mail Auskunft über Name und Anschrift des Adressaten geben, weil dieser bei ihm registriert ist.

Alle an einen bestimmten Benutzer adressierten E-Mails, die sich dieser per Web-Interface, also via HTTP-Protokoll, z.B. von einem Freemail-Provider abholt, können vom ISP jedoch *nicht* erfasst werden, weil die dafür erforderliche Information, wie vorher erläutert, Inhaltsdaten darstellt.

- Art 5 Abs 1 lit. c Z 2 – Datum, Uhrzeit, Dauer der Nachrichtenübermittlung

i) An- und Abmeldung beim Internetzugangsdienst
Die Zeiten einer klassischen An- und Abmeldung beim ISP sind nicht mehr so stark untergliedert wie z.B. im Zeitalter der Telefonmodems. Heutzutage überwiegen vor allem im städtischen Bereich Leitungen, die „always-on" sind, weil nicht mehr nach Zeit, sondern nach Datenvolumen vergebührt wird. Die An- und Abmeldung geschieht dann, wenn das Kabel- oder ADSL-Modem ein- und abgeschalten wird und dieser Zeitraum kann sich über Stunden, Tage oder länger erstrecken.

ii) An- und Abmeldung beim Internet-E-Mail-Dienst
Es ist zu klären, was in diesem Zusammenhang unter „Internet-E-Mail-Dienst" zu verstehen ist. Der Begriff könnte z.B. als Bezeichnung für den jeweiligen SMTP-Server ausgelegt werden. In diesem Fall entsprechen die Zeiten der An- und Abmeldung den Zeiten der Verbindungsaufnahme und –beendigung per TCP/IP. Die Dauer dieser Kommunikation ist von der Leitung zwischen dem Computer des Absenders und dem Server und von der Geschwindigkeit der Verarbeitung an der Serverseite, also von der Last auf diesem, abhängig und gibt somit keine qualitativen Informationen betreffend der Kommunikation zwischen Absender und Empfänger.

- Art 5 Abs 1 lit. d Z 2 – Art der Nachrichtenübermittlung

Es ist nicht klar, was in diesem Kontext unter dem Begriff „Internetdienst" zu verstehen ist. E-Mails werden mithilfe des SMTP-Protokolls von Server zu Server weitergeleitet und am Ende dieser Kette werden die Nachrichten entweder per HTTP-, POP- oder IMAP-Protokoll vom Benutzer abgeholt. Denkbar wäre es daher auch, dass unter dem Begriff „Internetdienst" das benutzte Protokoll zu verstehen ist.

Das SMTP Protokoll wird benutzt, um die Nachricht vom Absender bis zum letzten Mailserver in der Kette zu übertragen, wobei diese Kette im Normalfall keine oder nur sehr wenige Zwischenstationen hat. Auf diesem Server bleibt die Nachricht dann solange, bis sie der Empfänger per POP/IMAP abholt. Bei diesen Protokollen werden die Header der E-Mails wie z.B. Empfänger und Absender, die bei SMTP noch als Verkehrsdaten gelten, als Inhaltsdaten übermittelt und gehen in dieser Form, "unantastbar", über die Leitungen des Providers, sofern nicht dessen Mailserver an der Übermittlung beteiligt ist.

Weiters ist die Art des Internetdienstes nicht notwendigerweise feststellbar, wenn z.B. per Browser, über das HTTP-Protokoll also, darauf zugegriffen wird und die entsprechenden Daten daher auch Inhaltsdaten sind.

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

- Art 5 Abs 1 lit. e Z 3 – Endeinrichtung

Hier wird verlangt, die Endeinrichtung des Adressaten zu identifizieren. Wie bereits erwähnt, kennt der Provider bei einer sein Netz verlassenden Nachricht nur die E-Mail-Adresse des Empfängers ; Daten wie die IP-Adresse, Post-Adresse oder der Name des Empfängers sind ihm unbekannt. Genauso stehen ihm auch keine technischen Details zur Endeinrichtung desselben zur Verfügung.

Wartet nun eine E-Mail auf dem Mailserver des Providers auf Abholung per POP/IMAP, so ist es nicht zwingend notwendig, dass der Empfänger sie mithilfe der Endeinrichtung, die ihm vom Provider zur Verfügung gestellt wurde, also Wähl- oder Kabel-Modem o.ä., abholt. Damit könnte z.B. eine Mail, die auf dem Mailserver eines Providers liegt, von einem Benutzer, der Kunde bei diesem Provider ist, nicht über dessen Internet-Anschluss, sondern z.B. von der Arbeit, Schule, Universität, einem öffentlichen Internet-Terminal o.ä. aus, abgeholt werden, also von einer anderen Einrichtung, obwohl der Empfänger derselbe bleibt.

Über die ISPA:

Der Verband der österreichischen Internet Service Provider (ISPA) ist die Dachorganisation der Internet-Wirtschaft. Ihr Anliegen ist die Gestaltung der optimalen wirtschaftlichen und rechtlichen Bedingungen für die Entwicklung des Internet. Die ISPA betrachtet die Nutzung des Internet als entscheidende Kulturtechnik und nimmt die sich daraus ergebende gesellschaftspolitische Verantwortung wahr.

Wien, am 9.2. 20007

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977