Prof. Dr. Klaus-Peter Löhr
a.D. Freie Universität Berlin
Wangenheimstr. 44
14193 Berlin
Lohr@inf.fu-berlin.de

Prof. Dr. Hartmut Pohl
Hochschule Bonn-Rhein-Sieg
und softScheck GmbH
53757 Sankt Augustin
Hartmut.Pohl@softScheck.com

Prof. Dr. Kai Rannenberg
Goethe-Universität Frankfurt
60629 Frankfurt
Kai.Rannenberg@m-chair.de

- für den Präsidiumsarbeitskreis ‚Datenschutz und IT-Sicherheit' der Gesellschaft für Informatik (GI) e.V. –

Schleswig-Holsteinischer Landtag
Umdruck 18/5429

8. Januar 2016

Stellungnahme

zur Drucksache 18/3311,
Antrag der Fraktion der PIRATEN im Schleswig-Holsteinischen Landtag,
„Bundesratsinitiative zur technischen Sicherung des
Fernmeldegeheimnisses – Ende-zu-Ende-Verschlüsselung für das Telefon"

Grundsätzliches zu Kommunikation und Verschlüsselung

Technische Kommunikation erfolgt heute überwiegend ungesichert – d.h. ohne Maßnahmen zur Sicherung von Vertraulichkeit und Integrität. Dies ermöglicht das unberechtigte Abhören und die Manipulation jeder technischen Kommunikation in Deutschland (und der gesamten Welt). Es ist aber sehr wohl möglich, die Kommunikation zuverlässig zu sichern, und zwar durch den konsequenten Einsatz von Verschlüsselung. Insbesondere die Ende-zu-Ende-Verschlüsselung ermöglicht die vertrauliche Datenübertragung zwischen den Endgeräten der jeweiligen Partner. Damit ist die gesetzlich geforderte Vertraulichkeit der Kommunikation sowie deren Integrität auch technisch durchsetzbar.

Nach heutigem Stand der Technik gewährleisten die meisten Kommunikations-Provider die verschlüsselte Kommunikation zwischen ihren Systemen und den Endsystemen der Kunden (über das Protokoll *Transport Layer Security*, TLS). Verschlüsselt wird dabei aber *nicht durchgehend* zwischen den Kommunikationspartnern; vielmehr wird in den weiterleitenden Systemen der Provider regelmäßig entschlüsselt, so dass die Daten auf dem Weg zwischen den Kommunikationspartnern auf Zwischenstationen abgefangen werden können.

Im Gegensatz dazu bleibt bei der *Ende-zu-Ende-Verschlüsselung* die Nachricht auf dem gesamten Übertragungsweg zwischen Sender und Empfänger verschlüsselt: sie wird im Endgerät des Senders verschlüsselt und erst im Endgerät des Empfängers wieder entschlüsselt. Wer Nachrichten mitlesen will, muss entweder auf die Endgeräte zugreifen, um dort die unverschlüsselten Nachrichten abgreifen zu können („Quellen-TKÜ"), oder versuchen, die Verschlüsselung zu brechen, was bei guter Verschlüsselung selbst für starke Angreifer sehr aufwendig bis zu aufwendig ist.

IP-Telefonie

Bei der IP-Telefonie wird Sprache digitalisiert übers Internet übertragen, und zwar unter Einsatz des *Internet Protocol* (IP, daher auch *Voice over IP* - VoIP), das für beliebige digitale Daten eingesetzt werden kann. Die einschlägigen Protokolle sind genormt; im Wesentlichen handelt

es sich um das *Session Initiation Protocol* - SIP - für den Verbindungsaufbau und das *Real-Time Transport Protocol* - RTP - für die eigentliche Sprachübertragung. Für den Verbindungsaufbau muss der Teilnehmer sich an einen *SIP Server* des Providers wenden, kommuniziert anschließend aber direkt über RTP mit dem gewünschten Partner. Beim Einsatz von SIP/RTP wird nichts verschlüsselt. Ein gezieltes Abhören von Gesprächen ist damit - wenn auch technisch anders - ebenso möglich wie bei traditioneller Telefonie. Schon 2005 wies das Bundesamt für Sicherheit in der Informationstechnik darauf hin, dass unverschlüsselte IP-Telefonie vergleichsweise einfach und effizient abgehört werden kann.

Für die genannten Protokolle gibt es mit SIPS und SRTP/ZRTP (S für *secure*) erweiterte Versionen, die mit Verschlüsselung arbeiten. SIPS (2002/2009 genormt) sichert unter Einsatz von TLS den Kontakt mit dem Provider, und SRTP (2004 genormt) praktiziert eine Ende-zu-Ende-Verschlüsselung des Gesprächs zwischen den Teilnehmern. Somit sind genormte und ausgereifte technische Lösungen für die Sicherung der IP-Telefonie verfügbar.

Signalisierungsinformation kann nicht Ende-zu-Ende verschlüsselt übertragen werden, anderenfalls würde die Kommunikation ihr Ziel nicht erreichen – dies wäre nämlich bei verschlüsselter Empfängeradresse (gewählte Rufnummer) nicht möglich. Höchstens können Teile der Signalisierungsinformation streckenweise verbindungsverschlüsselt werden.

Der Stand der Technik erlaubt es, die genannten Protokolle so zu implementieren, dass die IP-Telefonie nicht mit Einbußen bei der Sprachqualität verbunden ist. Die flächendeckende Umstellung der Endgeräte auf VoIP ist zwar eine Aufgabe, die nicht von heute auf morgen zu bewerkstelligen ist. Ob dabei verschlüsselte oder unverschlüsselte Kommunikation realisiert wird, hat aber wenig Einfluss auf den zu erwartenden Aufwand.

Schlussfolgerungen

Dass nur eine flächendeckende Ende-zu-Ende-Verschlüsselung das Grundrecht auf Vertraulichkeit der Kommunikation sichern kann, ist seit 2001 (Bericht des EU-Parlaments zu Echelon) nicht mehr strittig. Die bevorstehende Umstellung der Telefonie auf VoIP bietet die Chance, statt SIP und RTP gleich die sicheren Versionen SIPS und SRTP einzusetzen; damit würde der Fehler vermieden, der weltweit für die zahlreichen Sicherheitsprobleme im Internet verantwortlich ist, nämlich Sicherheit nicht als *zentrales Qualitätsmerkmal*, sondern als optionalen Zusatz zu begreifen.

Mit der bisherigen Gesetzgebung zum Fernmeldegeheimnis in der Telekommunikation (TKG §88) ist der Staat der Fürsorgepflicht für seine Bürger nur unzureichend nachgekommen. Zwar hat der Bürger auf dem Papier ein Recht auf vertrauliche Kommunikation, und eine Verletzung dieses Rechts ist auch strafbewehrt (StGB §206). Seine tatsächliche Durchsetzung ist aber mit der rasanten technischen Entwicklung, speziell der Digitalisierung, und der Globalisierung der IT viel schwerer und in manchen Fällen unmöglich geworden: Angreifer können weltweit unbemerkt und ungestraft illegale Abhörmaßnahmen durchführen. Diese Situation ist nicht akzeptabel: bedroht ist nicht nur der Datenschutz für den Bürger, den Arzt, Anwalt, Abgeordneten etc., sondern auch die vertrauliche Kommunikation von Unternehmen. Auch Überwachung in großem Stil ist möglich, und die Demokratie ist nicht erst dann bedroht, wenn wir überwacht werden, sondern schon dann, wenn wir überwacht werden *können*.

Es sei daran erinnert, dass schriftliche elektronische Nachrichten (z.B. E-Mail) heute mit wenig Aufwand verschlüsselt werden können. Dies ist in das Belieben des Benutzers gestellt und wird leider noch wenig praktiziert – insbesondere von technikfernen Benutzern. Fatal ist,

dass der Gesetzgeber es bisher dem Markt überlässt, die Verschlüsselung so einfach nutzbar zu gestalten, dass eine schnelle flächendeckende Verbreitung möglich wäre. Deswegen wird auf EU-Ebene im Rahmen der *"Public consultation on the evaluation and the review of the regulatory framework for electronic communications networks and services"* darüber diskutiert, Verschlüsselung in den Funktionsumfang von Universaldiensten aufzunehmen.

Trotzdem hat der Gesetzgeber bisher auch bei der IP-Telefonie darauf verzichtet, die Anbieter auf eine Ende-zu-Ende-Verschlüsselung zu verpflichten. Der Effekt ist, dass negative Fakten geschaffen werden: Millionen neuer Anschlüsse für die IP-Telefonie arbeiten ohne Verschlüsselung. Unverzügliches Handeln ist notwendig, denn jetzt gibt es die Chance, durch gesetzgeberische Maßnahmen *von vornherein* zu gewährleisten, dass die Verschlüsselung von Telefonaten *nicht* in das Belieben der Anbieter gestellt bleibt. Mit einem solchen Schritt könnte die Bundesregierung zeigen, dass sie es ernst meint mit der Forderung, dass Deutschland zum "Verschlüsselungsstandort Nr. 1" werden müsse.

Im Übrigen könnte eine Landesregierung wie die von Schleswig-Holstein innerhalb von Deutschland Vorreiter werden, wenn sie entsprechende Verfahren für die Landesverwaltung einsetzen und die in Schleswig-Holstein aktiven Anbieter von IP-Telefonie und den entsprechenden Endgeräten zum Einsatz von Verschlüsselung motivieren würde.

Quellen und Dokumente:

https://de.wikipedia.org/wiki/IP-Telefonie
www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/KommunikationUeberInternet/Internettelefonie/internettelefonie_node.html
http://www.ip-insider.de/verschluesselt-telefonieren-mit-voip-a-487354/
VoIPSEC – Studie zur Sicherheit von Voice over Internet Protocol, Bundesamt für Sicherheit in der Informationstechnik, 2005
http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/VoIP/voipsec_pdf.html
http://ec.europa.eu/digital-agenda/en/news/public-consultation-evaluation-and-review-regulatory-framework-electronic-communications

Technischer Anhang: Beispiele für Geräte für die Verschlüsselung von IP-Telefonie

Ein Beispiel für ein IP-Telefon, das SIPS und SRTP unterstützt, ist das Auerswald COMfortel 3600 IP (http://blog.auerswald.de/comfortel-3600-ip/); andere Beispiele finden sich bei Snom (www.snom.com/de/nc/).

Ein VoIP-Telefon mit Ende-zu-Ende Verschlüsselung und Videotelefonie bieten Sirrix und Gigaset an (www.sirrix.de/content/news/67256.htm). Es verwendet das von der NATO unterstützte Secure Communication Interoperability Protocol (SCIP), das auf SIP und RTP aufsetzt.

SIPS und SRTP werden auch von mehreren Geräten, die IP-Routern sehr verwandt sind, unterstützt, z.B.:

- Der Asterisk-Open Source-Software-Nebenstellenanlagen (https://wiki.asterisk.org/wiki/display/AST/Secure+Calling+Tutorial).
- Nebenstellenanlagen wie z.B. die der Firma Auerswald, etwa COMmander 6000 oder COMpact 5000R (www.auerswald.de/de/produkte/telefonanlagen/business/commander-6000/produktbeschreibung.html).

Bei Smartphones verwendet die für iOS und Android erhältliche Software Signal (https://en.wikipedia.org/wiki/Signal_%28software%29; https://whispersystems.org) ein auf ZRTP aufsetzendes Protokoll. Die Firma Sirrix (www.sirrix.de) bietet verschiedene Lösungen für Smartphones, etwa mit Bizztrust (www.sirrix.de/content/pages/63769.htm), ein Smartphonesystem, das das NATO-SCIP verwendet.

Zu beachten ist auch, dass handelsübliche DSL-Router Verschlüsselung im Prinzip beherrschen, weil sie ja meist auch WLAN anbieten und die dafür benötigte Verschlüsselung unterstützen. Bei DSL-Routern gibt es auch Erfahrungen damit, Software und Firmware zu aktualisieren, um Verschlüsselung (für WLAN) zu ermöglichen.