Schleswig-Holsteinischer Landtag
Umdruck 18/5341

VATM e. V. • Frankenwerft 35 • 50667 Köln

Vorab per Mail: Innenausschuss@landtag.ltsh.de
Schleswig-Holsteinischer Landtag
Innen- und Rechtsausschuss
Frau Vorsitzende Barbara Ostmeier
Landeshaus
Düsternbrooker Weg 70
24105 Kiel

Ansprechpartnerin	E-Mail	Fax	Telefon	Datum
Iris Nolte	vatm@vatm.de	0221 3767726	0221 3767725	14.12.2015

Schriftliche Anhörung des Innen- und Rechtsausschusses des Schleswig-Holsteinischen Landtages zum Antrag der Fraktion der PIRATEN Bundesratsinitiative zur technischen Sicherung des Fernmeldegeheimnisses – Ende-zu-Ende-Verschlüsselung für das Telefon

Sehr geehrte Frau Ostmeier,
sehr geehrte Damen und Herren,

wir bedanken uns für die Möglichkeit zur Stellungnahme zu dem oben genannten Antrag, mit dem die Fraktion der Piraten eine Ende-zu-Ende-Verschlüsselung von VoIP-Telefonie fordert. Hierzu positionieren wir uns wie folgt:

Anders als der Antrag der Fraktion der Piraten dies suggeriert, ist VoIP-Telefonie gegenüber herkömmlicher Telefonie (analog und ISDN) keineswegs unsicherer. VoIP-Gespräche können grundsätzlich nur dann abgehört werden, wenn der Angreifer einen physischen Zugriff auf die Leitung des Nutzers erlangt, in dem er bspw. den im Keller befindlichen Verteilerkasten-Übergabepunkt anzapft. Dies ist bei Analog- und ISDN-Telefonie, die ebenfalls nicht verschlüsselt werden, identisch.

Grundsätzlich sollte zwischen VoIP-Telefonie und Internet-Telefonie unterschieden werden. Bei der VoIP-Telefonie handelt es sich um einen vom Provider gestellten VoIP-basierten Telefonanschluss, inklusive eines vom Provider zur Verfügung gestellten Netzabschlusses. Bei der Internet-Telefonie hingegen werden dem Endnutzer frei nutzbare VoIP-Accounts (z. B. Skype) zur Verfügung gestellt, welche dann mit einem frei wählbaren Endgerät oder entsprechender Software genutzt werden können. Da VoIP-Telefonie im Netz des Providers logisch vom Internet getrennt wird, ist das Abhören über einen Internetzugang gar nicht möglich.

Telekommunikationsanbieter unterliegen den strengen Anforderungen des § 109 TKG und müssen insoweit regelmäßig ausführliche Sicherheitskonzepte erstellen, die die Entwicklung neuer Technologien berücksichtigen. § 109 TKG verpflichtet alle Erbringer von Telekommunikationsdienstleistungen, technische Vorkehrungen und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten zu treffen. Dabei ist der Stand der Technik zu berücksichtigen. Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste

erbringt, muss darüber hinaus zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen führen und zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten, angemessene technische Vorkehrungen und sonstige Maßnahmen treffen. Zudem muss er Netz und Dienste gegen unerlaubte Zugriffe sichern sowie die Auswirkungen von Sicherheitsverletzungen für Nutzer oder für zusammengeschaltete Netze so gering wie möglich halten.

Diese Verpflichtungen gelten für Anbieter von VoIP-Dienstleistungen ebenso wie für die Anbieter herkömmlicher Festnetz- oder Mobilfunktelefonie.

Teilnehmer, die darüber hinaus einen besonderen Schutz ihrer Kommunikation wünschen, können dies über den Einsatz spezieller Endgeräte mit entsprechender Verschlüsselungssoftware erreichen. Eine Verschlüsselung wäre entgegen der Begründung im Antrag der Piratenpartei durchaus kostenintensiv, würde erhebliche Rechenkapazitäten binden und ist aufgrund der Liberalisierung der Endgeräte flächendeckend kaum umsetzbar. Verschlüsselung benötigt immer eine gewisse Zeit und erfordert erhebliche Ressourcen, die zusätzlich angeschafft werden müssten. Zudem wären Prozesse notwendig, um den sicheren Schlüsselaustausch zu gewährleisten. Auch müssten Regelungen getroffen werden, um die gesetzlich vorgeschriebene Telekommunikationsüberwachung sicherzustellen. Diesen Kosten und Aufwänden steht seitens der Nutzer keine entsprechende Nachfrage gegenüber.

Die geforderte Verschlüsselung würde zudem zu längeren Signallaufzeiten und zu einer – im Vergleich zum heutigen Sachstand – schlechteren Übertragungsqualität führen, was wiederrum die Akzeptanz der Nutzer deutlich verringern dürfte.

Technisch gesehen ist eine Ende-zu-Ende Verschlüsselung nur in einem in sich geschlossenen Netz möglich. Netzübergänge und die damit verbundenen Technologiewechsel hebeln eine Verschlüsselung aus.

Dies begründet sich dadurch, dass die erste Unterbrechung am Session Border Controller (SBC) stattfinden würde. Die SBCs dienen als Back-to-Back-User-Agent (B2BUA) und entschlüsseln die Verbindungen. Da die Gespräche sich nach der Übergabe an die SBCs im Netz des Providers befinden, findet hier in der Regel keine Verschlüsselung statt. Um diese Lücke in der Verschlüsselung zu schließen, müsste eine neue Verschlüsselungstechnologie implementiert werden.

Die zweite Unterbrechung der Verschlüsselung erfolgt bei der Übergabe an die PSTN-Gateways zur Weitervermittlung in das herkömmliche Telefonnetz (SS7). Diese Gateways werden die bestehende Verschlüsselung verwerfen müssen, um im nachfolgenden Netz die Gespräche weitervermitteln zu können. Zu einer weiteren Unterbrechung der Verschlüsselung kommt es bei der Übergabe der Gespräche an die SBCs von Fremdprovidern, wenn diese nicht über die PSTN-Gateways angebunden sind. In beiden Fällen gilt, dass der Provider des Kunden ab hier nicht mehr die Verschlüsselung der Gespräche garantieren kann, da sie sich nicht mehr in seiner Hoheit befinden. Durch die zusätzlichen Operationen, die auf den jeweiligen Systemen getätigt werden (Entschlüsseln, Verschlüsseln, etc.), kommt es zu einer höheren Last auf den involvierten Systemen, die nur durch die Anschaffung weiterer Hardware abgefangen werden kann. Hierdurch entstehen zusätzlich hohe Kosten für die Provider.

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Darüber hinaus ist der Wortlaut *„in Zukunft Gesprächsinhalte **und Signalisierungsinformationen** von Telefongesprächen sicher **Ende-zu-Ende**-verschlüsselt werden müssen“* wohl missverständlich formuliert, da dies in der Konsequenz dazu führen würde, dass kein Anbieter von Telefoniediensten mehr in der Lage sein würde, sein Geschäft wie bisher zu betreiben. Es wären anhand von signalisierten Rufnummern kein zielgerichtetes Routing sowie keine Entstörung aller Art mehr möglich, da keine Infos wie A- und B-Rufnummer mehr im Klartext lesbar sind. Dies entspräche in Analogie einer Verschärfung des Briefgeheimnisses durch Briefe mit geschwärztem Absender und Empfänger.

In Anbetracht der bereits bestehenden Maßnahmen zum Schutz des Fernmeldegeheimnisses und der vorhandenen endgeräteseitigen Optionen sowie der zu erwartenden geringen Akzeptanz und Nachfrage ist eine Verpflichtung der Netzbetreiber zur End-to-End-Verschlüsselung aus unserer Sicht daher nicht zielführend.

Für Fragen stehen wir selbstverständlich jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

I. Nolte

Iris Nolte

Im VATM sind 120 der im deutschen Markt operativ tätigen Telekommunikations- und Dienstleistungsunternehmen aktiv. Alle stehen im direkten Wettbewerb zum Ex-Monopolisten Deutsche Telekom AG und engagieren sich für mehr Wettbewerb im Telekommunikationsmarkt – zugunsten von Innovationen, Investitionen und Beschäftigung. Die VATM-Mitgliedsunternehmen versorgen 80 Prozent aller Festnetzkunden und nahezu alle Mobilfunkkunden außerhalb der Telekom. Seit der Marktöffnung im Jahr 1998 haben die Wettbewerber im Festnetz- und Mobilfunkbereich Investitionen in Höhe von rund 62 Mrd. € vorgenommen. Unmittelbar sichern die neuen Festnetz- und Mobilfunkunternehmen über 52.600 Arbeitsplätze in Deutschland sowie zusätzlich etwa 50 Prozent der Beschäftigung in den Zulieferbetrieben.

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de