Schleswig-Holsteinischer Landtag
Umdruck 18/5428

www.datenschutzzentrum.de

ULD · Postfach 71 16 · 24171 Kiel

Innen und Rechtsausschuss
des Schleswig-Holsteinischen Landtages

innenausschuss@landtag.ltsh.de

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Frau Hansen
Durchwahl: 988-1200

Aktenzeichen:
LD -50/03/15.005

Kiel, 8. Januar 2016

Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein zum Antrag der Fraktion der PIRATEN „Bundesratsinitiative Verschlüsselung bei Telefonaten", DR 18/3311

Sehr geehrte Frau Vorsitzende Ostmeier,
sehr geehrte Frau Schönfelder,
sehr geehrte Damen und Herren,

das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) bedankt sich für die Möglichkeit, zum Antrag der Fraktion der PIRATEN DR 18/3311 Stellung zu nehmen.

Der Antrag enthält eine Aufforderung an die Landesregierung, „*eine Bundesratsinitiative mit dem Ziel zu ergreifen, das Fernmeldegeheimnis im Telekommunikationsgesetz so zu erweitern, dass in Zukunft Gespräch[s]inhalte und Signalisierungsinformationen von Telefongesprächen sicher Ende-zu-Ende-verschlüsselt werden müssen*."

Als Begründung wird aufgeführt, dass Telefongespräche mit vergleichsweise geringem Aufwand abgehört werden können und dass bei der derzeit erfolgenden technischen Umstellung von Telefonanbietern auf IP-Telefonie eine einfache Möglichkeit bestünde, durch den verpflichtenden Einsatz von Verschlüsselungstechniken wieder vertrauliche Telefongespräche zu ermöglichen.

Hierzu nimmt das ULD wie folgt Stellung:

Ziel des Antrags

Das Ziel des Antrags, die tatsächliche **Ermöglichung vertraulicher Telefongespräche**, ist zu **begrüßen**. In der Tat bestehen aufgrund der Veränderungen bei der technischen Abwicklung von Telefonaten, der Zunahme von Anbietern von Telekommunikationsdiensten, des zunehmenden Outsourcings von Telefonanlagen und ihrer Steuerung („ Telefon in der Cloud“) sowie des Einsatzes weiterer Verfahren zum Austausch von Sprachnachrichten (z. B. „Internet-Telefonie“, „Skype“) Bedenken, inwieweit das Fernmeldegeheimnis in der Praxis gewahrt ist.

Der Antrag zielt primär auf die Gesprächsinhalte ab. Vom Fernmeldegeheimnis sind neben dem Inhalt der Telekommunikation auch „ihre näheren Umstände“ umfasst (§ 88 Abs. 1 Telekommunikationsgesetz (TKG)); dies betrifft insbesondere die Beteiligten an der Telekommunikation, aber auch die Dauer und erfolglose Verbindungsversuche.

Eine **moderne Regelung** sollte daher **auch darauf abzielen, die näheren Umstände der Kommunikation technisch zu schützen**. Dies kommt im Antrag durch die Formulierung *„… Signalisierungsinformationen von Telefongesprächen sicher Ende-zu-Ende-verschlüsselt werden müssen“* zum Ausdruck.

Bestehende gesetzliche Regelungen

Im Telekommunikationsgesetz (TKG) ist in § 109 („Technische Schutzmaßnahmen“) festgelegt, dass jeder Diensteanbieter erforderliche technische Vorkehrungen und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten zu treffen hat; dabei ist der Stand der Technik zu berücksichtigen.

Wenn technische Schutzmaßnahmen wie die Verschlüsselung von Gesprächsinhalten mit angemessenem Aufwand umzusetzen sind, sie wirksam sind (d.h. Angriffen standhalten) und in der Praxis erfolgreich verwendet werden können, dann gehört ihre Umsetzung zum „Stand der Technik“.

Sollte eine Verschlüsselung mit angemessenem Aufwand und wirkungsvoll umzusetzen sein, so ist denkbar, die bereits bestehenden Regelungen des § 109 TKG so anzuwenden, dass unter dem dort geforderten „Stand der Technik“ die Implementierung einer Ende-zu-Ende-Verschlüsselung verstanden wird. In diesem Fall wäre eine weitere gesetzliche Regelung obsolet, da dann § 109 TKG die Implementierung erfordern würde.

In der Praxis sind aber Fragestellungen, ob ein bestimmtes technisches Verfahren zum Stand der Technik gehört und daher aufgrund gesetzlicher Vorschriften zu implementieren ist (vgl. § 5 Landesdatenschutzgesetz (LDSG), Anlage zu § 9 Satz 1 Bundesdatenschutzgesetz (BDSG) oder § 109 Abs. 1 TKG), strittig und müssten im Einzelfall gegenüber den Betreibern durch die zuständigen Behörden durchgesetzt werden. Die datenschutzrechtliche Aufsicht über Telekommunikationsunternehmen fällt dabei in den Zuständigkeitsbereich der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI); Fragen der Datensicherheit fallen in den Zuständigkeitsbereich der Bundesnetzagentur und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) (vgl. § 109 Abs. 6 TKG, zu Datenschutzverletzungen § 109a TKG). Daher ist es sinnvoll, in Analogie zu zahlreichen neueren gesetzlichen Regelungen wie etwa dem De-Mail-

Gesetz detaillierte Regelungen zu treffen und die Implementierung von Verschlüsselungsverfahren explizit gesetzlich festzuschreiben.

Praktische Umsetzbarkeit

Voice-over-IP-Telefonie (VoIP) und Internet-Telefonie gibt es in verschiedenen technischen Ausprägungen. Dazu gehören u.a. das Angebot von Telekommunikationsdiensteanbietern im Sinne des TKG, die die bisherigen Analog- oder ISDN-Telefon-Anschlüsse derzeit auf VoIP umstellen, aber auch reine „Datendienste" wie Skype, dezentrale Telefonsysteme, Peer-to-Peer-IP-Telefonie und andere Messenger-Dienste, bei denen eine Anwendbarkeit des TKG unklar ist.[1]

Bedacht werden muss bei einer Regelung, dass Telefonendgeräte im Eigentum von Verbraucherinnen und Verbrauchern, Firmen und Behörden stehen und somit mit einer gesetzlichen Regelung ein Eingriff in die Eigentumsverhältnisse der Betroffenen entstehen könnte, wenn einzelne Geräte eine Verschlüsselung nicht unterstützen und daher ausgetauscht oder erweitert werden müssten.

Bedacht werden muss weiterhin, dass nicht alle an der Erbringung von Telefondienstleistungen Beteiligten den gesetzlichen Regelungen der Bundesrepublik Deutschland unterfallen (etwa bei Telefongesprächen ins Ausland, Telekommunikationsdiensteanbieter aus dem Ausland) und daher eine Regelung getroffen werden sollte, die auch diese Fälle berücksichtigt. Denkbar ist hier beispielsweise, die Betreiber zu verpflichten, die Nutzung einer Ende-zu-Ende-Verschlüsslung *bereitzustellen* und technisch *zu ermöglichen*, die Nutzung aber in die Entscheidungshoheit der Teilnehmer zu stellen.

Ob die vorgeschlagenen technischen Schutzmaßnahmen nach RFC 3261[2] wirksam sind (d.h. Angriffen standhalten) und in der Praxis erfolgreich verwendet werden können, kann durch das ULD nicht abschließend beurteilt werden. Zwar sind dem ULD zahlreiche Verfahren und technische Protokolle zur Umsetzung von Verschlüsselungsverfahren bei Internet-Telefonie bekannt, doch kann das ULD keine Aussage über die tatsächliche Sicherheit der Protokolle in den verschiedenen denkbaren Nutzungsszenarien treffen. Ebenso wenig kann das ULD die Praktikabilität einer bundesweiten Umsetzung in einer heterogenen Landschaft von Telefonanlagen, sowohl von Telekommunikationsanbietern als auch von Firmen, Behörden und Privatpersonen (lokale Telefonanlagen), sowie im Zusammenspiel mit nutzerbetriebener Hard- und Software beurteilen. Zu beiden Punkten werden im Rahmen der Anhörung jedoch zahlreiche Experten befragt.

---

[1] Vgl. z. B. Deutscher Anwaltsverein, Stellungnahme „SN 55/13: Anwendung des TKG auf neue Kommunikationsplattformen (bspw. WhatsApp)", http://anwaltverein.de/de/newsroom/id-2013-55?file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2013/DAV-SN55-13.pdf

[2] https://www.ietf.org/rfc/rfc3261.txt

Ende-zu-Ende-Sicherheit

Die Anforderungen einer „Ende-zu-Ende"-Verschlüsselung ist im Detail noch genauer zu betrachten: Mit dem Begriff „Ende-zu-Ende"-Verschlüsselung wird üblicherweise eine Verschlüsselung bezeichnet, auf die lediglich Absender und Empfänger bzw. unmittelbar unter ihrem Einfluss stehende Geräte, nicht aber Dritte oder Dienstleister Zugriff haben oder diese manipulieren könnten. Vereinfacht formuliert: Ende-zu-Ende-Verschlüsselung soll auch vor Risiken und Angriffen aus dem Kreis aller beteiligten Dienstleisten schützen, sich also nicht ausschließlich auf die Sicherheitsmechanismen der Anbieter stützen. Dies betrifft insbesondere die Schutzziele „Vertraulichkeit" und „Integrität" sowie „Nichtverkettbarkeit" im Sinne des § 5 Landesdatenschutzgesetz (LDSG).

Eine Signalisierungsinformation wie der Wunsch eines Gesprächsaufbaus muss den Empfänger erreichen können. Daher kann die Empfänger-Adresse nicht vollständig Ende-zu-Ende verschlüsselt werden, denn andernfalls wüsste (bis auf den Sender) niemand, an welchen Empfänger der Gesprächswunsch weitergeleitet werden soll.

Allerdings sind Protokolle denkbar, die eine Entschlüsselung der Empfänger-Adresse erst beim Telekommunikationsdiensteanbieter/Provider des Empfängers vornehmen und so diese Information vor anderen beteiligten technischen Systemen verbergen, die lediglich zur (netztechnischen) Anbindung des Telekommunikationsdiensteanbieters bzw. Providers des Empfängers „durchquert" werden.

Ein vergleichbares Beispiel aus dem Bereich der Briefpost wäre ein Schreiben an eine konkrete Person (= „Empfänger") innerhalb einer Organisation (= „Telekommunikationsdiensteanbieter/Provider"). Wird dieses Schreiben in einem weiteren Umschlag versandt, der lediglich an die Firma oder Behörde, nicht aber an den Empfänger adressiert ist, so bleibt der konkrete Empfänger allen am Transport der Nachricht Beteiligten – mit Ausnahme empfangenden Organisation – verborgen.

Weiterhin gibt es Protokollerweiterungen, die eine verschlüsselte Übermittlung zwischen einzelnen Knotenrechnern vorsehen („Hop-to-Hop"). Dies würde als „Transportsicherung" ein Abhören oder eine Manipulation auf Netzebene erschweren und wäre in der Briefwelt mit dem Transport von Postsendungen in abgeschlossenen Behältern und Transporten zu vergleichen, die einen Schutz vor Unbefugten bieten können, nicht aber einen Schutz vor Personen, die unmittelbar an der Postdienstleistung beteiligt sind (z.B. Zustellerinnen und Zusteller „Briefträger").

Eine solche Infrastruktur kann nicht vor sämtlichen denkbaren Angriffen Dritter (z.B. Vertauschen von kryptographischen Schlüsseln) oder Handlungen der Telekommunikationsdiensteanbieter (etwa: Deaktivierung der Verschlüsselungsfunktionen zwischen Knotenrechnern) schützen. Ebenso wird das Verhältnis zu § 100 a StPO zu erörtern sein.

Fazit

Eine Regelung zur Ende-zu-Ende-Verschlüsselung kann insgesamt das **Schutzniveau erhöhen** und es den **Nutzerinnen und Nutzern ermöglichen, ihrerseits Sicherheitsmechanismen zu verstärken**. Ein Beispiel hierfür ist eine automatisierte Verteilung kryptographischer Schlüssel an die Nutzenden. Dies ist für die Nutzenden bequem und wird zur Verbreitung von Verschlüsselungsverfahren beitragen, schützt jedoch nicht gegen bestimmte Angriffe wie einen Austausch kryptographischer Schlüssel durch Dritte). Nutzerinnen und Nutzer mit erhöhten Sicherheitsanforderungen können diesen Angriffen durch Kontrolle oder eigene Verteilung kryptographischer Schlüssel begegnen.

Das Ziel des Antrags ist unterstützenswert, bedarf aber bei den technischen und rechtlichen Umsetzungen weiterer Analysen im Hinblick auf Wirksamkeit und Umsetzbarkeit.

Dabei sollten insbesondere die für die Durchsetzung der Datenschutz- und Datensicherheitsmaßnahmen zuständigen Institutionen, die Bundesnetzagentur und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, beteiligt werden.

Mit freundlichen Grüßen

gez. Marit Hansen