Bundesamt
für Sicherheit in der
Informationstechnik

Schleswig-Holsteinischer Landtag
Umdruck 18/5427

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Schleswig-Holsteinischer Landtag
Innen- und Rechtsausschuss
Barbara Ostmeier

- per E-Mail -

Florian Schumacher

HAUSANSCHRIFT
Bundesamt für Sicherheit in
der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 228 99 9582-5346
FAX +49 228 99 10 9582-5346

Referat-B22@bsi.bund.de
https://www.bsi.bund.de

Betreff: Schriftliche Anhörung zum Antrag der Fraktion der PIRATEN (Drs. 18/3311 vom 26.08.2015)
hier: Bundesratsinitiative zur technischen Sicherung des Fernmeldegeheimnisses – Ende-zu-Ende-Verschlüsselung für das Telefon

Bezug: E-Brief vom Innen- und Rechtsausschuss des Schleswig-Holsteinischen Landtags vom 24. November 2015
Aktenzeichen: B22 001 00 008
Datum: 04.01.2016

Mit dem Schreiben vom 24. November 2015 baten Sie das BSI um Informationen zu o. g. Sachverhalt. Das BSI nimmt hierzu wie folgt Stellung:

VoIP[1]-Telefonie besteht aus zwei wesentlichen Komponenten: Erstens der Signalisierung zur Steuerung der Anrufe und zweitens der tatsächlichen Gesprächsinhalte.
Zur Steuerung werden so genannte „Metadaten“ übertragen. Diese sind zwingend notwendig, um eine Verbindung zwischen den Gesprächsteilnehmern aufzubauen. Hier ist allerdings nur eine Verschlüsselung zwischen den beteiligten Servern („Hop-zu-Hop“) möglich. Die Server empfangen dabei jeweils verschlüsselte Daten, entschlüsseln und verarbeiten diese, und verschlüsseln sie vor der Weiterleitung zum nächsten Server. Dieses Verfahren ist sicher, solange die Server nicht kompromittiert sind und dem Betreiber der Server vertraut wird.

Bei den Gesprächsinhalten ist eine Ende-zu-Ende-Verschlüsselung prinzipiell möglich. Das heute in vielen VoIP-Geräten verfügbare Verfahren[2] implementiert jedoch keine sichere Ende-zu-Ende-Verschlüsselung, da für die Signalisierungsserver auf dem Pfad prinzipiell alle notwendigen Informationen zur Entschlüsselung von Gesprächsinhalten vorliegen.[3]

1 Voice over Internet Protocol
2 Dieses wurde vermutlich im Abschnitt „Technischer Aufwand“ gemeint.
3 Es erfolgt also ebenfalls nur eine „Hop-zu-Hop“ Verschlüsselung.

Die von den PIRATEN vorgeschlagene Maßnahme der verbindlichen Nutzung von Ende-zu-Ende-Verschlüsselung bei Telefongesprächen ist mit vertretbarem Aufwand realisierbar und verbessert die Sicherheit. Sie erreicht allerdings nicht das Ziel einer echten Ende-zu-Ende-Verschlüsselung.

In der deutschen oder gar weltweiten Telefonieinfrastruktur eine echte Ende-zu-Ende-Verschlüsselung zu implementieren ist eine Herausforderung, die eine ausgeprägte technische wie politisch/regulatorische Komplexität aufweist. Ein wirksamer Schutz für Signalisierung/Metadaten ist sehr schwierig zu erreichen. Entsprechende Mechanismen könnten gegebenenfalls im Rahmen von akademischer Forschung entwickelt werden.

Im Auftrag

Samsel