89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

am 18. und 19. März in Wiesbaden

Entschließung:

Verschlüsselung ohne Einschränkungen ermöglichen

Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie im Interesse der ungestörten Kommunikation in Wirtschaft und Verwaltung sind neben entsprechenden gesetzlichen Regelungen und deren Umsetzung wirksame technische Vorkehrungen erforderlich, um elektronisch übermittelte und gespeicherte Daten vor Zugriffen Unberechtigter zu schützen. Schutzbedürftig sind neben der Kommunikation von Privatpersonen auch die geschäftliche Kommunikation von Wirtschaftsunternehmen, die Kommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (zum Beispiel Ärzte, Anwälte, Psychologen, Steuerberater), und die Kommunikation mit und innerhalb der öffentlichen Verwaltung.

Mit modernen kryptographischen Verfahren zur Verschlüsselung von Daten stehen datenschutzfreundliche Technologien zur Verfügung, die prinzipiell von jedermann genutzt werden können. Einer umfassenden und leicht nutzbaren Verschlüsselung stehen jedoch noch technische und organisatorische Hürden entgegen. Dies führt dazu, dass diese Schutzmaßnahmen bisher viel zu selten genutzt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher,

- eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,
- die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen Plattformen zu fördern,
- die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und
- kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert einen aktiven Einsatz der Politik bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Bundesregierung hat in ihren eigenen Zielstellungen aus der Digitalen Agenda 2014-2017 deutlich gemacht, wie wichtig eine zuverlässige und sichere Verschlüsselung ist[1]. Die Pläne der De-Mail-Anbieter für eine Ende-zu-Ende-Verschlüsselung ab April 2015 sind zwar ein erster Schritt in die richtige Richtung. Dennoch wird im Zusammenhang mit der Bekämpfung des internationalen Terrorismus in letzter Zeit erneut über eine Schwächung von Verschlüsselungstechnologien diskutiert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschränken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich.

[1] Zitat: „Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungsstandort Nr. 1 in der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden."