PRESSEMITTEILUNG

Staatlicher Zugriff auf Verschlüsselung ist kein zielführender Ansatz

Berlin, 26.01.2015: Die aktuelle Diskussion bezüglich staatlicher Einflussnahme auf Verschlüsselung mag angesichts der aktuellen Bedrohungslage von der grundsätzlichen Motivation her zwar nachvollziehbar erscheinen, gleichwohl bedarf das Thema "Verschlüsselung" der sorgfältigen Güter- und Interessenabwägung. Der Ansatz, bei Nutzung von Verschlüsselung dem Staat Schlüsselzugang gewähren, beachtet unzureichend die politische, rechtliche und technische Dimension. Derartige Erwägungen sind nicht zielführend. Die Politik sollte Konsultationsangebote der Fachleute nutzen.

Aus Sicht von TeleTrusT stehen die politischen Forderungen im Gegensatz zur Absicht der "Digitalen Agenda" der Bundesregierung, Deutschland zum Verschlüsselungsstandort Nr. 1 zu entwickeln. Sicherheitsbehörden haben durch das G10-Gesetz - nach richterlichem Beschluss - ohnehin schon weitreichende Zugriffsmöglichkeiten auf Providerdaten. Regelungen zur Schlüsselhinterlegung oder zur verpflichtenden Implementierung von Zugangsmöglichkeiten für Sicherheitsbehörden würden das sowieso schon angeschlagene Vertrauen in die IT-Wirtschaft und den Schutz durch staatliche Stellen weiter erschüttern. Ohnehin würden dadurch lediglich bestehende, bislang vertrauenswürdige IT-Technologien und -Standards geschwächt, und es ist davon auszugehen, dass kriminelle oder terroristische Organisationen auf andere Möglichkeiten der Kommunikation ausweichen. Folge wäre dann lediglich eine flächendeckende Schwächung der Kryptolandschaft und der IT-Sicherheit unserer Gesellschaft.

TeleTrusT hält eine Einschränkung von Verschlüsselung bzw. ein Verbot starker Verschlüsselung in der Praxis nicht durchführbar, nicht zweckmäßig und verfassungsrechtlich bedenklich. Ein solches Verbot bedingte eine Reihe von Ausnahmen und Abgrenzungsschwierigkeiten, z.B. hinsichtlich Gesundheitsdaten, Mandantenschutz bei Rechtsanwälten oder Quellenschutz bei Journalisten. Wie soll aber in der Praxis zwischen rechtmäßiger und rechtswidriger Hinterlegung der Schlüssel bzw. Nutzung der Schlüssel durch staatliche Stellen im Einzelfall unterschieden werden, wenn die Daten doch verschlüsselt sind? Wie soll ein Unterlaufen des Verbots, z.B. durch Steganografie, verhindert werden? Insbesondere wäre völlig unklar, wie eine Schlüsselhinterlegung technisch und rechtlich im Rahmen des grenzüberschreitenden Datenverkehrs greifen soll, insbesondere, wenn er durch "unsichere" Länder erfolgt?

Ein universeller Zugriff auf verschlüsselte Kommunikation könnte - wenn überhaupt - nur über eine Fülle von nachhaltigen Eingriffen in die Internet-Infrastruktur sichergestellt werden.

Im Internet werden ca. 15 % aller IP-Pakete verschlüsselt; der größte Teil mit SSL, z.B. die Verbindung zwischen Browsern und Web-Servern und ein kleinerer Teil mit IPSec für die Sicherung der Kommunikation zwischen Unternehmen oder Unternehmensteilen. Dies ist bei Weitem zu wenig.

Es ist an der Zeit zu erörtern, wie das Risiko eines Schadens für Bürger und Unternehmen im immer wichtiger werdenden Internet auf ein akzeptables Maß reduziert werden kann, z.B. durch stärkere Verbreitung und Nutzung von Verschlüsselungsanwendungen.

Eine Gesellschaft, die durch ihre freiheitliche, demokratische Verfassung auf die Eigenverantwortung des Einzelnen setzt, benötigt die Gewissheit, dass der Einzelne seine Privatsphäre wirksam schützen kann. Ungeachtet dessen muss sie darauf vertrauen können, dass auch die staatlichen Stellen ihrem verfassungsrechtlichen Auftrag zum Schutz der Grundrechte der Bürger hinreichend nachkommen.

TeleTrusT - Bundesverband IT-Sicherheit e.V., Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 /40054310, holger.muehlbauer@teletrust.de
www.teletrust.de