Pressemitteilung des Präsidiumsarbeitskreises „Datenschutz und IT-Sicherheit"
der Gesellschaft für Informatik e.V. (GI) vom 6. Februar 2015

Informatiker fordern uneingeschränkte, starke Verschlüsselung für Jedermann

Bonn, 6. Februar 2015 Um Nachrichten im Internet entschlüsseln zu können, fordert Innenminister de Maiziere derzeit zusammen mit ausländischen Kollegen, den Strafverfolgungsbehörden geheime Schlüssel der Internet-Nutzer zugänglich zu machen - durch Hinterlegung bei einer Stelle, die im Zweifel ohne Wissen der Nutzer den Zugriff ermöglicht. Die Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit" der Gesellschaft für Informatik e.V. (GI) hält diese Forderung für im Grundsatz verfehlt, weil sie die Sicherheit der Internetkommunikation massiv gefährdet.

„Das große Risiko der Schlüsselhinterlegung liegt darin, dass sich Dritte (fremde Nachrichtendienste, spionierende Unternehmen, die organisierte Kriminalität etc.) unberechtigt Zugriff auf die zentral hinterlegten Schlüssel verschaffen und damit bundesweit jegliche elektronische Kommunikation entschlüsseln und mitlesen", sagte Arbeitskreissprecher Hartmut Pohl. Jegliche Beschränkung der Verschlüsselung inklusive einer staatlichen Schlüsselverwaltung fördere also den Verlust von Vertraulichkeit. Jeder Bürger und jedes Unternehmen müsse aber uneingeschränkt vertraulich und integer digital kommunizieren können.

In einer Welt der vernetzten Internetkommunikation ist eine wirksame Datenverschlüsselung daher der einzige technisch effektive Mechanismus zum Schutz der Kommunikation für Unternehmen (vor allem gegen Wirtschaftsspionage und -sabotage) und Private (gegen Zugriff auf ihre personenbezogenen Daten). Die staatliche Förderung effektiver Verschlüsselungsmechanismen ist deshalb nach Grundgesetz und Europäischer Menschenrechtskonvention für alle staatlichen Stellen eine zwingende verfassungsrechtliche Verpflichtung.

Genau aus diesen Gründen hat sich bereits vor mehr als 15 Jahren die damalige Bundesregierung – ebenso wie die USA und Frankreich – gegen die Hinterlegung von Schlüsseln entschieden.

Der Arbeitskreis fordert daher:

1. Die Entwicklung wirksamer und insbesondere benutzerfreundlicher starker Verschlüsselungssoftware für Unternehmen und Private. Dies muss ohne jede Schwächung der Algorithmen oder gar Schlüsselhinterlegung erfolgen.
2. Die Entwicklung intelligenter Auswertungssoftware, die im Nachhinein die Auswertung der bereits vorhandenen, sehr großen Datenmengen wirksam unterstützt.

Hintergrundinformationen:

In der Informationsgesellschaft, in der Unternehmen, Behörden und Privatpersonen zunehmend Nachrichten über das Internet übertragen, wird die Forderung der Nutzer nach vertraulicher und integrer Kommunikation zur Verhinderung von Überwachung, Wirtschafts- und Industriespionage und Verhinderung von Manipulationen bis hin zur Verhinderung von Sabotage zur zentralen Frage.

Sogenannte "starke" Kryptographie (asymmetrische Verfahren) sind längst bekannt und praktikabel. Die Gesellschaft für Informatik fordert daher die Politik auf, IT-technische Anstrengungen zu unternehmen, ihre verfassungsmäßigen Pflichten für Bürger und Unternehmen zu erfüllen. Die Regierenden haben eine Schutzpflicht für die tatsächliche Realisierung der Grundrechte, nämlich des Rechts auf informationelle Selbstbestimmung, des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und der Rechte der Unternehmen auf Schutz ihrer Betriebs- und Geschäftsgeheimnisse. Es ist im Übrigen ein Irrglaube, dass es hier „nur" um Abwehr „befreundeter" oder fremder Geheimdienste geht. So ist z. B. Electronic Banking oder Shopping ohne starke Kryptographie gar nicht mehr denkbar.

Die Vertraulichkeit und Integrität des Internetverkehrs verschlechtern zu wollen, ist nicht nur aus praktischer Sicht kontraproduktiv, sondern auch verfassungsrechtlich bedenklich, weil sich der Staat durch eine Pflicht zur Hinterlegung geheimer und privater Schlüssel direkten Zugriff auf die grundrechtlich geschützte Kommunikation verschafft.

Suchmaschinenanbieter und Soziale Medien bieten im Übrigen international zunehmend starke Verschlüsselung entgeltfrei an. Daher sollte dies auch in Deutschland möglich sein.