



Verschlüsselungsfreiheit soll eingeschränkt werden

Bundesinnenminister Kanther plant, die freie Wahl von Verschlüsselungsverfahren einzuschränken. In Zukunft sollen demnach nur noch solche Verfahren erlaubt sein, die den Geheimdiensten und Ermittlungsbehörden das Mitlesen erlauben.

Verschlüsselungsverfahren dienen unter anderem dazu, Daten so zu übertragen, daß kein Unbefugter mitlesen kann. Dabei kann es sich im privaten Bereich zum Beispiel um E-Mails oder Kontoauszüge aus dem Internet handeln. In der Wirtschaft geht es z.B. um das Versenden von vertraulichen Angeboten über Fax oder von Konstruktionszeichnungen über elektronische Netze. Auch Ärzte oder Rechtsanwälte, die elektronische Kommunikationsmedien nutzen, sind auf Verschlüsselung angewiesen.

Ein zweiter Anwendungsbereich sind digitale Signaturen. Diese werden dazu verwendet, um die Unverfälschtheit und den Absender eines elektronischen Dokumentes zweifelsfrei zu beweisen. Ein Anwendungsbeispiel sind elektronische Unterschriften, zum Beispiel für Verträge, die mittels Internet zustande kommen.

Eine Beschränkung der zulässigen Verfahren bedeutet, daß nicht nur befugte staatliche Stellen die verschlüsselten Daten entschlüsseln oder digitale Unterschriften fälschen kön-

nen, sondern jeder, der über die entsprechende Rechenleistung verfügt. Und die ist schließlich in vielen Firmen und Universitäten vorhanden, von ausländischen Geheimdiensten ganz zu schweigen.

Für E-Mails würde dies also einem Verzicht auf das Briefgeheimnis gleichkommen - und wer von uns möchte nur noch Postkarten verschicken? Unsere Kontoauszüge würden für alle lesbar im Internet übertragen. Das Angebot einer deutschen Firma zum Bau eines Kraftwerks in Afrika würde von ausländischen Diensten mitgelesen, an deren heimische Mitbewerber übertragen und so das deutsche Angebot unterboten. Deutsche Softwarehersteller könnten keine Software mit qualitativ hochwertigen Verschlüsselungsverfahren mehr herstellen und wären damit international nicht mehr wettbewerbsfähig. Pläne für ein neues Auto oder sensible Patientendaten wären im Zugriff interessierter Kreise. Unbekannte könnten in unserem Namen Verträge im Internet abschließen oder abgeschlossene Verträge verändern.

Als wichtigstes Argument für ein Verschlüsselungsverbot wird die Bekämpfung des organisierten Verbrechens genannt. Dieses Argument läuft jedoch ins Leere. Zum einen sind sichere Verschlüsselungsverfah-

ren bekannt und können nicht über Nacht abgeschafft werden. Damit stehen sie den Verbrechern auch nach einem Verbot zur Verfügung. Und diese werden lieber eine Verurteilung wegen unerlaubter Verschlüsselung hinnehmen als ihre eigentlichen Delikte preiszugeben. Außerdem gibt es Möglichkeiten, Nachrichten so in anderen Daten zu verstecken, daß dies nicht mehr nachweisbar ist. Letztendlich kann über vereinbarte Codewörter auch scheinbar harmloser Text eine ganz andere Bedeutung erlangen. Zur Erreichung des vorgebliehen Ziels der Verbrechensbekämpfung ist ein Verschlüsselungsverbot also eine völlig ungeeignete Maßnahme. Damit bleibt als Anwendung nur noch die Überwachung von gesetzestreuen Bürgern und der Mißbrauch durch Kriminelle.

Anlässlich einer Tagung in Hamburg haben Netzsicherheitsexperten auf die beschriebenen Gefahren aufmerksam gemacht. Sie haben ihre ablehnende Haltung in der "Hamburger Erklärung für Verschlüsselungsfreiheit" zum Ausdruck gebracht, die man durch seine Unterschrift unterstützen konnte. Die Erklärung ist im Internet unter

<ftp://troll.hz.kfa-juelich.de/pub/KRYPTO/hh.htm> zu finden.

Viktor Schuppan

Studierende machen Radio

Für eingeschworene Radiohörer ist dies wirklich keine Neuigkeit mehr. Auf der Frequenz 94.5 MHz sendet das Münchner Ausbildungs- und Forschungsradio M 94.5.

Neben aktuellen Themen rund ums Studium zeichnet sich dieser Sender vor allem dadurch aus, daß er sich nicht auf das Abspielen eines halben Dutzends "topaktueller" Singles beschränkt. Hier kann man junge Bands erleben, die auch musikalische Nischen abdecken. Wortbeiträge sind bei diesem Sender noch nicht durch Werbejingles ersetzt worden.

Michael Engert