Krypto-Regulierung: Status Quo und Ausblick

Vortrag: *Andy Mueller-Maguhn, Sandel, Lutz Donnerhacke* <andy@ccc.de>

Bericht: *Sascha A. May* <sascha@may.de>

Referent: Herr Sandel, Bundeswirtschaftsministerium, Referat "Dialog mit gesellschaftlichen Gruppen und IT-Regulierung" Moderation: Andy Müller-Maguhn, Support: Lutz Donnerhacke

In den letzten Jahren arbeiten viele Helfer der Chaos-Family an der Verbreitung von Krypto-Methoden, um auch wirksamen Privatssphärenschutz in die Hände der breiten Masse zu geben. Kryptologie ist dabei das Verschlüsseln der übertragenen Information zwischen den Kommunikationsteilnehmern. Was von vielen Leuten als legitimer Schutz betrachtet wird, wird von den Strafverfolgungsbehörden mit Argwohn betrachtet, da ihnen ja ihre Arbeit schwerer gemacht wird.

Gerade nach der erfolgten Einigung verschiedener Staaten im Wassenaar Arrangement haben die Diskussionsteilnehmer versucht, die international unterschiedlichen Sichten - Bedrohung für den Staat oder Chance für BürgerInnen und Wirtschaft - darzustellen. Die politischen Vertreter der USA, unterstützt von denen Großbritanniens, bringen in allen Absprachen klar ihre Sicht von Krypto-Technologie vor: Krypto ist Bedrohung.

Ohne die einzelnen Paragraphen des Wassenaar Abkommens zu diskutieren, machte der Vertreter des Bundeswirtschaftsministeriums die Unterschiede der Sicht der deutschen Behörden zu denen der USA klar. So setzen die USA auf sog. "key-recovery"-Verfahren (s.a. key-escrow-Verfahren), die sie in den Jahren 1997 und 1998 versucht haben, den Softwareherstellern als Produktbestandteil "aufzudrücken." In vorauseilendem Gehorsam haben inzwischen namhafte Unternehmen die key recovery alliance (KRA) gegründet, in der sie sich verpflichten, solche Verfahren zu implementieren.

Neben dem Manko, daß die Technik noch nicht endgültig ausgereift ist, setzen die deutschen Behörden auch auf eine andere Strategie: Ihnen geht es nicht um eine komplette Überwachung der Kommunikation, sondern um eine "Rauschunterdrückung", nach der für den Massenmarkt einfache Verschlüsselung zugelassen ist, die auch in annehmbarer Zeit knackbar ist. Nur die starke Verschlüsselung soll reguliert werden, da niemand davon ausgeht, daß Menschen, die Nachrichten mit illegalem Inhalt senden und zu den dahinterstehenden Straftaten bereit sind, sich von einem Verschlüsselungsverbot abhalten lassen. Als Beispiel für schwache Verschlüsselung im Massenmarkt wurde Lotus Notes genannt; der Hersteller IBM ist eine treibende Kraft in der KRA. Gleichzeitig sind die langfristigen Wirkungen wie erhebliche Erschwerung der Strafverfolgung und das Szenario, daß alle Hinweise auf Straftaten irgendwo verschlüsselt sind, von den kurzfristigen Wirkungen, wie den geschützen Transaktionen und der damit verbundenen Entwicklung des Netzes zu trennen. Eine zwingende Verknüpfung darf auf staatlicher Seite nicht entstehen, die bedeuten würde, daß erst der Staat seine Schnüffelei geregelt hat und dann erst der Bürger verschlüsseln darf.

Für die anwesenden Hacksporttreibenden ist allerdings klar geblieben, daß die deutsche Regierung kein enger Bündnispartner für sie sein kann. Austausch ist sicher möglich und nötig, dennoch werden die Projekte für den Aufbau einer Zertifizierungsstruktur forciert, und an besserer Software - besonders für den Massenmarkt - wird gearbeitet.