SchnüfflerInnen taub auf beiden Ohren

Florian Hammel

Lieber Boris,
wann hast Du Zeit für einen gemeinsamen Saunagang? Ich brauche jetzt einen Freund, der mir in meiner Verzweiflung zur Seite steht. Die Situation des FCK und der Trainerwechsel bereiten mir schlaflose Nächte.
Viele Grüße, Dein Helmut.

Wer heute E-Mails wie diese verschickt, muß wissen, daß der Inhalt der Post vor dem Zugriff Dritter nicht mehr geschützt ist als eine Nachricht auf einer Postkarte.

Knotenrechner, sogenannte Message Transfer Agents (MTAs), reichen die Nachricht untereinander weiter. Dabei wird sie auf dem Knotenrechner im Klartext zwischengespeichert. Für AdministratorInnen dieser MTAs ist es ein leichtes, ein- und ausgehende E-Mails zu lesen, zu kopieren oder zu verändern. Dies gilt ebenso für in die Knotenrechner eingedrungene HackerInnen oder den BND, der auch die digitale Kommunikation auf Schlüsselwörter durchsucht und verdächtige E-Mails speichert.[1]

Um auszuschließen, daß der digitale Briefwechsel von den jeweiligen SystembetreuerInnen gelesen wird oder auf dem Tisch des BND landet, kann man sich jedoch zum Glück eines Verschlüsselungsprogrammes bedienen, mit dem die Daten vor dem Zugriff Unbefugter wirksam geschützt werden können. Aber auch die Tatsache, daß das Internet für die Wirtschaft zunehmend an Bedeutung gewinnt und immer mehr Verträge über das Internet abgewickelt werden, macht eine wirksame Verschlüsselungstechnik notwendig. Erst kryptologische Verfahren ermöglichen sichere finanzielle Transaktionen und elektronische Münzen. Und nicht zuletzt bei einer digitalen Unterschrift, die die Identität des Vertragspartners sicherstellen und auch gewährleisten soll, daß die Nachricht auf ihrem Weg nicht geändert wurde, bedient man sich der Verschlüs–selungstechnik.

Programme wie „Pretty Good Privacy" (PGP), das über das Internet frei für jedermann erhältlich ist, lösen diese Probleme. Das Programm verschlüsselt die Daten so sicher, daß eine Entschlüsselung ohne den dafür vorgesehenen Schlüssel derzeit unmöglich ist.

Entwaffnung der StrafverfolgerInnen

Doch nicht nur unter Staatsoberhäuptern (siehe oben), sondern auch unter Kriminellen erfreut sich das neue Kommunikationsmittel wegen der Möglichkeit der Verschlüsselung immer größerer Beliebtheit. Damit droht eine wichtige Waffe der Strafverfolgungsbehörden gegen die organisierte Kriminalität, das Abhören von Gesprächen, ihre Wirkung zu verlieren. Aus diesem Grund sieht zum Beispiel der ehemalige Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Dr. Otto Leiberich, in der Kryptographie schon eine Bedrohung für die Gesellschaft.[2] Auch von anderen MitarbeiterInnen im BSI wird die Ansicht vertreten, daß die Kryptographie der staatlichen Reglementierung unterliegen müsse, um eine Überwachung des organisierten Verbrechens zu ermöglichen.[3] Nicht zuletzt in Politikerkreisen scheint sich eine gewisse Panik breit zu machen. So verlangte Erwin Marschewski, innenpolitischer Sprecher der Unionsfraktion, ein Verbot von „Kryptogeräten", was ein Verbot aller Computer bedeuten würde, da jeder PC in der Lage ist, mit der entsprechenden Software Nachrichten zu verschlüsseln.[4] Es ist allerdings zu hoffen, daß zumindest dieser Vorschlag eines gesetzlichen Overkills auf mangelnder Sachkenntnis beruhte. Ein Zeichen, daß Regierungen und Geheimdienste starke Kryptographie als Bedrohung empfinden, ist auch das erst vor kurzem eingestellte Ermittlungsverfahren gegen Phil Zimmermann, den Entwickler von PGP, der sich wegen eines eventuellen Exportverstoßes in den USA zu verantworten hatte. Leistungsstarke Verschlüsselungsprogramme sind dort immer noch in der „United States Munitions List" aufgeführt, eine Liste von besonders gefährlichem Kriegsmaterial, dessen Ausfuhr vom Außenministerium genehmigt werden muß.[5]

Grundlagen der Verschlüsselung

Das gebräuchlichste Verschlüsselungsverfahren, mit dem auch PGP arbeitet, verwendet für die Verschlüsselung zwei

Schlüssel, die eigens für jede Teilnehmerin erzeugt werden. Ein Schlüssel ist geheim, während der andere öffentlich bekannt ist (asymmetrisches Verschlüsselungsverfahren). Will der Absender einer Nachricht, daß diese nur für die vorbestimmte Empfängerin lesbar ist, so verschlüsselt er sie mit dem öffentlichen Schlüssel der Empfängerin. Sie ist dann nur mit deren geheimen Schlüssel zu dekodieren. Dies hat den Vorteil, daß die KommunikationspartnerInnen sich nicht erst über einen gemeinsamen Schlüssel einigen müssen, da der Schlüssel, mit dem verschlüsselt wird ja öffentlich ist.

Ein weiterer Vorteil dieses Verfahrens ist, daß auf diese Weise auch die technischen Voraussetzungen für eine digitale Unterschrift geschaffen werden. Um eine Nachricht auf diese Weise zu signieren, muß sie der Absender mit seinem geheimen Schlüssel kodieren, und die Empfängerin kann die Nachricht dann mit dem öffentlichen Schlüssel des Absenders wieder entschlüsseln. Solange jedem Benutzer auch ein bestimmter öffentlicher Schlüssel zugeordnet werden kann, ist auch gewährleistet, daß die Nachricht wirklich vom angegebenen Absender stammt. Diese Zuordnung der öffentlichem Schlüssel zu den entsprechenden Personen könnte eine Schlüsselverwaltungsstelle (Trustcenter) übernehmen. Die Kenntnis der geheimen Schlüssel durch das Trustcenter wäre für diese Tätigkeit nicht erforderlich.

Kann eine Reglementierung der Kryptographie aber überhaupt eine Überwachung von organisiertem Verbrechen ermöglichen?

Die Kryptoanalyse ist inzwischen für die Strafverfolgung allein durch Bündelung aller fachlichen Computerkapazitäten aufgrund der fortgeschrittenen Verschlüsselungstechnik nicht mehr möglich. Derzeit prüft daher die Bundesregierung das Erfordernis einer gesetzlichen Regelung von Verschlüsselungsverfahren.[6]

Möglich wäre ein generelles Verbot der Verschlüsselung zur Geheimhaltung von Daten. Dieser Weg wurde beispielsweise in Frankreich beschritten, wo die Verschlüsselung, sofern sie nicht lediglich der Authentifizierung durch die digitale Signatur dient, einer Genehmigung des Premierministers bedarf. Erfahrungsgemäß wird diese Genehmigung nur Banken für relativ leicht zu entschlüsselnde Verfahren erteilt. Dies würde bedeuten, daß der Inhalt einer E-Mail legalerweise nicht vor dem Zugriff Dritter geschützt werden könnte.

Eine andere Möglichkeit wäre, die Herstellung von Schlüsseln dem Trustcenter zu übertragen. Dieses wäre dann nicht nur in Besitz des öffentlichen, sondern auch des geheimen Schlüssels.

Hier wird auch damit argumentiert, daß die Herstellung sicherer Schlüssel nicht dem Einzelnen überlassen werden könne. Die Realität sieht jedoch so aus, daß die Verschlüsselung durch die BenutzerInnen sehr wirkungsvoll ist.

Das Trustcenter könnte dann verpflichtet werden, den Ermittlungsbehörden aufgrund eines richterlichen Beschlusses den geheimen Schlüssel herauszugeben, so daß eine Entschlüsselung möglich wäre.

Voraussetzung dafür wäre jedoch, daß nur mit der lizensierten Software verschlüsselt wird. Die Verschlüsselung mit anderen Programmen müßte verboten werden.

Diese Überlegung liegt auch dem sog. „Clipper-Chip" zugrunde, dessen Einführung in den USA diskutiert wird. Es handelt sich dabei um ein Hardware-Teil, mit dem Daten verschlüsselt werden. Die Schlüssel sollen bei dieser Variante treuhänderisch von staatlichen Stellen verwaltet werden, die verpflichtet werden können, die zur Entschlüsselung notwendigen Daten den Ermittlungsbehörden mitzuteilen.

Verfassungswidrige Regelungen?

Ob derartige gesetzliche Beschränkungen der privaten Verschlüsselung rechtmäßig wären, ist allerdings fraglich.

Auch die Kommunikation über E-Mail stellt einen technisch vermittelten Nachrichtenaustausch über Entfernungen mit Hilfe von Fernmeldetechnik dar, ist also Telekommunikation. Diese wird durch Art. 10 Abs. 1 Grundgesetz (GG) geschützt. Das Fernmeldegeheimnis gilt dem Schutz der Vertraulichkeit einer fernmeldetechnisch vermittelten Kommunikation. Darunter fällt auch die Bestimmungsbefugnis der am Kommunikationsvorgang Beteiligten, wer von dem Inhalt Kenntnis erlangen soll. Dadurch, daß die Vertraulichkeit der Kommunikation in diesem Bereich so problemlos von Dritten angegriffen werden kann – und auch angegriffen wird –, können die BenutzerInnen ihr Grundrecht nur durch die Verwendung von Verschlüsselungsprogrammen wahrnehmen. Erst durch die Kodierung der Daten wird die Vertraulichkeit der Kommunikation überhaupt hergestellt.

Folglich würde sowohl ein Verbot der Verschlüsselung als auch eine Beschränkung auf staatlich lizensierte Verschlüsselungstechnik einen Grundrechtseingriff in Art. 10 Abs. 1 GG darstellen.

Ein solcher Grundrechtseingriff muß sich an dem Verhältnismäßigkeitsprinzip messen lassen. Der Eingriff muß also geeignet und erforderlich sein, ein verfassungsmäßig legitimes Ziel durchzusetzen. Weiterhin muß der Eingriff und der mit dem Eingriff verfolgte Zweck in einem wohl abgewogenen Verhältnis stehen. Das Ziel, das durch ein Verbot oder durch die Lizensierung erreicht werden soll, ist es, den StrafverfolgerInnen ihre Ermittlungstätigkeit zu erleichtern. Dabei handelt es sich um ein legitimes Ziel. Es muß jedoch bezweifelt werden, ob die oben genannten Maßnahmen überhaupt geeignet sind, dieses Ziel durchzusetzen. Die Nachfrage nach vom Staat lizensierter Verschlüsselungssoftware dürfte sich nämlich gerade bei Kriminellen in Grenzen halten.

Dagegen ist Software, die Daten sicher verschlüsselt, für jedermann kostenlos, zum Beispiel über das Internet, erhältlich. Mit einem gewissen Aufwand ließen sich derartige Programme auch selbst herstellen. Selbst die Tatsache, daß eine Nachricht überhaupt verschlüsselt wurde, läßt sich verbergen, indem die verschlüsselten Daten in einem unverschlüsselten Datenpaket „versteckt" werden (Steganographie).

Ein Kryptoverbot ließe sich also ohne großen Aufwand unterlaufen. Die Durchsetzung dieses Verbotes wäre von vornherein zum Scheitern verurteilt.

Der wirtschaftliche Nutzen bei Verstößen gegen ein solches Verbot durch organisierte Kriminelle dürfte in der Regel sehr hoch sein. Die Gefahr entdeckt und strafrechtlich für den Gebrauch von (nicht lizensierter) Verschlüsselungstechnik zur Rechenschaft gezogen zu werden, liegt dagegen nahezu bei Null. Auch von einer abschreckenden Wirkung derartiger Sanktionsnormen auszugehen, wäre daher reichlich naiv.

Eine Beschränkung der Benutzung von Verschlüsselungstechnik ist somit untauglich, das verfolgte Ziel durchzusetzen und würde damit gegen das Verhältnismäßigkeitsgebot verstoßen.

Trotz der Verfassungswidrigkeit der Reglementierung von Kryptographie sind derartige Normen für die Zukunft zu befürchten. Es wäre nicht das erste Mal, daß diese Regierung versuchen würde, den BürgerInnen mit Scheinaktionismus die Lösbarkeit von Problemen vorzutäuschen, anstatt den Tatsachen ins Auge zu sehen.

Florian Hammel studiert Jura in Regensburg.

Anmerkungen:

1 Pfeiffer / Diesler / Kauß *Chip* 8/1995, 48.
2 Leiberich *Kriminalistik* 1995, 413.
3 Fox *c't* Juni 6/1995, 46.
4 Schröder *Die Zeit*, 76.
5 Kuner *NJW-CoR* 1995, 413.
6 BT-Drucksache 13/3932.

Literatur:

Fox, Dirk, Krypto-Neid, in: *c't* 6/1995, 46 ff.
Kuner, Christopher, Rechtliche Aspekte der Datenverschlüsselung im Internet, in: *NJW-CoR* 1995, 413 ff.
Leiberich, Otto, Verschlüsselung und Kriminalität, in: *Kriminalistik* 1995, 731 ff.
Pfeiffer, Nikola / Diesler, Peter / Kauß, Uwe, Jeder ist verdächtig, in: *Chip* 8/1995, 48 ff.
Schröder, Burkhard, Schnüffler am Ende, in: *Die Zeit* v. 8.9.1995, 76.