Facharbeit Informatik

Kryptographie aus rechtlicher Sicht

Die Kryptodebatte

erarbeitet von Marcus Gick, Humboldt-Oberschule,
Grundkurs Informatik GINÜ3 (Herr Dietz), 2. Semester

Inhaltsverzeichnis

1.) Einleitung/Einführung in das Thema

2.) Gründe für eine Verschlüsselung

3.) Aufkommende Diskussionen: Die Kryptodebatte

- 3.1) Ursachen der Debatte
- 3.2) Pro & Contra
- 3.3) Argumentation in der Debatte
- 3.4) Thesen zur Einschränkung von Verschlüsselungsverfahren

4.) Reaktion der Politik auf die Diskussion

- 4.1) Wirtschaftsinteressen
- 4.2) Eckpunkte der Bundesregierung zur Verschlüsselung

5.) Schlussteil/Fazit

6.) Literaturverzeichnis

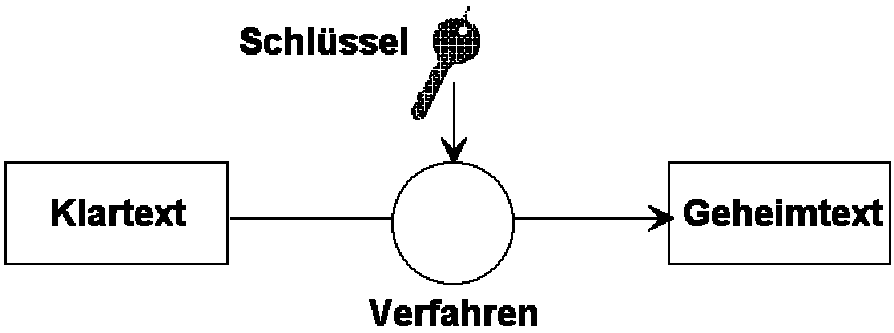
1.) Einleitung/Einführung in das Thema

Kaum ein anderes Thema im Bereich der Informationstechnologie hat in den letzten Jahren sowohl die Politik als auch die Wirtschaft und die Forschung mehr beschäftigt als die Frage danach, wie Verschlüsselungen von Nachrichten rechtlich zu handhaben seien.
Diese Problematik mündete in der sogenannten Kryptodebatte, d. h. der Frage, ob man das Recht eines jeden Einzelnen, Informationen verschlüsselt auszutauschen, einschränken kann und soll.
Neue und starke Kryptoverfahren haben eine erneute breite Diskussion angefacht.
In Deutschland steht eine endgültige Entscheidung noch aus, obwohl schon einige Weichen gestellt worden sind (⇒Eckpunkte der Bundesregierung zur Verschlüsselung).

Auf den folgenden Seiten soll ein Überblick über die Gründe für eine Verschlüsselung und die damit verbundenen Diskussionen gegeben werden. Die Debatte selbst wird im Hinblick auf Befürworter und Gegner eines Verschlüsselungsverbotes untersucht.
Ferner wird die Antwort der Politik auf diese Debatte, sowohl unter wirtschaftlichen als auch unter sicherheitspolitischen Aspekten, dargelegt.
Schließlich werden die von der Bundesregierung verabschiedeten Eckpunkte zur Verschlüsselung vorgestellt.

2.) Gründe für eine Verschlüsselung

Seit es Kommunikation gibt, ist auch der Versuch bekannt, Nachrichten, die nicht für Fremde bestimmt sind, zu verschleiern. Schon bei Caesar oder griechischen Feldherren war dies der Fall.
Das technische Verschlüsseln wurde in der jüngeren Vergangenheit hauptsächlich auf zwei Ebenen betrieben: auf militärischer und auf wirtschaftlicher Ebene. Für diese beiden Bereiche war es wichtig, dass sie Informationen austauschen konnten, die kein Dritter verstehen konnte (z. B. bei der Kriegs- und Wirtschaftsspionage).
Heutzutage, in Zeiten des Internets und der modernen Medien, wird auf der technischen Ebene die Verschlüsselung auch für Privatmenschen wichtig. Natürlich will jeder seine Privatsphäre schützen. Eine elektronisch verschickte Nachricht aber ist im Prinzip für jeden zugänglich. Da die Nachricht über sehr viele fremde Rechner läuft, kann sie an jeder Station eingesehen werden. Damit kann eine E-Mail der Willkür von vielen Menschen ausgeliefert sein. Um dies zu verhindern, schützt man seine Nachrichten mit Kryptographieprogrammen wie z. B. PGP (Pretty Good Privacy). Ein solches Programm verschlüsselt Botschaften und befähigt nur den Empfänger zu einer Entschlüsselung, da sich der erforderliche Schlüssel für ein Decodierungsverfahren im Normalfall nur in seinem Besitz befindet.



Verschlüsselung von Nachrichten

Neben dem Schutz der Privatsphäre kann es aber noch weitere Gründe geben, Nachrichten zu verschlüsseln. Dazu zählen die Erlangung eines taktischen oder strategischen Vorteils oder auch die Wahrung eines Wissensvorsprungs gegenüber Konkurrenten.

Kein anderes Phänomen ist so sehr mit der Existenz einer Gesellschaft verknüpft wie die Kommunikation. Fehlt sie, so brechen alle Strukturen auseinander. Kann man sie kontrollieren, so kontrolliert man auch die Gesellschaft. Dadurch wird verständlich, warum die Diskussion um die "Kryptoregulierung" so engagiert geführt wird.

3.) Aufkommende Diskussionen: Die Kryptodebatte

3.1) Ursachen der Debatte

Besonders Polizei und Behörden sind besorgt über die Möglichkeit, Informationen im Internet abhörsicher zu übertragen. Anlass zu dieser Sorge bietet die breite Verfügbarkeit von hochentwickelten Codierungsprogrammen, die mittlerweile so sicher verschlüsseln, dass die Computer aller Geheimdienste der Welt einige Jahrtausende beschäftigt wären, den Code zu decodieren. Dagegen ist das Verschlüsseln eines Textes für jeden Benutzer so einfach wie das Absenden einer E-Mail.

Bei einer solchen Verschlüsselung von Nachrichten, die durchgeführt wird, um nicht berechtigte Dritte auszuschließen, werden jedoch auch Stellen ausgeschlossen, denen es erlaubt ist, den Inhalt einer Nachricht mitzuverfolgen und anzusehen. Dazu zählen Sicherheits- und Strafverfolgungsbehörden, die einen Anspruch darauf haben, unter bestimmten, gesetzlich festgelegten Umständen, Beschränkungen des Fernmeldegeheimnisses nutzen zu können.

Daher erheben diese Behörden weltweit die Forderung, die Nutzung kryptographischer Verfahren so zu regulieren, dass ihnen der Zugang auf den Klartext der übertragenen Daten bei Bedarf ermöglicht wird. Eine Codierung soll nur dann zulässig sein, wenn der geheime Schlüssel bei einer Behörde hinterlegt wird. Im Fall, dass jemand abgehört werden soll, weil er beispielsweise wegen einer Straftat verdächtigt wird, wird sein geheimer Schlüssel den Sicherheitsbehörden übergeben, die dann seine Kommunikation überwachen.

Die Sicherheitskräfte verweisen auf die Notwendigkeit, abhören zu dürfen; namhafte Juristen halten eine Einschränkung der Kryptographie allerdings für verfassungswidrig.

3.2) Pro & Contra

Wie bereits erwähnt, wird die Frage, ob und in welchem Umfang die Nutzung kryptographischer Verfahren gesetzlich beschränkt werden soll, in vielen Industrieländern, darunter auch in Deutschland, kontrovers diskutiert. An der Diskussion beteiligen sich Vertreter aus Politik, Wirtschaft und zahlreichen gesellschaftlichen Gruppen und nehmen dabei grundsätzlich zwei gegensätzliche Positionen ein:

Pro

- für eine Reglementierung, gegen eine liberale Nutzung ohne Gesetzesgrundlage
- kryptographische Produkte sind nur dann erlaubt, wenn sie durch staatliche Stellen zugelassen sind
- Schlüssel für die Decodierung soll bei Sicherheitsbehörden hinterlegt werden

Contra

- für eine Nutzung ohne Beschränkung, gegen jegliche Reglementierung
- Forderung nach staatlicher Unterstützung für kryptographische Verfahren

3.3) Argumentation in der Debatte

Die Befürworter einer Reglementierung geben an, durch eine strengere Handhabung die Aufklärung derjenigen Straftaten fördern zu können, die von dem Einsatz kryptographischer Verfahren profitieren. Da sie mit einem Antrag auf ein totales Kryptoverbot beim Bundesverfassungsgericht keine Chancen auf Erfolg sahen, haben sie sich für eine oben bereits erwähnte Hinterlegung der Codierungsschlüssel bei den Behörden entschieden.

Von Gegnern einer Reglementierung wird neben dem Recht auf Meinungsfreiheit auch das Recht auf die Unverletzlichkeit des Brief-, Post- und Fernmeldegeheimnisses und der Wohnung angeführt. Außerdem beharrt man auf den Datenschutz. Des Weiteren gibt es auch im Bereich der Wirtschaft Widerstände. So ließen sich beispielsweise neue Geschäftsideen nicht umsetzen, da die erforderliche Sicherheit (durch Verschlüsselung) fehle. Ausländische Konkurrenten ohne Regulierung hätten dadurch einen Vorteil. Auch die eigene (deutsche) Kryptoindustrie leide darunter, da neue Entwicklungen in diesem Bereich gar nicht oder nur verzögert auf den Markt gebracht werden könnten.

3.4) Thesen zur Einschränkung von Verschlüsselungsverfahren

Die folgenden Thesen stammen von dem schleswig-holsteinischen Datenschutzbeauftragten Dr. Helmut Bäumler und geben seine Einstellung zum Verbot oder zur Einschränkung von Verschlüsselungsverfahren wieder.

- *„Kryptografie ist ein hervorragendes Instrument zur Sicherung des Datenschutzes“*

Durch sie könnten die Vertraulichkeit, die Authentizität und die Integrität wirksam geschützt werden.

- *„Wirksame Verschlüsselungsverfahren sind auch aus wirtschaftlichen Gründen wichtig für den Standort Deutschland“*

Die Wirtschaft müsse sich vor Ausspähung von Konkurrenten schützen können. Ein Kryptoverbot wäre wettbewerbsfeindlich.

- *„Ein Kryptoverbot wäre praktisch kaum durchsetzbar“*

Es sei kaum überprüfbar, ob verschlüsselte Daten vorliegen. Man könnte immer in Länder ausweichen, in denen kein Verbot besteht.

- *„Ein Verbot oder die Einschränkung der Verschlüsselung wäre verfassungsrechtlich nicht haltbar“*

Die Verfassung schütze im Grundgesetz die vertrauliche und unbeobachtete Kommunikation als „unverletzlich“.

- *„Gegen organisierte Kriminalität hilft am besten Verschlüsselung“*

Es müsse den Bürgern erlaubt sein, sich selbst wirksam vor organisierten Verbrechern zu schützen.

4.) Reaktion der Politik auf die Diskussion

4.1) Wirtschaftsinteressen

Die wirtschaftliche Bedeutung der deutschen Krypto-Industrie im internationalen Vergleich ist beträchtlich. Für die kommenden Jahre rechnet man mit einem erheblichen Wachstum auf dem Markt für Sicherheitsprodukte. Vor allem die elektronische Dienstleistungsgesellschaft hängt von der Verfügbarkeit starker und verlässlicher Krypto-Produkte ab.

Die Wachstumsraten in Deutschland betragen jährlich 30 Prozent. Die Exportquote für Krypto-Produkte liegt bei über 50 Prozent.

Fast die Hälfte der deutschen Krypto-Unternehmen wurde in den letzten fünf Jahren gegründet. Sie beschäftigen derzeit zwischen 2.000 und 3.000 Mitarbeitern.

Aufgrund dieser Zahlen wird ersichtlich, dass die Wirtschaft ein großes Interesse daran hat, dass es bei einer liberalen Nutzung kryptographischer Mittel in Deutschland bleibt.

4.2) Eckpunkte der Bundesregierung zur Verschlüsselung

Am 2. Juni 1999 entschied die Bundesregierung über die deutsche Haltung zur Nutzung von kryptographischen Verfahren. Der Beschluss wurde in fünf sogenannte Eckpunkte gefasst, die für die nächsten zwei Jahre ihre Gültigkeit behalten sollten.

Die Punkte lauten, verkürzt, im Einzelnen:

1. *Die Bundesregierung beabsichtigt nicht, die freie Verfügbarkeit von Verschlüsselungsprodukten in Deutschland einzuschränken. Sie sieht in der Anwendung sicherer Verschlüsselung eine entscheidende Voraussetzung für den Datenschutz der Bürger, für die Entwicklung des elektronischen Geschäftsverkehrs sowie für den Schutz von Untemehmensgeheimnissen. (...)*
2. *Die Bundesregierung strebt an, das Vertrauen der Nutzer in die Sicherheit der Verschlüsselung zu stärken. (...)*
3. *Die Bundesregierung hält aus Gründen der Sicherheit von Staat, Wirtschaft und Gesellschaft die Fähigkeit deutscher Hersteller zur Entwicklung und Herstellung von sicheren und leistungsfähigen Verschlüsselungsprodukten für unverzichtbar. (...)*
4. *Durch die Verbreitung starker Verschlüsselungsverfahren dürfen die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden zur Telekommunikationsüberwachung nicht ausgehöhlt werden. (...)*
5. *Die Bundesregierung legt großen Wert auf die internationale Zusammenarbeit im Bereich der Verschlüsselungspolitik. (...)*

Auch wenn der letzte Stand der Debatte eine große Zustimmung besitzt, darf man nicht übersehen, dass die „Eckpunkte“ die Wiederaufnahme der Diskussion offen lassen. Es wird sogar eine Überprüfung nach zwei Jahren festgelegt.

5.) Schlussteil/Fazit

Mit den „Eckpunkten“ wurde ein erster Schritt getan. Nachdem die Gesetzeslage zuvor völlig unklar war und für eine emotional geführte Debatte gesorgt hatte, wurde mit diesem Beschluss eine erste gewisse Ordnung hergestellt. Trotzdem ist er nicht endgültig.

Kriminelle würden sich sicher nicht davon abhalten lassen, kryptographische Mittel auch dann einzusetzen, wenn sie verboten wären. Dennoch sollte man gerade im Hinblick auf die Terrorakte vom 11. September die Möglichkeit einer gemäßigten Regulierung von kryptographischen Verfahren nicht völlig außer Acht lassen.

6.) Literaturverzeichnis

- [squat!net], Kryptographie und Datenschutz im Internet
- Schulzki-Haddouti, Christiane, Telepolis
- Schönleber, Claus, Argumente zur Kryptodebatte, Oktober 1997
- Amt für Datenschutz Berlin
- Bundesministerium für Wirtschaft und Technologie
- Bundesministerium des Innern
- Mekelburg, Hans-G., Verschlüsselte Botschaften, Die Kryptographiedebatte, 2002
- Birkenbihl, Klaus, Warum eigentlich eine Kryptodebatte?, Mai 1997