

Datenschutz und Datensicherheit

Arami Mitra

Vortrag vom 15.10.96

- [Kryptographie, rechtliche Situation](#)
- [Grundlagen der Datensicherheit / Methoden zur Datensicherung](#)
- [Datenschutz in Krankenhausinformationssystemen](#)
- [Kryptologie](#)

Wirksamer Datenschutz in offenen Systemen ist nur mit kryptologischen Methoden zu erreichen

Kryptographische Software, PGP(Pretty Good Privacy)

Information über PGP (Versionen, Bezugsquellen):

- [Das Verschlüsselungsprogramm PGP](#)
- [Pretty Good Privacy](#)
- [The International PGP Home Page](#)
- [ASCOM SYSTEC Home Page](#)

Newsgroups

[sci.crypt](#): more theoretical discussion about cryptography

[talk.politics.crypto](#): crypto policy

[alt.security.pgp](#): discussion about PGP

Abstract:

Im heute anbrechenden Zeitalter der Informationsgesellschaft kann das Briefgeheimnis nur durch Verschlüsselung der übertragenen Nachrichten gewährleistet werden. Dennoch gibt es weltweit Bestrebungen, die Anwendung von Verschlüsselung zu verbieten oder deren Sinn entscheidend zu untergraben. In diesem Papier wird die Situation leicht verständlich dargestellt und es werden Forderungen erhoben, die zum zukünftigen Schutz des Briefgeheimnisses erfüllt werden müssen.

Stellen Sie sich vor:

- Briefumschläge wären verboten und Sie müßten Ihre Korrespondenz mittels Postkarten abwickeln;
- Türschlösser wären registrierungspflichtig und Sie müßten einer Behörde einen

Nachschlüssel für jedes Schloß überlassen;

- Tresore wären nur erlaubt, wenn Sie bei einer Behörde auch die Kombination hinterlegen würden.

Das Briefgeheimnis in der Informationsgesellschaft

Heute ist die Kommunikation über Computernetze (insbesondere über das weltweite "Internet") mit dem Versenden von Postkarten vergleichbar. Verschicken Sie eine elektronische Nachricht, wird diese Nachricht über eine Reihe von miteinander durch Datenleitungen verbundenen Computern an den Empfänger weitergeleitet. Es ist dabei mit dem entsprechenden Wissen ohne weiteres möglich, Ihre Nachricht auf jeder dieser Datenleitungen bzw. Computer mitzulesen. Das gleiche gilt auch für alle anderen Datenbestände, die auf elektronischem Wege übertragen bzw. gespeichert werden. Verschlüsselung ist heutzutage für jedermann möglich.

Es gibt dafür freierhältliche Programme, die eine Nachricht so gut verschlüsseln können, daß sie nach menschlichem Ermessen von niemandem auf der Welt (außer dem beabsichtigten Empfänger) gelesen werden kann. Somit wäre es überhaupt kein Problem mehr, Geschäfts- und Privat-Korrespondenz über Computernetzwerke abzuwickeln. Ohne Furcht vor unerwünschten Mitlesern könnten Sie ihre Firmendaten, ihre Bankauszüge, ihre Kreditkartennummer, ihre Steuererklärung, ihre Liebesbriefe, usw. übertragen, d.h. Daten, die nur Sie und den Empfänger etwas angehen. Damit könnte die Informationsgesellschaft die neuen Kommunikationsmöglichkeiten endlich in ihrem vollen Umfang nützen. Die Einschränkungen Das Recht auf Verschlüsselung ist heute weltweit in Gefahr:

- Frankreich hat Verschlüsselung für private Personen und Organisationen verboten und bestraft deren Anwendung mit hohen Geld- oder sogar Freiheitsstrafen. Dies entspricht einem Verbot von Briefumschlägen und Türschlössern.
- In den USA ist kürzlich die sogenannte "Clipper-Chip" Initiative gescheitert. Diese wollte einen Verschlüsselungsmechanismus vorschreiben, der mit einer Hintertür für die Entschlüsselung jeder Kommunikation durch die Behörden ausgestattet worden wäre. Dies entspricht der Verpflichtung zur Anwendung einer bestimmten Serie von nummerierten Schlössern, bei deren Herstellung automatisch einer Behörde ein Zweitschlüssel geliefert wird.
- Die Kommission der Europäischen Union diskutiert soeben eine Vorlage, bei der jeder Anwender von Verschlüsselungsmethoden einen geheimen Schlüssel an bestimmte Stellen abliefern muß. Dies entspricht der Verpflichtung, beim Ankauf eines Türschlosses einer Behörde einen Zweitschlüssel zu übergeben. Die Begründung für alle diese Maßnahmen besteht im Wunsch von Polizeibehörden und Geheimdiensten, bei Bedarf die Kommunikation der Bürger abhören zu können, um so Aktivitäten krimineller Organisationen im vorhinein verhindern oder im nachhinein aufdecken zu können. Diese Entwicklung ist gefährlich und führt zu einer nicht zulässigen Einschränkung der Bürgerrechte.

Die Gegenposition

1. Der Schutz des Briefgeheimnisses.
2. Die fehlende Kontrolle.

3. Der verfehlte Zweck.

Die Forderungen

1. Freie Wahl der Verschlüsselungsmethode.
2. Geheimhaltung des Schlüssels.
 1. die Tatsache, daß Verschlüsselung eingesetzt wird,
 2. die Methode, die dafür verwendet wird, und insbesondere
 3. den für die Entschlüsselung notwendigen geheimen Schlüssel.
3. Gesetzliche Kontrollen.

Fazit:

Für Kommunikation und Datenhaltung soll also das gleiche Recht gelten, das jedermann bei der Durchsuchung seiner Räumlichkeiten durch die Exekutive hat. /UL

last update 06.12.1996 [Mitra ARAMI](#)