Einige Bemerkungen zu

# Anforderungen, Nutzen und staatlicher Reglementierung beim Einsatz von Verschlüsselungsverfahren

Hartmut Pohl[1]

## 1. Sicherheitsprobleme der International Information Infrastructure

Die zunehmende Vernetzung von Systemen der Informationsverarbeitung von Unternehmen, Behörden und Privaten im nationalen (National Information Infrastructure - NII der USA) und internationalen Bereich schafft Netze mit einer von Einzelnen derzeit nicht mehr überschaubaren Komplexität.

Wegen der Vielzahl angeschlossener IV-Systeme kann heutzutage auch nicht flächendeckend kontrolliert werden, in welchen angeschlossenen Systemen Fehlverhalten auftritt und von welchen Systemen unberechtigten Aktionen ausgehen wie z.B. Behinderung oder sogar Verhinderung der Kommunikation, unberechtigte Kenntnisnahme von Daten oder unberechtigte Veränderung. Zur vertrauenswürdigen Nutzung der Netze ist es auch notwendig, daß die übertragenen Nachrichten authentisch sind und dem Kommunikationspartner verbindlich zugeordnet werden können. Als weitere wünschenswerte Dienste kommen Anonymität und Pseudonymität der Kommunikation in Betracht. Zur Abwehr derartiger Ereignisse ist der Einsatz von Sicherheitsmaßnahmen erforderlich.[2]

In den letzten Jahren ist international wiederholt eine staatliche Reglementierung von Sicherheitsmaßnahmen in der Informationsverarbeitung und in Kommunikationssystemen diskutiert worden. Diese Diskussion ging von Fachleuten in den USA aus und wurde auch in die Öffentlichkeit getragen. In Europa wurde eine derart breite Diskussion bisher noch nicht geführt.

Eine besondere Bedeutung kommt der freien - in westlichen Staaten bisher unreglementierten - Anwendung von Verschlüsselungsverfahren und Geräten deswegen zu, weil eine Reihe von Sicherheitsmaßnahmen unabdingbar auf Verschlüsselung aufbauen; dies gilt insbesondere für die o.g. Sicherheitsziele und -probleme.

Die Bedeutung der Kommunikationssicherheit wird von Privaten, Unternehmen und Behörden zunehmend erkannt:

- Dies gilt sowohl für die Anwendungsmöglichkeiten der Verfahren: Zugriffskontrolle mit Identifizierung und Authentifizierung, Schutz vor unberechtigter Kenntnisnahme oder Veränderung von Daten bei der Speicherung und Übertragung.
- Klar erkannt werden auch die weltweiten Überwachungsmöglichkeiten jeglicher Kommunikation durch Dritte wie Behörden und Organisationen und das damit mögliche Mithören und Mitlesen - auch verschlüsselt übertragener Daten - bis hin zur Industriespionage[3].

Sichere Kommunikation zwischen Unternehmen, Behörden und Privaten ist daher ohne den Einsatz von Verschlüsselung in Sicherheitsmaßnahmen nicht realisierbar. Dabei muß berücksichtigt werden, daß qualitative hochwertige Verschlüsselungsprodukte (Hardware und Software) weltweit kommerziell auch verfügbar sind[4].

## 2. Interessenlage der Behörden

Seit einigen Jahren beklagen die Strafverfolgungsbehörden und auch die im Vorfeld arbeitenden Nachrichtendienste der Industriestaaten die Unfähigkeit, moderne Verschlüsselungsverfahren zu brechen;

---

[1] Hartmut Pohl, Fachbereich Wirtschaft der Abt. Bocholt, FH Gelsenkirchen und Institut für Informationssicherheit - ISIS, Essen.

[2] Vergl. (10). Darin ist eine umfangreiche Bibliographie - auch zur historischen Entwicklung enthalten.

[3] Einige Fälle finden sich in (1) und (7).

[4] Vergl. hierzu (6).

dies erscheint ihnen deswegen notwendig, weil die international aktive - meist organisierte - Kriminalität überwiegend verschlüsselt kommunizieren soll. Strafverfolgungsbehörden behaupten damit ihr Unvermögen, Kommunikation im wünschenswerten Umfang zu überwachen. Diese Behauptung kann von der Öffentlichkeit nicht verifiziert werden[5]. Eine weitere Schwachstelle dieser Argumentation ist die fehlende Darstellung oder gar der Nachweis des Zielerreichungsgrads, die Erläuterung der Erfolgsquote oder generell die Wirtschaftlichkeit der durchgeführten Abhörmaßnahmen. Zumindest merkwürdig erscheint die stark divergierende Anzahl der jährlich neu eingeleiteten Abhörmaßnahmen in Deutschland (4.000 Personen und/oder Institutionen) und z.B. der USA (1.500 bei mehrfacher Bevölkerungsgröße)[6].

### 3. Iniative der USA

Die Strafverfolgungsbehörden und Nachrichtendienste und die deren Interessen vertretenden Behörden fordern daher unter Federführung der USA dreierlei:

1. Grundsätzlich müssen Verschlüsselungsverfahren in Produkten so schwach sein, daß sie (ohne Kenntnis des Schlüssels) von diesen Behörden gebrochen werden können und jegliche Kommunikation mitgelesen werden kann. Dies gilt insbesondere für die internationale Kommunikation. Aus diesem Grunde kontrollieren viele Staaten den Export von Verschlüsselungsprodukten, d.h. es sind nur Produkte mit sog. schwachen Verfahren exportierbar. Bei diesem Vorgehen liegt allerdings ein Nachteil in der Tatsache, daß außer den Sicherheitsbehörden des exportierenden Landes auch andere Länder die derart schwach verschlüsselte Kommunikation entschlüsseln können.
2. Eine Verwendung starker Verfahren durch Nutzer des eigenen Landes (heimische Wirtschaft) soll zulässig sein, wenn die benutzten Schlüssel bei den Behörden hinterlegt werden.
3. Um internationale Kommunikation zu ermöglichen, werden "befreundete" Staaten und deren Private, Unternehmen und Behörden so behandelt, als seien sie Nutzer des eigenen Landes. Dies könnte beispielsweise für die NATO-Mitgliedsstaaten gelten.

Auf dieser Basis hat in den USA der Präsident eine sog. Direktive[7] erlassen.[8]

Dieser dreigliedrige Vorschlag ("ESCROW" und "Clipper") beschert sieben bisher ungelöste Probleme:

1. Voraussetzung für die Wirksamkeit des Verfahrens ist, daß auch das sog. internationale organisierte Verbrechen genau dieses Verfahren anwendet - und nicht etwa ein anderes - und auch die zutreffenden Schlüssel der Hinterlegungsbehörde mitteilt und nicht etwa modifizierte Schlüssel einsetzt[9]; ein Abhören derart verschlüsselter Kommunikation ist dann nicht möglich. Vorausgesetzt wird weiterhin, daß der Nutzer nicht bereits vor Einsatz des (zugelassenen) Verfahrens seine Daten mit einem anderen Verfahren verschlüsselt hat[10]. Überhaupt ist Voraussetzung, daß keine anderen Verfahren als dieses staatlich zugelassene benutzt werden. Eine Reihe von Staaten planen daher einen Genehmigungsvorbehalt für Kryptoprodukte. Eine kühne Forderung angesichts der mehr als 700 verschiedenen Verschlüsselungsgeräte und -programme, die von mehr als 300 Unternehmen aus 33 Ländern der Erde weltweit vertrieben werden.[11]
2. Verschlüsselte Kommunikation mit Drittländern kann nur mit schwachen (auch durch Dritte knackbaren) Verfahren durchgeführt werden. Dieser Verzicht auf den Einsatz jüngster Technologie erscheint vielen unzumutbar, weil er Wettbewerbsnachteile zur Folge haben dürfte (Konkurrenz liest

---

5 Der allgemein als sicher - und damit nicht knackbar - bezeichnete Data Encryption Standard kann binnen Stunden geknackt werden (12).

6 Zitiert nach (11). Die Gesamtzahl aller Abhöraktionen der berechtigten Behörden wird allerdings nicht veröffentlicht.

7 "Public Encryption Management" vom 16. April 1993.

8 Viele der einschlägigen Dokumente sind in (11) genannt; weiterhin findet sich dort eine Übersicht insbesondere der relevanten US-amerikanischen Literatur zur Clipper-Diskussion.

9 Nach Pressemeldungen ist es bereits gelungen, den Chip derart zu manipulieren und zu nutzen.

10 In (5) wird gezeigt, daß derartige Verfahren nicht oder mindestens schwer nachweisbar sind.

11 Vergl. (6).

mit!).

3. Der Anwender kann die Qualität der benutzten Verschlüsselungsalgorithmen sowie die des gesamten Verfahrens nicht beurteilen - der Algorithmus ist als Verschlußsache (SECRET, NOFORN) eingestuft und damit unzugänglich. Differenzierte Qualitätsbeurteilungen sind nicht veröffentlicht[12]. Gerade an Bewertungsparametern, Evaluierungen unabhängiger Institutionen und staatlichen Zertifikaten für Verschlüsselungsprodukte sind Anwender in hohem Maße interessiert.[13] Darüberhinaus können zukünftige eingehendere Untersuchungen des Verschlüsselungsalgorithmus doch noch eine (evtl. auch von den Entwicklern nicht beabsichtigte) "Falltür" offenlegen. Dann bliebe nur noch die Hoffnung, daß das Wissen um die Falltür nicht in "unberechtigte" Hände fällt - oder doch zumindest frühzeitig veröffentlicht wird.

4. Der den Algorithmus speichernde Chip soll sich bei Ausleseversuchen selbst zerstören. Dabei stellt sich die Frage, ob der Algorithmus nicht bereits ausgelesen worden ist oder auf anderem Wege in Erfahrung gebracht wurde. Schließlich kennen bereits heute viele Mitarbeiter der Behörden und der entwickelnden und produzierenden Unternehmen den Algorithmus und seine Implementierung. In jedem Fall dürften dem Adressaten dieser Sicherheitsmaßnahmen - dem internationalen organisierten Verbrechen - hinreichend große Geldbeträge zur Finanzierung von Untersuchungen des Chips sowie zum Nachbau zur Verfügung stehen. Ein Nachbau ist um so "sinnvoller" als das Verfahren selbst als sicher bezeichnet wird.. Weiterhin ist das Vertrauen von Privaten und Unternehmen in die Hinterlegungsbehörde(n) begrenzt. An die Verfassungsverträglichkeit müßten besondere Anforderungen gestellt werden[14].

5. Die Hinterlegungsinstanz - auch als trust center bezeichnet - trägt in jedem Fall ein unvergleichlich hohes Risiko, weil hier *alle* Schlüssel der Nation oder Nationen konzentriert sind. Der Angreifer, der diese Schlüsselzentralen klassisch-materiell oder DV-technisch knackt, kann alle privaten und wirtschaftlichen Informationen dieser Nationen unberechtigt mitlesen. Alle Informationen, die in der Vergangenheit gespeichert und übertragen wurden und in Zukunft verarbeitet werden - jedenfalls mindestens bis zur Entdeckung des erfolgreichen Angriffs. Durch die Errichtung von zwei Hinterlegungsbehörden kann das Sicherheitsrisiko der trust center nur graduell gesenkt werden.[15]

6. Außerdem wird die Möglichkeit der "unendlichen" legalisierten Abhöraktion gesehen, weil ein zurückgegebener Schlüssel gleichwohl weiterhin - und zwar dann unkontrolliert - zum Abhören benutzt werden kann; natürlich kann auch die gesamte Kommunikation der Vergangenheit entschlüsselt werden, sofern sie aufgezeichnet wurde.

7. Der im Chip gespeicherte Serienschlüssel ermöglicht die Identifikation und auch eine Lokalisierung von Sender und Empfänger - auch im Mobilfunk.

Diese Aspekte - und sicherlich noch eine Reihe weiterer - sollten in einer breiten öffentlichen Diskussion mit dem Ziel einer demokratischen Konsensbildung mit ihren technischen Problemen und Möglichkeiten (u.a. Informationssicherheit) und politischen Implikationen - insbesondere die Datenschutz- und Persönlichkeitsrechte sowie Staatsschutz und Innere Sicherheit tangierenden Aspekte - sowie die Anforderungen der Unternehmen dargestellt und gegeneinander abgewogen werden[16].

---

[12] Vergl. (2).

[13] Eine öffentliche Zertifizierung derartiger Produkte wurde vom Bundesamt für die Sicherheit in der Informationstechnik - BSI im Einvernehmen mit dem Bundesminister des Innern nicht vorgenommen (3).

[14] Vergl. (9).

[15] Als Hinterlegungsbehörden in den USA sind das National Institute for Standards and Technology (NIST) des Department of Commerce und die Automated Systems Division (ASD) des Department of Treasury festgelegt.

[16] In (4) wird darauf hingewiesen, daß sich die "klassische Sündenbockfunktion des Staates im Sinne der Polarisierung Staatsmacht bzw. "großer Bruder"/Bürgerrecht" erledigt haben könnte. "An die Stelle der Polarisierung (informationelle) Staatsmacht/Bürgerrecht könnte heute vielleicht eher die Polarisierung staatliche Ordnungsmacht/internationale Mafia treten."

## 4. Literatur:


(1) Bizer, J.: Die Kryptokontroverse. Innere Sicherheit und Sicherungsinfrastrukturen. In: Roßnagel, A. et al. (Hrsg.): Soziale und politische Implikationen einer künftigen Sicherungsinfrastruktur. provet Arbeitspapier 150. Darmstadt 1994

(2) Brickell, E. F.; Denning, D. E.; Kent, S. T.; Maher, D. P.; Tuchmann, W.: SKIPJACK Review Interim Report. The SKIPJACK Algorithm. Washington July 28, 1993

(3) Deutscher Bundestag: Gesetz über die Errichtung des Bundesamtes für die Sicherheit in der Informationstechnik (BSIG) vom 17. Dezember 1990, BGBl. I S. 2834

(4) Fiedler, H.: Informationelle Garantien für das Zeitalter der Informationstechnik. In: Tinnefeld, M.-T.; Philipps, L.; Weis, K.: Institutionen und Einzelne im Zeitalter der Informationstechnik. Machtpositionen und Rechte. München 1994

(5) Möller, S.; Pfitzmann, A.; Stierand, I.: Rechnergestützte Steganographie: Wie sie funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist. Datenschutz und Datensicherung 6, 318 - 326, 1994

(6) Pohl, H.: Sicherheitsperspektiven: Verschlüsselungsprodukte. Online 11, 50, 1994

(7) Pohl, H.; Hütte, L.: Computer-Spionage: Ist die Katastrophe unvermeidbar? Journal für Wirtschaft und Gesellschaft - bonntendenz 4, III 1989

(8) Raubold, E: Wieviel Information gebührt dem Staat? Gastkommentar: Computerwoche 28, 8, 9. Juli 1993

(9) Roßnagel, A.: Rechtliche Gestaltung informationstechnischer Sicherungsinfrastrukturen. In: Roßnagel, A. et al. (Hrsg.): Soziale und politische Implikationen einer künftigen Sicherungsinfrastruktur. provet Arbeitspapier 150. Darmstadt 1994

(10) Roßnagel, A.; Bizer, J.; Hammer, V.; Kumbruck, C.; Pordesch, U.; Schneider, M. J. (Hrsg.): Soziale und politische Implikationen einer künftigen Sicherungsinfrastruktur. provet Arbeitspapier 150. Darmstadt 1994

(11) Rueppel, R. A.: "Clipper" - Der Kryptokonflikt am Beispiel der amerikanischen ESCROW-Technologie. In: Tinnefeld, M.-T.; Philipps, L.; Weis, K.: Institutionen und Einzelne im Zeitalter der Informationstechnik. Machtpositionen und Rechte. München 1994

(12) Wiener, M.: DES Breaking Machine. Proceedings of the Crypto ´93. Berlin 1994