

Segen oder Fluch?

Vor- und Nachteile starker Kryptographie

(Johannes Nicolai)

Einleitung / Begriffsklärung

Unternimmt man einmal einen Streifzug durch die heutige IT – Messelandschaft, so fällt schnell auf, dass Informationssicherheit immer mehr Beobachtung findet und zu einem zentralen Thema in der Industrie avanciert [6]. Diese Beobachtung wird auch bei Analyse der Themenwahl von vielen Endrundenprojekten im Fachbereich Informatik / Mathematik des Bundeswettbewerbes Jugend Forscht bestätigt; kein Wunder bietet dieses Gebiet doch unzählige interessante Forschungstätigkeiten. Das Rückrat der Informationssicherheit bildet die Kryptographie, es empfiehlt sich also, damit etwas näher vertraut zu werden.

Kryptographie ist die Wissenschaft, die sich mit der Absicherung von Nachrichten beschäftigt. Sie wird von Kryptographen praktiziert. Eine Nachricht ist eine Information gleich welcher Art (z.B. Text, Daten, Programme etc.), die der Sender dem Empfänger zukommen lassen will. Eine unverschlüsselte Nachricht wird Klartext genannt, ihr verschlüsseltes Gegenstück Chiffretext. Um die Nachricht verschicken zu können, ist ein Übertragungsmedium (z.B. Post oder Datenleitung) notwendig. Je nachdem, ob dieses Übertragungsmedium abgehört werden kann oder nicht, spricht man von einem unsicheren bzw. sicheren Kanal. Eine Nachricht wird dann als verschlüsselt (chiffriert) angesehen, wenn sich aus dem Chiffretext nur sehr mühsam oder überhaupt nicht der Klartext rekonstruieren (wiederherstellen) lässt. Um einen Klartext zu einem Chiffretext umzuwandeln, muss ein Verschlüsselungsalgorithmus auf den Klartext angewandt werden. Um den Chiffretext entschlüsseln (dechiffrieren) zu können (aus dem Chiffretext den Klartext zu rekonstruieren) wird ein Entschlüsselungsalgorithmus benutzt. Damit nicht jeder Klartext zum selben Chiffretext verschlüsselt wird, braucht jeder Verschlüsselungs- und Entschlüsselungsalgorithmus einen Schlüssel, der bestimmt, wie der Klartext verschlüsselt, bzw. wie der Chiffretext entschlüsselt wird. Ohne diesen Schlüssel sollte es nicht möglich sein, den Chiffretext zu entschlüsseln. Algorithmen, bei denen der Schlüssel zum Verschlüsseln (Chiffrieren) derselbe ist wie der zum Entschlüsseln werden symmetrische Algorithmen genannt. Verfahren, bei denen der Schlüssel zum Verschlüsseln sich von dem zum Entschlüsseln unterscheidet, heißen asymmetrische (Public Key) Algorithmen. Ist die Funktionsweise eines Algorithmus nicht veröffentlicht, so spricht man von einem eingeschränkten Algorithmus. Diese sind in der heutigen Zeit kaum noch tragbar.

Krypt(o)analyse ist die Wissenschaft, die versucht, aus dem Chiffretext ohne Kenntnis des Schlüssels den Klartext zu erhalten (den Chiffretext zu »knacken«). Sie wird von Kryptanalytikern praktiziert. Oft wird ein Kryptanalytiker auch einfach nur »Angreifer« genannt. Die Verfahren, die zur »Aufbrechung« (Entschlüsselung) des Chiffretextes ohne Schlüssel eingesetzt werden, sind unter den Namen Attacken bekannt. Hier wird zwischen Brute Force (probiere alle möglichen Schlüssel aus) und differenzierteren Attacken unterschieden. Ein Algorithmus wird dann als sicher angesehen, wenn die Zeit, den Chiffretext zu knacken größer ist, als die Zeit, in der die Nachricht einen Wert hat. Weiterhin muss der Algorithmus sicher sein, auch wenn dem Kryptanalytiker die Funktionsweise bekannt ist. Eingeschränkte Algorithmen werden also nicht als sicher angesehen.

Werden bewährte Algorithmen in Verbindung mit hohen Schlüssellängen eingesetzt, hat man es mit starker Kryptographie zu tun, die als hochsicher angesehen werden kann.

Hochsicher heißt in diesem Fall, dass selbst großdimensionierte Rechenanlagen es nicht bewältigen können, nicht für sie bestimmte Daten in angemessener Zeit zu entschlüsseln. Großdimensioniert bedeutet in diesem Kontext keineswegs nur die Rechenkapazität einer Schule oder einer Firma; selbst größte Organisationen und Institutionen sollten nicht unerlaubt Zugriff zu sensiblen Informationen bekommen können.

Starke Kryptographie ist für die einen ein Segen, für die anderen ein Fluch. Kaum ein Thema wurde nach den Anschlägen am 11. September 2001 kontroverser diskutiert. Viele Kritiker wollen die Anwendungen von Kryptographie völlig verbieten lassen oder sprechen sich für entschärfte Varianten davon aus, welche richtige Sicherheit kaum noch gewährleisten können. Die Befürworter starker Kryptierverfahren wie der Datenschutzbeauftragte Schleswig Holsteins, Dr. Bäumler, sprechen wiederum von einem „Geschenk des Himmels“, vergleiche [7].

Ich möchte mich in diesem Artikel intensiv mit den Argumenten beider Seiten befassen und schlussendlich ein eigenes Fazit ziehen.

Zum besseren Textverständnis habe ich die Pro- und Kontraargumente in zwei unterschiedliche Kategorien eingeteilt, die der technischen Aspekte und die der gesellschaftlich moralischen Aspekte. Ich werde zunächst die gesellschaftlich, moralischen Problemfelder abhandeln, da diese in den meisten Diskussionen eine größere Rolle spielen.

Gesellschaftlich-moralische Aspekte

Als Ausgangspunkt für diese Sektion sei die These, „Kryptographie ist absolut unnötig, da konventionelle Mittel völlig ausreichen“, genannt. Sie ist häufig die erste Behauptung von Kritikern, welche Verschlüsselung im Ganzen ablehnen. Meistens haben sich diese über die Materie nur unzureichend informiert. So bleibt zum Beispiel schleierhaft, was mit konventionellen Mitteln gemeint ist und welche Aufgabenbereiche der Verschlüsselungstechnik diese bereits abdecken. Aus diesem Grunde möchte ich zunächst noch einmal ganz klar feststellen, welche Bedeutung und Funktion die Kryptologie heutzutage bereits inne hat.

Kryptologie ist die zentrale Voraussetzung für das Funktionieren der Informationsgesellschaft. Nur durch die Nutzung von unbrechbaren Verschlüsselungsverfahren kann überhaupt rechtsverbindlich über das Internet kommuniziert werden. Die Kryptographie stellt durch Schaffung von Vertraulichkeit, Authentizität und Integrität ein wichtiges Werkzeug zum Schutze des Bürgers dar. Nur wenn hundertprozentig garantiert ist, dass jeder wirklich der ist, der er vorgibt zu sein (Authentizität), eigene Informationen nicht von Dritten verfälscht werden können (Integrität) und sensible Daten nur für die zugänglich sind, für die sie auch vom Absender bestimmt waren (Vertraulichkeit), kann eine moderne Gesellschaft im Zeitalter des Internets überhaupt bestehen bleiben. In dem Moment, in dem es möglich geworden ist, die vollständige Identität einer Person aufzudecken, ist es auch möglich, dieser kräftig zu schaden. Man stelle sich bloß vor, jemand publiziere unter dem Namen einer von ihm ungeliebten Person rechtsradikale Schriften oder hätte Zugriff auf deren Privatkorrespondenz und Krankheitsverlauf. Kryptographie wahrt die Berufsgeheimnisse von Journalisten, Rechtsanwälten, Psychologen, Steuer- und Unternehmensberatern und Geistlichen.

Nicht auszudenken, was passieren würde, wenn diese sensiblen Informationen unverschlüsselt bleiben müssten. Ein Unternehmen, deren Werbestrategien und Kundendatei an die Konkurrenz gelangen würde oder sich nicht im Klaren sein könnte, ob die übermittelten Informationen wirklich von einem Mitarbeiter stammen und nicht mutwillig eingeschleuste Fehldaten von der Konkurrenz darstellen, würde bald Insolvenz anmelden müssen. Inwieweit „konventionelle Mittel“ diese Garantien übernehmen könnten, ist mehr als fraglich.

Neben diesem Kritikerargument gibt es allerdings auch wesentlich schwerwiegendere. Thesen wie „Durch den Einsatz von Kryptographie verliert der Staat die Kontrolle über die Bürger und ist der Kriminalität hoffnungslos ausgeliefert“ oder „Vertrauen ist gut, Kontrolle ist besser“, vergleiche [12] haben durchaus eine gewisse Berechtigung. Der Staat ist heutzutage tatsächlich nicht mehr in der Lage, jegliche Aktivität seiner Einwohner zu überwachen. Die derzeitig verfügbaren Chiffrierprodukte erlauben es, Nachrichten so unkenntlich zu machen, dass selbst Geheimdienste nicht mehr die Möglichkeit besitzen, diese wieder zu entschlüsseln. Will sich zum Beispiel ein Verbrechersyndikat darüber austauschen, wo und wann der nächste Raubzug stattfinden soll und tut dies auf einem kryptographisch gesicherten Wege, dürfte es den Behörden nicht möglich sein, aus dem abgehörten Code den Klartext wieder zu rekonstruieren. Aus diesem Grunde fordern Kritiker die Abhörmöglichkeit elektronischer Informationssysteme im Verdachtsfall, eben da [12]. Das Verbot von Kryptierverfahren erleichtert die Strafverfolgung und schützt den ehrlichen Bürger, der sowieso nichts zu verbergen habe, vor der Kriminalität.

Diese Regelung wäre allerdings sehr leicht zu umgehen, indem man sich für seine korrupten Geschäfte „virtuell“ in ein anderes Land begeben würde, was keine dieser Einschränkungen besitzt. Einmal gedachte Gedanken werden immer wieder aufgegriffen. Die Idee, einen neuen Algorithmus zu entwickeln, der (noch) nicht unter dieses Verbot fiel, würde sich geradezu zwingend auf tun. Das Hase-und-Igel-Spiel könnte die Regierung niemals gewinnen.

Allerdings stammen viele Straftäter aus einem Milieu, bei dem es sehr fraglich ist, ob diese überhaupt geistig in der Lage wären, Verschlüsselungstechniken gezielt für ihre Verbrechen zu nutzen. Weiterhin ist sehr fraglich, wie Deutschland die „Datenpolizei“, welche nach Verstößen gegen die Verordnung fahnden müsste, zu finanzieren gedenkt. Dafür wären absolut perfekt ausgebildete IT-Spezialisten in riesiger Anzahl erforderlich, die dieser Aufgabe auch noch freiwillig nachkommen wollten, statt ein Spitzengehalt in der Wirtschaft zu beziehen.

Die Praxis, die eigene Bevölkerung auszuhorchen, war sehr weit im Ostblock verbreitet und hat allerdings mit Demokratie, Rede- und Meinungsfreiheit nicht viel zu tun, vergleiche [2]. Den Kritikern ist vielleicht nicht ganz bewusst, was passieren müsste, wenn ihre Forderungen konsequent durchgeführt werden würden. Jeder Brief müsste erst einmal geöffnet werden, um kriminelle Handlungen oder den Einsatz von Kryptographie aufzudecken, alle Hausschlüssel sowie Safekombinationen und EC Geheimzahlen bei der Polizei hinterlegt werden, damit diese effizient im Verdachtsfall sofort ihre benötigten „Daten sichten“ könnte, bevor diese vernichtet werden können. Das Verbot von starker Chiffrierung hätte gravierende Nachteile für die informationelle Selbstbestimmung und Sicherheit der Bürger, die Schutzinteressen der Wirtschaft wären verletzt, ausländischer Industriespionage wären keine Grenzen mehr gesetzt. Das Verbot oder die Einschränkung von Kryptographie ist nach Artikel 10 GG (die vertrauliche, unbeobachtete Kommunikation ist unverletzlich) nicht zulässig, vielmehr hat der Staat die Pflicht, die Verwirklichung der Grundrechte zu fördern, statt sie massiv beschneiden zu wollen.

Der Einsatz von Kryptographie verhindert im Gegenteil viele Arten von Kriminalität, wie z. B. Spionage, Betrug und Manipulation, vergleiche [5]. Deutschland müsste seine Forschung in diesem Bereich noch verstärken, um den Anschluss nicht zu verlieren, vergleiche [4]. Mit der Erlaubnis, diese Möglichkeiten auch privat einzusetzen, kann der Staat einige seiner Kompetenzen mit dem Bürger teilen und wird somit schlanker, ein angestrebtes Ziel jeder modernen Demokratievorstellung.

Offenbar die überwältigende Mehrheit der Internet-Nutzungen erfolgt nicht zu kriminellen Zwecken. „Dies ist umso überraschender, als man kriminellen Missbrauch gerade bei garantierter Anonymität vermuten könnte“, sind die Schlussfolgerungen, die Helmut Bäumler aus einem Pilotprojekt namens An.ON zieht, vergleiche [13]. Dieser Dienst ermöglicht es Internetnutzern im World Wide Web zu surfen, ohne, dass ihre Verbindungsdaten beim Provider gespeichert werden. So ist es Strafverfolgungsbehörden nicht möglich, Rückschlüsse auf einzelne Personen zu ziehen. Trotz 1,2 millionenfacher Nutzung dieses Services innerhalb von 13 Monaten, wurden in dieser Zeitspanne nur 17 Anfragen bezüglich potentiell begangenen Straftaten gestellt. Die Studie beweist damit, dass auch bei völliger Anonymität im Internet „allem Anschein nach nicht mehr Straftaten begangen werden, als im realen Leben“, eben da [13].

Andere Stimmen aus dem Kritikerlager fürchten sich nicht vor der eigenen Bevölkerung, sondern vor fremden Mächten aus dem Ausland. „Mit dem Einsatz von Kryptographie können andere Staaten innerhalb unseres Landes Operationen planen und den Wirtschaftsstandort Deutschland bzw. dessen Demokratie gefährden“, ist ein Argument, was häufig aus den Reihen der Militärs und der inneren Sicherheit zu hören ist. Offensichtlich fürchtet man sich hier vor feindlichen Agenten, die im großen Stil Industriespionage betreiben und die entwendeten Daten für den innerdeutschen Geheimdienst unsichtbar aus Deutschland heraus transferieren. Eigentlich müsste dies ein Anreiz für die Unternehmen sein, ihre eingesetzten Chiffrierverfahren noch zu verstärken. „Das Militär hat die Angewohnheit, andere zu beschuldigen, Fähigkeiten zu besitzen, die sie selbst schon lang im Griff haben“, sagt Rosalie Bertell in „Planet Erde: Die neuste Kriegswaffe“ dazu, ein Zitat, welches keiner weiteren Erläuterung bedarf. Vielleicht sollte man dennoch erwähnen, dass auch andere Staaten wie die USA oder Großbritannien ein Verbot von Kryptographie bewogen haben, allerdings zu dem Entschluss gekommen sind, dies dann doch zu unterlassen, vergleiche [2].

Das wohl stärkste Argument gegen Kryptographie ist aber bis zu diesem Punkt noch gar nicht

genannt worden. Seit den Anschlägen vom 11. September 2001 hält sich hartknäckig die These, starke Verschlüsselung sei DAS Instrument für Terroristen, um deren Angriffe zu planen und geheim zu halten. Mit dieser Aussage wird jeder Entwickler von starken Chiffrierverfahren indirekt zum Mitschuldigen abgestempelt. Auf keinen Fall lässt sich abstreiten, dass starke Kryptographie die Planung von Terroraktionen erheblich erleichtern kann, falls diese fachgerecht eingesetzt wird. Selbst das CIA ist gegen heutige Algorithmen offensichtlich machtlos und vermag nicht, diese zu brechen. Allerdings würde ein Verbot von Kryptographie aus diesem Grunde absolut nichts nützen. Eine Strafandrohung ist nur dann wirksam, wenn sie höher ist als das Delikt, was verschleiert werden soll. Wer einen Massenmord begehen möchte und eine todsichere Möglichkeit hat, diesen zu vertuschen, wird diese nutzen, auch wenn er dafür eventuell ein Bußgeld zahlen müsste, wenn er dabei erwischt werden würde. Ein Terrorist würde sich des Weiteren sowieso nicht an irgendein Verbot halten. Wäre dem so, hätte kein einziger Anschlag stattgefunden, da diese bekanntlich auch unter Strafe stehen. Das Wegschließen von jeglicher kryptographischer Software, (ein unrealisierbares Unterfangen), stellt kein Hindernis für jemanden dar, der selbst über ein ausreichendes Budget verfügt.

Der einzige, welcher von dieser Regelung betroffen werden würde, wäre einmal wieder der normale Bürger, für den ein Chiffrierverbot einen starken Eingriff in seine Bürgerrechte und Verbraucherinteressen bedeuten würde. Es ist daher zu überlegen, ob die terroristische Bedrohung wirklich so groß ist, dass alle Mitglieder der Gesellschaft ihre Privatsphäre aufgeben sollten.

Fast jede Erfindung der Menschen hat ihre Sonnen- und Schattenseiten. So wurden bedeutende Entdeckungen in der Chemie (Sprengstoff), Pflanzenheilkunde (Gifte), Physik (Kernspaltung), Automobilindustrie (Panzer) und Metallindustrie (Waffenproduktion) für verwerfliche Ziele missbraucht. Selbst ein einfaches Teppichmesser kann als Mordwaffe genutzt werden. Dennoch würde niemand auf die Idee kommen, alle Teppichmesser oder Flugzeuge verbieten zu wollen. Das Problem der Kryptographie ist lediglich, dass sie sich noch nicht über tausende von Jahren als selbstverständlicher Gebrauchsgegenstand etablieren konnte.

Kryptographie ist definitiv nicht die Ursache von Verbrechen. Die Beweggründe der Terroristen hatten absolut nichts mit Verschlüsselungsverfahren zu tun. Solange genügend Anreize und Ursachen für kriminelle Handlungen existieren, wird sich die Kriminalität immer einen Weg suchen, ihre Ziele zu verwirklichen, mit welchen Mitteln auch immer.

Ein Verbot von starker Kryptographie aus gesellschaftlich moralischer Betrachtungsweise würde, meiner Meinung nach, mehr Schaden als Nutzen verursachen, da die damit assoziierten Ziele nicht erfüllt werden könnten. Die entstehenden Nachteile wiederum würden sowohl den Wirtschaftsstandort Deutschland als auch die Bürger- und Datenschutzrechte des Einzelnen erheblich schwächen, vergleiche [4].

Technische Aspekte

Wie bereits im vorherigen Abschnitt angesprochen, ist es ein großes Defizit, dass viele Politiker nicht das nötige Fachwissen haben, um die Konsequenzen ihrer Forderungen zu durchschauen. Mit dem Verbot starker Kryptographie erhofft man sich unter anderem, dass „Transparenz und Ordnung“ in das „chaotische“ Internet wieder einziehen, da das Netz endlich wieder bis in den letzten Winkel „durchleuchtet“ werden kann, vergleiche [12]. Mit der Abschaffung von Verschlüsselungsverfahren will man die Reinigung des Internets von sämtlichen kriminellen Inhalten bewirken. Wer nach dieser Regelung noch verschlüsselt, wird für sein Vergehen bestraft. Kryptographie sei schließlich nur eine Domäne von Nachrichtendiensten.

Diese populistische Forderung lässt sich schon rein technisch absolut nicht durchsetzen. Die Datenflut, welche täglich durch das Internet transferiert wird, ist so groß, dass noch nicht einmal bei einem kleinen Bruchteil überprüft werden könnte, ob diese Daten chiffriert wurden, vergleiche [8]. Zudem ist es fast unmöglich herauszufinden, ob eine Nachricht verschlüsselt wurde oder nicht. Eine Nachricht könnte beispielsweise mit unterschiedlichen Chiffrialgorithmen mehrfach verschlüsselt oder vorher komprimiert worden sein. Viele Verfahren bieten weiterhin den Modus einer variablen Rundenanzahl. Kennt man diese nicht, nützt einem selbst der korrekte Schlüssel kaum etwas, vergleiche [11].

Des Weiteren werden nur die wenigsten Daten, die geheim bleiben sollen, verschlüsselt

weitergeleitet. Dies wäre in vielen Fällen viel zu kompliziert und rechenintensiv. Stattdessen stützt man sich auf steganographische Algorithmen. Hierbei werden Daten in Bildern, Videos, Musik- oder selbst Textdateien integriert, wobei sich bei diesen keine sichtbaren bzw. hörbaren Veränderungen ergeben. Beim Kommunikationspartner angekommen, kann dieser die Daten aus dem harmlosen Informationsträger (z.B. Foto von der letzten Grillparty) mühelos und verlustfrei wieder herausextrahieren. Auch steganographische Softwareprodukte sind so konfigurierbar, dass nicht ohne weiteres herauszubekommen ist, ob Daten versteckt wurden. Eine (erfolglose) Suche nach allen verschlüsselten Inhalten des Datenverkehrs würde folglich keinen großen Fahndungserfolg mit sich bringen.

Viele Kritiker haben dies erkannt und fordern deshalb „lediglich“ den Verzicht auf Verschlüsselungsverfahren, welche mit riesigen Schlüssellängen operieren. Diese wären für den Privat- und Firmengebrauch absolut überdimensioniert und bräuchten deshalb auch nicht legalisiert zu werden. Auf diese Weise hätte man gleichzeitig ausreichende Sicherheit und vertretbare Rechenzeiten für die Verschlüsselungsalgorithmen (je länger der Schlüssel, desto länger benötigt der Algorithmus) erreicht. Je länger ein Schlüssel ist, desto höher ist der Rechenaufwand, um die Nachricht dechiffrieren zu können. Bei Geheimnissen, welche über 50 Jahre garantiert Geheimnisse bleiben sollen, zum Beispiel intime personenbezogene Daten, wie sie jeder Bürger besitzt, ist demzufolge ein entsprechend langer, „überdimensionierter“ Schlüssel zu benutzen, da die Rechentechnik und die Kryptoanalyse in 50 Jahren vermutlich wesentlich weiter sein wird, als dies heute der Fall ist, vergleiche [11]. Die Entwicklung von Quantencomputern, würde beispielsweise die mühelose Dechiffrierung von heute noch „angemessen“ verschlüsselten Informationen ermöglichen und könnte damit zu einem „Krypto-GAU“ führen, falls man die Benutzer von schwacher Kryptiersoftware weiter in falscher Sicherheit wägt.

Bruce Schneier, ein anerkannter Kryptographieexperte, meint, es gäbe nur 2 Arten von Kryptographie. Die eine hält die kleine Schwester von den Daten fern, die andere selbst große Regierungen, vergleiche [11]. Mit kleinen Schlüssellängen kann man nur die kleine Schwester fernhalten. Der beste Chiffrieralgorithmus ist nichts wert, wenn der Schlüssel nicht lang genug gewählt wurde. Die Entschlüsselung einer mit 56 BIT Schlüssellänge verschlüsselten Nachricht (auf vielen Systemen heute noch gebräuchlich) dauert bei einer Investition von 10 Millionen Euro in eine Rechenanlage weniger als 10 Minuten, eben da [11]. Dieses Computersystem könnte also mehr als 6 dieser Nachrichten pro Stunde „knacken“. 10 Millionen Euro sind ein Betrag, den sich viele Firmen und einige Privatpersonen als einmalige Investition durchaus leisten könnten, ganz zu schweigen von großen Regierungen. Investiert man noch mehr Geld, ist die Dechiffrierung auch in Bruchteilen von Sekunden zu schaffen, wenn von „vernünftigen“ Schlüssellängen ausgegangen wird.

Wenn nur die Verschlüsselung mit kurzen Schlüssellängen erlaubt wäre, wäre dies ein lohnendes Geschäft für jeden Industriespion oder Großkonzerne, die gezielt ihre Kundendatei um einige Details anreichern wollten. Im gleichen Maße würden sich ausländische Unternehmen oder Firmen mit Filialen im Ausland aus Deutschland zurückziehen, da sie hier nicht mehr sicher operieren könnten; Deutschland wäre kein vertrauenswürdiger Investitionsstandort mehr, siehe auch [4].

Weiterhin könnten deutsche Softwarefirmen ihre kryptographischen Produkte nicht mehr im Ausland verkaufen, da dort keine Schlüssellängenbeschränkung vorliegt.

Eine weiter häufig vorgeschlagene Lösung in der Kryptodebatte ist das „Key Escrow Center“. Bei dieser Regelung ist es jedem Bürger gestattet, beliebig starke Verschlüsselungsverfahren zu benutzen. Allerdings muss er bei den Behörden für jede seiner Aktionen einen „Nachschlüssel“ hinterlegen. Somit wäre dem Staat die Möglichkeit gegeben, jeglichen Datenverkehr bequem zu kontrollieren und andererseits könnten die Daten von Dritten nicht dechiffriert werden.

Das theoretische Modell eines Key Escrows ist wahrscheinlich gar nicht so ein schlechter Einfall. Aus diesem Grunde haben sich namhafte Expertenkomitees aus der USA, vergleiche [5] und Gruppen aus Deutschland (z.B. CCC), vergleiche [8] intensivst mit der praktischen Realisierung befasst. Die Ergebnisse sind allerdings alle sehr entmutigend und lehnen ein Key Escrow Center strikt ab. Nach der Einschätzung sämtlicher beteiligter Wissenschaftler ist ein Key Escrow Center im großen Rahmen sowohl kosten- als auch sicherheitstechnisch eine Katastrophe.

Da bei einem solchen Modell beispielsweise noch menschliche Eingriffe notwendig wären (z.B.

Administratoren, Wartungspersonal, Key Account Manager, Behörden, etc...), wäre die Gefahr, dass gespeicherte Daten für sachfremde Zwecke genutzt werden würden, viel zu hoch. Um sämtliche Nachschlüssel und Daten speichern zu können, käme ein unbezahlbarer Kostenberg auf Deutschland zu. Des Weiteren würde die Nachschlüsselverwaltung zum begehrtesten Ziel und Sammelpunkt sämtlicher Hacker und Cracker werden. Gelänge es auch nur einem, in dieses System einzudringen, oder ließe sich jemand in der Behörde bestechen oder erpressen, hätte die unabsehbare Folgen für die Sicherheit und Integrität der gespeicherten Daten. Kriminalität und Manipulation wären nicht mehr einzudämmen, eben da [8] und [5]. Dies sind nur wenige Punkte, welche die Experten gegen Key Escrow Center anführten.

Zusammenfassend konnte mich weder ein Totalverbot von Chiffrierverfahren, noch die Beschränkung der Schlüssellängen oder die Einführung eines bundesweiten Key Escrow Centers vom technischen Standpunkt aus überzeugen.

Fazit

Nachdem ich mich in den beiden vorigen Teilkapiteln ausführlich mit den technischen und gesellschaftlich moralischen Aspekten der Kryptodebatte auseinandergesetzt hatten, konnte ich persönlich keinen zwingenden Grund dafür finden, starke Kryptographie verbieten zu lassen. Ich sehe starke Verschlüsselung als legitimes Mittel an, die Datenschutzinteressen der Bürger und der Wirtschaft zu wahren. Das Hauptproblem der Kritiker besteht meiner Meinung nach darin, dass sich diese offensichtlich noch nicht im Klaren sind, dass ein Verbot von starker Chiffrierung nicht die Probleme lösen kann, welche sie mit dem Einsatz von Kryptographie in Verbindung bringen. Die Nebenwirkungen eines Verbotes wären allerdings verheerend, sowohl für die deutsche Wirtschaft als auch für das deutsche Demokratieverständnis und die Selbstkompetenz der Bürger, siehe auch [7].

Quellenverzeichnis / weiterführende Literatur

- [1] Autorenkollektiv: „BSI-Kurzinformationen zu aktuellen Themen der IT-Sicherheit "Sicherheit durch Verschlüsselung"", 1.01.2001, <http://www.bsi.bund.de/literat/faltbl/siverchl.htm>
- [2] Autorenkollektiv: „Civil Rights Organisations Support Strong Encryption Policy in Germany“, 9.05.1997, http://www.cpsr.org/cpsr/nii/cyber-rights/web/crypto_german_deutsch.html
- [3] Autorenkollektiv: „c't Linksammlung zur Kryptodebatte“, <http://www.heise.de/ct/pgpCA/krypto.shtml>
- [4] Autorenkollektiv: „Forschung: Vor Schaden durch Kryptogesetz gewarnt“, Deutscher Bundestag Heft 9/21.05.97, <http://www.iks-jena.de/mitarb/lutz/security/cryptoban/19970521.wib.html>
- [5] Autorenkollektiv (Abelson, Hal et. al.): „The Risks of Key Recovery, Key Escrow & Trusted Third Party Encryption“, report 1998, <http://www.cdt.org/crypto/risks98/>
- [6] Autorenkollektiv: „CeBIT 2005: Mittelstand soll Kernthema der Computermesse werden“, Heise Online 11.01.2005, <http://www.heise.de/newsticker/meldung/55000>
- [7] Bäumler, Helmut: „Thesen des schleswig-holsteinischen Datenschutzbeauftragten Dr. Helmut Bäumler zum Verbot oder zur Einschränkung von Verschlüsselungsverfahren“, 27. 02. 1997, <http://www.heise.de/ct/97/04/234/thesen.shtml>
- [8] Huhn, Michaela; Pfitzmann, Andreas: „Technische Randbedingungen jeder Kryptoregulierung“, 12. Chaos Communication Congress '95, <http://www.foebud.org/texte/ccc/ccc95/div/pfitz/krypto.htm>
- [9] Koch, Alexander; Neumann, Andreas: „The German Cyberlaw Project“, <http://www.Mathematik.Uni-Marburg.de/~cyberlaw/>
- [10] Reichelt, Nicolas: „Nicolas Reichelts Kryptographie - Seite“, <http://www.crypto.de>
- [11] Schneier, Bruce: „Angewandte Kryptographie“, 1996, Addison Wesley, Bonn
- [12] Schulzki-Haddouti, Christiane: „Kanthers Kurs auf das Kryptoverbot“, 21.03.1997, http://www.heise.de/bin/tp/issue/dl-artikel.cgi?artikelNr=1146&rub_ordner=inhalt&mode=html
- [13] Zarzer, Brigitte: „AN.ON. - Anonymität Online“, 21.08.2002, <http://www.heise.de/tp/deutsch/inhalt/co/13120/1.html>