Bericht

der Bundesregierung

zu den Auswirkungen der Nutzung kryptografischer Verfahren auf die Arbeit der Strafverfolgungs- und Sicherheitsbehörden (Ziffer 4 der Eckpunkte der deutschen Kryptopolitik vom 2. Juni 1999)

„Verschlüsselungsbericht“

1. Auftrag:

Die Bundesregierung hat mit Beschluss vom 2. Juni 1999 die deutsche Haltung zur Nutzung kryptografischer Verfahren (sog. Eckpunkte der deutschen Kryptopolitik) bestimmt. Sie hat entschieden, dass Verschlüsselungsverfahren und –produkte ohne Restriktionen entwickelt, hergestellt, vermarktet und genutzt werden dürfen. Sie hat ihren Willen bekräftigt, die Verbreitung sicherer kryptografischer Verfahren in Deutschland voranzutreiben, um den Schutz deutscher Nutzer in den weltweiten Informationsnetzen zu verbessern.

In den Eckpunkten der Kryptopolitik hat die Bundesregierung den Umstand mit berücksichtigt, dass die Strafverfolgungs- und Sicherheitsbehörden durch eine zunehmende Nutzung der Verschlüsselung durch kriminelle Kreise verstärkt vor Probleme gestellt sein könnten. Aus Aktualitätsgründen sind in die Betrachtungen der Bundesregierung zur Verschlüsselung die Folgen der Terroranschläge am 11. September 2001 in New York und Washington mit einzubeziehen. Der vorliegende Bericht setzt sich deshalb auch mit der Frage auseinander, inwieweit der Einsatz von Verschlüsselung durch terroristische Attentäter die Strafverfolgungs- und Sicherheitsbehörden vor Probleme stellen könnte.

Unabhängig davon, ob der Einsatz der Verschlüsselung einen allgemein kriminellen oder terroristischen Hintergrund hat, ist in jedem Fall sicherzustellen, dass rechtmäßig angeordnete staatliche Überwachungsmaßnahmen ihre Wirksamkeit uneingeschränkt behalten, auch wenn die Zielperson einer

Überwachungsmaßnahme die fraglichen Informationen durch Verschlüsselung schützt.

Ein Eckpunkt der Kryptopolitik (Ziffer 4) bestimmt daher: „Durch die Verbreitung starker Verschlüsselungsverfahren dürfen die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden zur Telekommunikationsüberwachung nicht ausgehöhlt werden. Die zuständigen Bundesministerien werden deshalb die Entwicklung weiterhin aufmerksam beobachten und nach Ablauf von zwei Jahren hierzu berichten."

2. Ist-Zustand

Gegenstand des vorliegenden Verschlüsselungsberichts ist die Beobachtung der Entwicklung, Verbreitung und Nutzung von (starken) Verschlüsselungsverfahren in Deutschland, die die Strafverfolgungs- und Sicherheitsbehörden in der Wahrnehmung ihrer gesetzlichen Aufgaben – insbesondere im Zusammenhang mit der Telekommunikationsüberwachung - beeinträchtigen können.

Starke Verschlüsselungsverfahren und –algorithmen können heute in allen Bereichen der Tele- und Datenkommunikationstechnologie Anwendung finden. Zur besseren Übersicht ist dabei die Verschlüsselung im Bereich der

- **Telekommunikation** (z.B. Telefon, Telefax, Mobilfunktelefone, SMS, Anrufbeantworter etc.),
- **Datenspeicherung** (z.B. Organizer, kryptierte Festplatten, Disketten, Magnetbänder, Speicherbausteine) und
- **Datenübertragung** (z.B. Internet-Telefonie, E-Mail, etc.)

zu unterscheiden.

Dies verdeutlicht, dass die Strafverfolgungs- und Sicherheitsbehörden sich mit Verschlüsselung nicht nur im Bereich der Telekommunikationsüberwachung[1] auseinandersetzen müssen. Die technische Komplexität der Tele- und

[1] gesetzliche Ermächtigung: Art. 10 - Gesetz (G 10); §§ 100a, b StPO und § 39 Außenwirtschaftsgesetz

Datenkommunikationstechnik erfordert die ständige Fortentwicklung der technischen Kompetenz und Instrumente sowohl bei den Netzbetreibern als auch bei den zuständigen Behörden. Die zuständigen Behörden können hierbei, abhängig von ihrer technischen Kompetenz, verschlüsselte Daten zu analysieren und zielgerichtet auszuwerten, unterschiedlich betroffen sein.

Um die Beobachtung der Entwicklung, Verbreitung und Nutzung starker Verschlüsselung sicher zu stellen, wurde im Jahr 1999 auf fachlicher Ebene der Arbeitskreis „Innere Sicherheit und Verschlüsselung“ eingerichtet, in dem das Bundesministerium des Innern, das Bundeskriminalamt, das Bundesamt für Verfassungsschutz, der Generalbundesanwalt, das Zollkriminalamt sowie geschäftsführend das Bundesamt für Sicherheit in der Informationstechnik (BSI) vertreten sind.

Die am Arbeitskreis beteiligten Behörden haben ein dezentrales Meldewesen vereinbart, d.h. alle für die Telekommunikationsüberwachung zuständigen Behörden aus Bund und Ländern sollen dem BSI über den Einsatz von Verschlüsselung bei TÜ-Maßnahmen (Telefonüberwachungs-Maßnahmen) und im Rahmen von Ermittlungsverfahren berichten. Das BSI, das die zuständigen Behörden bei der Entschlüsselung auf Antrag unterstützt, führt eine Statistik[2] über die gemeldeten Verschlüsselungsfälle. Dem BSI liegen hierbei keine Erkenntnisse darüber vor, inwieweit die Verschlüsselung bzw. die Dechiffrierung Auswirkungen auf die Ergebnisse der TÜ-Maßnahme oder das Ermittlungsverfahrens gehabt haben. Es ist gewährleistet, dass das BSI keinerlei Kenntnis von den Inhalten erhält.

a. Die Auswertung der Verschlüsselungsfälle bei den Strafverfolgungs- und Sicherheitsbehörden seit dem Kabinettbeschluss vom 2. Juni 1999 bis Ende Juni 2001 (im Folgenden: Berichtszeitraum) ergab folgendes Bild:

a.a Bundeskriminalamt:

Telekommunikation: In 4 Fällen waren Daten im Telefonregister chiffriert abgelegt. Die dazu gehörigen Rufnummern gehörten nicht deutschen Netzbetreibern – also

[2] Die Statistik ist VS-Vertraulich eingestuft und kann daher diesem Bericht nicht beigefügt werden.

außerhalb des Geltungsbereichs der StPO - und konnten daher nicht verifiziert werden.

Datenspeicherung: Im Berichtszeitraum wurden 16 Personalcomputer beschlagnahmt, auf denen Daten kryptiert abgelegt wurden. In allen Fällen ist es gelungen, die Chiffriermethode zu analysieren; zehn Fälle wurden bislang entschlüsselt. In einem Fall handelte es sich um einen verschlüsselten Organizer, dessen Verschlüsselung auch gelöst werden konnte.

Datenübertragung: Bezüglich der kryptierten Datenübertragung liegen keine Erkenntnisse vor. Es kamen lediglich Personalcomputer mit Modem oder Modemkarte zur Auswertung, die Programme beinhalteten, die zur kryptierten Datenfernübertragung geeignet waren. In einem Fall war eine mit einem entschlüsselungsresistenten Verfahren kryptierte E-Mail Gegenstand des Verfahrens.

a.b. Bundesamt für Verfassungsschutz

Telekommunikation: Keine Fälle
Datenspeicherung: Entfällt
Datenübertragung: Im Berichtszeitraum wurden 6 Fälle bearbeitet, bei denen Daten verschlüsselt übertragen worden sind.

a.c Zollkriminalamt

Im Berichtszeitraum sind weder bei der Telekommunikation noch bei der Datenspeicherung und Datenübertragung Verschlüsselungsfälle aufgetreten.

a.d Bundesgrenzschutz

Telekommunikation: Keine Fälle
Datenspeicherung: Ca. 2 % bei untersuchten Mobiltelefonen, keine bei Datenträgern von Personalcomputern und Laptops.
Datenübertragung: Keine Fälle

a.e Bundesländer

Die Strafverfolgungsbehörden der Länder haben auf der Sitzung der AG Kripo am 14./15. März 2001 die in ihrem Zuständigkeitsbereich aufgetretenen Verschlüsselungsfälle mitgeteilt:

Die Landeskriminalämter Baden-Württemberg, Berlin, Bremen, Sachsen, Sachsen-Anhalt und Schleswig-Holstein meldeten Fehlanzeige.

Die Meldungen der Landeskriminalämter Bayern, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz und Thüringen lassen sich wie folgt zusammenfassen: die Feststellung des Einsatzes von Kryptoprodukten durch Straftäter ist derzeit noch als Ausnahme zu betrachten. Das Bayerische Landeskriminalamt geht von 1 % und das Landeskriminalamt Nordrhein-Westfalen von 6 % auf die Gesamtzahl der Verschlüsselungsfälle gesehen aus, bei denen Kryptografie durch kriminelle Kreise eingesetzt wird. Die Landeskriminalämter Brandenburg, Hamburg und Saarland haben nicht gemeldet.

b. Die Auswertung der Verschlüsselungsfälle, die die Strafverfolgungs- und Sicherheitsbehörden dem BSI zur Dechiffrierung und Auswertung übersandt haben[3], ergab für den Berichtszeitraum folgendes Bild:

Im BSI wurden im Berichtszeitraum insgesamt 99 Verschlüsselungsfälle bearbeitet. In 8 Fällen waren die zugrundeliegenden Verschlüsselungsverfahren unlösbar bzw. die Lösung wurde nach dem heutigen Stand der Technik als unwirtschaftlich angesehen.

Neben den Fallzahlen ließen sich für den Berichtszeitraum die folgenden zusätzlichen Erkenntnisse gewinnen:

Im Bereich der Telekommunikation, insbesondere über Telefon (Festnetz) und Telefax wird bisher wenig verschlüsselt kommuniziert. Die Tätigkeit der

[3] Hierzu sei angemerkt, dass es sich hier nicht um neue – über die in Ziffer 2 genannten hinausgehende – Verschlüsselungsfälle handeln muss. Außer Betracht bleiben auch Verschlüsselungsfälle, die von den technischen Abteilungen der zuständigen Behörden - ohne Beteiligung des BSI - bearbeitet wurden.

Strafverfolgungs- und Sicherheitsbehörden ist hierdurch derzeit nur unwesentlich tangiert.

Die technische Entwicklung wird dadurch gekennzeichnet sein, dass mehr und mehr Mobiltelefone, die über eine (starke) Ende-zu-Ende-Verschlüsselung[4] verfügen, auf den Markt kommen. Auch international entwickelt sich die Nachfrage nach „Krypto-Handys". Der gegenwärtig (hohe) Anschaffungspreis (ca. 6.000 DM) wird die Verbreitung des Krypto-Handys allerdings zunächst bremsen. Nach Aussage des BSI, gibt es gegenwärtig keine Überwachungsmöglichkeiten durch die zuständigen Strafverfolgungs- und Sicherheitsbehörden.

Im Bereich der Datenspeicherung und Datenübertragung wurde die Verwendung der Verschlüsselungsmöglichkeiten beobachtet, die in Textverarbeitungs- und Tabellenkalkulationsprogrammen zur Verfügung stehen. In diesen Fällen konnten die Daten in der Regel lesbar gemacht werden. Ebenfalls wurden entschlüsselungsresistente Produkte (nach bisher vorliegenden Erkenntnissen) zur Verschlüsselung von Festplatten eingesetzt. Eine Dechiffrierung war ausschließlich auf Grund der freiwilligen Herausgabe der Passwörter möglich. Die Nutzung der Internet-Telefonie („Voice over IP") und der Steganografie[5] zur chiffrierten Datenübertragung kann – wegen der bisher geringen Verbreitung dieser Technik - noch nicht abschließend beurteilt werden.

Hinsichtlich der Zahl der Verschlüsselungsfälle und deren Auswirkungen auf die TÜ-Maßnahmen bzw. den Ermittlungsverfahren geht der Arbeitskreis „Innere Sicherheit und Verschlüsselung" von einem relativ großen Dunkelfeld aus. Dies hat mehrere Ursachen:

[4] Verschlüsselungstechnik wird nicht vom Netzbetreiber zur Verfügung gestellt, sondern ist bereits in den Endgeräten (z.B. Mobiltelefon) selbst installiert.
[5] Steganografie: Verfahren, bei dem eine Botschaft in einem scheinbaren Klartext, wie z.B. einer Bild- oder Tondatei versteckt wird.

- Aufgrund des „dezentralen Meldesystems“ im Bereich der Polizeien lässt sich eine verlässliche Aussage über die Gesamtzahl der bearbeiteten Verschlüsselungsfälle durch eine Abfrage des Bundeskriminalamts und der Landeskriminalämter nicht treffen. Hinzu kommt, dass z.B. bei verschlüsselten E-Mails aus wirtschaftlichen und logistischen Gründen in bis zu 95 % der Fälle von einer Auswertung abgesehen wurde. Dies hat zur Folge, dass nur ein Bruchteil der Verschlüsselungsfälle beim BSI zur Entschlüsselung gelangen. Außerdem nehmen die Sachbearbeiter in den Dienststellen häufig zu Unrecht an, dass die beschlagnahmten, verschlüsselten Daten vom BSI nicht lesbar gemacht werden können und geben diese Fälle auch aus diesem Grund nicht weiter.

- Das Dunkelfeld ist auch darin begründet, dass es auf Grund der vielen unterschiedlichen Datenformate und Software-Versionen zunehmend anspruchsvoller wird, die mitprotokollierten Datenströme zu erkennen und richtig zuzuordnen (sog. Signal- und Protokollerkennung).

- Es liegt kein rechtstatsächliches Material darüber vor, inwieweit Verschlüsselung in Wirtschaft und Verwaltung überhaupt eingesetzt wird. Somit ist es für die Behörden nicht feststellbar, zu welchem Prozentanteil - im Vergleich zum Gesamtaufkommen - Verschlüsselung überhaupt und zu welchem Prozentanteil von kriminellen Kreisen genutzt wird.

3. Ergebnis

Die Strafverfolgungs- und Sicherheitsbehörden sind gegenwärtig in der Wahrnehmung ihrer gesetzlichen Aufgaben durch Verschlüsselung der Tele- und/oder Datenkommunikation noch nicht (nachhaltig) beeinträchtigt. Dasselbe gilt im Hinblick auf die Verfolgung von Straftaten mit terroristischem Hintergrund.

4. Trendanalyse – künftige Entwicklungen der Verbreitung und Nutzung von Verschlüsselungsverfahren

Es ist allerdings zu erwarten, dass in den nächsten zwei bis drei Jahren der Einsatz von Verschlüsselung stark zunehmen wird. Dies hat folgende Gründe:

- Im Rahmen der Schaffung von vertrauenswürdigen Public Key Infrastrukturen ist in den nächsten Jahren auf breiter Ebene der Einsatz von Verschlüsselung in Verwaltung und Wirtschaft vorgesehen.
- Künftig wird „Office"-Software (also Textverarbeitung, Tabellenkalkulation, Datenbanken) standardmäßig Kryptofunktionen enthalten, die es dem Nutzer ohne besonderen Implementierungs- und Administrationsaufwand gestatten, gespeicherte oder per Mail zu versendende Daten mit starken Verschlüsselungsverfahren zu schützen. Diese Tendenz wird dadurch weiter gefördert, dass die US-Regierung Exportrestriktionen für Standard-PC-Software mit starker Kryptografie in Staaten wie die Bundesrepublik Deutschland faktisch aufgehoben hat und dieser Markt weitestgehend von US-amerikanischen Firmen beherrscht wird. In diesem Zusammenhang sei auf die Verabschiedung des US-Federal-Krypto-Standards „Advanced Encryption Standard", d.h. die Standardisierung eines Kryptoverfahrens ohne irgend eine erkennbare Entzifferungsmöglichkeit, hingewiesen.
- Wie oben bereits erwähnt, ist weltweit ein nahezu vollständiger Abbau der bisher gepflegten Exportrestriktionen auf dem Kryptosektor zu beobachten. Dies wird zu einer erhöhten Verfügbarkeit von derartigen Produkten auf dem deutschen Markt führen. Selbst wenn im Einzelfall deren Sicherheit nicht übermäßig hoch sein sollte, kann daraus kaum eine Chance für Strafverfolgungsbehörden abgeleitet werden, da regelmäßig nicht erwartet werden kann, dass die Herstellerfirmen die notwendigen Informationen über die Detailgestaltung solcher Produkte preisgeben werden.
- Nach dem Muster von „Pretty Good Privacy (PGP)" werden auch künftig starke Verschlüsselungsmechanismen frei abrufbar im Internet zur Verfügung stehen. Deren Implementierung auf dem häuslichen PC wird auch für potentielle Straftäter

- angesichts immer weiter verbreiteter Kenntnisse über PC-Einsatz und Internet-Nutzung - kein größeres Problem darstellen.

- Selbst die eigene Erstellung von Kryptosoftware auf einem PC ist für Personen mit Grundkenntnissen in Informatik keine besondere Schwierigkeit: die zu implementierenden mathematischen Algorithmen, wie etwa der Advanced Encryption Standard (s.o.) oder ein Public-Key-Verfahren zur Schlüsselverteilung, liegen dokumentiert und für jedermann zugänglich vor.
- Neben dem zu erwartenden verstärkten Einsatz von Kryptografie im Office-Bereich sind für den Sektor Sprachkommunikation Mobiltelefone mit integrierter Ende-zu-Ende-Verschlüsselung (siehe auch oben 2. b) als potentielle Gefährdung von Überwachungsmaßnahmen zu betrachten. Während der Einsatz von Sprachverschlüsselungssystemen als Zusatz zu Festnetzgeräten im privaten Bereich (auch wegen der damit verbundenen Auffälligkeit) eher die Ausnahme bleiben wird, werden „Krypto-Handys“ mit fallenden Preisen zunehmend attraktiv, zumal sie äußerlich kaum von normalen Geräten zu unterscheiden sind. Auch hier ist mit einem verstärkten Produktangebot in- und ausländischer Hersteller zu rechnen.

5. Vorbereitung der zuständigen Behörden auf künftige Entwicklungen

Die Strafverfolgungs- und Sicherheitsbehörden müssen künftig über ein deutlich breiteres Spektrum an Überwachungstechnik und an Technik zur Analyse von Verschlüsselung verfügen, da die Vielfalt der Tele- und Datenkommunikationsdienstleistungen und somit das Angebot für den Nutzer deutlich zugenommen hat. Erschwerend kommt hinzu, dass es bei der derzeitigen technischen Entwicklung nicht ausreichen wird, die vorhandene Überwachungstechnik lediglich zu ergänzen oder aufzurüsten. Neue Forschungen und Entwicklungen sind wegen des technischen Fortschritts notwendig.

In Anbetracht des aufgezeigten Ist-Zustandes und der Trends zur Verschlüsselung lassen sich für die zuständigen Behörden Handlungsfelder abstecken, um sachgerecht auf die künftigen Entwicklungen reagieren zu können.

a. Es muss darauf hingewirkt werden, dass die zuständigen Polizeibehörden im Rahmen des kriminalpolizeilichen Informations- und Kommunikationstechnologie-Meldedienstes (IuK-Meldedienst) und gegenüber dem BSI ihr Meldeverhalten verbessern. Dies gilt entsprechend für die Verfassungsschutzbehörden.
b. Die Fähigkeiten des BSI, die Strafverfolgungs- und Sicherheitsbehörden im Rahmen seines gesetzlichen Auftrages zu beraten und zu unterstützen, sollten gestärkt werden. Dies betrifft insbesondere die Unterstützung bei technischen Entwicklungen zur Signal- und Protokollerkennung.
c. Die Kompetenz und technische Ausstattung der zuständigen Behörden ist kontinuierlich und zeitgerecht zu verbessern, um Forschungs-, Entwicklungs- und Kompetenzlücken hinsichtlich neuer Tele- und Datenkommunikationstechnologien und der Überwachungstechnik zu vermeiden.
d. Aus kriminalpräventiven Gründen sollte eine Studie erstellt werden, die den Strafverfolgungs- und Sicherheitsbehörden als Entscheidungsgrundlage dienen kann, um die notwendigen technischen Entwicklungen zielgerichtet anstoßen zu können. Die Studie sollte u.a. auf die Entwicklung des Einsatzes von Krypto-Mobiltelefonen und von Internet-Telefonie (Voice over IP) sowie möglicher Umgehungsstrategien, wie z.B. der Nutzung von Steganografie, eingehen.

6. Beobachtung der internationalen Entwicklung

Das Thema Verschlüsselung spielt auch auf internationaler Ebene eine wichtige Rolle. Dieses gilt insbesondere auch vor dem Hintergrund der terroristischen Anschläge am 11.September 2001. Datennetze bieten auch Terroristen ein neues Betätigungsfeld, insbesondere als Mittel zur Kommunikation. Die Verschlüsselung bringt auch insoweit neue und schwierige Herausforderungen für die Strafverfolgungs- und Sicherheitsbehörden mit sich. Die Bundesregierung wird die internationale Entwicklung in diesem Bereich daher aufmerksam beobachten.

Eckpunkte der deutschen Kryptopolitik

Das Bundeskabinett hat in seiner Sitzung vom 2. Juni 1999 die deutsche Haltung zur Frage der Nutzung kryptographischer Verfahren beim Einsatz im elektronischen Geschäftsverkehr in Form von "Eckpunkten der deutschen Kryptopolitik" entschieden.

Eckpunkte der deutschen Kryptopolitik

Auf der Grundlage der bisherigen nationalen Diskussion sowie der internationalen Entwicklung beschließt die Bundesregierung die folgenden **Eckpunkte** ihrer **Kryptopolitik**:

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 Unternehmensgeheimnissen. Die Bundesregierung wird deshalb die Verbreitung sicherer Verschlüsselung in Deutschland aktiv unterstützten. Dazu zählt insbesondere die Förderung des Sicherheitsbewußtseins bei den Bürgern, der Wirtschaft und der Verwaltung.

2. Die Bundesregierung strebt an, das Vertrauen der Nutzer in die Sicherheit der Verschlüsselung zu stärken. Sie wird deshalb Maßnahmen ergreifen, um einen Vertrauensrahmen für sichere Verschlüsselung zu schaffen, insbesondere indem sie die Überprüfbarkeit von Verschlüsselungsprodukten auf ihre Sicherheitsfunktionen verbessert und die Nutzung geprüfter Produkte empfiehlt.

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. Sie wird Maßnahmen ergreifen, um die internationale Wettbewerbsfähigkeit dieses Sektors zu stärken.

4. Durch die Verbreitung starker Verschlüsselungsverfahren dürfen die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden zur Telekommunikationsüberwachung nicht ausgehöhlt werden. Die zuständigen Bundesministerien werden deshalb die Entwicklung weiterhin aufmerksam beobachten und nach Ablauf von zwei Jahren hierzu berichten. Unabhängig hiervon setzt sich die Bundesregierung im Rahmen ihrer Möglichkeiten für die Verbesserung der technischen Kompetenzen der Strafverfolgungs- und Sicherheitsbehörden ein.

5. Die Bundesregierung legt großen Wert auf die internationale Zusammenarbeit im Bereich der Verschlüsselungspolitik. Sie tritt ein für am Markt entwickelte offene Standards und interoperable Systeme und wird sich für die Stärkung der multilateralen und bilateralen Zusammenarbeit einsetzen.