Eckwertepapier der Bundesregierung zur Kryptopolitik

Bonn, den 2. Juni 1999

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.

Die Bundesregierung kommt damit der Notwendigkeit nach, im nationalen und internationalen Zusammenhang die deutsche Position in dieser vor allem für den elektronischen Geschäftsverkehr und E-Commerce wichtigen Frage darzulegen. Denn mit dem wachsendem Datenaufkommen in den weltweiten Informationsnetzen nehmen die Sicherheitsprobleme dort erheblich zu. Experten schätzen die Schäden durch das illegale Ausspähen, Manipulieren oder Zerstören von Daten jährlich in Millardenhöhe. Datensicherheit wird also zunehmend zu einem ernstzunehmenden Faktor im globalen Wettbewerb und tangiert damit auch Arbeitsplätze der betroffenen Unternehmen und Wirtschaftsbereiche.

Zentrales Anliegen der Kabinettentscheidung ist der verbesserte Schutz deutscher Nutzer in den weltweiten Informationsnetzen durch Einsatz sicherer kryptographischer Verfahren. Die Entscheidung stellt klar, daß in Deutschland auch künftig Verschlüsselungsverfahren und -produkte ohne Restriktion entwickelt, hergestellt, vermarktet und genutzt werden dürfen. Damit soll die bisher nur geringe Sensibilisierung der Nutzer gefördert werden. Dem dient auch die vom Bundesministerium für Wirtschaft und Technologie und dem Bundesministerium des Innern gemeinsam gestartete Initiative für ”Sicherheit im Internet” (siehe www.sicherheit-im-internet.de).

Ein weiteres wichtiges Ziel der Bundesregierung besteht in der Stärkung der Leistungsfähigkeit und der internationalen Wettbewerbsfähigkeit der deutschen Kryptohersteller, die im Hinblick auf einen wachsenden Nachfragemarkt ihre Anstrengungen intensivieren werden. Dazu dient auch die weitere Öffnung des EU-Binnenmarktes: gemeinsam mit den europäischen Partnern hat die Bundesregierung im Rahmen einer ersten Revision der EG-Dual-Use-Verordnung die innergemeinschaftlichen Exportkontrolle für kryptographische Massengüter abgeschafft. Auch eine Vereinfachung der Exportkontrollverfahren ist mit dem Bundesausfuhramt in Prüfung.

Es ist nicht auszuschließen, daß mit der zunehmenden Nutzung der Verschlüsselung auch der Mißbrauch dieser Technik für illegale Zwecke zunimmt. Deshalb werden die beteiligten Bundesministerien die weitere Entwicklung aufmerksam beobachten und nach zwei Jahren einen Bericht dazu vorlegen. In diesem Zusammenhang werden auch Anstrengungen unternommen, die technische Ausstattung der Strafverfolgungs- und Sicherheitsbehörden weiter zu verbessern.

Mit dieser ausgewogenen Position zu den Chancen und Risiken in der Nutzung der Informationstechnologie hat die Bundesregierung die Voraussetzungen geschaffen, daß Deutschland auch in Zukunft ein sicherer und leistungsfähiger Standort im Informationszeitalter ist.

Eckpunkte der deutschen Kryptopolitik

Einleitung

Programme und Chips zur sicheren Verschlüsselung von Nachrichten waren bis Anfang der Neunziger Jahre ein relativ unbedeutender Nischenbereich der Computerindustrie. Dieser Nischenbereich ist heute jedoch von erheblicher Bedeutung für die wirtschaftliche und gesellschaftliche Entwicklung der Informationsgesellschaft insgesamt. Denn immer mehr entwickelt sich der Produktionsfaktor “Information” zu einem begehrten Rohstoff. Der effektivere Schutz dieses Rohstoffs kann über Erfolg oder Mißerfolg von Unternehmen und damit über Beschäftigungschancen im Informationszeitalter entscheiden und nur durch den Einsatz starker kryptographischer Verfahren läßt sich dieser Schutz heute effektiv gewährleisten. In jedem Fall ist die Leistungsfähigkeit dieser Technologie heute größer als jemals zuvor.

Die Kryptokontroverse in Deutschland

Bei der Kryptokontroverse geht es um die Frage, ob und in welchem Umfang die Nutzung kryptographischer Verfahren gesetzlich beschränkt werden solle. Die Frage ist in vielen demokratischen Industrieländern in den letzten Jahren kontrovers diskutiert worden. Auch in Deutschland fand eine intensive Auseinandersetzung, an der sich die Bundesressorts mit unterschiedlichen Positionen, die Wirtschaft sowie zahlreiche gesellschaftliche Gruppen beteiligten, hierüber statt.

Im Oktober 1997 verabschiedete das Bundeskabinett den “Fortschrittsbericht der Bundesregierung Info 2000: Deutschlands Weg in die Informationsgesellschaft”, der eine Passage zur Kryptopolitik enthielt:

“Es wurde innerhalb der Bundesregierung Einvernehmen erzielt, in dieser Legislaturperiode auf eine gesetzliche Regelung des Inverkehrbringens und der Nutzung von Kryptoprodukten und -verfahren zu verzichten, so daß es bei der uneingeschränkten Freiheit der Nutzer bei der Auswahl und dem Einsatz von Verschlüsselungssystemen bleibt. Die Bundesregierung wird die weitere Entwicklung auf dem Gebiet der Kryptographie vor allem im Kontext der europäischen und internationalen Zusammenarbeit aufmerksam verfolgen und ggf. weitere Maßnahmen zur Umsetzung ihrer Ziele einleiten.”

Die Bundesregierung hat sich bislang allerdings noch nicht verbindlich und eindeutig positioniert.

Kryptographie und Wirtschaftsinteressen

Vor allem wegen der dynamischen Entwicklung des digitalen Geschäftsverkehrs verzeichnen heute auch die Märkte für Verschlüsselungsprodukte hohe Wachstumsraten. Wichtige Anwendungsbereiche für kryptographische Systeme sind heute (neben dem traditionellen Schutz der Vertraulichkeit) z.B. Urheberschutz, digitale Signatur sowie digitales Geld. Darüber hinausgehend ist Kryptographie eine Querschnittstechnologie, die für die Systemarchitektur und Entwicklung komplexer Electronic Commerce-Anwendungen unverzichtbar ist. Mittelbar geht es hier also um weit größere Märkte, z.B. den der Telekommunikation, des Online-Banking oder der Telemedizin.

Zwar sind heute Sicherheitsstandards, die noch vor wenigen Jahren wegen der hohen Kosten vor allem Großunternehmen und staatlichen Stellen vorbehalten waren, auch für mittelständische Betriebe und private Haushalte erschwinglich. Dennoch werden Verschlüsselungsprodukte in Deutschland derzeit nicht in dem erforderlichen Maße eingesetzt. Hier fehlt es vielfach an dem notwendigen IT-Sicherheitsbewußtsein, obwohl durch die unbefugte Ausspähung, Manipulation oder Zerstörung von Daten erhebliche wirtschaftliche Schäden entstehen können.

Deutsche Kryptohersteller haben gute Aussichten, im internationalen Wettbewerb um neue Märkte mitzuhalten, wenn die notwendigen Rahmenbedingungen hierfür gewährleistet sind. Angesichts der strategischen Bedeutung dieser Branche unternehmen viele wichtige Industriestaaten erhebliche Anstrengungen, um deren wirtschaftliche und technische Leistungsfähigkeit im eigenen Land zu stärken.

Kryptographie und Sicherheitsinteressen

Der Einsatz kryptographischer Verfahren ist von außerordentlicher Bedeutung für eine effiziente technische Kriminalprävention. Dies gilt sowohl für die Gewährleistung der Authentizität und Integrität des Datenverkehrs wie auch für den Schutz der Vertraulichkeit.

Andererseits kann dieser Schutz der Vertraulichkeit auch Straftäter begünstigen: So ist zu erwarten, daß mit zunehmender Benutzerfreundlichkeit der Verschlüsselungsprodukte auch ihre Verbreitung in kriminellen Kreisen zunimmt. Dies kann die Strafverfolgungsbehörden vor Probleme stellen. Rechtmäßig angeordnete richterliche Überwachungsmaßnahmen müssen ihre Wirkung behalten, auch wenn die Zielperson die betreffenden Informationen mit einem kryptographischen Verfahren schützt.

Bislang stellt der Mißbrauch von Verschlüsselung in Deutschland für die Strafverfolgung kein ernsthaftes Problem dar. Eine Prognose für die Zukunft läßt sich hieraus allerdings nicht herleiten. Es ist deshalb erforderlich, in Deutschland aktive Technikfolgenabschätzung im Hinblick auf die Belange

der Strafverfolgungs- und Sicherheitsbehörden zu betreiben, um Fehlentwicklungen so frühzeitig zu erkennen, daß ihnen - ggf. unter Zugrundelegung alternativer Strategien - wirksam begegnet werden kann.

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.