Deutscher Bundestag
13. Wahlperiode

Drucksache 13/4105

14. 03. 96

Antwort

der Bundesregierung

auf die Kleine Anfrage des Abgeordneten Dr. Manuel Kiper und der Fraktion BÜNDNIS 90/DIE GRÜNEN
— Drucksache 13/3932 —

Sicherheit der Informationstechnik und Kryptierung

Die Bedeutung der Sicherheit der Informationstechnik (IT-Sicherheit) wird häufig betont. Die Praxis zeigt jedoch, daß Probleme von großer Wichtigkeit nicht angegangen und grundsätzliche Fragen nicht gestellt werden. In besonderem Maße tritt dies bei solchen technischen Teilbereichen zutage, die wie die Kryptographie nicht allein der Herstellung von IT-Sicherheit dienen können, sondern den Interessen staatlicher Sicherheit untergeordnet werden.

Die Bundesregierung bereitet derzeit die Einführung einer elektronischen Unterschrift vor. Elektronische Daten werden dabei durch eine Verschlüsselung „versiegelt". Gleichzeitig wird auf diese Weise die Nutzung von kryptographischen Verfahren in großem Umfang begonnen. Pläne seitens der EU-Kommission zu ähnlichen Verfahren sind bekanntgeworden, die US-Regierung hat ihrerseits erste Überlegungen einer Neuausrichtung ihrer Kryptographie-Politik bekanntgegeben. Die Antwort der Bundesregierung auf eine Anfrage zur Kryptographie (Drucksache 13/1889) ist damit nicht länger aktuell.

Der bislang nicht gewährleistete Schutz persönlicher Daten, die auf elektronischem Weg verschickt werden, kann mit den Kryptierungsinitiativen vorangetrieben werden. Damit wird gleichzeitig die Frage nach einer internationalen Abstimmung notwendig, wenn Nutzung wie Handel mit Kryptiersystemen keinen künstlich errichteten Barrieren ausgesetzt werden sollen.

IT-Sicherheit besteht jedoch aus weit mehr als nur Kryptierung. Da nach der Antwort der Bundesregierung auf eine Kleine Anfrage zum Bundesamt für Sicherheit in der Informationstechnik (BSI) (Drucksache 13/3408) noch viele Fragen offengeblieben sind, ist es notwendig, verschiedene Bereiche der IT-Sicherheit erneut zu thematisieren.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 13. März 1996 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Vorbemerkung

Die Bundesregierung hat die Entwicklung sicherer kryptographischer Verfahren für staatliche Zwecke bereits seit den 50er Jahren mit erheblichen Mitteln gefördert. Die Ergebnisse sind zwischenzeitlich auch weitgehend in den zivilen Anwendungsbereich eingeflossen.

Sichere kryptographische Verfahren für Zwecke der

- digitalen Signatur (elektronischen Unterschrift),
- Identifikation/Authentisierung und Zugriffskontrolle (z. B. als „digitaler Ausweis" in Netzen) und
- Verschlüsselung

sind die Grundvoraussetzung für wirksame Datensicherheit und wirksamen Datenschutz beim Einsatz von Informationstechnik mit weltweiter Vernetzung. Die dafür erforderliche Technik steht zur Verfügung.

Die Bundesregierung prüft zur Zeit, in welchem Umfang künftig ein elektronisches Dokument mit digitaler Signatur einem Schriftdokument mit eigenhändiger Unterschrift rechtlich gleichgestellt werden soll.

Im übrigen wird auf die Drucksache 13/1889 verwiesen.

1. Gibt es offizielle Kontakte zwischen Mitarbeitern des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und Mitarbeitern der National Security Agency (NSA)?

   Wenn ja, in welchen Gremien, zu welchem Zweck, wann und aus welchem Anlaß fand die letzte Begegnung statt?
2. Welche offiziellen Kontakte gab es zwischen der NSA und Mitarbeitern der ehemaligen Zentralstelle für das Chiffrierwesen (ZfCh), und in welchem Umfang werden diese heute vom BSI weitergepflegt?

Wie das BSI und seine Vorgängerbehörden ist die NSA für die Entwicklung und Zulassung von Verschlüsselungssystemen im staatlichen Geheimschutzbereich zuständig. Es fand und findet deshalb ein regelmäßiger multilateraler Erfahrungsaustausch statt. Die letzte Begegnung erfolgte am 1. März 1996 im Rahmen der Zusammenarbeit des BSI mit NIST, NSA und den entsprechenden Behörden Kanadas, Großbritanniens, Frankreichs und der Niederlande zur Weiterentwicklung der Europäischen IT-Sicherheitskriterien (ITSEC) zu gemeinsamen Kriterien (Common Criteria).

3. Mit welchen Unternehmen hat die ZfCh bei der Entwicklung von Verschlüsselungstechnik zusammengearbeitet bzw., mit welchen arbeitet das BSI heute zusammen?

ZfCh bzw. BSI arbeiteten/arbeiten grundsätzlich mit allen deutschen Kryptoherstellern zusammen.

4. Gab bzw. gibt es dabei eine Zusammenarbeit mit Firmen der Nachrichtentechnik sowie Herstellern von Geräten und Systemen zur Elektronischen Kampfführung (EloKa)?
   Wenn ja, mit welchen und zu welchem Zweck?

Ja, die Zusammenarbeit diente vor allem der Entwicklung von Kryptogeräten für den Bereich des staatlichen Geheimschutzes.

5. Trifft es zu, daß für das BSI ein neuer leistungsfähiger Großrechner beschafft werden soll?
   Wenn ja, für welche Zwecke wird dieser Rechner benötigt?

Ja. Er soll der Entwicklung und Untersuchung kryptographischer Algorithmen (z. B. zur Verschlüsselung oder digitalen Signatur) dienen.

6. In welchem Umfang unterliegt der Export von Verschlüsselungssystemen in der Bundesrepublik Deutschland Exportbeschränkungen, und in welchem Umfang ist das BSI an der Erteilung von Exportlizenzen fachlich beteiligt bzw. war die vormalige ZfCh daran beteiligt?

Verschlüsselungssysteme sind in Deutschland, ebenso wie z. B. in den übrigen Mitgliedstaaten der EU, wegen ihrer doppelten Verwendungsfähigkeit in weitem Umfang einer Ausfuhrgenehmigungspflicht unterworfen. Die entsprechenden Ausrüstungen, Baugruppen, Bestandteile, einschlägige Prüf-, Test- und Herstellungseinrichtungen, Datenverarbeitungsprogramme und Technologie sind in der Ausfuhrliste – Anlage zur Außenwirtschaftsverordnung – im Teil I C Abschnitt 5 Teil 2 „Informationssicherheit" – im einzelnen aufgeführt. Die Genehmigungsbehörde ist angewiesen, bis auf wenige Ausnahmen – z. B. bei Bankautomaten – alle Anträge auf Genehmigung solcher Ausfuhren dem BSI zur fachlichen Begutachtung vorzulegen. Diese Begutachtung erfolgte früher durch die ZfCh.

7. Beabsichtigt die Bundesregierung regulative Änderungen bei der Vergabe von Exportlizenzen?

Das deutsche Exportkontrollsystem ist sowohl in seinen Rechtsnormen als auch in der administrativen Handhabung im Zuge der Harmonisierung durch die EG-Verordnung über die Ausfuhrkontrolle von Gütern mit doppeltem Verwendungszweck, gültig ab 1. Juli 1995, angepaßt worden. Weitere Anpassungen können aufgrund von Abstimmungen in Internationalen Regimen erforderlich werden. Zur Zeit sind keine konkreten Änderungen in Vorbereitung.

8. Ist der Bundesregierung eine Einflußnahme von für Kryptierungsfragen zuständigen Behörden auf die Entwicklung von Kryptiersystemen bekannt?

Das BSI nimmt Einfluß auf die Entwicklung von Verschlüsselungssystemen für den staatlichen Geheimschutzbereich, damit diese den dortigen besonderen Sicherheitsanforderungen entsprechen.

9. Ist der Bundesregierung eine Einflußnahme von für Kryptierungsfragen zuständigen Behörden auf die Exportfähigkeit von Kryptiersystemen bekannt?

Im Rahmen der Entscheidung über Ausfuhranträge sind die jeweils unterschiedlichen Interessen sorgfältig abzuwägen. Dabei hat die Genehmigungsbehörde den Sachverhalt unter Berücksichtigung aller Interessen aufzuklären. Auf Wunsch der Hersteller können entwicklungsbegleitende Beratungen mit dem Ziel der Erfüllung der rechtlichen Voraussetzungen für die Exportfähigkeit von Systemen erfolgen.

10. Ist der Bundesregierung die Ansicht von Kryptierexperten bekannt, bestimmte Verschlüsselungsstandards und -systeme seien durch Einflußnahme von für Kryptierungsfragen zuständigen Behörden, insbesondere der NSA, aufgeweicht worden, und welche Konsequenzen zieht sie hieraus?

Die restriktive Exportkontrollpolitik der USA auf dem Gebiet der Verschlüsselungstechnik ist allgemein bekannt; die Beratungspraxis des BSI gegenüber der öffentlichen Verwaltung und der deutschen Privatwirtschaft wahrt daher Zurückhaltung in der Empfehlung von derartigen Produkten US-amerikanischer Provenienz.

11. Ist der Bundesregierung bekannt, aus welchem Grund die International Standards Organization (ISO) ihren Gliederungen – Technical Committees – die Normung von Kryptieralgorithmen verboten hat?

    Wenn ja, welche Position hat die Bundesregierung dabei vertreten?

Nein. Nach Auffassung der Bundesregierung ist Normung grundsätzlich eine Angelegenheit der wirtschaftlich Beteiligten.

12. Welche Folgerungen zieht die Bundesregierung aus Berichten (Computer Zeitung vom 25. Januar 1996), daß der Softwarehersteller Lotus zur Erlangung einer Exportlizenz in den USA für die neue Version 4.0 seines Produktes Lotus Notes 24 der 64 Bits des Kryptierschlüssels US-Behörden bekanntgeben mußte?

Es wird auf die Antwort zu Frage 10 verwiesen.

13. Ist diese Software bei Bundesbehörden im Einsatz?

    Wenn ja, bei welchen?

Vollständige statistische Angaben hierzu liegen der Bundesregierung nicht vor und können von ihr in der für die Beantwortung einer Kleinen Anfrage zur Verfügung stehenden Frist nicht erhoben werden.

14. Hat die Bundesregierung bei der Beratung der Erfordernisse einer gesetzlichen Regelung kryptographischer Verfahren seit Mitte 1995 Fortschritte gemacht?

    Wenn ja, welche?

Nein.

15. Beabsichtigt die Bundesregierung, bei den angekündigten gesetzlichen Regelungen einer elektronischen Unterschrift, die funktional einem Verschlüsselungssystem gleichkommt, die Systeme einer Lizensierung zu unterwerfen?

    Wenn ja, nach welchen Kriterien soll die Lizensierung geschehen, vor allem auch im Hinblick auf die Sicherheit der Systeme?

Die Bundesregierung prüft zur Zeit, in welcher Weise eine elektronische Unterschrift (digitale Signatur) in das Gefüge der Schriftformen des BGB und der Vorschriften über den Urkundsbeweis eingefügt werden kann. Dabei wird auch geprüft, ob die mögliche gesetzliche Anerkennung von Verfahren der digitalen Signatur davon abhängig gemacht werden soll, daß die Verfahren bestimmten Sicherheitsanforderungen entsprechen, und ob die Erfüllung der Sicherheitsanforderungen vom BSI oder einer vom BSI anerkannten Stelle nach öffentlichen Kriterien geprüft und bestätigt werden soll.

16. Welches Modell einer Schlüsselverwaltung strebt die Bundesregierung dabei an?

Eine Entscheidung für ein bestimmtes Modell ist noch nicht getroffen. Denkbar wäre beispielsweise, daß die Beglaubigung (Zertifizierung) der Signaturschlüssel durch zugelassene Zertifizierungsinstanzen im freien Wettbewerb erfolgen soll. Voraussetzung für die Zulassung einer Zertifizierungsinstanz könnte sein, daß diese die erforderliche Zuverlässigkeit aufweist und nachweislich bestimmte technisch-organisatorische Sicherheitsvorkehrungen getroffen hat.

17. Beabsichtigt die Bundesregierung bei den genannten Systemen eine Beschränkung der Schlüssellänge?

Nein.

18. Hält es die Bundesregierung für notwendig, die Nutzung von bestimmten Kryptosystemen einzuschränken bzw. zu verbieten?

19. Wie realistisch ist nach Ansicht der Bundesregierung die Annahme, eine Beschränkung von Kryptiersystemen auf einige zugelassene sichere die Abhörmöglichkeiten für Strafverfolgungsbehörden und Nachrichtendienste?

Die Bundesregierung prüft das Erfordernis einer gesetzlichen Regelung des Einsatzes von Verschlüsselungssystemen. Diese Prüfung ist bislang nicht abgeschlossen.

20. Wie passen nach Ansicht der Bundesregierung ihre Pläne einer Regelung der elektronischen Unterschrift zu den Plänen sowohl auf EU-Ebene als auch den unterschiedlichen Plänen zur Kryptographie auf der Ebene der OECD-Staaten, und sieht die Bundesregierung Probleme bei der Abstimmung?

Die Entwicklung in den europäischen bzw. internationalen Gremien befindet sich derzeit im Fluß, so daß es für eine Bewertung der verschiedenen Aktionen noch zu früh ist.

21. Wie reagiert die Bundesregierung auf den Standpunkt der US-Administration, bei Export und Nutzung von asymmetrischen Kryptiersystemen auf solche Systeme hinzuwirken, die sicherstellen, daß Strafverfolgungsbehörden und Geheimdienste sowohl eingehende als auch ausgehende elektronische Kommunikation in bestimmten Fällen entschlüsseln können?

Die Bundesregierung prüft derzeit, welche Auswirkungen das Konzept der US-Administration auf den internationalen Waren- und Dienstleistungsverkehr hat, und welche Schlüsse daraus für die Politik der Bundesregierung abzuleiten sind.

22. Welche Ministerien, Behörden und Ämter des Bundes sind zum gegenwärtigen Stand über das Internet erreichbar, in welcher Weise sind diese Systeme mit den übrigen DV-Systemen der jeweiligen Einrichtungen verbunden, und wie werden dabei die Sicherheit und Integrität dieser Systeme gewährleistet?

Vollständige statistische Angaben hierzu liegen der Bundesregierung nicht vor und können von ihr in der für die Beantwortung einer Kleinen Anfrage zur Verfügung stehenden Frist nicht erhoben werden.

Soweit Rechner an das Internet angeschlossen sind, haben sie entweder keine oder eine über Gateways realisierte Verbindung mit den übrigen DV-Systemen der jeweiligen Einrichtungen.

Verfügbarkeit, Vertraulichkeit und Integrität von an das Internet angeschlossenen Rechnern und lokalen Netzen bzw. der dort verarbeiteten Daten werden durch eine der folgenden Maßnahmen gewährleistet:

- Es werden Einzelarbeitsplätze benutzt, die nicht mit anderen lokalen Rechnern vernetzt sind.
- Die Erreichbarkeit über das Internet ist auf wenige Dienste beschränkt (insbesondere Elektronischer Dokumentenaus-

tausch), wobei die Gateway-Rechner nur das Protokoll für den zugelassenen Dienst/die zugelassenen Dienste akzeptieren.

– Zukünftig werden zunehmend Firewalls zum Einsatz kommen.

23. Zwischen welchen Behörden findet ein Datenaustausch statt, und wie wird dieser gesichert?

In welchem Umfang hat das BSI Sicherheitskonzepte dafür erarbeitet?

Datenaustausch findet zwischen denjenigen Behörden statt, deren gesetzliche Aufgaben eine Zusammenarbeit erfordern. Die Anforderungen an Verfügbarkeit, Vertraulichkeit und Integrität sind dabei sehr unterschiedlich. Daher sind auch die erforderlichen Sicherheitsmaßnahmen verschieden. Die Bundesbehörden verfügen über IT-Sicherheitskonzepte, in denen die IT-Verfahren untersucht und die jeweiligen Sicherheitsmaßnahmen dargestellt werden. Das BSI hat sowohl für die Sicherung der Vertraulichkeit beim Datenaustausch zwischen Behörden, wie auch zur Absicherung von Internetzugängen Sicherheitskonzeptionen entwickelt.

24. Hat es bei einem derartigen Datenaustausch Sicherheitsanalysen durch den Bundesrechnungshof gegeben, und zu welcher Bewertung ist dieser gekommen?

Es gab verschiedene Sicherheitsanalysen mit unterschiedlichen Ergebnissen.

25. Ist ein Ministerium, eine Behörde oder ein Amt im Verantwortungsbereich des Bundes jemals Opfer eines „Hackers" geworden?

Wenn ja, um welche Behörde handelte es sich, wurde ein Angreifer identifiziert, ein Verfahren eingeleitet, und zu welchem Ergebnis kam dies?

Wurden überdies Daten manipuliert oder zerstört?

Der Bundesregierung ist nicht bekannt, daß Hacker nachweislich in eine der genannten Stellen eingedrungen sind.

26. Ist der Bundesregierung die amerikanische Software „PROMIS" (Prosecutor's Management System) bekannt, und ist sie in ihrem Verantwortungsbereich im Einsatz?

Wenn ja, zu welchem Zweck und bei welcher Behörde?

Nein.

27. Hat die Bundesregierung für die Beschaffung von Software Richtlinien, in denen IT-Sicherheitsaspekte berücksichtigt werden?

Ja, bereichsspezifisch.

28. Gibt es Bereiche, in denen nur sicherheitsgeprüfte Software zum Einsatz kommt?
Wenn ja, welche?

Nein.

29. Ist der Bundesregierung in einer Einrichtung des Bundes jemals ein Softwareprodukt zur Kenntnis gelangt, das ein unerklärliches Sicherheitsloch – eine Sicherheits-trapdoor – auswies?
Wenn ja, um welche Software handelte es sich?

Nein.

30. Lassen sich derartige Sicherheitslöcher nach Erkenntnissen des BSI ohne Kenntnis des Quellcodes systematisch aufspüren?
Wenn ja, mit welchem Aufwand?

Zum Aufspüren solcher Sicherheitslücken ist die Inspektion wesentlicher Teile des Quellcodes unerläßlich; jedoch ist dies allein nicht ausreichend. Manche Sicherheitslücken sind erst im sogenannten Object-Code zu erkennen; somit sind Compiler und Libraries der angewandten Programmiersprachen ebenfalls zu untersuchen. Arbeitet man nur auf der Basis einfacher Tests, so ergeben sich mehr zufällige Aussagen. Bestenfalls kann ein vermutetes Sicherheitsloch bestätigt oder widerlegt werden; die Abwesenheit von Sicherheitslöchern nachzuweisen, kann dagegen nur mit einer eingehenden Analyse von Quell- und Object-Code erfolgen. Dabei ist der Einsatz bestimmter Prüfwerkzeuge zwingend.

31. Trifft es nach Kenntnis der Bundesregierung zu, daß bundesdeutsche „Hacker", die in den 80er Jahren in bestimmte Rechnersysteme in den USA eindrangen, ein Sicherheitsloch in den VAX/VMS-Betriebssystemen der Versionen 4.4 und 4.5 benutzten?

Nach Kenntnis der Bundesregierung war in Version 4.4 VAX/VMS im Bereich „Security Service" ein Sicherheitsloch vorhanden, so daß auch unberechtigte Benutzer weitere Rechte vergeben konnten.

Druck: Thenée Druck, 53113 Bonn, Telefon 91781-0
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon (02 28) 3 82 08 40, Telefax (02 28) 3 82 08 44
ISSN 0722-8333