Deutscher Bundestag
13. Wahlperiode

Drucksache 13/7594

05. 05. 97

Kleine Anfrage

des Abgeordneten Dr. Manuel Kiper und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Lage der IT-Sicherheit in Deutschland

Mit der Verbreitung von Computersystemen und der steigenden Abhängigkeit von der Informationstechnik wächst auch die Einsicht, wie wichtig deren Sicherheit – die IT-Sicherheit – für das reibungslose Funktionieren vieler Bereiche ist. Zwar werden über zwei Drittel der Störungen an Computern weiterhin durch Mängel in den eingesetzten Softwareprodukten hervorgerufen, doch wird die Gefahr durch manipulative Eingriffe in Computersysteme von außen mittlerweile ernst genommen. Doch auch das gestiegene Bewußtsein um IT-Sicherheitsgefahren hat nicht zu einer Verbesserung der Sicherheitslage geführt. Es ist im Gegenteil zu beobachten, daß durch neue Verfahren in Softwareprodukten zusätzliche Gefahren hervorgerufen werden, die eigentlich beim erreichten Wissensstand um IT-Sicherheitsprobleme zu vermeiden gewesen wären.

Zu den immer noch nicht beseitigten Problemen zählt, daß bei der Installation von Software Dateien mit neuen Konfigurationsdaten unkontrolliert überschrieben und damit bisweilen unbrauchbar gemacht werden. Ein Sicherheitsproblem entsteht bei der Installation des Betriebssystems Windows 95, das Daten über die beim jeweiligen Nutzer vorgefundenen Systemeigenschaften und Software sammelt und die Daten bei der Anmeldung in das Microsoft Network an den Hersteller übermittelt, sofern dies nicht explizit unterbunden wird. Neue Softwaretechnologien führen zusätzlich zu einer deutlichen Steigerung der Manipulationsmöglichkeiten. Die Programmiersprache Java und die Netzwerk-Softwaretechnologie Active-X – als aktuelle Beispiele – verändern Daten und Programme auf den Computersystemen von Internet-Nutzern bereits bei bestimmungsgemäßer Anwendung ohne deren Zutun und oft auch ohne ihre Einwilligung und können damit Schäden bewirken. Die Defizite in den Sicherheitsmechanismen dieser Technologien eröffnen in unterschiedlich starker Weise für mißbräuchliche Nutzung Tür und Tor.

Mit dem Zweiten Gesetz zur Bekämpfung der Wirtschaftskriminalität wurden 1986 die Manipulation von Daten und die Störung des Betriebs von Datenverarbeitungsanlagen unter Strafe gestellt. Gedacht waren diese Rechtsnormen für sog. „Hackerdelikte", also vor allem das gezielte Ausspähen von

Daten. Ebenso wurde aber auch der Verlust von Integrität und Verfügbarkeit der Daten, die durch Computerviren, aber auch andere Eingriffe und Manipulationen, verursacht werden, unter Strafe gestellt. So wurde explizit von einer „Unbrauchbarkeit" von Daten ausgegangen, wenn sie „z.B. durch zusätzliche Einfügungen" nicht mehr ordnungsgemäß verwendet werden können (Drucksache 10/5058, S. 35). Die Strafbarkeit einer Veränderung von Daten nach § 303 a StGB ist ein weitreichender Tatbestand, der oftmals schon bei der Installation neuer Software Anwendung finden könnte. Neue Softwaretechniken sind in immer stärkerer Weise geeignet, mit diesem Gesetz in Konflikt zu geraten. Gleichzeitig zeigt aber allein die Zahl von nur 66 Ver- bzw. Abgeurteilten zwischen 1987 und 1993, daß derartige Probleme derzeit juristisch unbewältigt bleiben.

IT-Sicherheitsexperten betonen heute, daß jeder Kontakt von Computersystemen mit der Außenwelt – sei es durch die Installation neuer Software oder durch den Anschluß eines Computersystems an ein elektronisches Netzwerk – zu Sicherheitsrisiken führt. Der von der Bundesregierung angestrebte Weg in die Informationsgesellschaft ist dagegen durch die intensive Vernetzung verschiedenster Computerressourcen gekennzeichnet und damit durch die Potenzierung der Sicherheitsrisiken. Obwohl bis heute weder das Problembewußtsein für das Design zuverlässiger Software deutlich gestiegen ist noch andere lange bekannte Probleme der IT-Sicherheit gelöst sind, baut diese Gesellschaft in immer stärkerem Maße auf diese Technik. So große Mängel bei Zuverlässigkeit und Sicherheit würden bei keiner anderen ähnlich bedeutenden Technologie akzeptiert. Ein fundiertes Konzept der Bundesregierung zur Absicherung der auf der störungsfreien Funktion von IT-Systeme beruhenden Gesellschaft ist dabei nicht erkennbar. Die Debatte um die Regelung von Kryptierverfahren gefährdet überdies die Entwicklung und Nutzung neuartiger Sicherungstechniken.

Wir fragen die Bundesregierung:

1. Wie viele Ermittlungsverfahren nach § 202 a StGB (Computerspionage) und § 263 a StGB (Computerbetrug) wurden in den Jahren 1995 und 1996
   a) durchgeführt,
   b) wie viele Anklagen und Aburteilungen resultierten daraus, und
   c) welche Schäden wurden nach Schätzung der Bundesregierung dadurch verursacht?
2. Zu wie vielen Ab- und Verurteilungen wegen § 303 a und § 303 b StGB (Computer-Sabotage) kam es in den Jahren 1995 und 1996, und in wie vielen Fällen wurde dabei die Verbreitung von Software zur Veränderung von Daten (Computerviren etc.) geahndet?
3. Gab es nach Kenntnis der Bundesregierung bei der Installation von Software sowohl bei Bundesbehörden als auch bei

privaten Nutzern Fälle, in denen der Installationsvorgang zu strafrechtlich relevanten Eingriffen in Computersysteme führte, und wenn ja, um welche Fälle handelte es sich?

4. Sind der Bundesregierung in diesem Zusammenhang Vorfälle bekannt geworden, in denen es – etwa durch die Verbreitung von Computerviren bei der Installation oder ähnliches – aufgrund mangelhafter Qualitätskontrolle zu ungewollten Eingriffen kam, und wenn ja, um welche Fälle handelte es sich?

5. Sind der Bundesregierung Fälle bekannt, in denen es durch die Nutzung der Java- oder Active-X-Technologie zu strafrechtlich relevanten Eingriffen in Computersysteme oder zur Ausspähung von Daten gekommen ist, und wenn ja, um welche Fälle handelte es sich und, welche Schäden sind dadurch entstanden?

6. Bei welchen Bundesbehörden wurde das Betriebssystem Windows 95 installiert, und wurden dessen Merkmale und Gefährdungspotentiale vor der Installation analysiert?

7. Wie viele dieser Systeme sind an ein mit der Außenwelt verbundenes elektronisches Netz angeschlossen, und wie wird dabei mit den von Windows 95 gesammelten Nutzerdaten verfahren?

8. Welche Entwicklung hat – seit der Antwort der Bundesregierung auf eine Kleine Anfrage zur IT-Sicherheit (Drucksache 13/4105, Frage 22) – die Nutzung von Firewalls zum Schutz von Computersystemen bei Bundesbehörden genommen?

9. Gab es bei den Analysen des Bundesrechnungshofs (vgl. Drucksache 13/4105, Frage 24) Bewertungsergebnisse, nach denen ein Datenaustausch zwischen Behörden nicht den Sicherheitserfordernissen entsprach, und um welche Fälle ging es dabei?

10. Für welche Schutzstufe sind die im Informationsverbund Bonn–Berlin genutzten Systeme zum elektronischen Datenaustausch zugelassen?

11. Welche Sicherheitsanalysen gab es zur Nutzung dieser Systeme für verschiedene Schutzstufen, und für welche Schutzstufen wurden sie danach zugelassen, für welche nicht?

12. Ist die Bundesregierung der Ansicht, daß nichtöffentliche Stellen in der Lage sind, elektronischen Datenaustausch mit vergleichbarer oder höherer Sicherheit als Bundesbehörden zu bewerkstelligen, und hält die Bundesregierung ihre Sicherheitsanalysen auf nichtöffentliche Stellen für übertragbar?

13. Gab es – auch wenn der Nachweis eines Eindringens nicht geführt werden konnte – Verdachtsmomente für ein Eindringen von Hackern in das Computersystem eines Ministeriums, einer Behörde oder eines Amtes im Verantwortungsbereich des Bundes, und um welche Einrichtungen handelte es sich dabei?

14. Wie viele Fälle von versuchtem Eindringen in Computersysteme eines Ministeriums, einer Behörde oder eines Amtes im Verantwortungsbereich des Bundes gab es nach Kenntnis der Bundesregierung in den letzten fünf Jahren, und in welchem Verhältnis stehen diese Zahlen zu den aus den USA bekannten Vergleichswerten?

PC-Sicherungstechnik

15. Wie viele Beanstandungen der IT-Sicherheit bei der Verarbeitung von personenbezogenen Daten gab es in den letzten fünf Jahren durch Datenschutz-Kontrollinstanzen oder den Bundesrechnungshof, und welche Konsequenzen wurden daraus gezogen?

16. Welche Systeme sind der Bundesregierung bekannt, die PC mit den dafür verfügbaren Betriebssystemen technisch und organisatorisch gegen unbefugte Nutzung absichern und die Nutzung dieser Systeme revisionsfähig machen, d. h. solche, die zumindest eine durch Paßwort geschützte Identifikationsprozedur benötigen, aber auch Systeme, die erweiterten Schutz durch Verschlüsselungsmechanismen bieten?

17. Welches Marktvolumen haben derzeit nach Kenntnis der Bundesregierung IT-Sicherheitssysteme, und in welche Angebotsgruppen – Beratung, Software etc. – läßt sich dies einteilen?

18. Welche davon haben ein Sicherheitszertifikat des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder gleichwertiger Stellen?

19. Wie viele der (lt. Antwort der Bundesregierung in Drucksache 13/3408, Frage 7) 65 000 der in der Bundesverwaltung unter dem Betriebssystem MS-DOS oder dessen Derivaten eingesetzten PC-Systeme sind mit derartigen Schutzsystemen gegen unbefugte Nutzung ausgestattet, und welche Systeme werden dabei eingesetzt?

20. Auf wie vielen dieser PC-Systeme, die nicht mit Schutzsystemen ausgestattet sind, werden personenbezogene Daten verarbeitet, und auf welche Weise findet dort eine Sicherung gegen unbefugte Nutzung statt?

21. Wie viele portable Computersysteme (Laptops, Notebooks, Palmtops etc.) sind jeweils in welchen Bundesbehörden im Einsatz, auf wie vielen dieser Systeme werden personenbezogene Daten gespeichert, und wie werden diese Systeme gegen unbefugte Nutzung gesichert?

Digitale Vermittlungsstellen und ISDN-Anlagen

22. Welche in der ZDF-Sendung „Mit mir nicht" vom 26. März 1997 gezeigten Sicherheitsprobleme bei der Nutzung computergesteuerter Telekommunikations-Vermittlungsrechner sowohl bei digitalen Vermittlungsstellen als auch bei Neben-

stellenanlagen sind der Bundesregierung bekannt, und wie lange verfügt sie bereits über derartige Erkenntnisse?

23. Welche Manipulationsfälle bei derartigen Systemen sind der Bundesregierung bekannt geworden, welche Schäden entstanden dabei, und bei wie vielen kam es zu Ermittlungsverfahren bzw. Anklagen?

24. Gab es in den vergangenen Jahren auch vergleichbare Manipulationsfälle an digitalen Vermittlungsstellen der Deutschen Telekom AG?

25. Wie häufig wurde von der Deutschen Telekom AG eine auf Verschlüsselungsbasis arbeitende „intelligente TAE-Dose" eingesetzt, um Manipulationen an Telefonleitungen und -anschlüssen zu unterbinden?

26. Wie hoch ist der Schaden zu beziffern, der der Deutschen Telekom AG durch Manipulationen an Servicerufnummern entstanden ist?

27. Seit wann ist der Bundesregierung bekannt, daß ISDN-Anlagen anfällig gegen unautorisierte Zugriffe von außen und die Manipulation von Leistungsmerkmalen sind, und welche Konsequenzen hat sie daraus für Anlagen gezogen, die sowohl in Stellen der Bundesverwaltung eingesetzt werden, in denen Vorgänge der Schutzklasse I (VS-NfD, personenbezogene Daten, sensitive Informationen) als auch der Schutzklasse II (VS-Vertraulich und höher) bearbeitet werden?

28. In welcher Weise hat die Bundesregierung ihre Kenntnisse den betroffenen Nutzern derartiger Anlagen aus dem nichtöffentlichen Bereich weitergegeben?

29. Welche Gefährdungen durch Manipulationen an ISDN-Anlagen drohen nach Ansicht und Kenntnis der Bundesregierung in besonders sensitiven Einrichtungen wie den Bundesministerien einschließlich des Bundeskanzleramts, insbesondere aber den ISDN-Netzen der Bundeswehr und der Polizeibehörden?

30. Sind der Bundesregierung Manipulationen oder Versuche dazu an Systemen der Bundesverwaltung bzw. den ISDN-Netzen der Bundeswehr und der Polizeibehörden zur Kenntnis gelangt?

31. Durch wen wurden in der Bundesverwaltung Prüfungen von ISDN-Anlagen vorgenommen, und zu welchen Ergebnissen sind diese im einzelnen gekommen?

32. Welche über die Studie „Gefährdungen und Sicherheitsmaßnahmen beim Betrieb von digitalen Telekommunikationsanlagen" hinausgehenden Ergebnisse des BSI liegen derzeit vor, und an welchen entsprechenden Projekten finden Arbeiten statt?

Strafrechtliche Bewältigung

33. Welche Bedeutung hat nach Ansicht der Bundesregierung die strafrechtliche Bewältigung der Manipulation von Computersystemen, und wo hat diese ihre Grenzen?

34. Hält die Bundesregierung die bestehenden Gesetze angesichts der verfügbaren und absehbaren Softwaretechnologie für ausreichend und präzise genug, oder sieht die Bundesregierung Änderungsnotwendigkeiten an diesen Gesetzen?

35. Hat das BSI jemals das Verhalten von Software auf mögliche strafrechtliche Relevanz hin überprüft, und zu welchen Ergebnissen führte dies, insbesondere wurde die Öffentlichkeit informiert?

36. Gab es in der Bundesverwaltung Fälle, bei denen aus einer Veränderung von Daten bzw. eines Eingriffs in eine Datenverarbeitungsanlage von wesentlicher Bedeutung juristische Konsequenzen gezogen wurden – wenn ja, um welche Fälle handelte es sich?

37. In welcher Weise beteiligt sich die Bundesregierung am „Ständigen Komitee für Informationstechnologie" der Financial Crime Subdivision der Division II des Interpol-Generalsekretariats (vgl. Öffentliche Sicherheit 3/97, S. 24), und welche Aufgaben hat dieses Komitee?

38. Besteht in der Bundesrepublik Deutschland ein der President's Commission on Critical Infrastructure Protection (PCCIP) der USA vergleichbares Gremium, und wenn nicht, wie bewertet die Bundesregierung den Nutzen einer solchen Einrichtung für die Bundesrepublik Deutschland?

Forschung und Aufklärung

39. Welche Forschungs- und Entwicklungsarbeiten zur Sicherheit in Computernetzen und Sicherung von Computersystemen unterstützt die Bundesregierung über die Förderung des Bundesministeriums für Bildung, Wissenschaft, Forschung und Technologie hinaus, welche Ziele werden angestrebt, und welche Ergebnisse sind dabei besonders hervorzuheben?

40. Welche zusätzlichen Aktivitäten verfolgt die Bundesregierung zum Schutz vor Problemen der IT-Sicherheit?

41. Welche Informationsmöglichkeiten zur IT-Sicherheit für Informationstechnik-Anwender sind der Bundesregierung bekannt, und in welcher Weise unterstützt sie diese?

42. Wie weit ist die Vorbereitung des Informationsservers des BSI für das Internet gediehen (vgl. Drucksache 13/3408, Frage 7)?

43. Um welche Fälle, in denen das BSI zum Teil eklatante Mängel in der IT-Sicherheit bei elektronischen Zahlungsverfahren aufgedeckt und den Betreibern mitgeteilt hat und auf die sich der Bundesminister des Innern, Manfred Kanther, in seiner Eröffnungsrede des 5. IT-Sicherheitskongresses bezog, handelte es sich?

44. In welcher Weise fließen Erkenntnisse aus Fachkreisen und Gremien zur IT-Sicherheit in die Beratungen und Entscheidungen der Bundesregierung ein, und um welche Gremien handelt es sich dabei?

Verschlüsselung

45. In welchem Umfang werden nach Kenntnis der Bundesregierung in der Bundesrepublik Deutschland Verschlüsselungsverfahren genutzt?

46. Welcher Anteil an der Nutzung von Verschlüsselungsverfahren entfällt nach Kenntnis der Bundesregierung dabei jeweils auf Unternehmen, Behörden und Privatpersonen?

47. Wie hoch ist nach Einschätzung und Kenntnis der Bundesregierung bei Privatpersonen der Anteil solcher Verfahren, die mit entsprechendem Aufwand nicht zu entschlüsseln sind?

48. Welcher Aufwand ist nach Kenntnis der Bundesregierung nötig, um mit asymmetrischen Verfahren verschlüsselte Daten mit Schlüssellängen von 40, 56 und 128 Bit zu entschlüsseln, und wie groß ist nach Auffassung der Bundesregierung die für eine Verschlüsselung sensitiver Daten hinreichende Schlüssellänge für eine – auch über die nächsten fünf Jahre – sichere Übermittlung?

49. Bei wie vielen Ermittlungsverfahren kam es nach Erkenntnissen der Bundesregierung zu Behinderungen der Ermittlungstätigkeit, weil Verschlüsselungsverfahren eingesetzt wurden – aufgeschlüsselt nach Behinderungen durch verschlüsselte Kommunikation und Nutzung von Verschlüsselungsverfahren zur Datenspeicherung?

50. In welcher Beziehung hält die Bundesregierung den „Sicherheitswert steganographischer Verfahren" für überschätzt, wie der Bundesminister des Innern, Manfred Kanther, in seiner Eröffnungsrede des 5. IT-Sicherheitskongresses erklärte?

51. Welcher Sicherheitswert kann nach Auffassung der Bundesregierung Verschlüsselungsverfahren zugemessen werden, die auf PC-Systemen installiert sind, die ansonsten nicht gegen unbefugte Eingriffe geschützt sind?

52. Welcher Sicherheitswert kann nach Auffassung der Bundesregierung Verschlüsselungsverfahren zugemessen werden, bei denen der Schlüssel auf Chipkarten gespeichert ist und damit die Analyse durch die „Differential Fault Analysis" erlauben?

53. Welcher Sicherheitswert ist nach Auffassung der Bundesregierung somit der Nutzung von Verschlüsselungsverfahren durch Nichtspezialisten zuzumessen, zumal weitere Eingriffsmöglichkeiten in derartige Verfahren bekannt sind?

Bonn, den 25. April 1997

Dr. Manuel Kiper
Joseph Fischer (Frankfurt), Kerstin Müller (Köln) und Fraktion

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