Deutscher Bundestag
13. Wahlperiode

Drucksache 13/7753

22. 05. 97

Antwort

der Bundesregierung

auf die Kleine Anfrage des Abgeordneten Dr. Manuel Kiper und der Fraktion BÜNDNIS 90/DIE GRÜNEN
— Drucksache 13/7594 —

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,

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 22. Mai 1997 übermittelt.

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

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.

Vorbemerkung

Die Bundesregierung hat ihre Position zur Entwicklung der Informationsgesellschaft in ihrem Bericht „Info 2000 – Deutschlands Weg in die Informationsgesellschaft" formuliert. IT-Sicherheit hat dabei einen hohen Stellenwert.

1. Wie viele Ermittlungsverfahren nach § 202 a StGB (Computerspionage) und § 263 a StGB (Computerbetrug) wurden in den Jahren 1995 und 1996

   a) durchgeführt,

Aus der Polizeilichen Kriminalstatistik ergeben sich für 1995 zum § 202 a StGB 110 Fälle und zum § 263 a StGB 3 575 Fälle.

Für 1996 liegen noch keine Zahlen vor.

   b) wie viele Anklagen und Aburteilungen resultierten daraus, und

Die vom Statistischen Bundesamt herausgegebene Strafverfolgungsstatistik für das Jahr 1995 enthält folgende Angaben:

§ 202 a StGB: 3 Abgeurteilte
1 Verurteilter

§ 263 a StGB: 1 797 Abgeurteilte
1 541 Verurteilte

Für 1996 liegen noch keine Zahlen vor.

   c) welche Schäden wurden nach Schätzung der Bundesregierung dadurch verursacht?

Aufgrund der hohen Dunkelziffer in diesem Bereich sind zuverlässige Schätzungen nicht möglich.

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?

Zu den §§ 303 a und 303 b StGB enthält die Strafverfolgungsstatistik für 1995 folgende Angaben:

§ 303 a StGB: 11 Abgeurteilte
7 Verurteilte

§ 303 b StGB: 7 Abgeurteilte
3 Verurteilte.

Für 1996 liegen noch keine statistischen Erkenntnisse vor.

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?

Der Bundesregierung liegen keine Erkenntnisse vor.

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?

Aufgrund mangelhafter Qualitätskontrolle kam es zu folgenden ungewollten Eingriffen:

— Vorinstallierte Software auf neuen Rechnern waren mit einem Computer-Virus infiziert.

— Rechner kamen von der Reparatur mit einem Computer-Virus zurück.

— Service-Techniker infizierten Rechner bei Wartung vor Ort.

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?

Nein.

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?

In der Bundesverwaltung sind ca. 65 000 Windows-Betriebssysteme im Einsatz. Welcher Prozentsatz davon auf Windows 95 entfällt, ist statistisch nicht erfaßt.

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?

Allen Bundesbehörden wird empfohlen, sich bei Anschluß an das Internet durch eine Firewall abzusichern.

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?

Die Bundesregierung führt keine Auswertungsstatistik über Analysen des Bundesrechnungshofs.

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

Die im Informationsverbund Berlin-Bonn (IVBB) genutzten Systeme zum elektronischen Dokumentenaustausch sind für eine vertrauliche Kommunikation bis zum Grad „VS – Nur für den Dienstgebrauch" ausgelegt. Für die Übertragung höher eingestufter Verschlußsachen sind spezielle, vom BSI zugelassene Verschlüsselungsgeräte vorgesehen.

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

Zum Gesamtkonzept IVBB existiert ein durch das BSI erstelltes IT-Sicherheitskonzept, das während der gesamten Entwurfs- und Planungsphase fortgeschrieben wurde und in der anstehenden Realisierungsphase fortgeschrieben wird. Dieses IT-Sicherheitskonzept enthält eine Gefährdungs- und Risikoanalyse des Gesamtverfahrens sowie sich daraus ergebende Schutzmaßnahmen zur Minimierung des Risikopotentials. Eine Zulassung bis „VS – Streng Geheim" ist für das ISDN-Kryptogerät ELCRODAT 6-2 vorgesehen, das der Verschlüsselung der ISDN-Kommunikation u. a. innerhalb des IVBB dient.

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?

Die Sicherheit beim elektronischen Datenaustausch ist bei öffentlichen wie bei nicht-öffentlichen Stellen im wesentlichen eine Frage des Schutzes der Vertraulichkeit und der Integrität. Entsprechende Sicherheitsanalysen sind in der Regel immer auf einen Fall bezogen und damit nicht übertragbar.

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

Nein.

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?

Keine.

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?

Angaben hierzu enthalten die Tätigkeitsberichte des Bundesbeauftragten für den Datenschutz und die Prüfbemerkungen des Bundesrechnungshofs, die dem Deutschen Bundestag vorliegen.

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?

Soweit in Betriebssystemen für PC nicht schon geeignete Sicherheitsmechanismen integriert sind (z. B. UNIX, Windows NT), stehen insbesondere für MS-DOS- und Windows-basierte Systeme etwa ein Dutzend geeigneter Zusatzprodukte zur Verfügung.

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

Der Bundesregierung liegen keine Erkenntnisse vor.

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

Die Produktbezeichnungen können der „Liste zertifizierter IT-Produkte und -Systeme" entnommen werden, welche auf Anforderung beim BSI erhältlich ist.

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?

Diese Angaben werden von der Bundesregierung nicht erhoben.

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

Die in der genannten Sendung gezeigten Manipulationsmöglichkeiten wie das Telefonieren auf Kosten eines anderen Anlagenbetreibers oder der Mißbrauch von Leistungsmerkmalen der TK-Anlage, die ggf. das Abhören von Räumen ermöglichen sollen, wurden in erster Linie durch eine unzureichende Absicherung der Fernwartungszugänge und mangelhafte Konfiguration bzw. Administration der TK-Anlage ermöglicht. Diese Gefährdungen sind seit Anfang des Jahres 1994 bekannt und wurden durch das BSI publiziert.

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?

Der Bundesregierung ist lediglich bekannt, daß das BKA in einem Fall von Gebührenbetrug (unberechtigte Aufschaltung auf die Leitung des Anschlußeigners und anschließende fortgesetzte automatische Anwahl einer gebührenpflichtigen 0190-Nummer) gutachterlich tätig geworden ist.

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

Nach Angaben der Deutschen Telekom AG sind Manipulationen, wie sie in der ZDF-Sendung „Mit mir nicht" vom 26. März 1997 für private TK-Anlagen (Nebenstellenanlage) beschrieben wurden, bei digitalen Netzknoten des öffentlichen Telekommunikationsnetzes der Deutschen Telekom AG nicht möglich, weil diese aus konzeptionellen Gründen über solche Service-Zugänge nicht verfügen.

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?

Die Deutsche Telekom AG hat die Entwicklung der auf Verschlüsselungsbasis arbeitenden „intelligenten TAE" noch nicht abgeschlossen.

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

Die Deutsche Telekom AG kann z. Z. keine Aussagen dazu machen, in welcher Höhe durch Mißbrauch der Geschäftsbedingungen im Service-190-Verkehr Differenzen zwischen dem tatsächlichen Inkassoaufkommen und dem Entgeltanspruch nach AGB bestehen.

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?

Die genannten Manipulationsmöglichkeiten sind dem BSI seit Anfang des Jahres 1994 bekannt. Stellen der Bundesverwaltung, die zu diesem Zeitpunkt ISDN-TK-Anlagen einsetzten, sind durch Publikationen und Beratungsgespräche auf die vorhandenen Gefährdungen hingewiesen worden. Insbesondere für Anlagen mit erhöhtem Schutzbedarf wurde durch das BSI neben den Entwicklungsarbeiten für ein D-Kanal-Filter ein Prüftool erstellt, mit dessen Hilfe die ordnungsgemäße Konfiguration einer TK-Anlage überprüft werden kann.

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

Das BSI hat die Gefährdungen im Bereich digitaler Telekommunikationsanlagen in mehreren Publikationen veröffentlicht.

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?

Mögliche Gefährdungen für ISDN-TK-Anlagen und ISDN-Netze sind:

— unbefugte Nutzung der Fernadministrationsschnittstelle,

— Abhören von Räumen,

— Abhören von Gesprächen,

— Gebührenbetrug.

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

Nein.

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

Digitale Telekommunikationsanlagen im Bereich der Bundesverwaltung werden durch die Prüfgruppe des BSI geprüft. Hinweise auf Manipulationen sind nicht angefallen.

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?

Die Ergebnisse sind in folgenden Publikationen des BSI dargestellt:

— BSI 6001 – Gefährdungen bei Digitalen TK-Anlagen, April 1994

— IT-Grundschutzhandbuch, Kapitel 8, ab 1994 in jährlich aktualisierter Form

— BSI-Broschüre – Sicherheitsanforderungen an TK-Anlagen, Empfehlungen des BSI für den Bereich der Bundesbehörden in Zusammenarbeit mit dem ZVEI (Zentralverband der Elektrotechnik- und Elektroindustrie e. V.), Januar 1996.

In Vorbereitung ist:

— Muster-Leistungsverzeichnis für die Beschaffung von TK-Anlagen unter Beachtung des Sicherheitsaspekts in Zusammenarbeit mit dem ZVEI, voraussichtlich Sommer 1997.

Projekte zum Thema ISDN-Sicherheit:

- Revisionstool für digitale TK-Anlagen, Überprüfung der ordnungsgemäßen Konfiguration digitaler TK-Anlagen, vorhanden für SEL S12B, in Zusammenarbeit mit dem ZVEI (für weitere Anlagentypen unterschiedlicher Hersteller in Vorbereitung),
- Entwicklung eines D-Kanal-Filters für S_0- und S_{2M}-Schnittstellen.
- Entwicklung eines ISDN-Verschlüsselungsgeräts für S_0- und S_{2M}-Schnittstellen.

Strafrechtliche Bewältigung

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

„Manipulationen von Computersystemen", d. h. Mißbräuchen der Informations- und Kommunikationstechnik, die sich gegen Computer- und Telekommunikationssysteme und deren Bestandteile, insbesondere die Integrität, Verfügbarkeit und Authentizität von gespeicherten oder übermittelten Daten richten, oder zur Begehung von Straftaten benutzt werden, ist in erster Linie mit präventiven Maßnahmen zu begegnen. Zusätzlich notwendig sind aber auch strafrechtliche Regelungen, worüber national wie international Einigkeit besteht. In Deutschland ist in den letzten zwanzig Jahren ein umfassendes strafrechtliches Instrumentarium zur Bekämpfung von Computermißbräuchen entwickelt worden. Hinzuweisen ist hier insbesondere auf die durch das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität vom 15. Mai 1986 in das Strafgesetzbuch eingefügten Regelungen (§§ 202 a, 263 a, 269, 270, 303 a, 303 b mit zusätzlichen Änderungen der §§ 274 und 348) und die Ergänzung des § 17 UWG. In Teilbereichen einschlägig sind daneben u. a. § 43 Bundesdatenschutzgesetz (und entsprechende Regelungen in den Landesdatenschutzgesetzen), die §§ 106 ff. Urheberrechtsgesetz, § 10 Halbleiterschutzgesetz und §§ 94, 95 Telekommunikationsgesetz. Die Verfolgung dieser Straftaten setzt natürlich deren Nachweis voraus, was im Einzelfall Schwierigkeiten bedeuten kann.

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?

Die Bundesregierung hält die bestehenden strafrechtlichen Regelungen zur Bekämpfung von Computermißbräuchen grundsätzlich für ausreichend. Sie entsprechen weitgehend auch den Leitlinien des Europarates von 1989. Soweit in Einzelpunkten, insbesondere vor dem Hintergrund schnell fortschreitender technischer Entwicklung, sich ein Änderungsbedarf abzeichnet oder eine Überprüfung angezeigt ist, wird die Bundesregierung ent-

sprechende Initiativen ergreifen. Entsprechend dieser Linie hat sie in den Entwurf eines Informations- und Kommunikationsdienste-Gesetzes auch Vorschläge zu Änderungen des Straf- und Ordnungswidrigkeitenrechts aufgenommen. Ob sich auf der Grundlage der im Europarat Anfang April 1997 eingeleiteten einschlägigen Prüfungen künftig die Notwendigkeit von gesetzlichen Änderungen ergeben wird, bleibt abzuwarten.

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?

Im Bereich Computer-Viren hat das BSI häufig in entsprechenden Veröffentlichungen auf die mögliche strafrechtliche Relevanz hingewiesen. Im Bereich automatisch ausführbarer Programme (Java, ActiveX) hat das BSI vor möglichen Gefährdungen (z. B. in einer über dpa verbreiteten Pressemitteilung) gewarnt.

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?

Der Bundesregierung sind keine Fälle bekannt.

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?

Das Bundeskriminalamt ist im „Standing Committee on Information Technology (SCIT)" vertreten. Das SCIT befaßt sich mit folgenden Punkten:

- fortlaufende Analyse und Bewertung der I&K-Technik für Telekommunikationsverbindungen und IT-Verarbeitung von Interpol,
- Erarbeitung technischer und betrieblicher Regelungen für diese Bereiche und
- Unterstützung bei strategischen Entscheidungen auf dem Gebiet der Informationstechnologie und damit zusammenhängender Angelegenheiten.

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?

Eine der PCCIP entsprechendes Gremium besteht in Deutschland nicht und wird gegenwärtig nicht für erforderlich gehalten.

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?

Das BSI befaßt sich zur Zeit mit der Lösung von Sicherheitsfragen in Zusammenhang mit dem Einsatz von Softwareagenten, der Komposition von IT-Systemen sowie der Verifizierung „korrekter Software". Ein „Verification Support Environment (VSE)"-Werkzeug steht bereits zur Verfügung. Das BMVg läßt querschnittliche Untersuchungen zur technischen Sicherheit in der Informationstechnik und Studien durchführen. Wesentliche Untersuchungsbereiche sind z. Z. Sicherheitsarchitekturen, insbesondere für Systeme der Nachrichtenübermittlung, technische Standardlösungen für den sicheren Betrieb von IT-Systemen, Verfahren zur Online-Überwachung von IT-Systemen und Werkzeuge und Techniken zur vertrauenswürdigen Entwicklung von IT-Systemen bzw. zur Bewertung von handelsüblichen Produkten. Ziel der Untersuchungen sind die Verbesserung der IT-Sicherheit durch Vervollständigung der Regelwerke und Unterstützung der Vorhaben mit technischen Sicherheitslösungen sowie Erhöhung von Wirtschaftlichkeit und Interoperabilität durch Standardlösungen.

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

Zusätzlich zu den im Förderschwerpunkt Softwaretechnologie des BMBF geförderten Vorhaben sind FuE-Arbeiten zur IT-Sicherheit im geplanten Rahmenkonzept des BMBF zur Förderung der Informationstechnik vorgesehen. Darüber hinaus stellt das BSI Beratungskapazitäten für IT-Sicherheit für die Bundesverwaltung und ggf. für Landes- und Kommunalverwaltungen zur Verfügung. Das BSI bietet durch einschlägige Veröffentlichungen auch der Wirtschaft Hilfe zur Selbsthilfe an, insbesondere das IT-Grundschutz- und das IT-Sicherheitshandbuch. Die Bundeswehr hat ein Prüfzentrum IT-Sicherheit in der Bundeswehr eingerichtet. Es unterstützt die IT-Sicherheit in der Bundeswehr durch Prüfung, Bewertung und ggf. Zulassung von IT-Systemen und Einzelkomponenten sowie die Verantwortlichen für die IT-Sicherheit in der Bundeswehr bei Maßnahmen der Schadenssenkung, -begrenzung und -behebung beim Auftreten von Computeranomalien (z. B. Viren).

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

Der Bundesregierung sind zahllose Veröffentlichungen zur IT-Sicherheit bekannt, die allen IT-Anwendern zur Verfügung stehen.

Die Aufgabenstellung des BSI bietet umfangreiche zusätzliche Unterstützung für Anwender.

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

Der Inhalt des Informationsservers ist im wesentlichen fertiggestellt, eine Ausschreibung für Hardware ist erfolgt. Die Anbindung an das Internet erfolgt schnellstmöglich.

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?

Es handelt sich um das in der Einführung befindliche System Geldkarte sowie um das PIN-Verfahren bei der ec-Karte.

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?

Die Bundesregierung unterhält vielfältige Kontakte zu Fachkreisen und Gremien zur IT-Sicherheit auf nationaler und auch internationaler Ebene. Die dort gewonnenen Erkenntnisse werden in Beratungen und Entscheidungen der Bundesregierung angemessen berücksichtigt.

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?

Die Bundesregierung führt hierüber keine Statistik.

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?

Unter der Voraussetzung, daß für ein symmetrisches Verfahren keine andere Analysemethode bekannt ist als die vollständige

Absuche des Schlüsselraumes, lassen sich die nachstehenden Aussagen treffen:

- 40-Bit-Verfahren können – allerdings mit hohem zeitlichem und apparativem Aufwand mittels Hochleistungsrechnern oder auf dem Wege des „verteilten Rechnens" entziffert werden. Die genaue Höhe des Aufwandes ist verfahrensabhängig.
- 56-Bit-Verfahren erfordern zu ihrer Entzifferung den Einsatz von Spezialrechnern, die eigens zu diesem Zweck konstruiert werden müssen. Bei deren entsprechender Dimensionierung läßt sich der zeitliche Aufwand auf die Größenordnung von Stunden begrenzen.
- Die vollständige Absuche eines 128-Bit-Schlüsselraums entzieht sich jeder heute und in absehbarer Zeit verfügbaren Rechentechnik.

Ab einer Schlüssellänge von etwa 80 Bit kann – bei ansonsten entzifferungsresistentem Design – die Möglichkeit einer Analyse durch Absuche des Schlüsselraums für die überschaubare Zukunft, insbesondere die nächsten fünf Jahre, ausgeschlossen werden.

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?

Eine Statistik hierzu wird nicht geführt.

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?

Der Anwendungsbereich von Steganografie ist insofern begrenzt, als sie einen Übertragungskanal mit sehr viel höherer Bandbreite erfordert als die zu versteckende Information benötigt (typischer Fall: Textdatei, verborgen in einer Bilddatei). Liegen beide Bandbreiten in der gleichen Größenordnung (z. B. bei Sprachübertragung), ist ein sicheres Verbergen von Nutzinformation nicht mehr möglich.

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?

Derartige Verfahren sind dem Risiko manipulativer Angriffe ausgesetzt und bieten nur begrenzte Sicherheit. Ob diese als ausreichend anzusehen ist, kann nur im Einzelfall in Abhängigkeit vom Schutzbedarf der Daten und den Fähigkeiten eines potentiellen Angreifers beurteilt werden.

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?

Bis heute ist nicht nachgewiesen worden, daß eine „Differential Fault Analysis" – bei unbezweifelbarer theoretischer Machbarkeit – tatsächlich durchgeführt werden kann. Sie erfordert im übrigen auch, daß der Schlüssel nicht nur auf der Chipkarte gespeichert ist, sondern dort auch verarbeitet wird. Ferner kann diese Analysetechnik durch entsprechend redundante Systemarchitektur weitgehend blockiert werden.

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

Wesentliches Sicherheitsmerkmal eines Verschlüsselungssystems ist das Vorhandensein von Maßnahmen zum Schutz vor Fehlbedienung. Ein so ausgestattetes System kann durchaus auch in die Hände von Nicht-Spezialisten gegeben werden.

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