Deutscher Bundestag **Drucksache 13/3408**
13. Wahlperiode

27. 12. 95

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Manuel Kiper, Manfred Such und der Fraktion BÜNDNIS 90/DIE GRÜNEN
— Drucksache 13/3313 —

Das Bundesamt für Sicherheit in der Informationstechnik

Die Sicherheit von informations- und kommunikationstechnischen Systemen (IT-Sicherheit) und ihre zuverlässige Funktion gehört zu den Grundvoraussetzungen für die Beherrschbarkeit der technischen Risiken einer Informationsgesellschaft. Mit zunehmender Abhängigkeit von derartigen Systemen wächst das Bedürfnis sowohl nach sicheren Systemen als auch das nach Aufklärung, Beratung und Erforschung wie Beherrschung neuer Risikopotentiale. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat damit heute eine Aufgabe mit noch größerer Bedeutung für Bürgerinnen und Bürger als bei seiner Gründung.

Das BSI entstand 1991 aus der nur wenige Monate zuvor zur „Zentralstelle für Sicherheit in der Informationstechnik" mutierten ehemaligen „Zentralstelle für das Chiffrierwesen (ZfCh)", dem bundesdeutschen Pendant zu Chiffrier- und Dechiffrier-Organisationen wie die NSA (National Security Agency) oder das GCHO (General Communications Headquarter). Mit einer Gefahr durch Computer-Hacker und Computer-Viren begründete die Bundesregierung ihren Weg, eine mit Funktionen aus dem Geheimdienstbereich betraute Behörde unter neuer Bezeichnung mit Fragen der IT-Sicherheit zu beauftragen. Im Gegensatz dazu war zu diesem Zeitpunkt in den USA bereits die dortige zivile Standardisierungsbehörde NIST (National Institute of Standardization) mit entsprechenden Aufgaben betraut worden.

Mittlerweile ist der Aufbau des BSI abgeschlossen. Dabei haben sich einige der bei Errichtung des BSI geäußerten Bedenken in einer stärkeren Profilierung des BSI bei Beratung und Aufklärung niedergeschlagen. Trotz inhaltlicher Gewinne ist die Arbeit des BSI weiterhin auch dadurch bestimmt, Strafverfolgungsbehörden und Nachrichtendiensten zuzuarbeiten. Gleichzeitig werden Behörden beraten und Bürgerinnen und Bürgern in Fragen der IT-Sicherheit Auskunft erteilt. Zwiespältig am BSI ist also weiterhin die ungenügende Trennung zwischen nachrichtendienstlichen und polizeilichen Aufgaben einerseits und denen zur Erhöhung der IT-Sicherheit andererseits. Insbesondere bei Fragen der Kryptographie, aber auch auf anderen Gebieten der IT-Sicherheit gerät das BSI damit in einen Konflikt widersprechender Ziele, wenn der Bedarf nach Sicherheit der Wirtschaft und von Privatpersonen hinter den Interessen von Strafverfolgung und Nachrichtendiensten zurückzustehen hat.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 27. Dezember 1995 übermittelt.

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

Vorbemerkung

Die Beantwortung erfolgt im Rahmen der für den umfangreichen Fragenkatalog äußerst knappen Zeit für eine kleine Anfrage.

Die in der Vorbemerkung der Anfrage – insbesondere im letzten Absatz – vorgenommene Bewertung wird von der Bundesregierung nicht geteilt. Das BSI ist im Rahmen seines gesetzlichen Auftrags tätig. Ein Zielkonflikt besteht hier nicht.

Manipulation an Computersystemen, fehlerhafte Systeme und langfristige Entwicklung

1. Welche Fortschritte und Defizite sieht die Bundesregierung bei der Wahrung und Erhöhung der IT-Sicherheit?

   Welche Maßnahmen erscheinen ihr heute zu diesem Zweck vorrangig?

Die Sicherheit in der Informationstechnik ist eine wesentliche Voraussetzung für das Vertrauen in diese Technik. Das Bewußtsein für das Erfordernis von IT-Sicherheit wächst nicht zuletzt durch die Tätigkeit des BSI, dessen gesamte Aufgaben gleichermaßen der Förderung der IT-Sicherheit dienen.

2. Wie bewertet die Bundesregierung heute die durch die Begriffe Computer-Hacker und Computer-Viren beschriebenen Gefahren?

Die Gefahr, die von Computerviren und Hackern ausgeht, wird von der Bundesregierung ernstgenommen. Sie hält deshalb angemessene Schutzmaßnahmen und Aufklärung der Anwender für unerläßlich.

3. Wie viele Ermittlungsverfahren nach § 202a StGB (Computerspionage), § 303b StGB (Computersabotage) und § 263a StGB (Computerbetrug) wurden seit Inkrafttreten dieser Strafrechtsnormen

   a) durchgeführt,

   b) wie viele Anklagen und Aburteilungen resultieren daraus und

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

Die Zahl der „durchgeführten Ermittlungsverfahren" läßt sich mit Hilfe der Polizeilichen Kriminalstatistik (PKS) nicht feststellen. In der PKS werden lediglich polizeilich bekanntgegebene und aufgeklärte Fälle von Straftaten zum Zeitpunkt der Abgabe an die Staatsanwaltschaft gezählt. Dabei werden Fälle nach § 303b StGB (Computersabotage) nicht gesondert, sondern gemeinsam denjenigen nach § 303a StGB (Datenveränderung) ausgewiesen. Deshalb sind Zahlenangaben zu Fällen nach § 303b StGB nicht möglich.

Ausspähen von Daten (§ 202 a StGB)/Computerbetrug (§ 263 a StGB):

			1987 bis 1991 alte Länder	1991 bis 19.4. 1995 alte Länder mit Gesamt-Berlin	1993 und 1994 Bundesgebiet insgesamt
Ausspähen von Daten (§ 202 a StGB)	Fälle		248	362	268
	davon aufgeklärt		175	203	164
Computer-betrug (§ 263 a StGB)	Fälle		7 881	6 714	5 001
	davon	aufgeklärt	3 467	3 526	2 577
		vollendet	6 430	6 120	2 538*)

*) Nur 1994; für 1993 liegen diesbezüglich keine Angaben vor.

Nach den genannten Vorschriften Abgeurteilte und Verurteilte werden in der Strafverfolgungsstatistik ausgewiesen. Abgeurteilte sind Angeklagte, gegen die Strafbefehle erlassen wurden bzw. Strafverfahren nach Eröffnung des Hauptverfahrens durch Urteil oder Einstellungsbeschluß rechtskräftig abgeschlossen worden sind. Ihre Zahl setzt sich zusammen aus den Verurteilten und aus Personen, gegen die andere Entscheidungen (z. B. Einstellungen oder Freisprüche) getroffen wurden.

Die Anzahl der nach den genannten Vorschriften Abgeurteilten und Verurteilten ergibt sich aus der nachfolgenden Tabelle:

Wegen Ausspähens von Daten (§ 202 a StGB), Computerbetrug (§ 263 a StGB) bzw. Computersabotage (§ 303 b StGB) Abgeurteilte und Verurteilte in den Jahren 1987 bis 1993:

	§ 202 a StGB		§ 263 a StGB		§ 303 b StGB	
Jahr	Abgeurteilte	Verurteilte	Abgeurteilte	Verurteilte	Abgeurteilte	Verurteilte
1987	1	1	165	150	3	1
1988	4	2	366	317	–	–
1989	4	1	489	392	5	3
1990	1	–	599	504	13	6
1991[1])	1	–	732	536	9	5
1992[1])	3	1	963	824	7	4
1993[2])	5	1	1 150	967	5	5

Anmerkungen:
1) Ab 1991. – Alte Bundesländer.
2) 1993: Alte Bundesländer ohne Niedersachsen.

Quelle: Statistisches Bundesamt – Strafverfolgung 1987 Arbeitsunterlage, Tabelle 1, Strafverfolgung 1988–1991, 1993, Arbeitsunterlage Tabelle 2.1, Fachserie 10, Reihe 3 Strafverfolgung, 1992, Tabelle 2.1.

Schäden werden in der PKS nur zu den vollendeten Fällen des Computerbetrugs nach § 263 a STGB in folgender Höhe erfaßt:

	1987 bis 1991 alte Länder	1991 bis 19. 4. 1995 alte Länder mit Gesamt-Berlin	1994*) Bundesgebiet insgesamt
Schadenssumme in DM	23 Mio.	48,9 Mio.	9,3 Mio.

*) Für 1993 liegen diesbezüglich keine Angaben vor.

4. Wie bewertet die Bundesregierung im Vergleich dazu die Gefahren durch fehlerhafte Computersysteme und nachlässigen Umgang mit IT-Sicherheit?

Veröffentlichte Statistiken zu Schadensfällen bei Anwendung der IT (z. B. in KES 94/3) belegen eine hohe Schadensquote durch Fahrlässigkeit und Unwissenheit. Der Aufklärung und Beratung von IT-Anwendern in Fragen der IT-Sicherheit und möglicher Folgen unzureichender oder fehlender IT-Sicherheit kommt daher eine besondere Bedeutung zu.

5. Welche Schäden sind nach Kenntnis der Bundesregierung durch fehlerhafte Computersysteme und durch den meist auf Geringschätzung gegenüber IT-Sicherheitsproblemen beruhenden Ausfall von Computersytemen in diesem Zeitraum entstanden?

Statistische Angaben hierzu liegen nicht vor.

6. Sofern dies nicht oder nur partiell bekannt ist, wieso sind dazu keine Daten verfügbar?

Es besteht keine Pflicht zur Meldung entsprechender Daten.

7. Wie hoch ist der Anteil der mit Microsoft Betriebssystemen oder Benutzeroberflächen (MS-DOS bzw. Microsoft Windows) ausgestatteten Arbeitsplatzrechner in den Bundesbehörden?

   Wurden diese Systeme in der Bundesrepublik Deutschland oder einem anderen Land jemals evaluiert oder zertifiziert?

   Wenn nein, warum hat das BSI dies nicht getan?

Nach dem IT-Bestandsverzeichnis (Stand: 31. Dezember 1994) werden innerhalb der Bundesverwaltung auf ca. 60 000 Arbeitsplatzcomputern Microsoft Betriebssysteme/Benutzeroberflächen eingesetzt; auf weiteren ca. 5 000 Rechnern MS-DOS kompatible Betriebssysteme.

Eine Zertifizierung erfolgt auf Antrag und ist ohne Mitwirkung des Herstellers nicht möglich.

8. Welche IT-Sicherheitsrisiken – zu deren Minderung das BSI beitragen soll – sind nach Ansicht der Bundesregierung in den wichtigen, derzeit in Entwicklung befindlichen Projekten wie Bundesbehördennetz 2000, Informationsverbund Bonn—Berlin oder der Neugestaltung von INPOL und andere Projekten abzusehen, welche Maßnahmen will die Bundesregierung ergreifen, und wie hoch schätzt sie die Kosten dafür ein?

Die IT-Sicherheitskonzepte für die genannten Vorhaben werden zur Zeit noch erstellt. Darin werden die IT-Sicherheitsrisiken dargestellt. Daher kann zur Zeit auch zu den Kosten noch keine Aussage gemacht werden.

9. Beabsichtigt die Bundesregierung, in sensiblen Bereichen den Einsatz zuverlässiger, sicherheitsgeprüfter IT-Systeme vorzuschreiben?

   Wenn nein, warum nicht, und wie begründet sie diese im Vergleich zu ähnlichen technischen Risiken rechtssystematische Ausnahme?

Die Bundesregierung wird hierzu bei Bedarf bereichsspezifisch prüfen, ob Empfehlungen oder Verpflichtungen für den Einsatz sicherheitsgeprüfter IT-Systeme erforderlich sind.

10. In welchem Maße kommen die Angebote und Dienstleistungen des BSI privaten Nutzerinnen und Nutzern elektronischer Netzwerke und Dienste wie Home-Banking etc. zugute, die sich berechtigte Sorgen um ihre Sicherheit machen?

    Wurde insbesondere Home-Banking-Software schon einmal vom BSI evaluiert oder zertifiziert?

Privaten Nutzern stehen Erkenntnisse und Informationen, die das BSI über die genannten Dienstleistungen hat, zur Verfügung.

Home-Banking-Software wurde bisher nicht evaluiert bzw. zertifiziert.

11. Wie stellt sich das BSI die Entwicklung einer langfristigen IT-Sicherheitsinfrastruktur und einer entsprechenden IT-Sicherheitskultur mit der notwendigen akzeptablen Nutzbarkeit durch die Bürgerinnen und Bürger vor?

Die Bundesregierung prüft zur Zeit unter anderem eine Regelung zur „elektronischen Unterschrift". In diesem Zusammenhang wird auch die Schaffung einer Sicherheitsinfrastruktur geprüft.

Beratung zur IT-Sicherheit

12. An wen richtet sich das Beratungsangebot des BSI?

Das Beratungsangebot in Fragen der IT-Sicherheit richtet sich an Hersteller, Vertreiber und Anwender von IT.

13. Von wie vielen Personen aus welchen Bereichen – öffentlicher Dienst, Industrie, Bürgerinnen und Bürger – wurde die Beratung in den letzten fünf Jahren in Anspruch genommen?

Eine lückenlose Registrierung sämtlicher Beratungskontakte erfolgt nicht, weil sie zum größten Teil mit dem Tagesgeschäft erledigt werden. Eine Erfassung der genauen Personenzahl liegt deshalb nicht vor.

14. Welchen Anteil am Personalhaushalt des BSI hat die Beratungsaufgabe?

Der Anteil beträgt 15,8 % (1995).

15. Wie hat sich die Beratung thematisch entwickelt, insbesondere:
    a) Welche Aufklärung über IT-Sicherheit wird gegeben?
    b) Welches Beratungskonzept verfolgt die Beratungsgruppe des BSI?
    c) Wie ist die Gruppe zusammengesetzt?
    d) Welche pädagogischen Konzepte werden verfolgt?
    e) Wie wird die langfristige Risikoentwicklung in diesen Konzepten berücksichtigt?

a) Über Risiken sowie geeignete Schutzmaßnahmen.

b) Das Konzept verfolgt das Ziel, den IT-Anwender bei Planung, Realisierung und Aufrechterhaltung von IT-Sicherheit zu beraten und im übrigen auf die Entwicklung/Herstellung sicherer IT-Produkte hinzuwirken.

c) Für die Beratungsabteilung stehen Informatiker, Ingenieure, Physiker, Mathematiker und IT-erfahrene Verwaltungsfachleute zur Verfügung.

d) Das Konzept zielt auf Information, Aufklärung und Motivation ab.

e) Im Rahmen der Grundlagenarbeiten werden unter Einbeziehung der Erfahrungen aus der Beratung, Beobachtungen technologischer Entwicklungen und wissenschaftlicher Erkenntnisse neue Risiken analysiert sowie geeignete Sicherheitsvorkehrungen konzipiert.

16. Welche Anstrengungen werden unternommen, um die Beratung von Bürgerinnen und Bürgern zu verstärken?

Das BSI bietet im Rahmen des Informationsdienstes folgende Dienstleistungen für jedermann an:

— Schriftenreihe zur IT-Sicherheit (seit April 1994 sind sieben Bände erschienen),

— kostenlose Kurzinformationen in Form von Faltblättern,

- Einrichtung einer Mailbox, in der IT-Anwendern Informationen und Entscheidungshilfen zur IT-Sicherheit angeboten werden,
- ein spezieller Warndienst zu Computerviren,
- Informationsveranstaltungen und Workshops zu allen Arbeitsgebieten des BSI (z. B. jährliche IT-Grundschutzforen und Workshops zu Fragestellungen der Technikfolgenabschätzung).

17. Welche Auflage und Verbreitung hat die Zeitschrift „Kommunikations- und EDV-Sicherheit (KES)", in der das BSI einen eigenen Redaktionsteil verantwortet, welche Zielgruppe wird damit erreicht, und hält die Bundesregierung damit eine genügend große Breite für eine Aufklärung der Bürgerinnen und Bürger für gegeben?

Die Zeitschrift erscheint viermal pro Jahr in einer Auflage von 4 200 Exemplaren und zweimal pro Jahr (Messezeiten: CeBit, Sitech, Systems etc.) in einer Auflage von 5 200 Stück.

Die KES kann jede interessierte Zielgruppe erreichen, weil die Zeitschrift im Handel erhältlich ist. Sie ist eines von vielen Mitteln, um IT-Sicherheitsbewußtsein in die Öffentlichkeit zu tragen.

18. Sieht die Bundesregierung Veranlassung, daß das BSI Warnmeldungen und andere Informationen über elektronische Netze zur Verfügung stellt, wenn nein, warum nicht?

Seit Mitte 1995 werden an interessierte Nutzer Informationen und Warnmeldungen über Sicherheitslücken (u. a. im Internet) oder über das vom BSI verteilte Anti-Computer-Viren-Programm elektronisch verteilt.

19. Hält die Bundesregierung die Mailbox des BSI in Bonn für ausreichend, wenn ja, aus welchen Gründen?

Das Informationsangebot in der BSI Mailbox spiegelt den Informationsstand des BSI wider.

Die Einrichtung von Informationsservern für das Internet (World Wide Web, FTP) ist in Vorbereitung.

20. Hält es die Bundesregierung angesichts der Geschwindigkeit der technischen Entwicklung für ausreichend, IT-Sicherheit durch Schulung und Beratung zu verbessern oder wäre es nicht ökonomischer, bereits bei der Entstehung von Informations- und Kommunikationstechnologie stärker auf Sicherheitsaspekte hinzuwirken?

Es wird auf die Beantwortung der Frage 15 b) verwiesen.

Unterstützung

21. In welchem Umfang wurde eine Unterstützung durch das BSI in den letzten fünf Jahren jeweils in Anspruch genommen:
    a) von welchen Bundes- und Landesbehörden und
    b) in welchem gesetzlichen Zusammenhang?

Die Unterstützung wurde

1991 in 47 Fällen,
1992 in 77 Fällen,
1993 in 104 Fällen,
1994 in 181 Fällen,
1995 in 236 Fällen (bis 13. Dezember 1995)

in Anspruch genommen.

a) — BKA,
   — LKÄ (Bayern, Nordrhein-Westfalen, Hamburg, Hessen, Baden-Württemberg),
   — Zollfahndungsämter,
   — Polizeipräsidien,
   — Staatsanwaltschaften,
   — Zollkriminalamt;

b) Unterstützung gemäß § 3 Abs. 1 Nr. 6 BSIG.

22. Wodurch ist die im Haushalt 1996 beantragte Aufstockung des Personalbestandes für Unterstützungstätigkeiten notwendig geworden?

Durch die Steigerung der Unterstützungsersuchen an das BSI (siehe Antwort zu Frage 21).

23. Hat das BSI für Einheiten oder Stellen der Bundeswehr Beratungs- oder Unterstützungsleistungen erbracht, wenn ja, welche, wann und zu welchem Zweck?

Es fand keine Unterstützung gemäß § 3 Abs. 1 Nr. 6 BSIG für Stellen der Bundeswehr statt.

24. Hat das BSI für den BND, den MAD oder das Bundesamt oder ein Landesamt für Verfassungsschutz Unterstützungsleistungen erbracht, wenn ja, welche, wann und zu welchem Zweck?

Es fand keine Unterstützung gemäß § 3 Abs. 1 Nr. 6 BSIG für diese Behörden statt.

25. Hat das BSI für Staatsanwaltschaften oder Polizeibehörden Unterstützungsleistungen erbracht, wenn ja, welche, wann und zu welchem Zweck?

Es wird auf die Antwort zu Frage 21 verwiesen.

26. Welche Behörden hat das BSI darin unterstützt, die Abstrahlung elektronischer Geräte und Komponenten aufzufangen, und wann und zu welchem Zweck erfolgte dies?

Keine.

27. Welche Bundesbehörden haben die Länderpolizeien bei den jüngst durchgeführten Aktionen gegen die elektronische Verbreitung von Pornographie und politischem Extremismus jeweils wie unterstützt?

Gab es dazu insbesondere eine Unterstützung durch das BSI?

Das Bundeskriminalamt nimmt Aufgaben im Rahmen seiner Zentralstellenfunktion wahr. Eine Unterstützung durch das BSI ist nicht erfolgt.

28. Wie bewertet die Bundesregierung den Stand der Ausbildung und Ausrüstung der an den genannten Aktionen beteiligten und für ähnliche Aktivitäten gerüsteten Polizeieinheiten?

Trotz spürbarer Fortschritte bei einer entsprechenden Ausstattung der deutschen Polizei gilt es, die Ausrüstung weiter zu verbessern.

29. Welche Konsequenzen sieht sie darin für die Unterstützungsarbeit des BSI?

Keine.

Vierergruppe IT-Sicherheit

30. Mit welchen Behörden aus Frankreich, Großbritannien und den Niederlanden kooperiert das BSI in der sogenannten „Vierergruppe IT-Sicherheit", bei der es um neue operative Methoden der internationalen organisierten Kriminalität geht, und welche Abteilungen des BSI sind daran beteiligt?

Eine „Vierergruppe IT-Sicherheit", bei der es um neue operative Methoden der internationalen organisierten Kriminalität geht, ist der Bundesregierung nicht bekannt.

31. Welche konkreten Aufgaben hat die Vierergruppe IT-Sicherheit?

In der „Vierergruppe IT-Sicherheit" arbeiten die mit IT-Sicherheit befaßten Ministerien/Behörden Deutschlands, Frankreichs, Großbritanniens und der Niederlande mit dem Ziel zusammen, Erfahrungen auszutauschen, gemeinsame Kriterien und Verfahren für die Bewertung sicherer IT-Systeme zu entwickeln und fortzuschreiben und die nach gemeinsamen Sicherheitskriterien zertifizierten IT-Produkte und IT-Systeme gegenseitig anzuerkennen.

Zertifizierung

32. Wie viele Sicherheits-Zertifikate und für welche Sicherheits-Klasse hat das BSI ausgestellt?

33. Wie gliedern sich die zertifizierten Produkte nach Produktgruppen (Betriebssysteme, spezielle Sicherheitsprodukte etc.)?

Bis 1. Dezember 1995 sind 112 Zertifizierungsverfahren beantragt worden. Die Anzahl der bis zum 1. Dezember 1995 abgeschlossenen Verfahren beträgt 62, davon 45 mit Zertifikat. Die entsprechenden Zahlen sind der regelmäßig erscheinenden BSI-Druckschrift 7148 zu entnehmen.

Die nachfolgende Tabelle gibt eine Übersicht über die Produktkategorien:

Produktklassen	
Großrechner-Systeme	1
Mittlere Systeme	6
PC-Produkte	27
Datenübertragung (u. a. X.25- und ISDN-Sicherheit)	11
Chipkarten und Smartcards	58
Anwendungssoftware	1
Sonstige	7

Die Sicherheitsstufen (E1 = niedrigste, E6 = höchste Stufe) verteilen sich bei diesen Anträgen wie folgt:

E1	E2	E3	E4	E5	E6	hoch/nur Stärke d. Mechanismen
12	75	15	8	1	0	1

Die Sicherheitsstufen 1 und 2 vermitteln lediglich ein unteres Sicherheitsniveau (Ziel: Verhinderung von Fehlbedienungen und zufälligen Manipulationen durch Laien), während die Stufen 3 und höhere die Sicherheit vor qualifizierten Manipulationen und Penetrationen bestätigen, wenn die Prüfung auf der Grundlage anerkannter Sicherheitsanforderungen erfolgt.

34. Wie weit ist bei der Vergabe und gegenseitiger Anerkennung von Zertifikaten die internationale Abstimmung, insbesondere die auf EU-Ebene, gediehen?

Zwischen dem BSI und den britischen Stellen gibt es bereits eine Vereinbarung über die gegenseitige Anerkennung. Mit dem Schweizer Bundesamt für Informatik besteht eine Vereinbarung über die Anerkennung des BSI-Zertifikats.

Bei internationalen Projekten erhält das BSI auch Aufträge aus Skandinavien (Schweden, Finnland).

Über eine Vereinbarung auf europäischer Ebene wird zur Zeit verhandelt.

35. Wie bewertet die Bundesregierung den Aufbau einer Zertifizierungsstruktur?

Welcher Umfang von zertifizierenden Stellen erscheint ihr dabei angemessen?

Die BSI-Zertifizierung beruht auf einer ausgewogenen Arbeitsteilung zwischen privatwirtschaftlichen Prüfstellen und der Behörde BSI als Zertifizierungsstelle, welche unabhängig von kommerziellen oder produktbezogenen Interessen handelt. Das National Institute of Standardization baut zur Zeit in den USA eine Struktur nach ähnlichem Muster auf.

36. Ist das BSI im Bereich Zertifizierung personell so ausgestattet, daß es mit der technischen Enwicklung auch nur annähernd Schritt halten kann?

Derzeit ja.

37. Sieht die Bundesregierung die Notwendigkeit neuer Ansätze zu einer Zertifizierung?

Hat die Bundesregierung insbesondere die Absicht, die Zertifizierung gänzlich zu privatisieren, und wie will sie bei einer Privatisierung die Unabhängigkeit der Zertifizierung von kommerziellen Interessen garantieren?

Derzeit nein.

Forschung

38. Welche durch das BSI geleisteten Forschungsarbeiten waren nach Ansicht der Bundesregierung die wichtigsten, welche Schwerpunkte sieht sie für die nächsten Jahre?

Das BSI forscht nicht. Forschung gehört auch nicht zu den Aufgaben des BSI.

39. Hält die Bundesregierung im Zeitalter der Vernetzung von Computern – die bedeutet, Daten in den Computersystemen der unterschiedlichsten Organisationen zu lesen, aber auch zu manipulieren – die starke Betonung der Arbeiten des BSI bei der Verschlüsselung von Datenübertragungen noch für angemessen und sinnvoll?

Ja, Verschlüsselung ist eine unverzichtbare Maßnahme zum Schutz von Kommunikation und Datenverarbeitung gegen unbefugte Kenntnisnahme. Sie dient zugleich dem Schutz der Datenintegrität.

40. Welches Ergebnis hatte ein Projekt des BSI zur „Nutzung künstlicher Intelligenz zu Sicherheitsüberwachung von Anwenderhandlungen"?
    a) Welche Überwachungsprobleme sieht die Bundesregierung darin?
    b) Welche Schlußfolgerungen zieht sie aus dem Ergebnis?

Ein solches BSI-Projekt existiert nicht.

41. Welche Forschungsarbeiten zur Verbesserung der Sicherheit von Telekommunikationsanlagen sind nach Ansicht der Bundesregierung notwendig?
    Wo liegen ihrer Ansicht nach Schwachstellen?

Die Bundesregierung erarbeitet unter Beteiligung von Verbraucherverbänden und Wirtschaftsverbänden der Hersteller und Betreiber von Telekommunikationsanlagen einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen. Schwachstellen liegen insbesondere im Anschlußleitungsbereich.

42. Welche Erfordernisse sieht die Bundesregierung bei der Sicherheit zukünftiger Datennetze?
    a) Welche Forschungsaufgaben werden dazu vom Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie, und welche vom BSI betrieben?
    b) Warum leistet das BSI eigene Forschungsarbeiten?
    c) Inwieweit werden deren Ergebnisse der Allgemeinheit zur Verfügung stehen?

Seinem gesetzlichen Auftrag entsprechend betreibt das BSI keine Forschung. Im Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie (BMBF) läuft die Vorphase eines Projektes zur Sicherheit und zum Schutz in offenen Netzen („SSONET – Sicherheit und Schutz in offenen Netzen"), das darauf gerichtet ist, die national und international diskutierten und praktizierten technisch-organisatorischen Lösungen zur sicheren und geschützten Kommunikation und Transaktion in offenen Netzen zu bewerten und Empfehlungen abzuleiten. Ziel ist es, später eine international akzeptierte Lösung zu finden.

Außerdem hat der vom BMBF geförderte Verein zur Förderung eines Deutschen Forschungsnetzes (DFN-Verein) im Rahmen seines Entwicklungsprogramms Entwicklungs- und Betriebsprojekte angestoßen, weil die sichere Kommunikation auch in der Wissenschaft eine immer größere Bedeutung gewinnt. Dies gilt insbesondere für die Medizin, die Ingenieurwissenschaften, die Sozialwissenschaften und die Hochschulverwaltungen. So wurde ein Computer Emergency Response Team (CERT) eingerichtet, das die im Deutschen Forschungsnetz auftauchenden Sicherheitsprobleme registriert und mit den Nutzern präventiv und reaktiv Sicherheitslösungen erarbeitet. Außerdem wird im Deutschen Forschungsnetz ein geschützter Mail-Verkehr und die dazu erforderliche Schlüsselverwaltung realisiert und eingeführt.

Am Beispiel der räumlich verteilten Fachhochschule Rheinland-Pfalz wird die geschützte Übertragung sensitiver Daten im offenen Netz praktisch erprobt.

43. Wie bewertet die Bundesregierung das Marktpotential der Forschungsarbeiten des BSI zur Kryptierung?

    Sieht sie dabei Probleme für deren Nutzung aufgrund bestehender Verbote für Kryptierverfahren bzw. dann, wenn es auf EU-Ebene oder in den USA zu einer Regulierung von Kryptierverfahren kommt?

Arbeiten des BSI auf dem Kryptographiesektor haben die Bereitstellung von Verschlüsselungssystemen zum Ziel, die der öffentlichen Verwaltung sowie sensitiven Bereichen der deutschen Privatwirtschaft zur Verfügung stehen.

In der Bundesrepublik Deutschland bestehen keine Nutzungsverbote für Kryptierverfahren.

44. Wie viele Prototypen von Kryptiergeräten und -systemen hat das BSI entwickelt bzw. hat es entwickeln lassen?
    a) Welche davon werden heute von Unternehmen angeboten?
    b) Um welche Unternehmen handelt es sich?
    c) Wie wurde von diesen ggf. die Entwicklungsarbeit des BSI vergütet?

Das BSI hat bisher in diesem Bereich Entwicklungen ausschließlich für den staatlichen Geheimschutzbereich durchgeführt; diese Geräte werden nicht kommerziell angeboten. Privatwirtschaftliche Entwicklungen wurden vom BSI beratend begleitet.

Soweit das BSI Entwicklungsarbeiten nicht selbst durchführt, vergibt es Entwicklungsaufträge an die Industrie. In der Regel beteiligt sich die Industrie mit ca. 30 % an den Entwicklungskosten. Werden Seriengeräte an Dritte (Stellen außerhalb der Bundesverwaltung) verkauft, erfolgt ein anteiliger Rückfluß von Entwicklungsgeldern im Rahmen von Lizenzverträgen an das BSI.

45. In welchem Rahmen beteiligt sich das BSI an der Multilevel Informations Systems Security Initiative (MISSI) des US Department of Defense oder plant dies zu tun?

Das BSI beteiligt sich nicht; eine Beteiligung ist auch nicht vorgesehen.

46. In welchem Rahmen beteiligt sich das BSI am International Cryptographic Experiment (ICE) des Shape Technical Centres der NATO oder plant dies zu tun?

Das BSI beteiligt sich nicht; eine Beteiligung ist auch nicht vorgesehen.

47. In welchem Rahmen beteiligt sich das BSI an der Entwicklung eines Cryptographic Application Program Interface (CAPI) oder plant dies zu tun?

Welche wirtschaftlichen Potentiale sieht die Bundesregierung in dieser Entwicklung?

Das BSI ist Mitglied des Vereins TeleTrust e. V. und beteiligt sich in diesem Rahmen an der Definition einer kryptographischen Schnittstelle (API). Die Normierung einer solchen – herstellerunabhängigen – Schnittstelle fördert den Wettbewerb und die Interoperabilität von Systemen.

Personal

48. Wie weit ist der personelle Aufbau des BSI fortgeschritten, welcher Anpassungsbedarf hat sich dabei ergeben?

Der personelle Aufbau des BSI ist weitgehend abgeschlossen. Zur Zeit besteht im wesentlichen kein Anpassungsbedarf.

49. Wie setzt sich die Qualifikation der Mitarbeiterinnen und Mitarbeiter der Fachabteilungen des BSI zusammen (aufgegliedert nach Naturwissenschaften, Geisteswissenschaften etc.)?

In den Fachabteilungen des BSI sind u. a.

— 167 Naturwissenschaftler und Ingenieure,

— 5 Geisteswissenschaftler,

— 27 Techniker (oder ähnliche Fachausbildung)

tätig.

50. Wie viele aller und wie viele der heutigen Mitarbeiterinnen und Mitarbeiter des BSI haben zuvor jeweils in der Vorgängerorganisation des BSI, der Zentralstelle für das Chiffrierwesen (ZfCh) gearbeitet, und wie viele beim Zentralen Chiffrierorgan (ZCO) der DDR?

Von der Zentralstelle für Sicherheit in der Informationstechnik hat das BSI insgesamt 93 Mitarbeiter übernommen, wovon 13 Mitarbeiter ausgeschieden sind. Von der ZCO sind keine Mitarbeiter übernommen worden.

51. Ist die Ausstattung mit Sachmitteln adäquat oder wo liegen nach Ansicht der Bundesregierung Defizite?

Die Ausstattung mit Sachmitteln ist ausreichend.

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