Deutscher Bundestag **Drucksache 14/6321**

14. Wahlperiode 20. 06. 2001

Antwort

der Bundesregierung

auf die Große Anfrage der Abgeordneten Norbert Geis, Erwin Marschewski (Recklinghausen), Wolfgang Bosbach, weiterer Abgeordneter und der Fraktion der CDU/CSU – Drucksache 14/4173 –

Wirksamer Schutz vor Computerattacken

Das Internet als weltweites Datennetz hat in den letzten Jahren eine explosionsartige Entwicklung genommen. Es ist mittlerweile ein bedeutender Wirtschaftsfaktor, aber auch ein überaus wichtiger Träger von Informationen und Kommunikation in nahezu sämtlichen Lebensbereichen. Sowohl öffentliche Einrichtungen als auch Wirtschaft und Privatpersonen nutzen die durch das Internet eröffneten Informations- und Kommunikationsmöglichkeiten, und zwar mit steil ansteigender Tendenz.

Seiner Idee nach ist das Internet auf Offenheit und Freiheit angelegt. Jedermann kann an dem freien Austausch von Informationen teilnehmen. Zugleich wird das Internet jedoch auch für kriminelle Handlungen missbraucht. Wenngleich der Missbrauch der Datennetze im Vergleich zu deren legaler Nutzung lediglich einen verschwindenden Ausschnitt bildet, muss davon ausgegangen werden, dass die Datennetzkriminalität in den vergangenen Jahren – auch im Verhältnis zu anderen Deliktsbereichen – stetig zugenommen hat.

Eine besonders besorgniserregende Form des Missbrauchs der Datennetze bilden Angriffe auf fremde Computersysteme zu Zwecken der Sabotage oder Spionage. Computerattacken der jüngeren Vergangenheit unter Verwendung so genannter Virenangriffsprogramme belegen in alarmierender Weise, dass die weltweiten Datennetze in hohem Maße für Zugriffe Unbefugter anfällig sind. Sie liefern auch dafür Zeugnis, dass Einzelne mit vergleichsweise einfachen Mitteln und innerhalb kürzester Zeit Schäden in Milliardenhöhe anrichten können. Nach Einschätzung von Experten muss nach dem „Love-Letter-Virus“ auch künftig mit ähnlich folgenschweren Angriffen über das Internet gerechnet werden. Dies beeinträchtigt auch das Vertrauen der Nutzer und hemmt so die wirtschaftliche Entwicklung dieses Sektors.

Dieses Bedrohungspotenzial begründet ein offenkundiges Bedürfnis nach einem wirksameren Schutz insbesondere vor Computerattacken in offenen Netzwerken. Notwendig ist ein Bündel von Maßnahmen vor allem im Bereich der Prävention. Die Hersteller von Programmen sind aufgerufen, ihre Produkte sicherer zu machen. Aber auch die Nutzer müssen nachhaltig sensibilisiert werden. Dies gilt namentlich auch für die Wirtschaft in Bezug auf die besonders schadensträchtige Wirtschaftsspionage. Für den Bereich des Strafrechts ist

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 20. Juni 2001 übermittelt.

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

bereits im „Vierten Zwischenbericht der Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft“ vom 22. Juni 1998 die Empfehlung enthalten, den derzeitigen Strafrechtsschutz gegen das Freisetzen von Computerviren und ähnlichen Programmen ebenso wie die Praktikabilität des geltenden Strafverfahrensrechts einer Prüfung zu unterziehen (Bundestagsdrucksache 13/11002, S. 125). Der Bundesrat hat in seiner Entschließung vom 9. Juni 2000 (Bundesratsdrucksache 275/00 – Beschluss) eine Überprüfung des nationalen Strafrechts ebenso angemahnt wie eine Verbesserung der internationalen Zusammenarbeit.

Gleichwohl ist die Bundesregierung offensichtlich nicht bereit, das nationale Strafrecht im Benehmen mit Praxis und Wissenschaft einer umfassenden Prüfung zu unterziehen. Sie will vielmehr zunächst den Abschluss von Verhandlungen auf internationaler Ebene abwarten (vgl. u. a. Bundestagsdrucksache 14/3615, S. 2 bis 5), was zugleich die Gefahr begründet, dass der Deutsche Bundestag und die Länder faktisch vor vollendete Tatsachen gestellt werden und die gebotene umfassende Prüfung des deutschen Computerstrafrechts letztlich unterbleibt.

Vorbemerkung

Die Bundesrepublik Deutschland ist auf dem Weg in eine moderne Informationsgesellschaft. Informations- und Kommunikationstechnologien durchdringen alle Lebensbereiche. Wirtschaft und Gesellschaft erleben einen tiefgreifenden Strukturwandel. Dieser Strukturwandel erfordert von Unternehmen, Arbeitnehmern und Politik ein hohes Maß an Anpassungsfähigkeit und -bereitschaft. Das Internet ist ein Motor der Innovation in der Gesellschaft. Mit den Programmen „Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts und „Internet für alle – 10 Schritte auf dem Weg in die Informationsgesellschaft“ sowie in Zusammenarbeit mit der „Initiative D21“ begleitet und gestaltet die Bundesregierung diesen Entwicklungsprozess aktiv, um Wohlstand, Gerechtigkeit und Arbeitsplätze dauerhaft zu sichern.

Die zunehmende Verbreitung und Nutzung des Internets bedeutet zugleich eine Zunahme illegaler und schädigender Handlungen in diesem Bereich. Der grenzüberschreitende Charakter des Internets stellt die Sicherheits- und Strafverfolgungsbehörden vor neue Anforderungen.

Zur sicheren Nutzung des Internets gehört daher auch ein angemessener und wirkungsvoller Schutz vor kriminellem Missbrauch. Deshalb müssen die Strafverfolgungs- und Sicherheitsbehörden in der Lage sein, den bekannten und neuen Begehungsformen der Internet- und Datennetzkriminalität und der damit verbundenen potentiellen Bedrohung der öffentlichen Sicherheit wirksam zu begegnen. Das Internet darf bei den anstehenden Entwicklungen nicht zu einem rechtsfreien Raum werden.

Hinsichtlich der Kriminalität im Internet reicht die Bandbreite der Delikte z. B. von Pornografie, Volksverhetzung, der Verbreitung extremistischer Propaganda, dem betrügerischen Anbieten von Waren und Dienstleistungen, insbesondere dem Kreditkartenbetrug, verbotenem Glücksspiel bis hin zu unlauterer Werbung, Urheberrechtsverletzungen, dem illegalen Verkauf von Waffen, Betäubungsmitteln und Medikamenten.

Die sog. Hackingdelikte umfassen im Wesentlichen die Tatbestände der Datenveränderung (§ 303a StGB), der Computersabotage (§ 303b StGB) oder des Ausspähens von Daten (§ 202a StGB).

Der Kampf der Bundesregierung gegen kriminellen Missbrauch bezieht sich auf alle Aspekte der Computerkriminalität. Die Bekämpfung dieser als internationales Phänomen zu begreifenden Kriminalität allein im nationalen Rahmen kann allerdings nur zum Teil erfolgreich sein. Internationalen Organisationen und der Europäischen Union fällt daher bei der Entwicklung von Bekämpfungsstrategien in diesem Bereich eine wichtige Funktion zu.

Einen besonderen Schwerpunkt bilden hierbei die Vorbereitungen eines Übereinkommens zur Datennetzkriminalität (Draft Convention on Cyber-Crime) auf der Ebene des Europarats. Die internationale Dimension der Datennetzkriminalität stellt eine völlig neue Herausforderung für die Strafverfolgungs- und Sicherheitsbehörden weltweit dar. Erkennbar ist der Trend der Straftäter, im Internet die unterschiedlichen nationalen Rechtsnormen auszunutzen, um sich der Strafermittlung und/oder -verfolgung zu entziehen bzw. diese zu behindern.

Bei ihren umfassenden Bemühungen im Kampf gegen die Datennetzkriminalität arbeitet die Bundesregierung eng mit den Bundesländern, der Wirtschaft, insbesondere auch den Internetprovidern, zusammen. Im Mittelpunkt aller Bemühungen stehen die Bürgerinnen und Bürger als Nutzer des Internets.

Es gibt vielfältigen Handlungsbedarf. Von ganz entscheidender Bedeutung ist dabei, dass Regierung und Wirtschaft, aber auch der einzelne Anwender, gemeinsam dazu beitragen, die Sicherheit in der Anwendung der Informationstechnik zu verbessern. Die Partnerschaft von Staat und Wirtschaft ist gerade auf diesem Gebiet stark gefordert.

A. Allgemeines

1. Welche Arten von Computerattacken (Computersabotage und -spionage) in offenen sowie in geschlossenen Netzwerken, z. B. Intranet oder Firmennetzwerken, sind der Bundesregierung bekannt?

Computerattacken im Internet und Intranet richten sich im Allgemeinen gegen die Verfügbarkeit, die Integrität oder die Vertraulichkeit von Informationen. Angriffe können entweder durch Schadensprogramme (z. B. Computerviren, Trojanische Pferde etc.) oder direkt („online“) über Netze (Internet oder auch Intranets) erfolgen. Schadensprogramme und auch Direktangriffe nutzen in der Regel Fehler und/oder Defizite in der Konzeption, Programmierung oder Konfiguration der beteiligten Computer- und Netzsysteme aus; Schwachstellen in der verwendeten Software bzw. in den entsprechenden Kommunikationsprotokollen sind ebenfalls ein Ansatzpunkt für Computerattacken.

Im Einzelnen geht es hierbei um das

- Ausspähen, Verändern und Löschen von Daten und Dateien (z. B. durch Ausnutzen von Konfigurationsfehlern, durch Erzeugen eines „Buffer Overflow“-Fehlers[1], durch Einsatz von Software-Sniffern[2], durch Port-Scanning[3] etc.)
- Einbringen von Trojanischen Pferden[4] und Computer-Viren[5] mit den verschiedensten Schadensfunktionen (deren Ziel das unberechtigte Löschen oder Verändern von Datenträgern, die unberechtigte „Fernwartung“ von Rechnern, die Vorbereitung weiterer Angriffe etc. ist).

---

1 „Buffer-Overflow“-Fehler: sog „Speicheruberlauf“. Hierbei handelt es sich um Fehler, bei denen eine Routine zum Einlesen von Zeichen nicht prüft, ob die Länge der eingegebenen Zeichenkette mit der Länge des dafür vorgesehenen Speicherbereiches übereinstimmt Dadurch ist es Angreifern möglich, eine überlange Zeichenfolge zu übertragen, so dass hinter dem für die Eingabe reservierten Speicherbereich zusätzliche Befehle gespeichert werden können, die zur Ausführung gebracht werden.

2 Software-Sniffer: Programme, die Informationen im Netz sammeln und für eine weitere Auswertung zur Verfugung stellen. Sie dienen zur Fehlersuche der Netze, können aber auch zum Abhören benutzt werden.

3 Port-Scanning: sog Anklopfen bei Rechnern, die mit dem Internet verbunden sind.

4 Trojanische Pferde/Trojaner: Meist in Anhängen von E-Mail, aber auch in ausführbaren Download-Programmen oder aufgerufenen Webseiten verborgen übersandte Schadensprogramme, die entweder direkt Informationen auf dem Zielrechner sammeln und an den Versender der Schadensprogramme senden – beispielsweise auch Information über Nutzer und Passworte – oder die auf dem Zielrechner „Hintertüren“ installieren, die es einem Angreifer ermöglichen, sich unberechtigt in den Rechner einzuwählen und dort mit Nutzer- oder gar Administratorrechten Zugriff auf Daten und Programme zu haben, etwa um diese auszulesen, zu manipulieren oder den Rechner für seine Zwecke zu nutzen.

5 Computer-Viren: unbefugtes Einbringen von Programmen in ein fremdes Computersystem. Die Viren können, je nach Funktionsweise, sich entweder eigenständig selbst replizieren, die Rechnerkapazität überbeanspruchen, bestimmte Dateien löschen, verstecken oder Eintragungen in der Systemsteuerung vornehmen und im schlimmsten Fall auch Hardware oder Datenträger komplett zerstören.

- Beeinträchtigung der Verfügbarkeit (z. B. durch einfache oder auch verteilte „Denial of Service"-Attacken" (DoS)[6] und „Distributed Denial of Service-Attacken" (DDoS)[7], Mailbombing/Spamming[8]).

2. Welche Erkenntnisse hat die Bundesregierung über die Häufigkeit von Computerattacken mit Tatort (Tätigkeits- oder Erfolgsort) im Inland seit dem Jahr 1990 (bitte mit Jahresangaben aufschlüsseln nach Art der Computersabotage bzw. -spionage und Branche der betroffenen Unternehmen)?

Der Begriff „Computerattacken" stellt keine rechtliche Kategorie dar. Deshalb kann nicht ohne weitere Differenzierungen eine Beziehung zu relevantem strafwürdigen Verhalten nach dem Tatort (Tätigkeits- oder Erfolgsort) hergestellt werden. Dennoch ist unzweifelhaft, das die einzelnen, oben in der Antwort zu Frage 1 beschriebenen Fallvarianten von Computerattacken, in der einen oder anderen Erscheinungsform strafrechtlich unter verschiedenen Straftatbeständen des Strafgesetzbuches erfasst und geahndet werden. Zu erwähnen sind in diesem Zusammenhang insbesondere die Straftaten Computerbetrug (§ 263a StGB), Fälschung beweiserheblicher Daten (§ 269 StGB), Datenveränderung (§ 303a StGB), Computersabotage (§ 303b StGB), Ausspähen von Daten (§ 202a StGB) [umgangssprachlich Computerspionage], Störung öffentlicher Betriebe (§ 316b StGB), Störung von Telekommunikationsanlagen (§ 317 StGB), Verstöße gegen Urheberrechtsbestimmungen und die sog. Softwarepiraterie.

Im Zusammenhang mit der Computerkriminalität liegen der Bundesregierung Zeitreihen aus der Polizeilichen Kriminalstatistik (PKS) für die damit in Zusammenhang stehenden Deliktsformen – Computerbetrug, Datenveränderung, Computersabotage und Ausspähen von Daten – seit 1990 vor. Die neuen Länder sind erst seit 1993 mit erfasst. Die Zeitreihen umfassen u. a. auch die Aufklärungsquoten. Details der Tatausführung, z. B. Branchenzugehörigkeit geschädigter Unternehmen, sind aus der PKS nicht ersichtlich. Eine Differenzierung zwischen Straftaten in Zusammenhang mit dem Internet und sonstiger Computerkriminalität erfolgt in der PKS ebenfalls nicht.

Die PKS weist auch Straftaten gegen Urheberrechtsbestimmungen und sog. Softwarepiraterie aus.

Hingegen sind die Tatbestände der §§ 269, 316b und 317 StGB nach den geltenden PKS-Erhebungsmodalitäten als „sonstige Straftaten gemäß StGB" nicht einzeln darstellbar. Mit Einführung des neuen „Informationssystems Polizei" (Inpol-Neu) werden zukünftig alle registrierten Delikte einzeln von den Ländern zugeliefert und können in der PKS dargestellt werden.

6 Denial of Service-Attacken (DoS): Überfluten von Rechnern mit „Anfragen" (auf verschiedenen Ebenen der Netzprotokolle) in solcher Menge, dass deren Aufnahme- bzw. Verarbeitungskapazität nicht ausreicht und somit der Zugang für berechtigte Kontaktaufnahmen blockiert wird.

7 Distributed Denial of Service-Attacken (DDoS): Eine Unterart der DoS-Attacken, bei denen zunächst eine Vielzahl anderer Rechner mit den beschriebenen Methoden „gehackt" wird, um auf ihnen Angriffssoftware zu installieren, die dann koordiniert gleichzeitig DoS-Attacken auf einen Zielrechner ausführt.

8 Mail-Bombing/Spamming: Hier wird ausschließlich der E-Mail-Dienst von Rechnern blockiert, indem Unmengen automatisiert erzeugter, meist unsinniger E-Mails im Sekundenabstand an eine E-Mail-Adresse gesandt werden.

Polizeiliche Kriminalstatistik					**Tabelle 01**						
Grundtabelle - **ohne** Tatortverteilung-					Bereich:						
Ab 1990					20 = Bundesgebiet insgesamt (ab 93 einschl. der neuen Länder)						
					22 = alte Länder mit Ost-Berlin						
Schl.-				Häufigkeitszahl			**Aufklärung**		Gesamtzahl		
zahl	Be-		Erfaßte		von Spalte 4				der ermittelten	Nichtdeutsche	
Der Tat	reich	**Jahr**	Fälle	(erfaßte Fälle pro 100.000 Einwohner)	Versuche			in %	Tatver-	Tatverdächtige	
					Fälle	in %	Fälle	(AQ)	dächtigen	Anzahl	in %
1	2	3	4	4a	5	6	9	10	11	14	15
Computerbetrug § 263a StGB											
5175	20	1990	787	1,3	116	14,7	501	63,7	488	120	24,6
5175	22	1991	1.003	1,5	99	9,9	555	55,3	500	95	19,0
5175	22	1992	2.009	3,1	150	7,5	1.032	51,4	803	167	20,8
5175	20	1993	2.247	2,8	177	7,9	1.151	51,2	1.074	150	14,0
5175	20	1994	2.754	3,4	216	7,8	1.426	51,8	1.145	167	14,6
5175	20	1995	3.575	4,4	361	10,1	1.879	52,6	1.381	217	15,7
5175	20	1996	3.588	4,4	413	11,5	1.980	55,2	1.523	237	15,6
5175	20	1997	6.506	7,9	539	8,3	3.738	57,5	2.262	1.009	44,6
5175	20	1998	6.465	7,9	469	7,3	3.927	60,7	2.487	1.143	46,0
5175	20	1999	4.474	5,5	467	10,4	2.457	54,9	1.721	363	21,1
Datenveränderung, Computersabotage §§ 303a, 303b StGB											
Schl.-				Häufigkeitszahl			**Aufklärung**		Gesamtzahl		
zahl	Be-		Erfaßte		von Spalte 4				der ermittelten	Nichtdeutsche	
Der Tat	reich	**Jahr**	Fälle	(erfaßte Fälle pro 100.000 Einwohner)	Versuche			in %	Tatver-	Tatverdächtige	
					Fälle	in %	Fälle	(AQ)	dächtigen	Anzahl	in %
1	2	3	4	4a	5	6	9	10	11	14	15
6742	20	1990	95	0,2	11	11,6	45	47,4	66	6	9,1
6742	22	1991	122	0,2	3	2,5	49	40,2	46	6	13,0
6742	22	1992	88	0,1	1	1,1	32	36,4	38	5	13,2
6742	20	1993	137	0,2	8	5,8	50	36,5	59	9	15,3
6742	20	1994	188	0,2	1	0,5	58	30,9	73	5	6,8
6742	20	1995	192	0,2	5	2,6	80	41,7	79	4	5,1
6742	20	1996	228	0,3	2	0,9	86	37,7	127	6	4,7
6742	20	1997	187	0,2	5	2,7	99	52,9	109	8	7,3
6742	20	1998	326	0,4	11	3,4	131	40,2	150	22	14,7
6742	20	1999	302	0,4	13	4,3	174	57,6	204	36	17,6
Ausspähen von Daten § 202a StGB											
Schl.-				Häufigkeitszahl			**Aufklärung**		Gesamtzahl		
zahl	Be-		Erfaßte		von Spalte 4				der ermittelten	Nichtdeutsche	
Der Tat	reich	**Jahr**	Fälle	(erfaßte Fälle pro 100.000 Einwohner)	Versuche			in %	Tatver-	Tatverdächtige	
					Fälle	in %	Fälle	(AQ)	dächtigen	Anzahl	in %
1	2	3	4	4a	5	6	9	10	11	14	15
6780	20	1990	77	0,1	0	0,0	45	58,4	57	5	8,8
6780	22	1991	58	0,1	0	0,0	27	46,6	29	3	10,3
6780	22	1992	67	0,1	0	0,0	32	47,8	38	0	0,0
6780	20	1993	103	0,1	0	0,0	59	57,3	67	6	9,0
6780	20	1994	165	0,2	0	0,0	105	63,6	68	3	4,4

6780	20	1995	110	0,1	0	0,0	67	60,9	68	6	8,8
6780	20	1996	933	1,1	0	0,0	886	95,0	119	9	7,6
6780	20	1997	213	0,3	0	0,0	128	60,1	123	6	4,9
6780	20	1998	267	0,3	0	0,0	214	80,1	152	13	8,6
6780	20	1999	210	0,3	0	0,0	137	65,2	141	9	6,4

Straftaten gegen Urheberrechtsbestimmungen
(UrheberrechtsG, MarkenG, §17 UWG, GebrauchsmusterG
GeschmacksmusterG, KunsturheberrechtsG, PatentG)

Schl.-zahl	Be-		Erfaßte	Häufigkeitszahl	von Spalte 4		Aufklärung		Gesamtzahl der ermittelten	Nichtdeutsche	
Der Tat	reich	Jahr	Fälle	(erfaßte Fälle pro 100.000 Einwohner)	Versuche			in %	Tatver-	Tatverdächtige	
					Fälle	in %	Fälle	(AQ)	dächtigen	Anzahl	in %
1	2	3	4	4a	5	6	9	10	11	14	15
7150	20	1990	5.423	8,7	240	4,4	4.653	85,8	4.187	368	8,8
7150	22	1991	3.400	5,2	100	2,9	3.030	89,1	2.990	385	12,9
7150	22	1992	2.180	3,3	70	3,2	2.035	93,3	2.133	299	14,0
7150	20	1993	3.201	4,0	63	2,0	2.926	91,4	2.667	689	25,8
7150	20	1994	2.459	3,0	62	2,5	2.246	91,3	2.494	792	31,8
7150	20	1995	2.844	3,5	61	2,1	2.668	93,8	2.793	907	32,5
7150	20	1996	2.462	3,0	56	2,3	2.338	95,0	2.536	726	28,6
7150	20	1997	3.504	4,3	52	1,5	3.405	97,2	2.677	651	24,3
7150	20	1998	3.025	3,7	44	1,5	2.923	96,6	2.976	683	23,0
7150	20	1999	5.444	6,6	71	1,3	5.306	97,5	3.429	709	20,7

Softwarepiraterie
(private Anwendung z.B. Computerspiele) - Wird erst ab 1991 ausgewiesen -

Schl.-zahl	Be-		Erfaßte	Häufigkeitszahl	von Spalte 4		Aufklärung		Gesamtzahl der ermittelten	Nichtdeutsche	
Der Tat	reich	Jahr	Fälle	(erfaßte Fälle pro 100.000 Einwohner)	Versuche			in %	Tatver-	Tatverdächtige	
					Fälle	in %	Fälle	(AQ)	dächtigen	Anzahl	in %
1	2	3	4	4a	5	6	9	10	11	14	15
7151	22	1991	1.036	1,6	26	2,5	905	87,4	970	79	8,1
7151	22	1992	542	0,8	14	2,6	495	91,3	488	30	6,1
7151	20	1993	501	0,6	16	3,2	476	95,0	467	25	5,4
7151	20	1994	267	0,3	4	1,5	256	95,9	272	24	8,8
7151	20	1995	363	0,4	1	0,3	355	97,8	303	24	7,9
7151	20	1996	192	0,2	1	0,5	185	96,4	187	18	9,6
7151	20	1997	546	0,7	1	0,2	542	99,3	290	25	8,6
7151	20	1998	362	0,4	3	0,8	349	96,4	330	42	12,7
7151	20	1999	972	1,2	6	0,6	961	98,9	542	39	7,2

Softwarepiraterie
In Form gewerbsmäßigen Handelns - Wird erst ab 1994 ausgewiesen -

Schl.-zahl	Be-		Erfaßte	Häufigkeitszahl	von Spalte 4		Aufklärung		Gesamtzahl der ermittelten	Nichtdeutsche	
Der Tat	reich	Jahr	Fälle	(erfaßte Fälle pro 100.000 Einwohner)	Versuche			in %	Tatver-	Tatverdächtige	
					Fälle	in %	Fälle	(AQ)	dächtigen	Anzahl	in %
1	2	3	4	4a	5	6	9	10	11	14	15
7152	20	1994	89	0,1	3	3,4	82	92,1	90	9	10,0
7152	20	1995	120	0,1	2	1,7	111	92,5	131	15	11,5
7152	20	1996	187	0,2	1	0,5	180	96,3	169	20	11,8
7152	20	1997	772	0,9	1	0,1	763	98,8	146	10	6,8
7152	20	1998	289	0,4	3	1,0	284	98,3	212	26	12,3
7152	20	1999	1.252	1,5	9	0,7	1.242	99,2	338	92	27,2

3. Wie hoch beziffert bzw. schätzt die Bundesregierung die Gesamthöhe der hierdurch seit dem Jahr 1990 verursachten Schäden (bitte mit Jahresangaben aufschlüsseln nach Art der Computersabotage bzw. -spionage und Branche der betroffenen Unternehmen)?

Eine über die PKS hinausgehende Schadensstatistik wird nicht geführt. Die in den Medien häufig veröffentlichen Aufstellungen über Schäden und Schadenshöhen lassen sich nicht verifizieren.

Anhaltspunkte zur Einschätzung der Höhe durch Computersabotage bzw. -spionage verursachten Schäden sowie zur Schadenshäufigkeit liefern die Ergebnisse dreier Studien.

Das Computer Security Institut (CSI) und die Computer Intrusion Squad des FBI haben für die USA die Ergebnisse einer gemeinsamen Umfrage (Report: „Issues and trends: 2000 CSI/FBI Computer Crime and Security Survey“) vorgelegt, an der 643 Wirtschaftsunternehmen und Behörden beteiligt waren. Danach haben 70 % der Firmen und Behörden, die Mitglieder des Instituts sind, im Jahr 2000 die unbefugte Benutzung ihres Systems festgestellt. Im Jahr davor waren es noch 62 %. Der Gesamtschaden, der durch die Computerattacken entstanden sein soll, beläuft sich bei den befragten Unternehmen auf 266 Mio. US-$.

Nach der „Sicherheitsstudie 2000 – Hacker und Viren: die Welt in der Internetfalle?“ (Gerhard Hunnius in Zeitschrift für Kommunikations- und EDV-Sicherheit, KES 03/04 2000, S. 22) gaben von 176 befragten Unternehmen und Behörden in Deutschland, Österreich und der Schweiz 81% an, in der Vergangenheit mindestens einmal einer Virenattacke ausgesetzt gewesen zu sein. Des Weiteren wird berichtet, dass 40% der größeren Internetprovider[9] der drei genannten Länder in der Vergangenheit mindestens einmal das Ziel von Hackern waren oder unzulässige Manipulationen ihrer Internetdienste bemerkten.

Nach den Ergebnissen einer Untersuchung des Hamburger Forschungs- und Beratungsunternehmens MediaTransfer AG (http:// www.chip.de) führte der „I love you“-Virus bei 21 % der mit Computern ausgestatteten Firmenarbeitsplätze innerhalb Deutschlands zu Behinderungen und Ausfällen. Allerdings konnten die meisten Schäden innerhalb von 24 Stunden behoben werden.

4. In welchem Maße waren von den Angriffen auch Computersysteme der Bundesregierung sowie der ihr nachgeordneten Behörden betroffen (bitte mit Jahresangaben aufschlüsseln nach Art der Computersabotage bzw. -spionage und Höhe des verursachten Schadens)?

Hierzu liegen keine statistischen Angaben vor, da für derartige Angriffe keine Meldepflicht besteht. Allerdings haben die Erfahrungen mit dem „I love you“-Virus im letzten Jahr gezeigt, dass es nicht zu nennenswerten Beeinträchtigungen bei der Bundesverwaltung gekommen ist.

5. Wie hoch ist die Aufklärungsquote bei den festgestellten Computerattacken (bitte mit Jahresangaben aufschlüsseln nach Art der Computersabotage bzw. -spionage und Höhe des verursachten Schadens)?

Es wird auf die Antwort zu Frage 2 verwiesen.

---

9 Internetprovider: Inhaltlich unterscheidet man Content-, Service- und Accessprovider. Contentprovider können sowohl private als auch öffentliche Institutionen sein, die eigene Webseiten entwerfen und im Internet verfügbar machen, aber auch z. B. Magazine, welche ihre Artikel im Internet veröffentlichen. Serviceprovider sind solche, die eigene Informationen, auch fremde Inhalte Dritter zur Nutzung auf ihren Rechnern bereithalten. Accessprovider vermitteln lediglich den Zugang zu den Ressourcen des Internets, betreiben jedoch keine eigenen Datenspeicher.

6. Wie wurden die festgestellten Einzelfälle strafrechtlich geahndet (bitte mit Jahresangaben aufschlüsseln nach Art der Computersabotage bzw. -spionage, Höhe des verursachten Schadens, angewandten Strafvorschriften und Höhe der festgesetzten Strafe)?

Angaben über Verurteilungen nach den §§ 202a, 263a, 269, 303a und 303b StGB in den Jahren 1990 bis 1999 sowie über Art und Höhe der verhängten Strafen können den folgenden Tabellen des Statistischen Bundesamtes entnommen werden. Die Statistiken erfassen nicht, inwieweit sich die Straftäter bei der Tatbegehung der Zuhilfenahme des Internets bedient haben. Auch wird statistisch nicht erfasst, wenn in Einzelfällen Delikte, die nicht unmittelbar der Computerkriminalität zugerechnet werden (z. B. Verbreitung pornografischer Schriften, Gewaltdarstellung u. a.), mittels des Internets begangen werden. Aus den neuen Bundesländern liegen nur teilweise Erkenntnisse vor. Deshalb beziehen sich die Angaben der Bundesstatistik lediglich auf das frühere Bundesgebiet seit 1995 einschließlich Berlin-Ost.

Tabelle 1.1:

Wegen Ausspähens von Daten (§ 202a StGB) Verurteilte nach Art der strafrechtlichen Sanktion 1990 bis 1999

Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte								
	Insgesamt	nach allgemeinem Strafrecht				nach Jugendstrafrecht			
		zusammen 1)	Nach der schwersten Sanktion			zusammen	nach der schwersten Sanktion		
			Freiheitsstrafe		Geldstrafe		Jugendstrafe	Zuchtmittel	Erziehungsmaßregel
			Zu-Sammen	Dar. Straf-Aussetzung					
1990	-	-	-	-	-	-	-	-	-
1991	-	-	-	-	-	-	-	-	-
1992	1	1	-	-	1	-	-	-	-
1993	1	1	-	-	1	-	-	-	-
1994	1	1	-	-	1	-	-	-	-
1995	1	-	-	-	-	1	-	-	1
1996	7	7	-	-	7	-	-	-	-
1997	8	8	-	-	8	-	-	-	-
1998	4	3	-	-	3	1	-	1	-
1999	3	3	-	-	3	-	-	-	-

1) Einschl. der Verurteilungen zu Strafarrest.

Tabelle 1.2:

Wegen Ausspähens von Daten (§ 202a StGB) zu Geldstrafe Verurteilte nach Anzahl der Tagessätze 1990 bis 1999

Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte nach allgemeinem Strafrecht zu Geldstrafe						
		davon mit einer Anzahl von Tagessätzen von					
	Insgesamt	5 bis 15	16 bis 30	31 bis 90	91 bis 180	181 bis 360	361 und mehr
1990	-	-	-	-	-	-	-
1991	-	-	-	-	-	-	-
1992	1	-	-	1	-	-	-
1993	1	-	-	-	-	1	-
1994	1	-	1	-	-	-	-
1995	-	-	-	-	-	-	-
1996	7	1	-	3	3	-	-
1997	8	1	1	6	-	-	-
1998	3	-	1	1	1	-	-
1999	3	-	-	2	1	-	-

Tabelle 2.1:

Wegen Computerbetrugs (§ 263a StGB) Verurteilte nach Art der strafrechtlichen Sanktion 1990 bis 1999

Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte								
	Insgesamt	nach allgemeinem Strafrecht				nach Jugendstrafrecht			
		zusammen 1)	nach der schwersten Sanktion			zusammen	nach der schwersten Sanktion		
			Freiheitsstrafe		Geldstrafe		Jugendstrafe	Zuchtmittel	Erziehungsmaßregel
			zusammen	Dar. Strafaussetzung					
1990	504	365	137	96	228	139	31	85	23
1991	636	450	152	102	298	186	45	114	27
1992	824	608	191	136	416	216	41	158	17
1993	1 129	814	281	213	533	315	62	229	24
1994	1 352	1 043	330	219	713	309	69	219	21
1995	1 541	1 159	400	291	759	382	79	277	26
1996	1 742	1 307	442	326	864	435	86	326	23
1997	1 980	1 509	480	319	1 029	471	91	351	29
1998	2 470	1 946	563	396	1 382	524	96	403	25
1999	2157	1629	565	375	1064	528	108	389	31

1) Einschl. der Verurteilungen zu Strafarrest.

Tabelle 2.2:

Wegen Computerbetrugs (§ 263a StGB) zu Freiheitsstrafe Verurteilte nach Dauer der Freiheitsstrafe 1990 bis 1999

Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte nach allgemeinem Strafrecht zu Freiheitsstrafe							
	Ins-gesamt	darunter mit einer Dauer von						
		unter 6 Monate	6 Monate	6 Monate bis einschl. 1 Jahr	über 1 Jahr bis einschl. 2 Jahre	über 2 Jahre bis einschl. 3 Jahre	über 3 Jahre bis einschl. 5 Jahre	über 5 Jahre bis einschl. 10 Jahre
1990	137	49	24	53	7	3	1	-
1991	152	60	31	38	19	3	1	-
1992	191	68	42	58	20	2	1	-
1993	281	94	56	102	24	4	1	-
1994	330	101	49	132	40	5	2	1
1995	400	103	66	165	60	4	2	-
1996	442	108	79	191	56	6	1	1
1997	480	121	94	174	73	14	3	1
1998	563	143	99	222	84	12	1	2
1999	565	121	98	236	91	16	3	-

Tabelle 2.3:

Wegen Computerbetrugs (§ 263a StGB) zu Geldstrafe Verurteilte nach Anzahl der Tagessätze 1990 bis 1999

Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte nach allgemeinem Strafrecht zu Geldstrafe						
	Ins-gesamt	davon mit einer Anzahl von Tagessätzen von					
		5 bis 15	16 bis 30	31 bis 90	91 bis 180	181 bis 360	361 und mehr
1990	228	16	45	147	18	2	-
1991	298	14	67	190	26	1	-
1992	416	7	98	269	41	1	-
1993	533	12	115	360	45	1	-
1994	713	22	167	443	76	5	-
1995	759	19	128	488	115	8	1
1996	864	12	127	538	174	13	-
1997	1 029	33	165	655	168	8	-
1998	1 382	62	300	786	222	11	1
1999	1064	16	199	657	179	11	2

Tabelle 2.4:

Wegen Computerbetrugs (§ 263a StGB) zu Jugendstrafe Verurteilte nach Dauer der Jugendstrafe 1990 bis 1999

Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte nach Jugendstrafrecht zu Jugendstrafe						
	Insgesamt	darunter mit einer Dauer von					
		6 Monate	6 Monate bis einschl. 1 Jahr	über 1 Jahr bis einschl. 2 Jahre	über 2 Jahre bis einschl. 3 Jahre	über 3 Jahre bis einschl. 5 Jahre	über 5 Jahre bis einschl. 10 Jahre 1)
1990	31	8	9	11	1	1	1
1991	45	10	19	13	3	-	-
1992	41	7	11	19	3	1	-
1993	62	14	26	18	3	1	-
1994	69	7	26	30	5	1	-
1995	79	15	35	24	4	1	-
1996	86	13	37	27	8	1	-
1997	91	17	39	27	8	-	-
1998	96	17	37	32	9	1	-
1999	108	16	43	39	10	-	-

1) Einschl. der Verurteilungen zu Strafarrest.

Tabelle 3.1:

Wegen Fälschung beweiserheblicher Daten (§ 269 StGB) Verurteilte nach Art der strafrechtlichen Sanktion 1990 bis 1999

Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte								
	Insgesamt	nach allgemeinem Strafrecht				nach Jugendstrafrecht			
		zusammen 1)	nach der schwersten Sanktion			zusammen	nach der schwersten Sanktion		
			Freiheitsstrafe		Geldstrafe		Jugendstrafe	Zuchtmittel	Erziehungsmaßregel
			zusammen	Dar. Strafaussetzung					
1990	15	14	3	3	11	1	-	-	1
1991	11	10	3	2	7	1	-	1	-
1992	15	12	3	2	9	3	1	2	-
1993	6	5	3	2	2	1	-	1	-
1994	13	13	4	1	9	-	-	-	-
1995	9	7	1	1	6	2	1	1	-
1996	21	18	6	5	12	3	2	1	-
1997	26	22	11	7	11	4	1	2	1
1998	164	153	19	15	134	11	2	6	3
1999	78	75	12	10	63	3	-	3	-

1) Einschl. der Verurteilungen zu Strafarrest.

Tabelle 3.2:

Wegen Fälschung beweiserheblicher Daten (§ 269 StGB) zu Freiheitsstrafe Verurteilte nach Dauer der Freiheitsstrafe
1990 bis 1999
Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte nach allgemeinem Strafrecht zu Freiheitsstrafe							
	Ins-gesamt	darunter mit einer Dauer von						
		unter 6 Monate	6 Monate	6 Monate bis einschl. 1 Jahr	über 1 Jahr bis einschl. 2 Jahre	über 2 Jahre bis einschl. 3 Jahre	über 3 Jahre bis einschl. 5 Jahre	über 5 Jahre bis einschl. 10 Jahre
1990	3	1	1	1	-	-	-	-
1991	3	-	2	1	-	-	-	-
1992	3	2	-	1	-	-	-	-
1993	3	1	-	2	-	-	-	-
1994	4	2	-	1	1	-	-	-
1995	1	-	-	1	-	-	-	-
1996	6	2	-	3	-	-	1	-
1997	11	2	-	5	4	-	-	-
1998	19	2	3	9	3	2	-	-
1999	12	3	-	3	6	-	-	-

Tabelle 3.3:

Wegen Fälschung beweiserheblicher Daten (§ 269 StGB) zu Geldstrafe Verurteilte nach Anzahl der Tagessätze
1990 bis 1999
Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte nach allgemeinem Strafrecht zu Geldstrafe						
	Ins-gesamt	Davon mit einer Anzahl von Tagessätzen von					
		5 bis 15	16 bis 30	31 bis 90	91 bis 180	181 bis 360	361 und mehr
1990	11	1	5	5	-	-	-
1991	7	-	1	6	-	-	-
1992	9	-	1	5	2	1	-
1993	2	-	1	1	-	-	-
1994	9	-	7	2	-	-	-
1995	6	-	4	2	-	-	-
1996	12	-	1	6	2	3	-
1997	11	-	4	7	-	-	-
1998	134	3	11	108	11	1	-
1999	63	1	3	56	3	-	-

Tabelle 3.4:

Wegen Fälschung beweiserheblicher Daten (§ 269 StGB) zu Jugendstrafe Verurteilte nach Dauer der Jugendstrafe 1990 bis 1999

Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte nach Jugendstrafrecht zu Jugendstrafe						
	Ins-gesamt	darunter mit einer Dauer von					
		6 Monate	6 Monate bis einschl. 1 Jahr	über 1 Jahr bis einschl. 2 Jahre	über 2 Jahre bis einschl. 3 Jahre	über 3 Jahre bis einschl. 5 Jahre	über 5 Jahre bis einschl. 10 Jahre 1)
1990	-	-	-	-	-	-	-
1991	-	-	-	-	-	-	-
1992	1	-	1	-	-	-	-
1993	-	-	-	-	-	-	-
1994	-	-	-	-	-	-	-
1995	1	-	-	1	-	-	-
1996	2	1	1	-	-	-	-
1997	1	-	-	1	-	-	-
1998	2	-	1	1	-	-	-
1999	-	-	-	-	-	-	-

1) Einschl. der Verurteilungen zu Strafarrest.

Tabelle 4.1:

Wegen Datenveränderung (§ 303a StGB) Verurteilte nach Art der strafrechtlichen Sanktion 1990 bis 1999

Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte								
	Ins-gesamt	nach allgemeinem Strafrecht				nach Jugendstrafrecht			
		zu-sammen 1)	nach der schwersten Sanktion			zu-sammen	nach der schwersten Sanktion		
			Freiheitsstrafe		Geldstrafe		Jugend-strafe	Zucht-mittel	Erziehungs-maßregel
			zu-sammen	Dar. Straf-Aussetzung					
1990	4	4	-	-	4	-	-	-	-
1991	6	5	-	-	5	1	-	1	-
1992	4	4	-	-	4	-	-	-	-
1993	5	5	-	-	5	-	-	-	-
1994	5	2	-	-	2	3	-	3	-
1995	7	5	1	-	4	2	-	2	-
1996	5	5	-	-	5	-	-	-	-
1997	10	7	1	1	6	3	-	3	-
1998	4	4	-	-	4	-	-	-	-
1999	4	3	-	-	3	1	-	1	-

1) Einschl. der Verurteilungen zu Strafarrest.

Tabelle 4.2:

Wegen Datenveränderung (§ 303a StGB) zu Freiheitsstrafe Verurteilte nach Dauer der Freiheitsstrafe 1990 bis 1999

Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte nach allgemeinem Strafrecht zu Freiheitsstrafe							
	Ins-gesamt	darunter mit einer Dauer von						
		unter 6 Monate	6 Monate	6 Monate bis einschl. 1 Jahr	über 1 Jahr bis einschl. 2 Jahre	über 2 Jahre bis einschl. 3 Jahre	über 3 Jahre bis einschl. 5 Jahre	über 5 Jahre bis einschl. 10 Jahre
1990	-	-	-	-	-	-	-	-
1991	-	-	-	-	-	-	-	-
1992	-	-	-	-	-	-	-	-
1993	-	-	-	-	-	-	-	-
1994	-	-	-	-	-	-	-	-
1995	1	1	-	-	-	-	-	-
1996	-	-	-	-	-	-	-	-
1997	1	-	-	1	-	-	-	-
1998	-	-	-	-	-	-	-	-
1999	-	-	-	-	-	-	-	-

Tabelle 4.3:

Wegen Datenveränderung (§ 303a StGB) zu Geldstrafe Verurteilte nach Anzahl der Tagessätze 1990 bis 1999

Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte nach allgemeinem Strafrecht zu Geldstrafe						
	Ins-gesamt	davon mit einer Anzahl von Tagessätzen von					
		5 bis 15	16 bis 30	31 bis 90	91 bis 180	181 bis 360	361 und mehr
1990	4	3	1	-	-	-	-
1991	5	2	3	-	-	-	-
1992	4	1	1	2	-	-	-
1993	5	-	5	-	-	-	-
1994	2	-	-	2	-	-	-
1995	4	-	4	-	-	-	-
1996	5	1	2	2	-	-	-
1997	6	-	3	2	1	-	-
1998	4	1	1	2	-	-	-
1999	3	1	1	-	1	-	-

Tabelle 5.1:

Wegen Computersabotage (§ 303b StGB) Verurteilte nach Art der strafrechtlichen Sanktion 1990 bis 1999

Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte								
	Insgesamt	nach allgemeinem Strafrecht				nach Jugendstrafrecht			
		zusammen 1)	nach der schwersten Sanktion			zusammen	nach der schwersten Sanktion		
			Freiheitsstrafe		Geldstrafe		Jugendstrafe	Zuchtmittel	Erziehungsmaßregel
			zusammen	Dar. Straf-Aussetzung					
1990	6	5	-	-	5	1	-	-	1
1991	5	4	-	-	4	1	-	1	-
1992	4	2	-	-	2	2	-	2	-
1993	5	5	1	1	4	-	-	-	-
1994	2	2	1	1	1	-	-	-	-
1995	3	3	1	-	2	-	-	-	-
1996	2	2	1	-	1	-	-	-	-
1997	3	2	-	-	2	1	-	1	-
1998	2	1	-	-	1	1	-	1	-
1999	4	3	1	1	2	1	-	1	-

1) Einschl. der Verurteilungen zu Strafarrest.

Tabelle 5.2:

Wegen Computersabotage (§ 303b StGB) zu Freiheitsstrafe Verurteilte nach Dauer der Freiheitsstrafe 1990 bis 1999

Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte nach allgemeinem Strafrecht zu Freiheitsstrafe							
	Insgesamt	darunter mit einer Dauer von						
		unter 6 Monate	6 Monate	6 Monate bis einschl. 1 Jahr	über 1 Jahr bis einschl. 2 Jahre	über 2 Jahre bis einschl. 3 Jahre	über 3 Jahre bis einschl. 5 Jahre	über 5 Jahre bis einschl. 10 Jahre
1990	-	-	-	-	-	-	-	-
1991	-	-	-	-	-	-	-	-
1992	-	-	-	-	-	-	-	-
1993	1	-	1	-	-	-	-	-
1994	1	-	1	-	-	-	-	-
1995	1	-	-	1	-	-	-	-
1996	1	-	-	-	1	-	-	-
1997	-	-	-	-	-	-	-	-
1998	-	-	-	-	-	-	-	-
1999	1	-	-	-	1	-	-	-

Tabelle 5.3:

Wegen Computersabotage (§ 303b StGB) zu Geldstrafe Verurteilte nach Anzahl der Tagessätze 1990 bis 1999

Früheres Bundesgebiet, seit 1995 einschl. Berlin-Ost

Jahr	Verurteilte nach allgemeinem Strafrecht zu Geldstrafe						
	Insgesamt	Davon mit einer Anzahl von Tagessätzen von					
		5 bis 15	16 bis 30	31 bis 90	91 bis 180	181 bis 360	361 und mehr
1990	5	2	1	2	-	-	-
1991	4	2	2	-	-	-	-
1992	2	-	1	-	1	-	-
1993	4	-	1	3	-	-	-
1994	1	-	-	1	-	-	-
1995	2	-	1	1	-	-	-
1996	1	-	-	1	-	-	-
1997	2	1	-	1	-	-	-
1998	1	-	-	1	-	-	-
1999	2	-	2	-	-	-	-

7. Welches Ausmaß haben nach den Erkenntnissen bzw. Schätzungen der Bundesregierung die nicht bekannt gewordenen Fälle der Computersabotage und -spionage (so genanntes Dunkelfeld)?

Für den Bereich der Computersabotage bzw. -spionage gibt es derzeit noch keine konkreten polizeilichen Erkenntnisse. Es wird aus den folgenden Gründen angenommen, dass ein erhebliches Dunkelfeld existiert:

- Häufig kommt die Computersabotage bzw. -spionage über eine bloße Vorbereitungshandlung nicht hinaus, da in den meisten Fällen bereits technische Sicherheitsvorkehrungen, z. B. Virenscanner, präventiv eine größere Ausbreitung des Virus und damit die Schädigung einer DV-Anlage verhindern.
- DoS-Attacken und Ausspähversuche bzw. Hackingangriffe werden in vielen Fällen nicht als solche erkannt, sondern als technische Störung interpretiert.
- In der IT-Branche tätige Unternehmen sehen vielfach von einer Strafanzeige bei den Polizeibehörden ab, da sie befürchten, bei einem möglichen Bekanntwerden des Vorfalles in der Öffentlichkeit einen Imageverlust oder Vertrauensschaden zu erleiden. Dies kann bei jungen börsennotierten „Start-up-Firmen“ zu enormen Kursverlusten führen und letztendlich die Existenz des betreffenden Unternehmens bedrohen.

8. Welche Erkenntnisse liegen der Bundesregierung über Häufigkeit, Ausmaß, Aufklärung sowie strafrechtliche Ahndung von Computerattacken im Ausland (insbesondere in den Mitgliedstaaten der Europäischen Union) vor?

Erkenntnisse über Computerattacken im Ausland, insbesondere in den Mitgliedstaaten der Europäischen Union, liegen nur in Einzelfällen vor. Aussagekräftige und statistisch gesicherte Aussagen über Häufigkeit, Ausmaß, Aufklärung sowie strafrechtliche Ahndung von Computerattacken im Ausland können nicht getroffen werden.

9. Welche System- und Programmarten sind nach Auffassung der Bundesregierung besonders anfällig für Computerattacken?

Nach den vorliegenden Erkenntnissen erhöht die steigende Komplexität von Programmen, wie z. B. bei Rechnern, die Serverdienste[10] anbieten, deren Anfälligkeit für ausnutzbare Fehler bei der Programmierung oder Konfiguration. Mangelhafte Administration ist ebenfalls ein Indiz für die Anfälligkeit gegenüber Computerattacken.

Eine weitere Gefährdung resultiert aus dem Marktdruck, in schneller Abfolge neue – unter Umständen nicht hinreichend getestete – Programmversionen zu generieren.

Als besonders anfällig für Computerattacken gelten solche proprietären, d. h. herstellergebundenen Systeme, auf denen bereits eine Vielzahl unterschiedlicher Programme und Dateien vorinstalliert sind und die nicht – wie beispielsweise Open-Source-Produkte – von einer sehr großen Zahl von Testern bis auf die Quelltextebene kontrolliert werden können. Aus der Sicht der IT-Sicherheit lässt dies den Schluss zu, dass möglichst offen mit Informationen über das „Innenleben“ von Produkten umgegangen werden sollte.

B. Maßnahmen auf nationaler Ebene

10. Welche konkreten Maßnahmen hält die Bundesregierung auf nationaler Ebene für geboten, um der zunehmenden Datennetzkriminalität im Allgemeinen und der Bedrohung durch Computerattacken im Besonderen entgegen zu treten, und in welchem zeitlichen Rahmen und auf welche Weise gedenkt die Bundesregierung eine Umsetzung der erwogenen Maßnahmen?

In rechtlicher Hinsicht ist wesentlichen Aspekten der Datennetzkriminalität und der Computerstraftaten bereits mit dem derzeit geltenden materiellen Computerstrafrecht und dem Strafprozessrecht Rechnung getragen. Die notwendigen nationalen Maßnahmen der Bundesregierung werden dabei in einen internationalen Kontext eingebettet. Besonders geboten sind Maßnahmen der Kriminalprävention und der technischen Prävention. Im Bereich der technischen Prävention ist vor allem die Wirtschaft gefordert, sichere Informations- und Kommunikationssysteme, -produkte und -komponenten zu entwickeln und auf den Markt zu bringen. Hierdurch sollen Straftaten nach Möglichkeit von vornherein verhindert werden, damit Schäden für den Einzelnen oder für unsere Informationsgesellschaft erst gar nicht entstehen.

10 Serverdienste sind Dienste, die von anderen Rechnern über das Netz genutzt werden können.

a) Mit dem derzeit geltenden materiellen Computerstrafrecht wird der heutigen Datennetzkriminalität in weitem Umfang wirksam begegnet. Durch das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität vom 15. Mai 1986, WiKG, BGBI. l 721, sind zusätzliche Strafvorschriften zur Bekämpfung der Computerkriminalität im Strafgesetzbuch verankert worden (§§ 202a, 263a, 269, 270 – mit Ergänzungen der §§ 274 und 348, §§ 303a, 303b), ergänzt durch eine Erweiterung des § 17 des Gesetzes gegen unlauteren Wettbewerb (UWG). Diese Regelungen, bei deren Schaffung auch Empfehlungen auf internationaler Ebene (Schlussfolgerungen einer OECD-Arbeitsgruppe von 1985) berücksichtigt wurden, entsprechen durchweg den vom Lenkungsausschuss für Strafrecht des Europarates 1989 empfohlenen Leitlinien zur Computerkriminalität. Die Wirksamkeit des geltenden Rechts zeigt sich daran, dass die DDoS-Attacken des vergangenen Jahres durch die Regelungen des Strafgesetzbuches erfasst worden sind. Auch wenn bei diesen Taten die Handlung (z. B. Freisetzen von Viren) in vielen Fällen im Ausland vorgenommen wird, ist das deutsche Strafrecht anwendbar, sobald deren Erfolg (z. B. eine Datenveränderung) im Inland auftritt (§§ 3, 9 StGB).

b) In strafprozessualer Hinsicht kommt der schnellen Sicherung von Datenspuren und ihrer raschen Zurückverfolgung bis zum Computer, der sie hinterlassen hat, besondere Bedeutung zu. Im Strafverfahrensrecht überprüft die Bundesregierung deshalb die Wirksamkeit des bereits bestehenden Ermittlungsinstrumentariums, beispielsweise die durch § 100a Strafprozessordnung (StPO) und § 12 Fernmeldeanlagengesetz (FAG) eröffneten Möglichkeiten.

c) Die Aktivitäten internationaler Organisation, wie z. B. des Europarates und der Europäischen Union, beeinflussen und flankieren die nationalen Maßnahmen in den jeweiligen Mitgliedstaaten.

   Im Hinblick auf kommende internationale Bestimmungen werden zusätzliche Regelungen im Bereich des Straf- und des Strafverfahrensrechts zu prüfen sein. Hier gehen die Erwartungen von einem Übereinkommen zur Datennetzkriminalität des Europarates (Convention on Cyber-Crime) aus, das im Entwurf vorliegt.

   Vor dem Hintergrund, dass die Sicherheit von Netzen und die Bekämpfung der Computerkriminalität eines der Ziele des im Juni 2000 vom Europäischen Rat in Feira angenommenen „eEurope“-Aktionsplanes ist, hat die EU-Kommission in 2001 eine Mitteilung zur Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität an den Rat und das Europäische Parlament veröffentlicht (Korn (2000) 890 endg. v. 26. Januar 2001). Die darin angesprochene Vorgehensweise findet die Unterstützung der Bundesregierung.

   Kurzfristig hat die EU-Kommission in diesem Zusammenhang am 21. Dezember 2000 den Entwurf eines Rahmenbeschlusses zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie (Dokument 5206/01 Droipen 2) vorgelegt, mit dem eine Angleichung der strafrechtlichen Bestimmungen der Mitgliedstaaten zur sexuellen Ausbeutung von Kindern und zur Kinderpornografie, einschließlich der Verbreitung im Internet, angestrebt wird; dieser Vorschlag wird gegenwärtig in der Rats-Arbeitsgruppe „Materielles Strafrecht“ erörtert.

   Langfristig plant die EU-Kommission, im Rahmen der Zusammenarbeit „Justiz und Inneres“ Legislativvorschläge zur weiteren Angleichung der materiellen Strafrechtsvorschriften für den Bereich der Computerkriminalität vorzulegen.

   Schließlich beabsichtigt die Kommission zu prüfen, inwieweit Maßnahmen zur Bekämpfung von Rassismus und Fremdenfeindlichkeit sowie des Dro-

genhandels im Internet ergriffen werden können. Weiter möchte die Kommission den Schutz vor Computerstraftaten durch die Angleichung und ggf. durch Verleihung neuer strafprozessualer Befugnisse für die Strafverfolgungsbehörden verbessern.

d) Zur Prävention im Bereich Datennetzkriminalität und Computerstraftaten sind folgende Maßnahmen ergriffen worden:

Der Bundesminister des Innern hat im Februar 2000 die Task Force „Sicheres Internet“ ins Leben gerufen. Die aus Vertretern des Bundesministeriums des Innern (BMI), des Bundesministeriums für Wirtschaft und Technologie (BMWi), des Bundesministeriums der Justiz (BMJ), des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Bundeskriminalamtes (BKA) bestehende Task Force prüft Art und Umfang der Bedrohung in Deutschland und erarbeitet Gegenmaßnahmen, um die Schäden für unsere Informationsgesellschaft zu minimieren. Bisher wurden zwei Maßnahmenkataloge zur Abwehr von DDoS-Attacken (http://www.bsi.de/taskforce/ddos.htm) und zum Schutz vor Computerviren (http://www.bsi.de/taskforce/viren.htm) erarbeitet und der Öffentlichkeit im Internet zur Verfügung gestellt. Die Maßnahmenkataloge leisten einen wichtigen Beitrag, den kriminellen Missbrauch des Internets zu erschweren bzw. zu verhindern.

Die weiteren Aktivitäten der Task Force „Sicheres Internet“ konzentrieren sich darauf, die Maßnahmenempfehlungen in Standardprodukten, wie etwa Internetbrowsern und E-Mail-Programmen, bereits für die Produktentwicklung nutzbar zu machen, um die Sicherheit dieser Produkte zu erhöhen. Berücksichtigt werden müssen dabei allerdings die üblichen Entwicklungszyklen in der Wirtschaft. Die Bundesregierung steht hier im intensiven Dialog mit den entsprechenden Herstellern.

Daneben fördert das BMWi mit dem Wettbewerb VERNET gezielt die Entwicklung und Erprobung neuer Technologien für sichere und verlässliche Transaktionen in offenen Kommunikationsnetzen. Dabei geht es insbesondere um den sicheren und verlässlichen Datenaustausch zwischen Unternehmen, Verwaltungen und Privatpersonen, den Schutz privater Daten und geistigen Eigentums und die Gewährleistung der Authentizität von Informationen und Transaktionen. Acht Projekte wurden ausgewählt, für die rd. 20 Mio. DM an Fördermitteln bereitgestellt werden. Konsortien aus Industrie, Forschungseinrichtungen und Anwendern müssen einen angemessenen Eigenbeitrag leisten (Unternehmen mind. 50 %). Förderfähige Projekte können bereits im Frühsommer starten.

Ein Erfolg des Städtewettbewerbs „Media(@)Komm“, der ebenfalls vom BMWi gefördert wurde, stellt u. a. die Entwicklung des neuen Schnittstellenstandards OSCI – Online Services Computer Interface – dar. Dieser berücksichtigt die Anforderungen für den sicheren Informationsaustausch zwischen Bürger und Verwaltung und findet auf nationaler Ebene immer breitere Akzeptanz. Wichtige Elemente dieses Standards sind die Gewährleistung der Authentizität von Daten und die Wahrung der Anonymität des Anwenders gegenüber unbefugten Dritten. Die digitale Signatur bildet dabei einen wichtigen Kern.

Daneben verfolgt die Bundesregierung den Ansatz, durch den flächendeckenden Einsatz von Standard-IT-Sicherheitsmaßnahmen für alle Arten von Computersystemen und -netzen das Schutzniveau von Computersystemen so weit anzuheben, dass auch ein weiterer wichtiger kriminalpräventiver Beitrag geleistet wird. Hierzu hat das BSI das IT-Grundschutzhandbuch entwickelt. Für typische informationstechnische Systeme und Komponenten enthält das IT-Grundschutzhandbuch praxiserprobte Standard-Sicherheitsmaßnahmen mit detaillierten Hinweisen zu deren Umsetzung, um wirksam vor Computerkriminalität und Computerattacken zu schützen. Das IT-Grundschutzhandbuch hat sich innerhalb kurzer Zeit als Standardwerk zur IT-Sicherheit etabliert und

steht jedermann kostenfrei unter „http://www.bsi.de/gshb/start.htm“ zur Verfügung. Zu den bisher ungefähr 5 000 freiwillig registrierten Anwendern in Deutschland (gemeint sind hier Institutionen, Unternehmen, Behörden etc.) treten noch zahlreiche international namhafte Unternehmen und öffentliche Einrichtungen hinzu.

Das BSI leistet darüber hinaus im Rahmen seiner gesetzlichen Aufgaben weitere wichtige Beiträge im Zusammenhang mit technischer Kriminalprävention durch sichere Informationstechnik. Hierzu gehören unter anderem die Analyse und Bewertung von Kryptoalgorithmen (z. B. im Zusammenhang mit dem Signaturgesetz), die IT-Sicherheitsberatung und die Produktzertifizierung.

e) In administrativer Hinsicht benötigen die Strafverfolgungsbehörden entsprechend den technischen Entwicklungen eine adäquate Ausstattung, um Straftäter in Datennetzen wirksam verfolgen zu können. Staatsanwälte und Polizeibeamte müssen zudem über das erforderliche Fachwissen zum Einsatz dieser Technik verfügen, das aufgrund der rasanten Entwicklung in der Informationstechnologie ständig aktualisiert werden muss.

Weiterhin arbeiten Strafverfolgungs- und Sicherheitsbehörden und Einrichtungen der Wirtschaft gut und vertrauensvoll zusammen, wenn es darum geht, strafbare Inhalte öffentlich zugänglicher Internetseiten aufzudecken oder Verdächtiges den Ermittlungsbehörden zu melden. Die Bemühungen der Wirtschaft um den Aufbau einer effizienten freiwilligen Selbstkontrolle werden von der Bundesregierung begrüßt. Ein gutes Beispiel ist die freiwillige Selbstkontrolle Multimedia e. V. (FSM), die als Zusammenschluss von Medienunternehmen 1997 gegründet wurde. Eine Überwachungspflicht der von Internetanbietern vermittelten Inhalte besteht allerdings nicht und ist nach der europäischen Richtlinie über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Abl. EG L 178 S. 1 vom 17. Juli 2000) auch nicht vorgesehen. Das BKA unterhält gute informationelle Kontakte zu den im Bereich der Informations- und Kommunikationstechnologien tätigen Unternehmen und hat mehrfach gut besuchte Tagungen zu diesem Thema durchgeführt. Dieser Dialog wird auch künftig fortgesetzt. Darüber hinaus wird zur Zeit geprüft, ob „Hotlines“ für geschädigte Bürgerinnen und Bürger sowie Unternehmen eingerichtet werden können.

11. Welcher Handlungsbedarf besteht nach Auffassung der Bundesregierung im Bereich der technischen Prävention (über die eingerichtete Task Force „Sicheres Internet“ sowie die bereits erfolgte Gründung einer Partnerschaft „Sichere Internet-Wirtschaft“ durch führende Vertreter deutscher Wirtschafts- und Computerverbände, führende Unternehmen und den Bundesminister für Wirtschaft und Technologie hinaus), um die Sicherheit von Computersystemen zu verbessern und das Problembewusstsein der Nutzer zu wecken bzw. zu stärken?

Ergänzend zu den bereits ergriffenen Maßnahmen sollte durch gezielte Sensibilisierungskampagnen an Schulen und Hochschulen langfristig und dauerhaft das Problembewusstsein für den Bereich der IT-Sicherheit gefördert werden.

Zudem hat sich die Forschung und Lehre des Themas IT-Sicherheit angenommen. Die Ruhr-Universität Bochum bietet im Zusammenhang mit den drei Lehrstühlen für System-, Kommunikations- und Informationssicherheit bei den Fakultäten für Mathematik sowie Elektrotechnik den Rahmen für einen regulären Studiengang „IT- Sicherheit“ an.

Im Übrigen wird auf die Antworten zu den Fragen 12 und 17 verwiesen.

12. Wie unterstützt die Bundesregierung den Aufbau einer Infrastruktur von „Computer Emergency Response Teams“ sowie die Einrichtung von „Incident Response Teams“ und worin besteht der Arbeitsschwerpunkt dieser Teams?

In Deutschland arbeiten seit einigen Jahren verschiedene „Computer Emergency Response Teams“ (CERT). Im BSI ist bereits seit 1993 ein CERT eingerichtet. Auch wenn diese z. T. bereits in der internationalen Dachorganisation FIRST (Forum of Incident Response Teams) organisiert sind, soll die internationale und nationale Zusammenarbeit bei der Reaktion auf Sicherheitsvorfälle und im präventiven Bereich, beispielsweise bei der Analyse von potentiellen Schwachstellen im Internet, verstärkt werden.

Bereits seit April 2000 wird eine neue, verbesserte CERT-Struktur in Deutschland angestrebt, bei der sog. Dach-CERT als zentrale Ansprechpartner in den Bereichen Wissenschaft, Wirtschaft und Behörden existieren, um so bei IT-Sicherheitsvorfällen (wie z. B. konzertierten Hackerangriffen) schneller reagieren zu können. Sicherheitsvorfälle von übergreifender, nationaler Bedeutung werden von den betroffenen Dach-CERT in direkter Absprache analysiert. Danach werden die erforderlichen Gegenmaßnahmen eingeleitet und koordiniert.

Die Aufgaben der Computernotfallteams haben sowohl präventiven als auch reaktiven Charakter. Im präventiven Bereich bewerten sie neue Entwicklungen (Schwachstellen, Angriffsprogramme etc.), weisen bedarfsgerecht ihre Kunden auf Sicherheitsgefährdungen hin und geben konkrete Handlungsempfehlungen zum Schutz vor Angriffen. Weiterhin sind sie erste Ansprechpartner im Falle eines IT- Sicherheitsvorfalls. Die Notfallteams können fachkundig und schnell auf einen Vorfall reagieren und Kontakt zu den entsprechenden Ansprechpartnern anderer betroffener Institutionen herstellen.

Im Bereich Wissenschaft und Forschung nimmt das CERT des Deutschen Forschungsnetzes (DFN-CERT) diese Aufgabe wahr. Im Behörden-Bereich erfolgt dies durch das CERT-BUND des BSI. Eine entsprechende Einrichtung innerhalb der Wirtschaft steht noch aus. Die Bundesregierung würde die Einrichtung eines eigenen Dach-CERT der Wirtschaft sehr begrüßen.

Das BSI unterstützt und berät auf Anfrage Organisationen bei der Gründung von Notfallteams im Rahmen von CERT.

Der Aufbau dieser nationalen Infrastruktur von CERT in Deutschland ist auch Gegenstand eines Projektes der „Initiative D21“ in der Arbeitsgruppe 6 „Sicherheit und Vertrauen im Internet“. Dort erarbeiten Wirtschaft und Bundesregierung gemeinsam Konzepte, um die Defizite der bisherigen Infrastruktur festzustellen und zielführend abzustellen.

13. Zu welchen Erkenntnissen bzw. Ergebnissen oder Zwischenergebnissen sind die Arbeitsgruppe „Informationstechnische Bedrohungen für kritische Infrastrukturen“ (Kritis) und der Arbeitskreis „Schutz vor Infrastrukturen“ (Aksis) gelangt und welche Konsequenzen zieht die Bundesregierung daraus?

Weshalb hat die Bundesregierung bislang nicht von sich aus über Ergebnisse dieser Arbeitsgruppen informiert?

Die Informationstechnik spielt für das reibungslose Funktionieren der Infrastruktursysteme in Deutschland eine zunehmend wichtige Rolle. Computerattacken auf wichtige Infrastrukturbereiche wie

– Telekommunikation,

– Transport- und Verkehrswesen,

– Energieversorgung (Elektrizität, Öl, Gas und Atomenergie),

– Gesundheitswesen,

– Behörden und Organisationen mit Sicherheitsaufgaben, Regierung, Bundes- und Länderverwaltung

– sowie Bank-, Finanz- und Versicherungswesen

können öffentliche und private Dienstleistungen empfindlich stören und zu einer krisenhaften Entwicklung führen.

Die Bundesregierung will aufbauend auf den Erkenntnissen der Arbeitsgruppe „Kritische Infrastrukturen“ handlungsorientiert die IT-Sicherheit in den kritischen Aufgaben- und Funktionsbereichen dieser wichtigen Infrastrukturen erhöhen. Sie ist sich dabei ihrer Vorbildfunktion im Hinblick auf den Schutz ihrer eigenen kritischen Infrastrukturen bewusst. Derzeit wird die Kritikalität von IT-Systemen in der Bundesverwaltung ermittelt, um auf der Grundlage eines hierzu speziell entwickelten Verfahrens mögliche Schwachstellen zu identifizieren und gezielt die IT-Sicherheit zu erhöhen. Das BSI unterstützt diese Arbeiten im Rahmen eines Aufgabenschwerpunktes.

Die Sicherheit in den jeweiligen Infrastrukturbereichen obliegt den einzelnen Versorgern, Dienstleistern etc. jedoch in eigener Verantwortung. Hier setzt sich die Bundesregierung verstärkt dafür ein, dass alle erforderlichen Sicherheitsmaßnahmen ergriffen werden.

Der Arbeitskreis „Schutz kritischer Infrastrukturen (AKSIS)“ wurde in der Wirtschaft initiiert und setzt sich aus Vertretern der Wirtschaft, insbesondere von Telekommunikationsanbietern, Energieversorgern und Verkehrsunternehmen sowie Vertretern der Ministerien, nachgeordneter Behörden sowie Landesbehörden (auch Polizei) zusammen. Die Thematik wird dort umfassend diskutiert, um die tatsächliche Bedrohungslage zu ermitteln und sich – nach Möglichkeit – über gemeinsame Sicherheitskonzepte abzustimmen. Die Zusammensetzung und die Aktivitäten des Arbeitskreises machen deutlich, wie eng Staat und Wirtschaft auf diesem Gebiet zusammenarbeiten.

Die Bundesregierung wird in Abstimmung mit den betroffenen Infrastrukturbereichen zum gegebenen Zeitpunkt diejenigen Informationen zur Verfügung stellen, deren Bekanntwerden kein Sicherheitsrisiko darstellen.

14. Setzt die Bundesregierung im Bereich der technischen Prävention primär auf eine Selbstregulierung durch die betroffenen Unternehmen, Kunden und Provider?

    Wenn ja: Welche Formen der Selbstregulierung werden von der Bundesregierung angestrebt?

Die Bundesregierung setzt im Bereich der technischen Prävention nicht primär auf eine Selbstregulierung. Das Maß der Regulierung hängt entscheidend davon ab, in welchem Technikbereich die präventiven Maßnahmen Wirkung entfalten sollen. In der Datennetzkriminalität und bei Computerattacken ist der Staat weitestgehend selbst gefordert, den Regelungsrahmen zu setzen, da der Bürger einen Anspruch auf staatlichen Schutz hat. Weiterhin besteht Regelungsbedarf zur Schaffung der Rahmenbedingungen für sichere elektronische Signaturen. Hier bestehen Vorgaben nach der europäischen Signaturrichtlinie, die bis Mitte 2001 umzusetzen sind. Die Neufassung des Signaturgesetzes zur Umsetzung der Richtlinie ist inzwischen verabschiedet. Im Bereich des E-Commerce bzw. E-Business kann zum größeren Teil auch auf die Selbstregulierung durch Unternehmen, Kunden und Provider gesetzt werden.

Im Bereich der technischen Prävention ist die Bundesregierung in verschiedener Hinsicht bereits tätig geworden. Das Bundesministerium des Innern hat die Task Force „Sicheres Internet“ eingerichtet, die technische Maßnahmenkataloge zum Schutz vor Computerattacken herausgegeben hat. Als weitere wichtige Maßnahmen zur technischen Prävention ist das IT-Grundschutzhandbuch des BSI sowie die Einrichtung und Erweiterung einer CERT-Infrastruktur zu nennen.

15. Beabsichtigt die Bundesregierung, von der Industrie vereinbarte Sicherheitsstandards und Selbstverpflichtungen gesetzlich festzuschreiben und Verstöße dagegen mit Sanktionen verwaltungs-, zivil- oder auch strafrechtlicher Art zu belegen?

Die Bundesregierung sieht gegenwärtig keine Notwendigkeit für gesetzliche Regelungen.

16. Welche Rolle spielt nach Auffassung der Bundesregierung das Produkthaftungsrecht für den Aufbau eines wirksamen Schutzes vor Computerattacken?

    Sieht die Bundesregierung insoweit Möglichkeiten, die Sicherheit von Soft- und Hardware, insbesondere im Bereich des Online-Banking, mittel- oder langfristig durch eine Ausweitung der Produkthaftung zu erhöhen und inwieweit lassen sich gegebenenfalls Dienstleistungen im Internet in ein solches Haftungssystem einbeziehen?

Das Produkthaftungsrecht regelt den Ausgleich von entstandenen Schäden durch fehlerhafte Produkte der Hersteller. Nach Sinn und Zweck ist das Gesetz auf die Befriedung von Einzelfällen gerichtet und stellt daher kein geeignetes Instrument dar, um zum Aufbau einer wirksamen präventiven Schutzstruktur vor Computerattacken beizutragen. Auch sind die Ersatzmöglichkeiten, die das Produkthaftungsgesetz bietet, nicht auf die Fälle von Schädigungen durch fehlerhafte oder unsichere Soft- und Hardware zugeschnitten; abgesehen von der strittigen Frage, ob Software ein „Produkt“ im Sinne des Produkthaftungsgesetzes darstellt, ist etwa darauf hinzuweisen, dass Vermögensschäden, die durch fehlerhafte oder virenverseuchte Software hervorgerufen werden, nicht nach dem Produkthaftungsgesetz ersatzfähig sind.

Vor diesem Hintergrund stellt die Produkthaftung auch kein geeignetes Mittel dar, um die Sicherheit im Bereich des Onlinebankings gezielt zu erhöhen. Ebenso wenig lassen sich Dienstleistungen, bei denen die Haftungsfragen grundlegend anderer Natur sind, in ein System der Produkthaftung einbeziehen.

17. Beabsichtigt die Bundesregierung im Hinblick darauf, dass besonders jugendlichen Tätern das enorme Schädigungspotenzial von Computerattacken unter Umständen nicht in vollem Umfang bewusst ist und dass insoweit Angriffe auf fremde Computersysteme mitunter weniger auf einer Schädigungsabsicht als auf einer Faszination über die technischen Möglichkeiten beruhen, eine entsprechende Aufklärung in den Schulen und in den Medien zu initiieren, z. B. unter Beteiligung des Bundesministeriums für Wirtschaft und Technologie oder der Bundeszentrale für politische Bildung?

Aufgrund polizeilicher Erkenntnisse trifft es zu, dass der im Zusammenhang mit Hackingdelikten bekannt gewordene Tätertypus weitgehend dem Klischee des jugendlichen Hackers entspricht, der nicht mit außergewöhnlich hoher krimineller Energie und mit Bereicherungsabsicht agiert. Im Vordergrund steht vielmehr ein

Geltungsbedürfnis sowie – teilweise – auch die Unkenntnis über die potentielle Tragweite des eigenen Handelns. Mit Blick auch auf diesen Kreis der jugendlichen Internetnutzer hat die Bundesregierung die folgenden Aktivitäten gestartet:

Im Rahmen des Programms „Neue Medien in der Bildung“ fördert das Bundesministerium für Bildung und Forschung ein Vorhaben zur Entwicklung multimedialer Lehr- und Lerninhalte, die Schülern an berufsbildenden und weiterführenden Schulen sowie Auszubildenden in Betrieben informationstechnische Sicherheitskompetenz vermittelt. Ziel ist es, Schülerinnen und Schüler für Fragen des Datenschutzes und der Sicherheit beim Umgang mit Computern und Internet zu sensibilisieren. Es sollen dabei neben den technischen Grundlagen anhand von Alltagsbeispielen auch die aus unerlaubten Eingriffen in Computersysteme entstehenden Gefahren vermittelt werden; insbesondere soll über die damit verbundenen ethischen, sozialen und strafrechtlichen Fragen aufgeklärt werden. Die multimedialen Lehr- und Lerninhalte und Arbeitsmaterialien werden für den Unterricht in den Fächern Informatik, Wirtschafts- und Sozialkunde und Ethik entwickelt.

Im Geschäftsbereich des BMI baut die Bundeszentrale für politische Bildung den neuen Fachbereich „Multimedia/IT“ zu einem zukünftigen Schwerpunkt ihrer Arbeit aus. Dabei wird u. a. die Stärkung der Medienkompetenz, insbesondere der jugendlichen Zielgruppen, die Vermittlung medienethischer Grundwerte bei der Internetnutzung, das Thema „Sicherheit im Netz“ und der Datenschutz eine entscheidende Rolle spielen.

18. Welche weiteren Möglichkeiten der außerstrafrechtlichen Prävention gegen Computersabotage und -spionage sieht die Bundesregierung, welche Erfolgschancen räumt sie ihnen jeweils ein und welche Aktivitäten entwickelt die Bundesregierung zur Umsetzung der einzelnen Maßnahmen?

Die Bundesregierung sieht folgende Möglichkeiten der außerstrafrechtlichen Prävention:

Es wird mit verschiedenen Sensibilisierungs- und Informationskampagnen (z. B. der gemeinsamen Initiative des Bundesministeriums für Wirtschaft und Technologie sowie des Bundesministeriums des Innern „Sicherheit-im-Internet“) auf Präventionsmaßnahmen hingewiesen.

Für konkrete Bedrohungen, wie z. B. DDoS-Angriffe oder E-Mail-Viren, hat die Task Force „Sicheres Internet“ Maßnahmenkataloge entwickelt.

Das BSI unterstützt Projekte, die der Entwicklung einer sicheren Informationstechnik dienen. Diesbezüglich wären zu nennen:

- Sensibilisierung der Öffentlichkeit für Fragen der IT-Sicherheit (z. B. Deutscher IT-Sicherheits-Kongress, Veröffentlichungen),
- Erarbeitung von empfohlenen Maßnahmen (Grundschutzhandbuch, Grundschutztool),
- Unterstützen des Einsatzes von Open-Source-Produkten,
- Unterstützen des Einsatzes sicherheitsgeprüfter Produkte,
- Entwicklung entsprechender Werkzeuge und Hilfsmittel (z. B. USEIT[11]),
- Einsatz zertifizierter Komponenten in besonders sicherheitsempfindlichen Bereichen und
- Aufbau eines Meldewesens IT-Sicherheitsvorkommnisse in Deutschland unter Einbindung des CERT-BUND.

11 USEIT: UNIX Security Enhancement and Information Tool (Werkzeug für sichere UNIX-Administration).

19. Wie beurteilt die Bundesregierung das Bestreben nach verstärktem Patentschutz für Computerprogramme und hätte ein verstärkter Patentschutz Auswirkungen auf die Sicherheit von Computerprogrammen?

Die Bundesregierung strebt nicht generell einen verstärkten Patentschutz für Computerprogramme an. Gegenwärtig wird in Europa darüber diskutiert, ob die Voraussetzungen, unter denen Patentschutz für Computerprogramme erteilt wird, klarer im Gesetz formuliert werden sollten.

Computerprogrammbezogene Erfindungen können auf Antrag durch Patente geschützt werden, wenn die allgemeinen Patentierungsvoraussetzungen, § 1 Patentgesetz, Artikel 52 Europäisches Patentübereinkommen, vorliegen. In den Absätzen 2 und 3 beider Bestimmungen wird klargestellt, dass lediglich Datenverarbeitungsprogramme „als solche“, also ohne technischen Effekt, nicht als Erfindungen angesehen werden können. Ist dagegen eine computerprogrammbezogene Erfindung gemacht worden, so muss auch Patentschutz zur Verfügung gestellt werden, wenn die übrigen Patenterteilungsvoraussetzungen vollständig vorliegen. Mit dem von der Europäischen Kommission beabsichtigten Vorschlag für eine Richtlinie zur Softwarepatentierung sollen aus Sicht der Bundesregierung diese rechtlichen Voraussetzungen für die Patentierbarkeit nicht grundsätzlich verändert, sondern lediglich präzisiert werden.

Ob und in welchem Umfang Patentschutz auf Software-Erfindungen Auswirkungen auf die Sicherheit von Computerprogrammen haben kann, bedarf einer gründlichen und breiten Diskussion, wie sie von der Bundesregierung auch auf Gemeinschaftsebene angestrebt wird.

20. Welche Bedeutung kommt – bei Behörden in Bund, Ländern und Kommunen einerseits und in der Privatwirtschaft andererseits – der „open-source-software“ (OSS) im Hinblick auf die Sicherheit von Software zu und in welchem Umfang setzt die Bundesregierung derartige Software ein bzw. fördert deren Einsatz?

Die Bundesregierung misst der Entwicklung und dem Einsatz von Open-Source-Software (OSS) bei der Verwaltung und in der Privatwirtschaft eine hohe Bedeutung bei. Durch die generelle Verfügbarkeit des Quellcodes bei OSS stehen neben den funktionalen auch sämtliche Implementierungseigenschaften der OSS einer breiten Fachwelt zur Verfügung. Die Praxis zeigt, dass hierdurch die Erkennungswahrscheinlichkeit von Schwachstellen deutlich höher ist als bei proprietärer, herstellergebundener Software. Hierdurch wird auch die Möglichkeit des absichtlichen Einbaus von Schwachstellen deutlich reduziert und damit das Vertrauen in die Herkunft der Software gestärkt. Der entstehende kontinuierliche Verbesserungsprozess wirkt sich positiv auf die Qualitäts- und damit Sicherheitseigenschaften von OSS aus. Die Entwicklungsdynamik von OSS entspricht dem innovativen Charakter von heutigen IT-Lösungen und deren zunehmend globalem Charakter. Gleichwohl bedürfen IT-Sicherheitslösungen für einen höheren Schutzbedarf einer zusätzlichen profunden Sicherheitsanalyse, die im Falle von OSS jedoch bereits auf einem hohem Niveau aufsetzen kann.

Das BMWi richtet sich mit der Broschüre „Open-Source-Software – Ein Leitfaden für kleine und mittlere Unternehmen“ insbesondere an potentielle Anwender. Diese informiert über Vorteile und Chancen, aber auch über Risiken der Anwendung von Open-Source-Software. Sie ist Teil der Strategie des BMWi zur Unterstützung von Sicherheit und Wettbewerb in der Informationsgesellschaft, bei der insbesondere die Potentiale von Open-Source-Software gesehen werden. Das BMWi fördert in diesem Zusammenhang den Aufbau eines nationalen Kompetenzzentrums für Open-Source-Software „BerliOS“ in Berlin, das als Plattform für Open-Source-Entwickler und -Anwender fungieren und Informationen

für Nutzer bereitstellen soll. Daneben unterstützt das BMWi das Projekt „GNU Privacy Guards (GnuPG)“ zur Entwicklung einer vertrauenswürdigen, nutzerfreundlichen und offenen Verschlüsselungssoftware.

Die im BMI bestehende „Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung“ (KBSt) hat im September 2000 einen Workshop zum Thema Open-Source-Software in der öffentlichen Verwaltung durchgeführt. Das Protokoll des Workshop ist als Band 49 der Schriftenreihe der KBSt erhältlich; seine Ergebnisse stehen im Internet unter der Adresse „http://linux.kbst.bund.de“ zum Abruf bereit. Wesentliches Ergebnis war, dass OSS in der Bundesverwaltung bereits ihren festen Platz eingenommen hat. Ferner wurde für den Workshop eine Erweiterung der Wirtschaftlichkeitsbetrachtungen bei Einsatz und Migration der IT in der Bundesverwaltung (IT-WiBe) vorgenommen. Dies führt dazu, dass bei jeder Einführung neuer Software in der Bundesverwaltung OSS in die Betrachtung einbezogen werden muss. Der Kriterienkatalog zur Migration von OSS ist als KBSt-Brief Nummer 3/2000 veröffentlicht.

Die Bundesregierung fördert darüber hinaus den Einsatz von OSS durch Pilotprojekte in der Bundesverwaltung. Die Pilotprojekte werden durch die KBSt begleitet und unterstützt. Ziel ist es, das Potential zu untersuchen und zu entwickeln, das OSS insbesondere unter wirtschaftlichen Gesichtspunkten und Sicherheitsaspekten für die öffentliche Verwaltung bietet.

In den Projekten des BSI „Sichere Netzanbindung (SINA)“ und „LINUX Sicherheitsanalyse (LISA)“ wird ebenfalls konsequent auf den Einsatz von OSS gesetzt. Entwicklungen und Sicherheitsanalysen, die im Rahmen dieser Projekte durchgeführt werden, fließen unmittelbar wieder der „OSS-Gemeinde“ zu. Es handelt sich von daher um eine deutliche Unterstützung des OSS-Gedankens durch ein konkretes IT-Sicherheitsprojekt der Bundesverwaltung. Im Gegenzug kann durch den Rückgriff auf umfangreiche Entwicklungsleistungen der „OSS-Gemeinde“ ein komplexes IT-System zeitnah und kostengünstig realisiert werden.

21. Anhand welcher Kriterien zieht die Bundesregierung die Trennungslinie zwischen Verhinderung von Computerattacken und der Sicherung von Informationsfreiheit?

Der Schutz der Bürgerinnen und Bürger vor Computerattacken wird mit dem Instrumentarium des Strafrechts gewährleistet. Die Trennungslinie zwischen dem Informationsanspruch der Bürgerinnen und Bürger gegenüber dem Staat einerseits und dem Schutz vor Datennetzkriminalität andererseits ist inhaltlich anhand der materiellen Gesetze zu ziehen.

22. Welche Gefahren ergeben sich nach Ansicht der Bundesregierung durch die zunehmenden Fälle der Computersabotage und -spionage für die Rechtssicherheit der Bürger sowie für den Daten- und Verbraucherschutz und welche Konsequenzen zieht die Bundesregierung daraus?

Eine gesicherte Aussage über drohende Gefahren für die Rechtssicherheit der Bürger sowie für den Daten- und Verbraucherschutz kann nicht getroffen werden. Tatsache ist, dass ein Ausspähen von Daten mittels weit verbreiteter Tools ohne größeren Aufwand durchgeführt werden kann, wenn der vermeintlich Betroffene nicht angemessene Sicherheitsvorkehrungen trifft. Für alle Arten von Attacken stehen im Internet frei zugänglich bzw. auf CD-ROM käuflich erhältlich eine große Anzahl von Hacker-Werkzeugen zur Verfügung, so dass häufig kein großes Know-how mehr erforderlich ist, sondern Angriffe durch einfaches

Anklicken in menügesteuerten Hacker-Tools gestartet werden können. Ferner lässt der zunehmende Einsatz von Computersystemen in privaten Haushalten, verbunden mit deren gesteigerter Nutzung im Zusammenhang mit eBanking, eCommerce und zukünftig eMoney, weitere Gefahren für den ungeschulten Internetnutzer erwarten.

23. Sieht die Bundesregierung Anhaltspunkte dafür, dass durch die Datennetzkriminalität der gerade im Aufschwung befindliche elektronische Handel und die von ihm erwarteten neuen Arbeitsplätze in der Bundesrepublik Deutschland gefährdet werden?

    Falls ja: Beabsichtigt die Bundesregierung den Unternehmen bei der Errichtung von Sicherheitssystemen fachliche oder finanzielle Unterstützung zukommen zu lassen?

Es gibt keine verlässlichen Daten zu wirtschaftlichen Schäden und daraus folgenden Arbeitsplatzverlusten durch Datennetzkriminalität. Die jährlich erscheinende Studie der Zeitschrift „Informationweek“ zeigt allerdings auch für Deutschland steigende Schadensmeldungen der Unternehmen. Mehr als ein Drittel der befragten Unternehmen gaben dabei gegenüber dem Vorjahr zunehmende finanzielle Schäden an.

Die ausreichende Sicherung der IT-Infrastruktur ist Teil der Eigenverantwortung im Rahmen der Unternehmenspolitik. Eine finanzielle Unterstützung zum Einsatz von Sicherungssystemen durch die Bundesregierung ist nicht vorgesehen. Allerdings ist die Bundesregierung bereits seit 1998 bei der Sensibilisierung vor allem von kleinen und mittleren Unternehmen für Fragen der IT-Sicherheit aktiv: über eine eigens eingerichtete gemeinsame Webseite „www.sicherheit-im-internet.de“ des BMWi und des BMI, die Beteiligung an Fachveranstaltungen, Messen und Kongressen wird über die Möglichkeiten des besseren Schutzes informiert.

24. Ist die Bundesregierung der Auffassung, dass durch die einschlägigen Strafbestimmungen (insbesondere durch die §§ 202a, 303a, 303b, 316b StGB sowie § 17 UWG) alle strafwürdigen Formen von Angriffen auf fremde Computersysteme angemessen erfasst und – insbesondere unter Präventionsgesichtspunkten – wirksam geahndet werden können (bitte aufschlüsseln im Sinne der Antwort zu Frage 1)?

    Falls nein: Wann und auf welche Weise beabsichtigt die Bundesregierung, die erkannten strafrechtlichen Lücken zu schließen?

Die gegenwärtig bekannten Angriffe auf Computersysteme lassen sich weitgehend unter die einschlägigen Strafrechtsnormen subsumieren. Insgesamt haben sich die 1986 durch das 2. WiKG eingefügten Straftatbestände bewährt. Sollten sich Strafbarkeitslücken zeigen, auch im Hinblick darauf, dass Missbrauchsfälle zahlen- und qualitätsmäßig eher noch zunehmen, wird die Bundesregierung die notwendigen Ergänzungen des Strafrechts prüfen. Im Übrigen wird auf die Antwort zu Frage 10 verwiesen.

Im Einzelnen:

a) Aufgrund der bewussten Entscheidung des Gesetzgebers im Zusammenhang mit dem Entwurf 2. WiKG (vgl. Drucksache 10/5058, S. 28f) gibt es im deutschen Strafrecht keine Strafvorschrift gegen das bloße Eindringen in ein Computersystem (sog. Hacking). Angesichts der Vielzahl von Hackingangriffen, die u. a. der Vorbereitung anderer Delikte dienen können, wird aber zu prüfen sein, ob § 202a StGB auf den unbefugten Zugang zu Computer-

systemen oder Daten unter Überwindung von Sicherheitsvorkehrungen, z. B. Firewalls, erweitert werden muss. Die Bundesregierung wird die weiteren Entwicklungen aufmerksam beobachten.

b) Beim Verbreiten von Viren ist eine Strafbarkeit nach den §§ 202a, 303a, 303b StGB dann gegeben, wenn der Virus vorsätzlich, also bewusst und gewollt, aktiviert wird und Datenveränderungen oder weitergehende Schäden hervorruft. Die Zurverfügungstellung und der Besitz von Vorrichtungen, die der Begehung von Computerstraftaten dienen (z. B. Virenprogramme), sind bisher nicht generell strafbar. Diese sog. Hackerwerkzeuge enthalten allerdings ein großes Gefährdungspotential, da aufgrund ihrer derzeit legalen Verbreitung ein Anreiz gegeben ist, sich diese zu kriminellen Zwecken zu beschaffen. Hinsichtlich einer möglichen Strafbarkeit wird auf die Antwort zu Frage 30 verwiesen.

c) Die bloße Angabe einer unrichtigen Adresse vor dem Zugang ins Internet oder die Verwendung eines Pseudonyms im E-Mail-Verkehr (sog. Spoofing) stellt für sich genommen keine strafbare Handlung dar. Ein solches Verhalten ist vergleichbar der (straflosen) Angabe eines falschen Namens oder einer falschen Adresse im normalen Schriftverkehr. Unter dem Gesichtspunkt des Datenschutzes gibt es ein legitimes Interesse der Nutzer des Internets zu einem anonymen oder pseudonymen Vorgehen. Auch wenn diese Möglichkeiten genutzt werden, die eigene Datenspur zu verschleiern, um z. B. eine DoS-Attacke durchzuführen oder unter falschem Namen eine Bestellung aufzugeben (strafbar nach § 303b StGB oder u. U. nach den §§ 263, 267, 269 StGB), besteht daher insoweit keine Strafbarkeitslücke.

d) Hinsichtlich von Sabotagehandlungen, etwa DDos-Attacken/Spamming, gilt, dass § 303b StGB regelmäßig alle solchen Angriffe auf Datenverarbeitungsanlagen von wesentlicher Bedeutung für Unternehmen, Betriebe oder Behörden erfasst. Da jedoch Datenverarbeitungsanlagen zunehmende Bedeutung auch im Privatbereich gewinnen, ist auch hier eine etwaige Ausdehnung des strafrechtlichen Schutzes zu prüfen.

25. Wie hat sich die Bundesregierung ihr Meinungsbild bezüglich ihrer Antwort zu Frage 24 verschafft?

Was das materielle Strafrecht angeht, so besteht eine fortlaufende Diskussion zur Frage der Einführung von Tatbeständen zur Bekämpfung der Computerkriminalität bzw. zur Ergänzung des geltenden Rechts seit über 20 Jahren (auf nationaler Ebene: Erörterungen in der Kommission zur Bekämpfung der Wirtschaftskriminalität, Anhörung im Deutschen Bundestag im Rahmen des 2. WiKG, Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft“ in der 13. Legislaturperiode, Berichte des BKA zur Computer-/Internetkriminalität; auf internationaler Ebene: OECD seit 1983, Europarat: insbesondere Empfehlungen von 1985 und 1989, Evaluierung der Umsetzung in Europaratsstaaten Anfang der 90er Jahre durch Prof. Kaspersen, AIDP-Kongress 1994, Vereinte Nationen: Verbrechensverhütungskongress im April 2000, Arbeiten der G8 „High-tech Crime“-Gruppe[12], Mitteilung der EU-Kommission vom Januar 2001).

Änderungsüberlegungen sind im Wesentlichen durch diese Diskussion und im Jahr 2000 auch immer mehr durch die Arbeiten im Rahmen einer Expertengruppe des Europarates (PC-CY) und die Veröffentlichung von deren Entwürfen über ein Übereinkommen des Europarates zur Datennetzkriminalität (Draft Convention on Cyber-Crime) ausgelöst worden. Anhand der Entwürfe ist eine Dis-

12 G8: Arbeitskreis der 8 wichtigsten Industrienationen (USA, Kanada, Großbritannien, Italien, Frankreich, Deutschland, Japan und Russland).

kussion mit den Ländern (die ihrerseits Praxisbefragungen durchführten) und der Wirtschaft (Verbände) sowie innerhalb der Bundesregierung unter Einbeziehung des Bundesbeauftragten für den Datenschutz, des BKA und BSI in Gang gekommen.

Außerdem basieren die gewonnenen Erkenntnisse auf den Meldungen der Länderpolizeien im Rahmen des polizeilichen Meldedienstes „Kriminalität in Verbindung mit Informations- und Kommunikationstechnik“ (IUK-Meldedienst), auf der Vorgangsbearbeitung des BKA, auf der Tätigkeit der Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD) des BKA sowie auf zahlreichen Fachgesprächen mit IT-Unternehmen.

26. Ist in naher Zukunft mit einem Referentenentwurf seitens des Bundesministeriums der Justiz zur umfassenden Reform des nationalen Computerstrafrechts zu rechnen?

    Falls nein: Wie rechtfertigt die Bundesregierung ihre Absicht, mit notwendigen Änderungen im Bereich der nationalen Gesetzgebung zuzuwarten, bis auf internationaler Ebene Beschlüsse gefasst sind?

Eine umfassende Reform des materiellen Computerstrafrechts hält die Bundesregierung derzeit nicht für notwendig. Insoweit wird auch auf die Antworten zu den Fragen 10 und 24 verwiesen. Vorschläge zu etwaigen Ergänzungen werden insbesondere im Zusammenhang mit der Umsetzung von in dem künftigen Übereinkommen des Europarates zur Datennetzkriminalität (Convention on Cyber-Crime) enthaltenen Regelungen entwickelt werden. Eine Reform mit angemessen aufeinander abgestimmten Maßnahmen würde vorrangig die auf internationaler Ebene festgelegten Mindeststandards, wie sie z. B. in der erwähnten Konvention festgelegt werden, berücksichtigen.

27. Anhand welcher Kriterien legt die Bundesregierung fest, ob sie gesetzgeberische Maßnahmen zu ergreifen hat, die über das angestrebte Übereinkommen des Europarates (Convention on Cyber-crime) hinausgehen?

Es wird – wie bei jedem Gesetzgebungsvorhaben – überprüft werden, ob ein praktischer Bedarf für weitergehende Regelungen besteht. Auf die Antwort zu Frage 24 wird hingewiesen. Bei künftigen Überlegungen wird ein besonderes Augenmerk darauf zu richten sein, ob die derzeit geltenden Straftatbestände der hohen Sozialschädlichkeit und Gefährlichkeit bestimmter Handlungen Rechnung tragen. Darüber hinaus wäre insbesondere zu prüfen, ob die in dem vorgesehenen Übereinkommen geplanten verfahrensrechtlichen Regelungen den Strafverfolgungsbehörden in ausreichender Zahl wirksame Instrumente zur effektiven Strafverfolgung an die Hand geben.

28. Sind die hierzulande geltenden Strafdrohungen nach Auffassung der Bundesregierung ausreichend, um der hohen Sozialschädlichkeit und Gefährlichkeit von Computerattacken größeren Ausmaßes in angemessener Weise Rechnung zu tragen?

Die geltenden Strafdrohungen sind nach Auffassung der Bundesregierung ausreichend. Eine Ausweitung der gesetzlich vorgesehenen Strafrahmen erscheint nicht notwendig, da das geltende System der Strafzumessung den Gerichten einen weiten Spielraum zubilligt, um in jedem Einzelfall eine schuldangemessene Strafe zu finden. Bei diesem Vorgang hat der Richter eine Vielzahl von Gesichtspunkten zu berücksichtigen und abzuwägen. Wichtig ist es daher insbesondere, dass der gesetzlich vorgegebene Spielraum nicht zu eng ist, etwa weil er durch

eine unangemessen niedrige Höchstgrenze beschränkt wird. Dass dieses Höchstmaß der Strafe dann nur in den allerwenigsten Fällen von den Gerichten ausgeschöpft wird (vgl. hierzu die Antwort zu Frage 6), liegt in dieser Grundstruktur unseres Strafzumessungssystems begründet. Hierbei unterscheiden sich die Computerdelikte in keiner Weise von anderen Straftaten.

29. Welche Gründe sprechen nach Ansicht der Bundesregierung dagegen, beim Straftatbestand des § 202a StGB ein Einschreiten von Amts wegen zu ermöglichen?

    Hält es die Bundesregierung für geboten, den Versuch des Ausspähens von Daten im Sinne dieser Vorschrift unter Strafe zu stellen?

Eine Umgestaltung des § 202a StGB in ein relatives Antragsdelikt (grundsätzlich Strafantrag erforderlich, außer wenn ein besonderes öffentliches Interesse an der Strafverfolgung vorliegt) könnte im Zusammenhang mit einer Neuausrichtung seiner Schutzwirkung auf Computersysteme (zz. nur Daten als Schutzgut) in Betracht kommen. Dies, wie auch eine Erfassung von Versuchshandlungen, wird im Rahmen der Umsetzung von in dem künftigen Übereinkommen des Europarates über Datennetzkriminalität (Convention on Cyber-Crime) enthaltenen Regelungen geprüft werden.

30. Inwieweit beabsichtigt die Bundesregierung auch solche Handlungen spezifisch strafrechtlich zu erfassen, die typischerweise im Vorfeld der Computersabotage und Computerspionage angesiedelt sind, etwa die bloße Herstellung, der Besitz oder die Verbreitung von Angriffsprogrammen, das bloße Eindringen in fremde Computersysteme (so genanntes Hacking), die Fälschung von Absenderadressen und andere Formen des so genannten Spoofings sowie die Anleitung zu solchen Handlungen?

    Inwieweit steht einer Pönalisierung entgegen, dass im Internet verfügbare „Hacking-Programme“ potentiellen Geschädigten die Möglichkeit bieten, die von ihnen getroffenen Sicherheitsmaßnahmen zu überprüfen?

Die strafrechtliche Erfassung von bestimmten Vorbereitungshandlungen zur Begehung von Computerdelikten (Herstellung, Einfuhr, Veräußerung, Verbreitung von Computerprogrammen und anderen Vorrichtungen) wird im Zusammenhang mit den zu erwartenden Regelungen zur Umsetzung des künftigen Übereinkommens des Europarates zur Datennetzkriminalität (Convention on Cyber-Crime) erfolgen. Die Strafbarkeit sollte dabei nur solche Vorrichtungen erfassen, die objektiv bestimmt und geeignet sind, bestimmte Computerdelikte zu begehen, z. B. den Zugangsschutz unbefugt zu überwinden, und die auch mit einer entsprechenden Absicht eingesetzt werden. Nicht erfasst werden sollten Werkzeuge, die eigens für das Testen oder für den Schutz von Computersystemen geschaffen wurden. Hier bedarf es – etwa für die Hersteller von Antivirenprogrammen – einer Ausnahmeregelung (vergleichbar § 94 i. V. m. § 65 TKG).

31. Sollte nach Auffassung der Bundesregierung in bestimmten Fällen, etwa bei Eintritt schwerwiegender Schäden, der leichtfertige Umgang mit Angriffsprogrammen unter Strafe gestellt werden?

Es bestehen grundsätzliche Bedenken, bereits „leichtfertiges“ Verhalten in einem Bereich, in dem es im Regelfall um wirtschaftliche Schäden geht, unter Strafe zu stellen. Insbesondere die vielfältigen Softwareangebote des Internets bergen po-

tentielle Gefahren, die der „normale“ Nutzer nicht einzuschätzen weiß und die deshalb zu Bedienungsfehlern führen können. Der ggf. bestehende Rückgriff auf zivilrechtliche Schadensersatzansprüche erscheint als ausreichend.

Die Begrenzung des Strafrechts entspricht auch der von internationalen Organisationen bisher entwickelten Haltung, die eine Strafbarkeit nur für vorsätzliches Verhalten empfohlen haben (Committee for Information, Computer and Communications Policy der OECD, 1985; Lenkungsausschuss für Strafrecht des Europarates, 1989; Empfehlung des XV. Internationalen Strafrechtskongresses der Association International de Droit Pénal, 1994; Entwurf eines Übereinkommens zur Datennetzkriminalität [Draft Convention on Cyber-Crime]).

32. Gedenkt die Bundesregierung auf die in jüngster Vergangenheit wiederholt aufgetretenen Störungen von Webseiten durch massenhafte Datenübertragungen oder Datenabfragen (so genanntes Spamming bzw. Distribute Denial of Service-Attacken) im Wege einer Reform der einschlägigen Straftatbestände zu reagieren?

Auf die Antwort zur Frage 24 wird verwiesen.

33. Sieht die Bundesregierung im Bereich der Aufklärung von Computerstraftaten Defizite, die einen gesetzgeberischen Handlungsbedarf begründen, und wenn ja, welche?

Auf die Antwort zu Frage 10 wird verwiesen. Die Bundesregierung legt hinsichtlich der Verbesserung der Aufklärungsmöglichkeiten für Computerdelikte besonderen Wert auf die grenzüberschreitende Zusammenarbeit, z. B. im Rahmen der G8-Arbeitsgruppe „High-tech-Crime“, die technische Ausstattung der Ermittlungsbehörden und schließlich auch auf die Kooperation von Staat und Wirtschaft, die Bestandteil jeder erfolgreichen Strategie zur Bekämpfung von Computerstraftaten ist.

34. Erwägt die Bundesregierung zur Steigerung der Effektivität und zur Beschleunigung von Strafverfahren eine Änderung bzw. Ergänzung der Vorschrift des § 110 StPO, um den ermittelnden Polizeibeamten – gegebenenfalls auf Weisung der Staatsanwaltschaft – eine Durchsuchung von Computern und anderen Datenträgern ohne Hinzuziehung des Staatsanwalts oder eines Richters zu gestatten?

Die Bundesregierung beabsichtigt eine Reform des Strafverfahrens, die auch auf eine Optimierung des Ermittlungsverfahrens abzielt. Durch die der Staatsanwaltschaft eingeräumte Sachleitungsbefugnis wird die Einhaltung des Legalitätsprinzips, die Vollständigkeit der Sachverhaltserforschung und die Justizförmigkeit des Verfahrens gewährleistet. Auch bei der Überprüfung der Vorschrift des § 110 Abs. 1 StPO wird daher zu beachten sein, dass die Sachleitungsbefugnis der Staatsanwaltschaft gewahrt bleibt.

35. Ist nach Ansicht der Bundesregierung eine Änderung der Strafprozessordnung sinnvoll, um die Durchsuchung erforderlichenfalls auf weitere Computersysteme auszudehnen, die durch ein Netzwerk mit dem zunächst durchsuchten Datenträger verbunden sind?

    Wenn ja: Bedarf es nach Ansicht der Bundesregierung weiterer Änderungen des geltenden Rechts, um den Strafverfolgungsbehörden eine Beschlagnahme der aufgefundenen Daten zu ermöglichen, und wie lässt sich nach Ansicht der Bundesregierung eine praktikable Abgrenzung zu solchen Computersystemen formulieren, die gleichfalls in das Netzwerk integriert sind, für die jedoch ein Durchsuchungsgrund nicht besteht?

Ergibt sich im Verlaufe der Durchsuchung eines Computers, dass dieser mit einem weiteren Computersystem vernetzt ist, stehen den Strafverfolgungsbehörden zwei Möglichkeiten zur Verfügung, um rasch Kenntnis von dort gespeicherten Daten zu erlangen: Durchsuchung des Aufbewahrungsorts des Speichermediums mit anschließender Beschlagnahme des Datenträgers nach den allgemeinen Regeln der §§ 94 ff., 102 ff. StPO (bei Gefahr in Verzug, z. B. drohender Löschung oder Veränderung von Daten, Möglichkeit der Anordnung durch die Staatsanwaltschaft oder deren Hilfsbeamte, § 98 Abs. 1 Satz 1, § 105 Abs. 1 Satz 1 StPO) oder einmaliger, heimlicher (Online-)Zugriff auf nicht für die Öffentlichkeit bestimmte und auf einem externen Server (zwischen-)gespeicherte Nachrichten durch die ermittelnde Behörde, z. B. der Abruf von E-Mails von einem Mail-Server oder von Sprachnachrichten von einer Voice-Box, unter sinngemäßer Anwendung der für die Telekommunikationsüberwachung geltenden Voraussetzungen der §§ 100a und 100b Abs. 1 StPO (d. h. bei Ermittlungen hinsichtlich der in § 100a StPO genannten Straftaten; Anordnung durch einen Richter, bei Gefahr im Verzug Möglichkeit der Anordnung durch die Staatsanwaltschaft, binnen drei Tagen Bestätigung durch den Richter erforderlich).

Mit Blick auf das Instrumentarium zur Durchsuchung von Computersystemen sieht die Bundesregierung gegenwärtig keinen unmittelbaren kurzfristigen gesetzgeberischen Handlungsbedarf. Dies schließt die aufmerksame Beobachtung der technischen und rechtlichen Entwicklung – auch im Hinblick auf Online-Durchsuchungen – nicht aus.

36. In welchem Maße wird nach Auffassung der Bundesregierung die erfolgreiche Aufklärung von Computerstraftaten durch geltende Datenschutzbestimmungen erschwert und auf welche Weise können insoweit – unter Beachtung des Rechts auf informationelle Selbstbestimmung – Verbesserungen erreicht werden?

Die Ermittlungsarbeit der Sicherheitsbehörden und die von den Prinzipien der Datenvermeidung und -sparsamkeit geprägten Regelungen des Datenschutzes sowie das Recht auf informationelle Selbstbestimmung stehen in einem natürlichen Spannungsverhältnis.

Die Bundesregierung ist bestrebt, in diesem Spannungsfeld einen Ausgleich der Interessen herbeizuführen, der das unabweisbare Bedürfnis einer wirksamen Strafverfolgung, insbesondere die zügige und erfolgreiche Aufklärung von schweren Straftaten, mit dem Grundrecht auf informationelle Selbstbestimmung in ein ausgewogenes Verhältnis bringt.

In ihre Überlegungen bezieht die Bundesregierung auch internationale Aktivitäten und Maßnahmen mit ein. So hat die EU-Kommission u. a. zur Klärung des Spannungsfeldes zwischen Strafrecht und Datenschutz in ihrer Mitteilung vom 26. Januar 2001 ein Diskussionsforum aller Beteiligten vorgeschlagen. Dieser Ansatz wird von der Bundesregierung unterstützt.

37. Wie will die Bundesregierung darauf reagieren, dass Daten, die zur Ermittlung der Tat und zur Identifizierung der Täter unerlässlich sind, vielfach gelöscht werden, bevor ein Zugriff der Ermittlungsbehörden erfolgen konnte?

Die erlaubte Verarbeitung personenbezogener Daten steht unter dem Vorbehalt des Gesetzes beziehungsweise der Einwilligung des Betroffenen. Liegen diese Voraussetzungen nicht mehr vor, besteht eine gesetzliche Löschungsverpflichtung. Die Speicherfristen hängen davon ab, ob die Daten für den durch das Gesetz oder die Einwilligung vorgesehenen Zweck noch benötigt werden. Diese Löschungsverpflichtung vermindert im Einzelfall den Zugriff der Ermittlungsbehörden auf ermittlungsrelevante Daten. Sie gewährleistet jedoch zugleich den Datenschutz der Bürger, die jedenfalls dann ein Recht auf die Löschung ihrer personenbezogenen Daten haben, wenn sie nicht einer Straftat verdächtigt werden. Die Frage, ob und in welchem Umfang hier durch gesetzliche Mindestspeicherfristen Abhilfe zu schaffen ist, ist Teil der bereits in der Antwort zu Frage 36 angesprochenen Klärung dieses Spannungsfeldes.

Die Bundesregierung beteiligt sich aktiv an Arbeiten und Diskussionen auf EU-, Europarats- und G8-Ebene, die die Frage der Speicherung von Verbindungs- und Nutzungsdaten zu Strafverfolgungszwecken betreffen. Da die Bekämpfung der Computerkriminalität nicht nur eine nationale, sondern eine globale Aufgabe darstellt, hofft die Bundesregierung, auf diesem Feld vorrangig international verbindliche Lösungen zu erreichen, da dieses Vorgehen die besten Erfolge bei der Bekämpfung der Computerkriminalität verspricht.

Auf nationaler Ebene wurde in der Telekommunikations-Datenschutzverordnung (TDSV) die Höchstspeicherfrist für bestimmte Verbindungsdaten, die für Abrechnungszwecke benötigt werden, auf die Dauer von sechs Monaten nach Rechnungslegung verlängert. Die Novellierung des Teledienstedatenschutzgesetzes (TDDSG) sieht eine entsprechende Regelung für bestimmte Nutzungsdaten vor, die für Abrechnungszwecke benötigt werden.

Je häufiger in Zukunft die Abrechnung der Dienstleistungen auf einer Pauschalbasis, sog. Flatrate, erfolgen wird, desto seltener wird ein Grund für die Speicherung von Verbindungsdaten vorliegen, da diese für Abrechnungszwecke nicht mehr benötigt werden.

Deshalb werden bei Überlegungen hinsichtlich einer Einführung von weitergehenden Speicherfristen für die Provider die tatsächlichen und rechtlichen Gegebenheiten, insbesondere die Grundsätze der Verhältnismäßigkeit sowie der Datenvermeidung und -sparsamkeit und die Interessen der Wirtschaft einerseits und die Interessen der Sicherheitsbehörden andererseits, abzuwägen sein. Auf die Erforderlichkeit einer Diskussion auf internationaler Ebene bei der Einführung weitergehender Regelungen wurde eingangs bereits hingewiesen.

Daneben prüft die Bundesregierung derzeit zur Verhinderung der Löschung ermittlungsrelevanter Daten die Möglichkeit, bereits gespeicherte Verbindungsdaten für einen angemessenen Zeitraum aufgrund einer von Strafverfolgungsbehörden zu erlassenden Anordnung durch die Internet-Provider vorläufig sicherstellen zu lassen.

38. Hält die Bundesregierung eine Änderung des § 89 Abs. 1 Satz 3 Telekommunikationsgesetz (TKG) dahin gehend für erforderlich, dass im Interesse einer effektiven Strafverfolgung nicht nur Höchst-, sondern auch Mindestfristen für die Speicherung von Daten vorgesehen werden?

§ 89 Abs. 1 Satz 3 TKG sieht eine Festlegung von Höchstspeicherfristen für personenbezogene Daten durch eine Rechtsverordnung vor. Auf dieser Vorschrift beruht die oben bereits erwähnte Regelung in der TDSV. Auf die Antwort zu Frage 37 wird verwiesen.

39. Hält die Bundesregierung im Hinblick darauf, dass Computerattacken vielfach nicht zur Anzeige gebracht werden, weil die betroffenen Unternehmen ihre Sicherheitslücken nicht offenbaren wollen, die Einführung einer entsprechenden Meldepflicht für sinnvoll?

Nach Einschätzung der Bundesregierung ist die Einführung einer Meldepflicht zur Aufhellung des Dunkelfeldes bei Computerattacken nicht sinnvoll. Eine gesetzliche oder mit der Wirtschaft vereinbarte Meldepflicht bedarf einer staatlichen Kontrolle. Derartige Kontrollen widersprechen der Haltung der Bundesregierung, auf dem Gebiet der IT-Sicherheit vertrauensvoll mit der Wirtschaft zusammenzuarbeiten. Sollte sich die Wirtschaft ihrerseits zu freiwilligen Meldungen bereit erklären, würde die Einrichtung einer zentralen Meldestelle in Betracht gezogen werden können.

40. Inwieweit beeinträchtigt der Gebrauch von Verschlüsselungsprogrammen eine wirksame Strafverfolgung und welche Konsequenzen zieht die Bundesregierung aus der insoweit gewonnenen Erkenntnis?

Die Bundesregierung hat mit ihren Eckpunkten zur Kryptopolitik vom 2. Juni 1999 festgestellt, dass „durch die Verbreitung starker Verschlüsselungsverfahren die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden zur Telekommunikationsüberwachung nicht ausgehöhlt werden dürfen." Die zuständigen Bundesministerien werden deshalb die Entwicklung weiterhin aufmerksam beobachten und nach Ablauf von zwei Jahren hierzu berichten.

Beim BSI wurde hierzu ein Arbeitskreis „Innere Sicherheit und Verschlüsselung" eingerichtet. Die Erfahrungen mit Verschlüsselungsfällen im Zusammenhang mit Straftaten durch die zuständigen Strafverfolgungs- und Sicherheitsbehörden von Bund und Ländern werden gegenwärtig ausgewertet.

Die Bundesregierung wird ihren ersten Erfahrungsbericht über die Entwicklungen zu Ziffer 4 der Eckpunkte der Kryptopolitik spätestens zur Innenministerkonferenz im Herbst abgeben.

C. Maßnahmen auf internationaler Ebene

41. Welchen Reformbedarf begründet der Entwurf eines Übereinkommens über Datennetzkriminalität (PC-CY [2000] Draft No. 19) nach den bisherigen Ergebnissen der Beratungen des zuständigen Sachverständigenausschusses des Europarates?

Für den Bereich des materiellen Strafrechts besteht nach dem derzeitigen Stand der Beratungen ein punktueller Ergänzungsbedarf. Geprüft wird insbesondere die Erfassung des unerlaubten Zugangs zu Computersystemen (Hacking) über die bisherige Regelung des Ausspähens von Daten (§ 202a StGB) hinaus, die Strafbarkeit des unbefugten Erfassens und Aufzeichnens von Datenübertragun-

gen im Telekommunikationsverkehr über die §§ 201, 202a StGB hinaus, die Beeinträchtigung auch privater Computersysteme über § 303b StGB (Computersabotage) hinaus (vgl. Antwort zu Frage 24) sowie als neuer Tatbestand das Inverkehrbringen von Vorrichtungen bzw. Programmen, die z. B. wie Hackertools spezifisch dafür bestimmt sind, die Begehung bestimmter Computerdelikte zu ermöglichen (vgl. Antwort zu Frage 30).

Bezüglich des im Interesse wirksamer (grenzüberschreitender) Strafverfolgung im Bereich des nationalen Strafprozessrechts bestehenden Prüfungsbedarfs wird auf die Antwort zu Frage 10 verwiesen. Im Hinblick auf das gegenwärtig vom Europarat erarbeitete Übereinkommen zur Datennetzkriminalität bedarf hierbei insbesondere die Frage der Überprüfung, inwieweit Änderungen des nationalen Rechts erforderlich sind, um (auch auf Anforderung eines ausländischen Staates) eine unverzügliche vorläufige Sicherung gefährdeter Datenbestände zu bewirken. Gleiches gilt für die Frage, ob für die – de lege lata bereits auf Grundlage des § 100a StPO mögliche – Erfassung von Verbindungsdaten in Echtzeit eine abgeschichtete Regelung sachgerecht wäre.

42. Welche Vorbereitungen trifft die Bundesregierung zur Umsetzung des angestrebten Übereinkommens und wie gedenkt die Bundesregierung eine Beratung im Parlament zu gewährleisten, die der rechtlichen und tatsächlichen Komplexität der Materie in angemessener Weise Rechnung trägt?

Im Zusammenhang mit den laufenden Verhandlungen des Europarates ist auch eine erste Prüfung der bei Ratifikation erforderlichen Gesetzesänderungen eingeleitet worden, die in Zukunft fortgesetzt wird. Nach Annahme des Übereinkommens durch das Ministerkomitee kann eine etwaige Ratifikation vorbereitet und ein Entwurf in das Gesetzgebungsverfahren eingebracht werden. Darauf folgt in jedem Fall eine Beratung im Deutschen Bundestag, die ggf. auch mit einer von den zuständigen Ausschüssen zu beschließenden Expertenanhörung verbunden werden kann. Ob unabhängig davon der Deutsche Bundestag sich mit der Materie schon in einem früheren Zeitpunkt befassen möchte, obliegt seiner Entscheidung.

43. Verfolgt die Bundesregierung Bestrebungen zur Einrichtung einer dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) entsprechenden Europäischen Behörde, und wenn ja, welche Zuständigkeiten und Befugnisse sollten einer solchen Behörde nach Ansicht der Bundesregierung übertragen werden?

Der Bundesminister des Innern hat auf dem Treffen der Innen- und Justizminister der Europäischen Union im Juli 2000 in Marseille angeregt, eine dem Bundesamt für die Sicherheit in der Informationstechnik vergleichbare europäische Einrichtung zu schaffen, um die technische Prävention in der Bekämpfung der High-Tech- Kriminalität zu stärken. Dieser Vorschlag wurde von der schwedischen Präsidentschaft aufgegriffen und wird in Kürze im Rahmen einer Resolution des Rates zur Informations- und Netzsicherheit erörtert werden. Hierbei steht aber nicht nur die Einrichtung einer neuen europäischen Institution im Vordergrund, sondern vielmehr die technische Prävention und die unabhängige Sach- und Fachkompetenz für die IT-Sicherheit als Aufgabe, soweit sie bisher noch nicht in anderen europäischen Gremien aufgegriffen worden ist.

44. Welche Aktivitäten entfaltet die Bundesregierung im Rahmen der G8-Konferenz, die in ihrer Abschlusserklärung vom 17. Mai 2000 auf die Notwendigkeit internationaler Kooperation innerhalb und außerhalb der G8-Gruppe hingewiesen hat?

Als Folgetreffen zur Pariser GS-Konferenz vom Mai 2000 hatte die Bundesregierung schon im Oktober 2000 zu einem weiteren G8-Treffen eingeladen. Hervorzuheben ist, dass hier wie auch schon auf der Pariser Konferenz Wirtschaft und Regierungen gleichberechtigt mitgewirkt haben. Wichtige Themen waren die „Prävention vor Angriffen auf Netzfunktionen“ und die „Bekämpfung von Straftaten im Internet“. Es bestand Einigkeit, dass die internationale Kooperation sowohl für die Fragen der Verfolgbarkeit von Straftaten im Internet wie für die Verbesserung des Schutzes vor Computerattacken verstärkt werden soll.

Um den auf G8-Ebene begonnenen, sehr fruchtbaren Dialog zu vertiefen und konkreten Ergebnissen zuzuführen, befindet sich die Bundesregierung in stetigen Konsultationen mit der deutschen Wirtschaft. Zuletzt hat im Mai 2001 in Tokio eine weitere Konferenz stattgefunden. Die Ergebnisse der Konferenz bedürfen noch der Auswertung.

45. Welche weiteren Maßnahmen zur Verbesserung des Schutzes vor Computerattacken erwägt die Bundesregierung auf internationaler Ebene?

Auf die bereits beschriebenen Aktivitäten der Bundesregierung im Rahmen von G8, dem Übereinkommen zur Datennetzkriminalität des Europarates sowie eEurope wird verwiesen.

Das BSI wird auf internationaler Ebene seine bestehende Zusammenarbeit mit FIRST (Forum of Incident and Response and Security Teams) weiter ausbauen.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
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