Deutscher Bundestag **Drucksache 14/4173**

14. Wahlperiode 26. 09. 2000

Große Anfrage

der Abgeordneten Norbert Geis, Erwin Marschewski (Recklinghausen), Wolfgang Bosbach, Ronald Pofalla, Meinrad Belle, Bernd Neumann (Bremen), Dr. Martin Mayer (Siegertsbrunn), Ilse Aigner, Günter Baumann, Dr. Joseph-Theodor Blank, Sylvia Bonitz, Hartmut Büttner (Schönebeck), Axel E. Fischer (Karlsruhe-Land), Dr. Jürgen Gehb, Dr. Wolfgang Götzer, Martin Hohmann, Volker Kauder, Hartmut Koschyk, Beatrix Philipp, Hans-Peter Repnik, Norbert Röttgen, Dr. Klaus Rose, Dietmar Schlee, Dr. Rupert Scholz, Bärbel Sothmann, Dr. Wolfgang Freiherr von Stetten, Thomas Strobl (Heilbronn), Dr. Susanne Tiemann, Dr. Hans-Peter Uhl, Andrea Voßhoff, Hans-Otto Wilhelm (Mainz), Bernd Wilz, Wolfgang Zeitlmann und der Fraktion der CDU/CSU

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 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.

Deshalb fragen wir die Bundesregierung:

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?
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)?
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)?
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)?
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)?
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)?

7. Welches Ausmaß haben nach den Erkenntnissen bzw. Schätzungen der Bundesregierung die nicht bekannt gewordenen Fälle der Computersabotage und -spionage (so genanntes Dunkelfeld)?
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?
9. Welche System- und Programmarten sind nach Auffassung der Bundesregierung besonders anfällig für Computerattacken?

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?
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?
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?
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?
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?
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?
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?

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?

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?

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

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?

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

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?

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?

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?

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

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?

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?

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?

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?

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?

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

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?

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

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?

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?

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?

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?

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?

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?

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

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?

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?

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?

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?

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

Berlin, den 26. September 2000

Norbert Geis
Erwin Marschewski (Recklinghausen)
Wolfgang Bosbach
Ronald Pofalla
Meinrad Belle
Bernd Neumann (Bremen)
Dr. Martin Mayer (Siegertsbrunn)
Ilse Aigner
Günter Baumann
Dr. Joseph-Theodor Blank
Sylvia Bonitz
Hartmut Büttner (Schönebeck)
Axel E. Fischer (Karlsruhe-Land)
Dr. Jürgen Gehb
Dr. Wolfgang Götzer
Martin Hohmann
Volker Kauder
Hartmut Koschyk
Beatrix Philipp
Hans-Peter Repnik
Norbert Röttgen
Dr. Klaus Rose
Dietmar Schlee
Dr. Rupert Scholz
Bärbel Sothmann
Dr. Wolfgang Freiherr von Stetten
Thomas Strobl (Heilbronn)
Dr. Susanne Tiemann
Dr. Hans-Peter Uhl
Andrea Voßhoff
Hans-Otto Wilhelm (Mainz)
Bernd Wilz
Wolfgang Zeitlmann
Friedrich Merz, Michael Glos und Fraktion

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