



Antwort

des Innenministers

auf die Kleine Anfrage

des Abg. Dr. Olderog (CDU)

Computer-Kriminalität

Mit der weiten Verbreitung von EDV-Anlagen wachsen auch die Gefahren einer mißbräuchlichen Verwendung des Computers. In der Presse werden Fälle der Computer-Kriminalität, einer relativ jungen Variante der Wirtschaftskriminalität, veröffentlicht.

1. Was wird unter dem Begriff „Computer-Kriminalität“ verstanden?

Computer-Kriminalität ist eine neue Erscheinungsform der Betriebskriminalität. Dabei ist der Computer Werkzeug oder Ziel von Unrechthandlungen in Betrieben der Privatwirtschaft und der öffentlichen Verwaltung.

Unter den Begriff der Computer-Kriminalität fallen:

- das Manipulieren von EDV-Programmen
- das Manipulieren von Datenbeständen
- das Manipulieren beim Bedienen eines Computers
- der „Diebstahl“ von Daten
- der computerbegünstigte Betrug durch Außenstehende (z. B. durch Anzapfen von Fernverarbeitungsleitungen)
- Sabotage

2. a) Welche Fälle sind ihr aus der Verwaltung und der Wirtschaft — gegliedert nach „Verfälschung, Ausspähung, mißbräuchliche Nutzung sowie Vernichtung von Daten, Datenbeständen oder Programmen“ oder „Veränderung, Beschädigung und Zerstörung von EDV-Anlagen“ — bekannt?

b) Welche Fälle sind unter a) nicht erfaßt?

In Schleswig-Holstein ist lediglich ein Fall bekanntgeworden, in dem ein Angestellter eines Datenverarbeitungsbetriebes versucht hat, Daten auszuspähen.

3. Mit welcher der in der Wissenschaft vertretenen Meinungen stimmt die Regierung überein, wonach entweder bei der gegebenen Sach- und Rechtslage die geltenden Vorschriften ausreichen, um sämtliche Fälle zu erfassen und schuldangemessen zu ahnden, oder Veranlassung für die Schaffung besonderer Straftatbestände gegeben ist?

Nach dem gegenwärtigen Stand der Sach- und Rechtslage reichen die geltenden Vorschriften aus, sämtliche Fälle von Computer-Kriminalität zu erfassen und schuldangemessen zu ahnden.

Die künftige computergesteuerte Zusammenführung personenbezogener Daten wird eine neue Lage schaffen. Die voraussichtliche Entwicklung auf diesem Gebiet fordert eine grundsätzliche Klärung. Da die geltenden Vorschriften für die dann möglichen Tatbestände nicht ausreichen, sieht der Entwurf des Bundesdatenschutzgesetzes neue Straftatbestände und entsprechende Strafsanktionen vor, die der Landesregierung ausreichend erscheinen.

4. Welche sonstigen z. B. technischen Vorschriften zur weiteren Vorsorge gegen mögliche Computer-Kriminalität werden für notwendig erachtet?

Der Schutz vor Computer-Kriminalität kann durch organisatorische und technische Maßnahmen erhöht werden. Dazu gehören

1. organisatorische Maßnahmen

- 1.1 Einsetzen eines besonderen Beauftragten in den Datenverarbeitungsbetrieben,
- 1.2 Einrichten einer unabhängigen staatlichen Überwachungsstelle für Datenschutz (z. B. Datenschutzbeauftragter, Datenschutzausschuß),
- 1.3 Herauslösen der eigentlichen Datenverarbeitung aus den Fachbetrieben und Verwaltungen durch Einrichtung selbständiger Datenverarbeitungsstellen wie die Datenzentrale Schleswig-Holstein,
- 1.4 Herauslösen der Programmierung aus den Fachverwaltungen und strikte Trennung der Programmierung von dem Analysebereich,
- 1.5 Verbot der Computer-Bedienung durch Programmierer,
- 1.6 Zugangsbeschränkungen für Computerräume sowie Programm- und Datenarchive,

2. technische Maßnahmen

- 2.1 Bau von sabotagegeschützten Räumen für Computer (z. B. Bunker),
- 2.2 Sicherung von Computerräumen gegen Vernichtung oder Veränderung von Programmen und Daten durch Hochfrequenzstrahlen (Bau eines „Faraday'schen Käfigs“),

- 2.3 Automatische Protokollierung jedes Eingriffs in die Tätigkeit des Computers,
- 2.4 Einbau und Prüfung von Berechtigungsschlüsseln in die Verarbeitungsprogramme,
- 2.5 Herstellung von Programm- und Datenduplikaten und Lagerung bei Rechenzentrum und auftraggebendem Betrieb.

Die Landesregierung hat bereits 1968 die Gründung der Datenzentrale Schleswig-Holstein als zentrale Datenverarbeitungsstelle für die öffentliche Verwaltung in Schleswig-Holstein veranlaßt. Die Datenzentrale führt die Datenverarbeitung getrennt von den auftraggebenden Verwaltungen nach konkreten Vorgaben dieser Verwaltungen durch. Die Verwaltungen schreiben die erforderlichen Kontrollen in den Programmen vor und testen die Programme anhand der bei ihnen vorhandenen Duplikate mit besonders erstellten Testdaten.

Die Landesregierung hat frühzeitig damit begonnen, die Programmierung vollständig aus den Verwaltungen herauszulösen und der Datenzentrale zu übertragen und treibt dies ständig weiter voran. Die Datenzentrale hat die Maßnahmen Nr. 1.5 (Verbot der Computer-Bedienung durch Programmierer), Nr. 1.6 (Zugangsbeschränkungen), Nr. 2.1 (Bau des Rechenzentrums Altenholz), Nr. 2.3 (automatische Protokollierung), Nr. 2.4 (Berechtigungsschlüssel) und Nr. 2.5 (Duplikate) durchgeführt. Die Maßnahme Nr. 2.2 (Hochfrequenzstrahlen) wird z. Z. untersucht.

Titzack