Staat und Recht im Imperialismus

Computerkriminalität in den kapitalistischen Industrieländern

Prof. Dt. sc. DIETMAR SEIDEL,
Sektion Rechtswissenschaft
der Karl-Marx-Universität Leipzig

Mit der Computerkriminalität ist eine neue Form nationaler und zunehmend internationaler Kriminalität im kapitalistischen Wirtschaftssystem hinzugekommen — noch raffinierter, noch weniger zu durchschauen und zu bekämpfen als das traditionelle Treiben der White-Collar-Verbrecher mit den bekannten Schädigungen der Wirtschaft und der Gesellschaft in gewaltigen Dimensionen. Was Art und Umfang dieser Verbrechensform, was angebliches und tatsächliches Raffinement und Undurchschaubarkeit dieser Deliktsart und auch was ihre Tendenzen und Ausbreitungsgeschwindigkeiten in der Zukunft anbelangt, gibt es Tatsachen und gibt es Schätzungen. Ernsthafte wissenschaftliche Analysen hierzu lagen bereits Anfang der siebziger Jahre vor. In dieser Zeit trat R. A. H. von Zur M ü h l e n *, einer der Experten in der BRD, mit konkreten Resultaten an die Öffentlichkeit. Sich auf die Computermanipulationen, die vorsätzliche Veränderung von EDV-Daten, konzentrierend, hatte er zu diesem Zeitpunkt 120 Fälle zusammengetragen, was bei einer Dunkelziffer zwischen 90 und 95 Prozent noch recht wenig auszusagen vermochte, indes jedoch alarmierende Tatsachen an das Licht der Öffentlichkeit beförderte. Sie veranlaßten ihn wie andere Kenner der Materie zu dem Schluß, daß man es mit der Computerkriminalität als einer äußerst gefährlichen Erscheinungsform der Wirtschaftskriminalität hier, heute und fürderhin zu tun haben wird.

Erscheinungsbild und potentielle Gefahren

Von H. G l i s s * [2] stammt die neuere folgende Übersicht, die wohl zeigt, welche Vielfalt im Erscheinungsbild der Computerkriminalität bereits in den entwickelten kapitalistischen Industriestaaten existiert und welche Gefahrenpotenzen diese Kriminalitätsform verkörpert:

Eingaben- und Ausgabenmanipulation
Wiederholungsläufe
Abbrüche
Tests mit echten Daten
Simulation echter Verarbeitung durch Testprogramme
Umgehung von Kontrollmechanismen, des Vier-Augen-Prinzips und der Funktionstrennung
Umgehung von Systemprüfungen, Protokollen, Abstimmungen
Anzapfen von Datenbeständen (Kenntnisnahme)
Ausspähen von Paßworten, Benutzeridentifikation und ähnlichen Zugangsberechtigungen zum Zwecke der Simulation eines berechtigten Nutzers gegenüber dem System
Abhören des Datenverkehrs, von Terminal-Aktivitäten und von Programmabläufen innerhalb eines Rechners
Manipulation von Prioritätenlisten und von Zugriffsberechtigungen
Verarbeitung von Daten mit unautorisierten Programmen und von Daten mit Hilfe von Dienstprogrammen
Provozieren von Hardware- und von Softwareausfällen
Mißbrauch von Wartungsroutinen
Abfangen von Nachrichten bei der Datenübertragung
Einschleusen von Nachrichten bei der Datenübertragung
Modifikation bei der Datenübertragung durch zwischengeschaltete Datenverarbeitungsgeräte
Raubkopien (Software)[3]

Zum Problemfeld Computermanipulationen und insonderheit der Computerkriminalität gehört zweifellos die Tatsache, daß künftig kein wichtiger Bereich in Staat, Wirtschaft und Gesellschaft mehr ohne Datenverarbeitung und Telekommunikation arbeiten und auskommen wird. Auch die Erhöhung der Treffsicherheit medizinischer Diagnosen und Therapien wird ohne Computereinsatz undenkbar; und in nahezu allen menschlichen Tätigkeitsbereichen, in denen mit Daten und Informationen Erkenntnisse ganz neuer Dimension erreicht werden sollen, ist dies ohne den Einsatz immer leistungsfähigerer Computer undenkbar.

Zu den Schätzungen gehört hingegen die Erwägung, wie schnell und wie sicher es den potentiellen Mißbräuchlern gelingt, im jeweiligen Bereich festen Fuß zu fassen, in welchem Maße sich Qualität und Quantität der Delikte mit Hilfe des Computers entwickeln und in welche Tiefen die Gesellschaft und der einzelne Mensch durch den mißbrauchten Computer namentlich in den entwickelten kapitalistischen Industrieländern gestürzt werden kann und wird. Daß dies geschieht, beweisen die Tatsachen bereits hinlänglich, und es ist allein schon besorgniserregend, ständig der Gefahr zu unterliegen, daß kräftige Konkurrenten auf dem kapitalistischen Markt ihre Kämpfe zu Lasten des geschäftlichen Gegners und sehr vieler Betroffener mit Hilfe des Computers austragen. Die Computerkriminalität und die Computerkriminellen sind nachgerade Indikatoren dafür, wie der Computer als Fortschrittselement mit nie dagewesener Durchschlagsgeschwindigkeit und als Regressionsfaktor mit nie dagewesenem Ausbreitungsgrad und mit hohem Gefahrenpotential zugleich wirkt. Während die einen verharmlosend und fälschlicherweise meinen, die Computerkriminalität sei mindestens von der Quantität her noch kein Thema[4], weisen andere sehr drastisch darauf hin, daß diese Kriminalität in den kapitalistischen Industrieländern so rasch zunimmt, wie die Zahl der genutzten Computer Wächst. Sie machen darauf aufmerksam, daß gegenwärtig nur etwa ein Prozent aller Computerdelikte entdeckt wird und davon wiederum allenfalls 14 Prozent zur Anzeige gelangen. J. S o y κ a [5] [6] bekennt, gestützt auf profunde Quellen, daß von 22 000 Computerkriminellen, die man irgendwo und irgendwann faßte, nur ein einziger vor den Richter mußte.

Manipulationsmöglichkeiten und kapitalistischer Konkurrenzkampf

Die Hacker vom „Chaos Computer Club“ (CCC) in Hamburg hatten der Post und Sparkasse der Hansestadt Ende des Jahres 1984 bewiesen, daß die posteigene Bildschirmtext (Btx)-Software keineswegs vor unbefugten Zugriffen sicher ist. Sie förderten aus dem Btx-System der Post sensible Daten eines anderen Benutzers, und zwar das besonders geschützte Kenn- und Paßwort („usd 70000“) für den Btx-Dienst der Hamburger Sparkasse (Haspa) zutage. Mit dem Kenn- und Paßwort gegenüber dem Post-Rechner als Haspa ausgewiesen, konnten sie sich in dem Btx-System frei bewegen und dem Haspa-Computer Order erteilen, wieder und wieder eine mit 9,97 DM belastete Btx-Seite des CCC abzurufen. Insgesamt liefen auf diese Weise annähernd 135 000 DM Gebühren zugunsten des CCC auf.6

„Unfug“ sei das, wie man beschwichtigend in den Medien formulierte, denn kriminelle Tatfolgen seien nicht bewirkt worden; dazu war die Sache weder angelegt, noch war das angesichts vorheriger Absprachen mit dem Landesdatenschutzbeauftragten zö befürchten, da man ja nur die Unsicherheiten beweisen und die Schwachstellen aufdecken wollte. Aber bestürzt waren die Betroffenen schon: Was hätte da nicht alles von der Haspa wegtransferiert werden können, wenn Kriminelle am Spiel gewesen wären.

Ebenso erging es amerikanischen Sicherheitsexperten, als ihnen Computer-Craeks von der University of Southern California das von einem Studenten entwickelte „Programm Virus“ demonstrierten und nachwiesen, daß man eine „Virus-Befehlskette“ in normale Computerprogramme einschleusen und nach Belieben Unheil der verschiedensten Art anrichten kann: Schlagartig lähmen dann die inzwischen tausendfach vervielfältigten Computerviren die befallenen Programme, sorgen für heilloses Durcheinander in den Rechnern, löschen lebenswichtige Programmteile aus den Speichern, ganz so, wie es vorher eingegeben worden ist.

Allein diese noch auf Heimwerker-Niveau zusammengebastelten „Viren“ für unterschiedliche, teils weithin benutzte Systemprogramme machten deutlich, wie hoch das Sicher-

---

X R.A.H. von Zur Mühlen, Computer-Kriminalität, Gefahren und Abwehrmaßnahmen, Neuwied und Berlin(West) 1972.

2 H. Gliss, „Computerkriminalität — Erscheinungsformen, Bedrohungspotential und Wachstumstrends“, Betriebswirtschaftliche Forschung und Praxis (Berlin[West|) 1985, Heft 1, S. 36.

3 Andere Kenner der Materie wählen andere Systematiken und Übersichten, ohne indes zu gravierend anderen Tatsachenfeststellungen zu gelangen. Vgl. insb. U. Sieber, Computerkriminalität und Strafrecht, Köln/Berlin(West)/Bonn/München 1980.

4 So. z. B. H. Stülienberg, „Von der Quantität her noch kein Thema“, Kriminalistik (Hamburg) 1986, Heft 8/9, S. 409 ff.

5 J. Soyka, Computer-Kriminalität, München 1986, S. 51 f.

6 **Vgl. Der Spiegel (Hamburg) vom 26. November 1984, S. 238.**