

Christian K. Bschorr: Computerkriminalität; Gefahren und Abwehr
 ECON-Verlag; Düsseldorf, Wien, New York; 1987.
 ISBN 3-430-11587-6, 256 S.

Der Verfasser — Vertriebsleiter bei einem der größten Computerunternehmen der Welt — berät Industrieunternehmen und öffentliche Institutionen in Fragen der Computerkriminalität. „Computerkriminalität“, ein beliebtes Thema der Medien der achtziger Jahre und der Verfasser fügt einen weiteren Titel hinzu.

Der Verfasser stellt systematisch Computersysteme mit ihren technischen Gegebenheiten, dem personellen Umfeld, den Anwendungen und den spezifischen Gefahren vor. Verfasser behandelt die Technik der Personalcomputer, Minicomputer, Mainframes und von Netzwerken. Ein weiteres Kapitel ist der Informationssicherung vorbehalten. In jedem Kapitel stellt der Verfasser eindrucksvoll spezifische Gefahren der mißbräuchlichen Verwendung von Computern vor.

Zwischen der Vorstellung der Technik/Anwendungen und der Vorstellung der spezifischen Gefahren wäre jedoch eine vertiefte Risikoanalyse für die Bereiche Organisation, Betriebssystemsoftware, Anwendungssoftware, Hardware, Verfahren und physische Sicherheit zu erwarten. Diese Erwartung wird enttäuscht. Eine an Risiko- und Gefahrenanalyse anschließende Vorstellung von Sicherungssystemen für die Risikominderung und die Gefahrenabwehr erfolgt leider nur summarisch. In technischer Hinsicht bietet der Verfasser dem technisch versierten Leser daher nur wenig Neues im Hinblick auf konkrete Probleme der Computerkriminalität.

In juristischer Hinsicht gibt der Verfasser einen recht knappen Einblick in die noch sehr junge Materie der Computerkriminalität. Er behandelt dabei in erster Linie die Modalität der Tat und deren Folgen auf Seiten des Tatopfers. Diese beiden bedeutenden Aspekte sind vom kriminologischen Standpunkt aus gesehen verständlich und unkompliziert dargestellt worden. Dem Verfasser kommt dabei sehr seine eigene Erfahrung als Praktiker zugute. Leider übergeht er die in diesem Zusammenhang wichtigen strafrechtlichen Fragen fast völlig. Verfasser begnügt sich damit, auf die Existenz von Gesetzen zum Thema Computerkriminalität hinzuweisen. Jedoch ist es gerade dieser Bereich, der den Juristen gegenwärtig große Schwierigkeiten bereitet, was z. B. an den vielfältigen Kommentierungen zu den neuen Normen abzulesen ist, die durch das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität in das Strafgesetzbuch aufgenommen wurden. Schon die zum Teil verunglückten Gesetzesformulierungen selbst (z. B. zu § 202 a II StGB: *Daten im Sinne des Absatzes 1*

sind nur solche, die ...) zeigen, welche Probleme die neue Materie den Juristen bereitet. Zur Lösung dieser Schwierigkeiten trägt das Werk nicht bei.

Verfasser erweckt bereits durch den Einstieg in die Materie und auch später durch die auffällig häufige Nennung der „Hacker“, „Knacker“ und „Crasher“ den Eindruck, als stellten diese die Tätergruppe schlechthin dar. Als Verfasser jedoch auf deren tatsächliche Gefährlichkeit eingeht, kommt er zu dem Schluß, daß die tatsächlichen Fälle der Computerkriminalität nicht dieser Tätergruppe zuzurechnen sind. Wenn er dennoch — sogar noch nach jenem Fazit — die „Hacker“ usw. mit „den“ Tätern der Computerkriminalität gleichsetzt, liegt die Vermutung nahe, es gehe ihm sehr darum, die Erinnerungen an sensationelle Fälle (z. B. Kinofilm „Wargames“) und deren Ausmaße wachzuhalten. Durch eine derartig realitätsverzerrende Aufbauschung wird der Gesamteindruck von einer sauberen Abhandlung zum Thema Wirtschaftskriminalität erheblich getrübt.

Verfasser geht im Detail näher auf die Haftungsproblematik und auf Diebstahlsfälle ein. Man wird jedoch voraussetzen können, daß ein Unternehmer in allen Bereichen seines Unternehmens darauf bedacht sein wird, für Fehler seiner Mitarbeiter nicht haften zu müssen. Daß PC's wie auch Disketten Tatobjekte eines Diebstahls gemäß § 242 StGB sein können, bedarf unter Juristen keiner näheren Erläuterung.

Zum Thema Diebstahl äußert sich Verfasser auch in einem anderen Zusammenhang. Er bezeichnet das dort beschriebene unautorisierte Kopieren von Computerprogrammen als „Programmdiebstahl“. Auf die in diesem Zusammenhang äußerst interessante Frage, wie man dies nicht nur urheberrechtlich, sondern eventuell auch strafrechtlich sanktionieren kann, geht der Verfasser leider nicht ein.

Die Beispielfälle, anhand derer der Verfasser die vielfältigen Konstellationen der Computerkriminalität darstellt, sind anschaulich und verständlich bearbeitet worden. Die Problembeschreibung endet jedoch (so z. B. ausdrücklich auf S. 32) dort, wo es für Juristen interessant wird. Der Verfasser eröffnet also — auch hier — keine neue Perspektiven.

Bei aller Kritik darf aber nicht übersehen werden, daß Juristen, die insbesondere an Detailfragen zur Computerkriminalität interessiert sind, wohl nicht zu dem Kreis von Lesern gehören, die durch das Buch angesprochen werden sollen. Und nichtsdestotrotz wird das Buch vor allem der breiten Masse der Juristen, die mit der Computertechnik noch nicht in Berührung kamen, eine willkommene Hilfe beim Einstieg in diesen Bereich sein.

Bertold Egbringhoff/Michael Rösler

In der Mailbox „Informatik und Recht“ (NUA 456 121 33061) wird versucht, so weit als möglich vollständig über aktuelle Fälle von Computerkriminalität, spektakuläre Fälle von ‚Hacking‘ oder Neues zu Computerviren zu berichten. Anregungen zur Berichterstattung werden dort gerne entgegengenommen.