„Technische Möglichkeiten zur kriminellen Einflußnahme auf Daten und Datenverarbeitung" (Teil 1)

Carsten Zobel

A. Thematische Abgrenzung

I. Einführung

Wie überall in der Welt, so entwickelt sich der Einsatz von Informations- und Kommunikationstechniken auch in der Bündesrepublik Deutschland recht rasant: Jährlich entstehen ca. 500000 neue Computerarbeitsplätze. Bereits heute ist jeder dritte Arbeitsplatz mit dieser Technik ausgerüstet; im Jahre 2000 werdem es schon zweidrittel aller Arbeitsplätze sein [1]. Mit dieser zunehmenden Technisierung besteht jedoch auch die Möglichkeit, der zunehmenden kriminellen Betätigung auf diesem Gebiet. Zwar sind bisherige Untersuchungen von recht wenigen Fällen ausgegangen - so geht Sieber [2] für den Zeitraum von 1963 - 1976 von nur 31 Fällen aus -, doch glauben Experten an eine Dunkelziffer von bis zu 99 % [3]. Auch die Berichterstattung in den Medien [4] belegt, daß Computerkriminalität existiert und nicht nur die Erfindung von trickreichen Unternehmens- oder Sicherheitsberatern ist [5].

II. Eingrenzung der Tatobjekte

Nach der Feststellung, daß Computerkriminalität existiert, stellt sich die Frage, welche Möglichkeiten der kriminellen Einflußnahme es gibt, welche Tatobjekte denkbar sind. Bei der thematischen Erfassung der Computerkriminalität werden herkömmlich folgende Fallgruppen gebildet [6]: Computermanipulationen, Zeitdiebstahl, Verletzung des Urheberpersönlichkeitsrechts, Wirtschaftsspionage mit Hilfe der EDV und Sabotage im EDV-Bereich. Aus diesen Fallgruppen lassen sich die Objekte und Mittel der Computerkriminalität ermitteln. Als Objekte kommen dabei die Hardware -also die DV-technischen Anlagen-, die Verarbeitungsvorgänge und die Daten in betracht[7]. Dabei sind unter Daten die Programme und die zu verarbeitenden Informationen zu verstehen[8]. Die möglichen Mittel sind das Entwenden, die Manipulation, die mißbräuchliche Nutzung und die Zerstörung[9]. Da das Tatobjekt Hardware meist Objekt bloßer Sachbeschädigungshandlungen sein wird[10] ist für einen Angriff darauf kein detailliertes technisches Wissen erforderlich. Fälle dieser Art werden hier daher nicht behandelt. Es bleiben daher als Tatobjekt nur die zu bearbeitenden Informationen, die die Verarbeitung steuernden Daten (=Programme) und die jeweils sich aus diesen Komponenten ergebenden Verarbeitungsvorgänge.

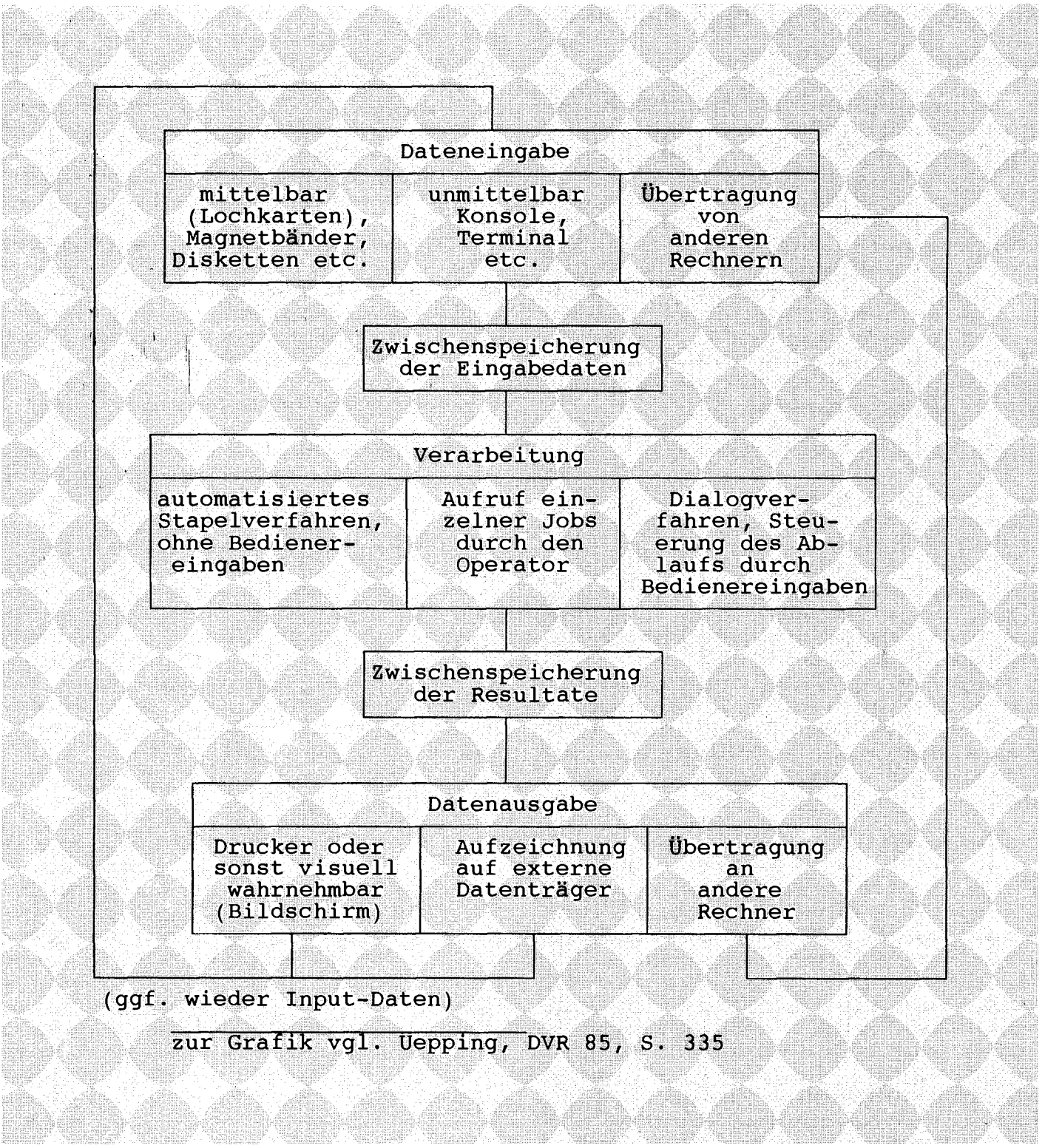
III. Ansatzmöglichkeiten der Einflußnahme

An die Bestimmung der Tatobjekte knüpft sich nunmehr die Problematik, wo sich innerhalb der EDV eine Beeinflussung vornehmen läßt und welche Personen diese Beeinflussung durchführen können.

1) Lokalisation der Tatobjekte

Um die Tatobjekte innerhalb der EDV lokalisieren zu können, bedarf es zunächst eines Überblicks über die einzelnen Vorgänge bei der Verarbeitung der Daten. Dazu dient die nebenstehende Grafik:
Die Grafik verdeutlicht den Datenfluß bei einem „normalen" Datenverarbeitungsvorgang. Ergänzend sei hinzugefügt, daß sich Daten nicht zwingend nur innerhalb dieses Datenverarbeitungsvorganges lokalisieren lassen, sondern zusätzlich als gespeicherte Daten auf Speichermedien (z.B. Magnetbändern und -platten, Disketten etc.) abgelegt sein können. Besonders bedeutsam sind -bezüglich der Beeinflussungsmöglichkeiten- die 3 großen Schritte der Dateneingabe, der -verarbeitung und der -ausgabe. Zwar kann festgestellt werden, daß „Systemangriffe (...) in jedem Glied der Kommunikationskette möglich" sind[11]. Eine Beeinflussung der jeweiligen Zwischenspeicherungen ist aber entweder technisch nicht besonders anspruchsvoll -so hätte die Unterbrechung der Stromzufuhr u.U. den Datenverlust in den Zwischenspeichern zur Folge- oder sie sind technisch so anspruchsvoll, daß die gewünschte Beeinflussung mit weniger Aufwand während anderer Verarbeitungsschritte zum gleichen Ziel führen würde. Wenn aber der technische Aufwand dem Nutzen des Erlangten nicht äquivalent gegenübersteht, der sogenannte Arbeitsfaktor (work factor) zu groß wird, dann ist eine kriminelle Beeinflussung weitgehend auszuschließen[12]. Aus diesem Grund wird die Beeinflussung von Daten während der Zwischenspeicherung nicht eingehender betrachtet. Für eine Untersuchung der für potentielle Täter interessanten Einflußnahme bleiben daher die Daten in den Verarbeitungsstadien Dateneingabe,Datenverarbeitung und Datenausgabe.

1) zu diesen Zahlen vgl. Frankfurter Allgemeine Zeitung (FAZ) vom 7.10.88 ältere, u.a. auf Werte bezogene Angaben bei Sieg, Jura 86, S. 352 m.w.N.
2) Nachweis bei Sieg, Jura 86, S. 353
3) Herrmann, Der Kriminalist 86, 462; Möhrenschlager, wistra 86, 128; Steinke, NStZ 84, 297
4) Süddeutsche Zeitung vom 31.08.88, „In Bruchteilen einer Sekunde kriminell"; FAZ vom 16.9.88, „Verfahren gegen Software-Diebe werden meist eingestellt"; FAZ vom 24.10.88, „Elektronische Post der Regierung mitgelesen"; FAZ vom 7.11.88, „Ein 'Wurm' legt tausende von Computern lahm"; hierzu auch am 9.11. und 22.11.88; Bericht über das Eindringen von Hackern in einen NASA-Rechner in der Panorama-Fernsehsendung vom 22.11.88
5) so aber Betzl, DSWR 72, S. 475
6) Sieber, DSWR 74, 246; ähnlich Winkelbauer, CuR 85, 41 ff.
7) Mohr, Öffentliche Anhörung zu den Entwürfen zum 2. WiKG, S. 218 f.; Wiesel, data report 73, S. 26
8) wie auch in § 202 a, vgl. Dreher/Tröndle, Rn. 6 zu § 202 a
9) wie Fn. 2)
10) vgl. Fälle 1, 2 und 3 bei Sieg, Jura 86, 354
11) Kruse, CuR 87, S. 793
12) Uepping, DVR 85, S. 333



zur Grafik vgl. Uepping, DVR 85, S. 335

2) Abgrenzung interne - externe Beeinflussung

Um die thematische Eingrenzung abzuschließen bedarf es noch der Beantwortung der Frage, welche Personen als mögliche Täter in Betracht kommen.
Generell läßt sich dazu sagen, daß jeder, der Zugang zu Daten und Datenverarbeitung hat, diese auch beeinflussen kann. Anknüpfend an die Möglichkeit des Zugangs lassen sich potentielle Täter allerdings zwei Gruppen zuordnen: einem internen und einem externen Personenkreis[13]. Zum internen Personenkreis gehören dabei die autorisierten Benutzer, Systembetreuer, Programmierer etc., also all diejenigen, die aus der Sicht des Betreibers einer EDV-Anlage (vertraglich) berechtigt sind, durch ihre Tätigkeit Einfluß auf die Datenverarbeitung zu nehmen. In der Regel dürfte es sich bei diesen Personen um Betriebsangehörige handeln[14]. (Dies ist z. B. anders bei Auftragsarbeiten). Demgegenüber gehören zum externen Personenkreis regelmäßig die Personen, die sich als Betriebsfremde ohne Wissen und Billigung des Berechtigten Zugang zu einer EDV-Anlage oder zu den Daten verschaffen[15].

13) Uepping, DVR 85, S. 342 f.
14) Uepping, DVR 85, S. 342
15) Uepping, DVR 85, S. 343

B. Darstellung einzelner Eingriffsmöglichkeiten

I. Interner Personenkreis

Täter, die zum internen Personenkreis gehören,werden vorwiegend die Möglichkeit der Computermanipulation verwenden: diese Personen haben nämlich sowohl Zugang zu Daten und EDV-Anlagen als auch die Möglichkeit eventuelle organisatorisch bedingte Entdeckungen ihrer Manipulation zu verhindern. Dabei wird ein Täter aus diesem Kreis versuchen, durch „die unberechtigte Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms oder Einwirkung auf seinen Ablauf oder die Schaffung bzw. Verwendung unrichtiger oder unvollständiger optisch nicht unmittelbar lesbarer Daten (...) sich oder einem Dritten einen Vermögensvorteil zu verschaffen" [16]. Aus obigem Datenflußplan (vgl. S. 95) lassen sich die drei nun folgenden Manipulationsformen ableiten.

1) Manipulationen während der Dateneingabe

Von der Manipulation während der Dateneingabe, auch Input-Manipulation genannt[17], spricht man, wenn der Täter durch Fortlassen oder Hinzufügen von Daten ein für ihn vorteilhaftes Ergebnis der Datenverarbeitungsanlage herbeiführt. So wurden beispielsweise im Kindergeldfall[18] durch einen kinderlosen Sachbearbeiter, Lochkarten erstellt, die -in die EDV eingeleseneine Kindergeldzahlung an ihn bewirkten. Alle Input-Manipulations-Fälle[19] stellen für den Täter keine hohen Anforderungen technischer Art. Vielmehr geht es darum, organisatorische Hindernisse zu umgehen. Im eben genannten Fall war es z. B. zusätzlich erforderlich, diejeweiligen Listen der Zahlungen zu manipulieren. Diese Handlung gehört allerdings schon zu einer anderen Manipulationsform, der Ausgabemanipulation.

2) Manipulationen während der Datenausgabe

Die Manipulation der Datenausgabe, die sogenannte Output-Manipulation[20], geht wie eben gezeigt oft mit der Input-Manipulation einher. Da die Ausgabe der Datenverarbeitungsergebnisse häufig in Form von Ausdrucken vorliegt, wird dieser Manipulationsform die computerspezifische Besonderheit abgesprochen; vielmehr werden sie den typischen Urkundsdelikten zugeordnet[21]. Dies Ergebnis ist allerdings dann angreifbar, wenn die Datenausgabe nicht durch Drucker, sondern beispielsweise in Form einer Datenspeicherung auf Disketten erfolgt. Ein Beispiel dafür bietet der sogenannte beleglose Datenträgeraustausch der Banken. Bei diesem Verfahren werden Last- und/oder Gutschrift-Daten auf einer Diskette gespeichert. Diese wird anschließend an die kontoführende Bank geschickt. Dort wird die Diskette vom Bankrechner eingelesen, die Last- und/oder Gutschriften werden ausgeführt. Ein Täter der auf diese Diskette vorm Absenden an die Bank zugreifen kann, hat die Möglichkeit, die darauf gespeicherten Daten nachträglich zu verändern. Dazu wird lediglich ein Programm benötigt, mit dem die Daten gelesen und verändert werden können (sog. Diskmonitor; u.U. reicht das zum Lieferumfang des Betriebssystems MS-DOS gehörende Programm „debug.exe" schon aus). Kennt (oder erkennt) der Täter dann noch den Aufbau der Datensätze[22], so könnte er beispielsweise den seinem Konto gutzuschreibenden Betrag ändern.
Da nach einer eventuellen Änderung die neuen Daten nach Abschicken an die Bank in den dortigen Computer eingelesen werden, ließe sich eine solche Manipulation eventuell auch den Input-Manipulationen zuordnen. Dem Wesen nach steht die Änderung eines Disketten-„Outputs" aber der Output-Manipulation näher, zumal DV-technisch immer von einer Ausgabe gesprochen wird, gleichgültig, auf welches Ausgabegerät („device") Daten geleitet werden. Als Ergebnis der Betrachtung zur Input- und zur Outputmanipulation kann -unter Hinzuziehung der Grafik zum Datenfluß- festgehalten werden, daß eine Trennung zwischen beiden Manipulationsformen nicht immer eindeutig vorzunehmen ist, denn manipulierte Output-Daten können ihrerseits wieder (unrichtige) Input-Daten sein. Beide Formen benötigen nur dann DV-technische Kenntnisse, wenn es um die Manipulation von Datenträgern als Speichermedien geht. Die übrigen Einflußnahmen setzen vorwiegend Kenntnisse von der jeweiligen Arbeitsorganisation voraus.

3) Manipulationen während der Verarbeitung

Diese Manipulationsform läßt sich entsprechend dem Arbeitsablauf der EDV zwei Unterformen zuordnen: der Programmanipulation und der Konsolmanipulation[23]. Beide Arten wirken sich zwar in der eigentlichen Verarbeitungsphase aus; ihre Ursachen fallen jedoch zeitlich auseinander. Die Programmanipulation erfolgt bei Erstellung des Programmes, also zeitlich vor der Verarbeitungsphase. Die Konsolmanipulation hingegen geschieht im Zeitpunkt des Verarbeitungsvorganges. Ein weiterer Unterschied besteht in ihrer Quantität. Der Eingriff in ein Programm kann einmalig durchgeführt werden, um trotzdem bei jedem Programmdurchlauf zu unrichtigen, vom Täter erwünschten Ergebnissen zu führen. Bei der Konsolmanipulation kann das jeweils erwünschte Ergebnis nur durch immer erneute Eingriffe erfolgen.

a) Konsol-Manipulationen

Bei der Konsolmanipulation nutzt der Täter die besondere und heute wohl gängige Form der Programmsteuerung durch den Bediener (Operator). Während bei sogenannten Stapelverfahren oder in der Prozeßdatenverarbeitung der gesamte Verarbeitungsvorgang über fertige Stapel-(Batch-) Programme bzw. über sensorerfaßte Daten gesteuert wird, hat bei der bedienergesteuerten Programmausführung der jeweilige Anwender die Möglichkeit, bestimmte Arbeitsschritte festzulegen. Dies kann im wesentlichen auf zwei Arten geschehen. Zum einen kann der Operator bestimmte Programme -auch Jobs genannt- die sich auf Daten auswirken starten. So kann er beispielsweise Daten löschen oder diese kopieren[24], wodurch dem Betreiber der DV-Anlage Schäden, dem Täter jedoch Vorteile erwachsen könnten. Die andere Möglichkeit der Einflußnahme ergibt sich aus dem sogenannten Dialogverfahren (Menüsteuerung).

16) Kindergeldso die Definition der Computermanipulation der AG Kripo, bei Steinke, NStZ 84, 295
17) Sieber, DSWR 74, 245
18) Sieber, BB 82, 1434
19) weitere Fälle bei Sieg, Jura 86, S. 354 f.
20) Sieber, DSWR 74, 245
21) Sieg, Jura 86, S. 356
22) den er im übrigen in den „Sonderbedingungen für den beleglosen Datenträgeraustausch" der Sparkassen nachlesen kann
23) Sieber, DSWR 74, 245
24) vgl. zum Kopieren von Daten auch unten (S. 17 ff.)

Darunter versteht man die Möglichkeit durch Drücken besimmter Tasten ein Programm zu einer bestimmten Aktion zu veranlassen, z. B. einen bestimmten Vorgang nochmals auszuführen oder eine Ausführung abzubrechen. Letztere Möglichkeit machten sich einige Devisenhändler zum Nachteil der Herstatt-Bank zunutze[25]. Bei Kleincomputern dieser Bank konnte der Ausdruck eines Abrechnungsformulars dadurch unterbrochen werden, daß eine als „Abbruch-Taste" definierte Taste gedrückt wurde. Die ausgedruckten Daten wurden in diesem Fall nicht als ausgegebene Daten aufgezeichnet. Damit aber zwischen Ausdruck und gespeicherter Information keine Diskrepanzen bestanden, mußte der abgebrochene Ausdruck als ungültig gekennzeichnet werden. Diese Möglichkeit war programmseitig vorgesehen. Nach Drücken der „Abbruch-Taste" wurde das Wort „Abbruch" auf das ausgegebene Formular gedruckt. Die Täter verhinderten diesen die Manipulation aufdeckenden Aufdruck dadurch, indem sie das bedruckte Formular schnell genug aus dem Drucker nahmen, so daß der Vermerk „Abbruch" nur auf die Druckerwalze geruckt wurde. Dieser Fall sowie das oben erwähnte unberechtigte Starten von Jobs machen deutlich, daß der Täter einer Konsolmanipulation nur etwas technisches Wissen benötigt, um diese Einflußnahme auszuüben. Ähnlich wie in den Fällen der Input- und Output-Manipulation benötigt er vielmehr organisationstechnisches Wissen, damit durch innerbetriebliche Kontrollen seine Tätigkeiten nicht entdeckt werden.

b) Programmanipulationen

Programmanipulationen sind denkbar durch Verändern, Hinzufügen, Löschen von Programmablaufschritten oder durch Modifizieren von konstanten Größen[26]. Dabei erfordert diese Art der Manipulation sowohl DV-technisches als auch Wissen um die Betriebsorganisation. Einerseits muß der Täter in der Lage sein, ein Programm so zu gestalten, daß ein von ihm erwünschtes Ergebnis erzielt wird (Manipulation des Ergebnisses); andererseits muß er aber gleichzeitig wissen, welche betrieblichen Kontrollen bestehen, damit er diese durch seine manipulierten Programme umgeht (Verdeckung der Manipulation). Als Beispiel für beide Komponenten der Programmanipulation möge der hierzu wohl bekannteste Fall, der sogenannte Rundungstrick-Fall gelten[27]. Auch wenn z.T. an der Authentizität dieses Falles gezweifelt wird[28], läßt sich an ihm das prinzipielle Vorgehen bei der Programmanipulation gut verdeutlichen.

aa) Sachverhalt des Rundungstrick-Falles

Das Programm, das der Täter zu erstellen hatte, sollte Zinsberechnungen für eine Bank ausführen. Die Zinsen wurden dabei auf Zehntel-Pfennige genau berechnet. Bevor die Zinsen bei den Bankkunden zur Gutschrift kamen, wurden sie auf ganze Pfennige abgerundet. Die aus Zehntel-Pfennigen bestehenden Differenzbeträge sammelte der Täter auf einem stillen Konto, von dem er sie dann auf sein Konto überwies. Dabei soll ein Betrag von 500000 DM zustande gekommen sein.

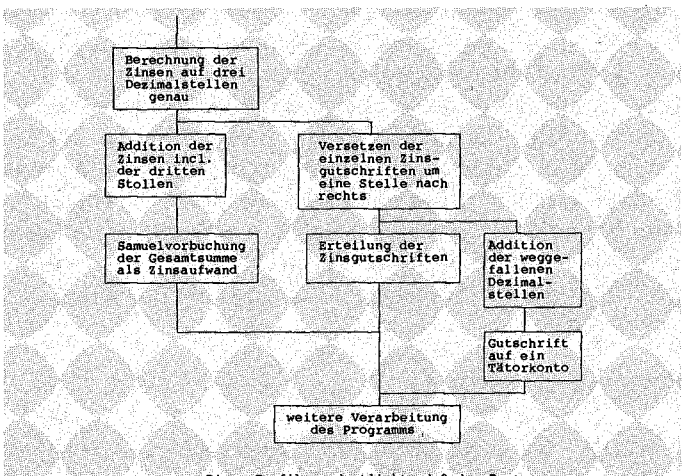
bb) Realisierbarkeit[29]

(1) Manipulation des Ergebnisses

Zunächst muß der Programmierer die entsprechend fälligen Zinsen auf drei Nachkommastellen genau berechnen lassen. In einer Programmiersprache wie COBOL[30] ist dies kein Problem, da nur eine Variable entsprechend definiert werden muß. Die eigentliche Manipulation besteht nun darin, die dritte Nachkommastelle des Zinsbetrages „abzuschneiden", anschließend die „abgeschnittene" Zahl durch 1000 zu teilen (da es sich nur um Zehntel-Pfennige handelt) und den so erhaltenen Betrag dem Täterkonto gutzuschreiben. Zum Verdeutlichen ein Beispiel: Der errechnete Zinsbetrag beträgt 45,568 DM. Durch Verschieben einer Variable in eine andere Variable erhält man die Zinsgutschrift des Bankkunden in Höhe von 45,56. In einer anderen Variable steht nun die „abgeschnittene" Zahl 8. Dies Ergebnis wird durch 1000 geteilt und der sich ergebende Betrag von 0,008 DM wird anschließend dem Täterkonto gutgeschrieben. Damit ist die erwünschte Manipulation des Ergebnisses schon erreicht.

(2) Verdeckung der Manipulation

Die eigentlichen Manipulation des Ergebnisses bedarf nunmehr einer Verdeckung, damit sie nicht durch augenscheinliche Auffälligkeiten entdeckt wird. Im vorliegenden Fall muß der Programmierer dafür sorgen, daß der auf Zehntel-Pfennige berechnete gesamte Zinsaufwand auch als Buchung in entsprechender Höhe erscheint, da sonst Differenzen zwischen den verbuchten und den tatsächlich abgebuchten Beträgen entstehen würden. Die folgende Grafik[31] macht das Verfahren deutlich:



Durch die Sammelverbuchung der Gesamtzinsbeträge (das bedeutet, daß nicht für jede einzelne Zinsgutschrift eine Einzelgegenbuchung erfolgt, sondern diese Gegenbuchung als eine Soll-Buchung auf einem Konto, das beispielsweise mit „Zinsaufwand" bezeichnet wird, erfolgt) einschließlich der dritten Stellen besteht Übereinstimmung zwischen der gebuchten und der tatsächlichen Ausgabe. Diese Grafik verdeutlicht, daß der Programmierer auch Kenntnisse über die Organisation benötigt, da er sein Programm sonst nicht mit den erforderlichen „Umgehungsmechanismen" ausgestalten könnte.

25) Sieber, BB 82, 1435
26) be–Wiesel, data report 73, S. 25
27) Bei-Sieg, Jura 86, S. 355 m.w.N.
28) Ammann/Lehnhardt, S. 177; Betzl, DSWR 72, 319 f.
29) vgl. Programmlisting
30) Common Business Oriented Language: höhere Programmiersprache zur Bearbeitung kommerzieller und kaufmännischer Aufgaben, die im kaufmännischen Bereich nach wie vor als Standard gilt; vgl. Computer persönlich, Heft 26/88, S.65 iur, Heft 5/86, S. 239 f.
31) von zur Mühlen/ Sieben, DSWR 72, 401

4) Zusammenfassung

Zusammenfassend läßt sich sagen, daß Einflußnahme durch Täter aus dem internen Personenkreis weitgehend eingehendere Kenntnis der betrieblichen Organisation voraussetzt, um eventuelle Kontrollmechanismen auszuschalten. DV-technisches Wissen ist dabei nur für den Fall der Programmanipulation und gegebenenfalls bei der die Speicherung von Daten beeinflussenden Output-Manipulation erforderlich.

II. Externer Personenkreis

Da es sich bei den zum externen Personenkreis gehörenden Tätern um Betriebsfremde handelt, besteht für diese zunächst das Problem, sich Zugang zu den Daten zu verschaffen. Sollte dieser Zugang erreicht sein, so wird es den externen Tätern nicht um Manipulationen der oben beschriebenen Art gehen, da hierzu das notwendige organisationstechnische Wissen in der Regel nicht vorhanden sein wird. Vielmehr dürfte es Ziel der Externen sein, den in den Daten verkörperten wirtschaftlichen Wert zu nutzen oder zwecks Schadenszufügung die Daten zu zerstören. Bei krimineller Einflußnahme durch externe Personen wird es sich demnach um Delikte der Computerspionage und Computersabotage handeln[32]. Die Frage, ob auch ein sogenannter Hacker, „meist Jugendliche, die mit ihren kleinen Heimcomutern fremde Rechnersysteme anzapfen"[33]unter den Tatbestand der Computerspionage und/oder den der Computersabotage fällt und somit kriminellen Einfluß auf die EDV ausübt, kann hier unbeantwortet bleiben, da beim „hacking" zumindest aus technischer Sicht wie bei der Computersabotage/-spionage vorgegangen wird (allenfalls mit beschränkteren Mitteln). Nach dem Gesagten sind nunmehr zwei Fragen zu beantworten, nämlich wie kann sich ein Täter Zugang zu fremden Daten verschaffen (Computerspionage und -sabotage) und wie können Daten zerstört werden (Computersabotage).

1) Zugang zu den Daten

Normalerweise befinden sich die Daten, auf die zugegriffen werden soll, innerhalb eines bestimmbaren Bereiches, regelmäßig den Betriebsräumen eines Anwenders. Dieser Bereich wird hier als Anwenderbereich bezeichnet. Der Zugriff auf diese Daten kann - grob unter teilt - auf zwei Weisen erfolgen: die Daten „verlassen" den Anwenderbereich und der Zugriff auf die Daten erfolgt außerhalb dieses Bereiches oder der Täter „begibt" sich in den Anwenderbereich und dort erfolgt der Zugriff.

d) Datenzugriff außerhalb des Anwenderbereichs

Außerhalb des Anwenderbereichs kann notwendigerweise nur dann zugegriffen werden, wenn die Daten aus dem Anwenderberich hinausgelangen. Dies ist im wesentlichen in drei Situationen der Fall: bei Datenübertragung, bei kommerziellem Vertrieb von Daten und beim Datendiebstahl.

ad) Datenübertragung

Es kann erforderlich sein, daß Daten von einem Anwenderbereich in einen anderen Anwenderbereich transportiert werden müssen. Ein Besispiel dazu wurde bereits oben[34] dargestellt: der beleglose Datenträgeraustausch. Hier werden die Daten auf einer Diskette gespeichert und verschickt. Ein anderes Beispiel bietet die sogenannte Datenfernverarbeitung: Es kann sinnvoll sein, Daten an einem Ort zu erfassen, sie aber an einem anderen Ort zu verarbeiten. Erforderlich ist dies beispielsweise bei Bankfilialen, denn sofern die jeweiligem Kontostände der Kunden in einem Zentralrechner abgespeichert sind, müssen Aus- und Einzahlungen dort verbucht werden; die Daten sind also von der Filiale zum Zentralrechner zu übertragen[35]. Neben der Datenfernverarbeitung kann die Datenübertragung auch in anderen Bereichen erforderlich sein. Vorstellbar ist beispielsweise der Ergebnisaustausch von dezentralisiert arbeitenden Forschungseinrichtungen oder von Einzelunternehmen innerhalb eines Konzerns. In diesen Fällen des Datenaustauschs spricht man von Datenfernübertragung. Als Übertragungsmedien kommen dabei Freileitungen, Kupfer- oder Glasfaserkabel und auch Funkverbindungen in Form von erdgebundenen Richtfunkstrecken oder Satellitenübertragungen in Betracht[36]. In all den beschriebenen Fällen sind Sabotage- und Spionagehandlungen technisch machbar. Die Sabotage kann im einfachsten Fall durch Zerstörung der jeweils zur Datenübertragung genutzten Medien geschehen. Sie ist insofern weder technisch anspruchsvoll noch EDV-spezifisch. In den Fällen der Spionage kommt es ebenso auf das jeweilige Übertragungsmedium an: Speichermedien können mit entsprechenden EDV-Geräten wieder gelesen werden. Bei der Übertragung mittels metallischer Kabel lassen sich die Daten, da sie als elektrische Impulse vorliegen, durch direkte Kabelanbindung oder über induktive Abkopplung „abzapfen"[37], d.h. zu der EDV-Anlage des Täters leiten. Technisch problematischer ist das „Abhören" eines Glasfaserkabels. Weil die Daten hier nicht als elektrische sondern als optische Impulse vorliegen, bedarf es immer eines Eingriffs in das Kabel, der die weitere Datenübertragung gefährdet[38]. Auch in diesem Fall muß die Weiterleitung der Impulse zu einem tätereigenen Computer erfolgen. Das Empfangen von mittels Funk übertragenen Daten wird technisch durch entsprechende Antennenanlagen ermöglicht[39], die ihrerseits wieder die empfangenen Signale an eine EDV-Anlage weiterleiten. Bei all diesen technisch möglichen Datenzugriffsmöglichkeiten stellt sich allerdings die Frage, wie lohnenswert sie sind. Denn besonders sensible Daten dürften wohl nur in verschlüsselter Form transportiert werden, eine Entschlüsselung kann mitunter (fast) unmöglich sein. Da es hier thematisch jedoch nur um die kriminelle Einflußnahme auf die EDV, nicht jedoch um die (wirtschaftliche) Verwendbarkeit von Daten geht, und durch den beendeten Zugriff auch die Einflußnahme beendet ist, kann diese Problematik offen bleiben[40].

32) Winkelbauer, CuR 85, S. 43 f.
33) so Ammann/Lehnhardt, S. 8; dort mehr zum Begriff der Hacker
34) vgl. Seite 7
35) dies und weitere Beispiele bei Zeeb, Computer-Praxis abc, Gruppe 3/32, S. 1
36) Tiemeyer, Computer-Praxis abc, Gruppe 3/38, S. 1
37) Leicht, iur 87, S. 51
38) Leicht, iur 87, S. 51
39) Leicht, iur 87, S. 51
40) zu dieser Thematik vgl. Leicht, iur 87, S. 51 f. m.w.N. FAZ v. 25.10.88 „Auf der Suche nach den Primfaktoren immer größerer Zahlen"

bb) Kommerzieller Vertrieb von Daten

Möglich ist, daß Daten aus dem Anwenderbereich hinausgelangen, weil der Anwender diese Daten anderen Anwendern käuflich oder gegen ein Nutzungsentgelt überläßt. Hierzu gehört vor allem der Vertrieb von Programmen. Diese werden von den Herstellern in der Regel auf Speichermedien aufgezeichnet und in dieser Form vertrieben. Somit gelangen die Daten aus dem Anwenderbereich hinaus; der Zugriff auf diese Daten ist Tätern nunmehr möglich. Eingeschränkt ist der Zugriff allerdings dadurch, daß er regelmäßig von einer Entgeltzahlung abhängig gemacht wird. Ein potentieller Täter wird jedoch Interesse daran haben, sich diesen Zugriff unentgeltlich zu verschaffen. Es wird daher versuchen, die Zahlung zu umgehen, indem er sich bei einem Berechtigten Kopien des jeweiligen Speichermediums anfertigt. Durch sogenannte „Raubkopien" [41] hat der Täter anschließend die Möglichkeit, unentgeltlich und beliebig oft auf die nunmehr duplizierten Daten zuzugreifen. Die Möglichkeiten der technischen Einflußnahme auf Daten liegt bei dieser Fallgruppe somit im Kopieren von Speichermedien (meist dürfte es sich um Disketten handeln). Im konkreten Fall mag es beispielsweise darum gehen, daß von einem auf Diskette gespeicherten Programm eine Kopie hergestellt werden soll. Ob dies überhaupt möglich ist, hängt davon ab, wie der Hersteller des Programms dieses auf der Diskette gespeichert hat. In vielen Fällen lassen sich Kopien mit Hilfe sogenannter Kopierprogramme herstellen. In einfacher Form besitzt diese Kopierprogramme jeder EDV-Anwender, da sie für die Sicherung eigener Daten erforderlich sind. Die Handhabung eines solchen Programmes ist technisch anspruchslos: nachdem es gestartet wurde, erfolgt der eigentliche Kopiervorgang automatisch. Technisch anspruchsvoller ist das Kopieren jedoch dann, wenn der Hersteller seine Programme in einer besonderen Form auf der Diskette abgespeichert hat. Wie sich die Einflußnahme durch das Kopieren in diesen Fällen gestaltet, ist vom jeweiligen Einzelfall abhängig und kann hier daher nur exemplarisch geschildert werden. Denkbar ist beispielsweise, daß ein Programmhersteller zusätzlich zu dem eigentlichen Programm noch ein Kopierprogramm mitliefert, mit dessen Hilfe ein Anwender sich das Programm auf die Festplatte seines Computers kopiert. (Dies ist für den Anwender wünschenswert, da er dies Programm dadurch besser nutzen kann.) Durch das Kopieren wird das kopierte Programm jedoch so modifiziert, daß eine nochmalige Kopie zu nicht lauffähigen Programmversionen führen würde. Ein Raubkopierer wird in solch einem Fall versuchen, jedes einzelne gespeicherte Zeichen des kopierten Programms mit jedem Zeichen eines nicht kopierten Programmes zu vergleichen. Dabei kann er sich eines Programmes bedienen, das diese Vergleiche für ihn übernimmt. Duch diesen Vergleich kann die Modifikation festgestellt werden. Nunmehr gibt es technische Möglichkeiten, die Modifikationen -abermals unter Zuhilfenahme von bestimmten Programmen- wieder rückgängig zu machen. Ist dies geschehen, so kann das dann unverändert vorliegende Programm beliebig oft kopiert werden. Eine andere Möglichkeit zum Schutz hat der Hersteller durch die physikalische Veränderung der Disketten. Der Raubkopierer müßte diese physikalische Änderung auch an der kopierten Diskette vornehmen. Eine solche Änderung dürfte nur mit ähnlichen Geräten machbar sein, wie sie der Hersteller verwendet hat; der Kopierer müßte dann also technisch so ausgestattet sein wie der Programmhersteller. Andere technische Möglichkeiten sind denkbar, ergäben sich aber -wie oben betont- aus den vielfältig möglichen Vorgaben des jeweiligen Programmherstellers.

cc) Datendiebstahl

Beim Datendiebstahl handelt es sich meist um eine Kombination von bisher Beschriebenem. Die Fallkonstellation beim Datendiebstahl stellt sich häufig so dar, daß betriebswichtige Daten wie Forschungsergebnisse oder Kundenadressen aus dem Anwenderbereich hinaus in die Hände von Konkurrenten gelangen[42]. Da der jeweilige Anwender ein Fehlen der Daten jedoch bemerken würde, was nicht im Interesse des bzw. der Täter liegen dürfte, werden die Daten kopiert. Dies ist technisch mit Programmen durchführbar (s.o.). Die zu kopierenden oder schon kopierten Daten befinden sich ursprünglich im Bereich des Anwenders. Sie von dort nach außerhalb zu bringen, dürfte jedoch weniger ein technisches als vielmehr ein organisatorisches Problem darstellen. Daher wird diese Handlung wohl von einer zum internen Kreis rechnenden Person vorgenommen[43]. Natürlich sind beim Datendiebstahl auch andere Fälle denkbar. Ein leitender Angestellter könnte beispielsweise Datenspeicher aus dem Anwenderbereich mitnehmen, um diese als zusätzliche Kopie zuhause aufzubewahren oder dort weiter zu bearbeiten. Dieser Mitarbeiter könnte nun auch gewaltsam zur Herausgabe der Daten gezwungen werden. Allerdings handelt es sich in diesen Fällen nicht mehr um technische Einflußnahmen.

b) Datenzugriff innerhalb des Anwenderbereichs

Der Datendiebstahl, besonders in der letztgenannten untechnischen Form macht deutlich, daß ein Zugriff auf Daten nur dann außerhalb des Anwenderbereichs erfolgen kann, wenn die Daten aus diesem hinausgelangen. Ist das nicht der Fall, so wird ein Täter versuchen, sich Zugang zum Anwenderbereich zu verschaffen, um dort auf die Daten zugreifen zu können. Zunächst ist es für den Täter unter Umständen möglich, sich persönlich in den Anwenderbereich zu begeben. Insofern sind die jeweiligen Zugangsprobleme allerdings keine DV-spezifischen; die Probleme sind die, die ein Einbrecher oder Betriebsspion hat. Allenfalls beim eigentlichen Datenzugriff sind gegebenenfalls technische Einflußnahmen möglich. Diese dürften dann entweder im -oben schon beschriebenen- Kopieren von Daten bestehen oder in der Zerstörung von Daten oder EDV-Geräten. Bei der Zerstörung ergeben sich keine technischen Besonderheiten; einschränkend sei jedoch festgestellt, daß bei magnetischen Speicherungen (z. B. Magnetbänder, Disketten), die momentan die Regel in der EDV darstellen, die Zerstörung recht unauffällig vorgenommen werden kann. So reicht es, daß ein Saboteur mit einem Magneten über diese Speichermedien streicht, um die gespeicherten Daten unberechenbar zu verändern oder zu löschen[44]. Da durch die Speicherung viele Daten auf kleinstem Raum untergebracht werden, kann eine solche Zerstörung schnell bedrohliche Folgen auslösen. Für einen Computerspion oder -saboteur dürfte allerdings eine andere Form des Zugriffs vorzugswürdiger sein, denn „der Computerstraftäter dringt nicht wie ein gewöhnlicher Einbrecher mit Taschenlampe und Brechwerkzeugen in eine DV-Anlage ein, sondern kann das, bestimmte Gegebenheiten vorausgesetzt, von seinem Personalcomputer (...) aus der Anonymität des eigenen Kämmerleins tun"[45].

41) Wulff, BB 1985, S. 427
42) Fallmaterial bei Liebl/Grosch, CuR 85, S. 162 ff.
43) Liebl/Grosch, CuR 85, S. 162 ff. (164)
44) Sieber, DSWR 74, S. 247
45) Kruse, CuR 87, 792