Computersabotage — Sabotageprogramme — Computerviren

Rechtliche Probleme von § 303b StGB

Karl-Heinz Volesky/Hansjörg Scholten

A. Überblick über die gesetzliche Regelung
I. Geschütztes Rechtsgut
II. Schutzgegenstand
III. Tathandlung
IV. Täter
V. Vorsatz
VI. Deliktscharakter
VII. Konkurrenzen
VIII. Strafantrag
B. Rechtliche Probleme des Tatbestands
I. Die wesentliche Bedeutung einer Datenverarbeitung
II. Die Störung der Datenverarbeitung
1. Aufhebung der Funktionsfähigkeit
2. Einschränkung der Funktionsfähigkeit
3. Einflußnahme auf das Ergebnis der Datenverarbeitung
4. Unbefugtes Erstellen oder Sichverschaffen einer Kopie
C. Computersabotage durch Sabotageprogramme
I. Sabotageprogramme
II. Computerviren
1. Begriff, Eigenschaften und Möglichkeiten
2. Arbeitsweise
3. Erstellung und Verbreitung
4. Die Reaktion auf Viren

A. Überblick über die gesetzliche Regelung

Mit zunehmendem Einsatz von Datenverarbeitungsanlagen in Wirtschaft und Verwaltung ist die Abhängigkeit vom störungsfreien Funktionieren derartiger Systeme gewachsen. Technische Innovation im Soft- und Hardwarebereich hat daneben auch die Mißbrauchsmöglichkeiten vervielfacht. Bedrohlich sind insbesondere für private Unternehmen die durch Manipulation hervorgerufenen potentiellen Schäden. Werden z. B. Buchführung und Lohnabrechnung in einem Rechenzentrum lahmgelegt, so kann das nicht nur für dessen Betreiber, sondern auch für die mit diesem zusammenarbeitenden Unternehmen zum wirtschaftlichen Ruin führen[1]. Da unbefugte Eingriffe Dritter trotz innerbetrieblicher Sicherungsmaßnahmen nicht ausgeschlossen werden können, ist nach verbreiteter Auffassung auch ein verstärkter Strafrechtsschutz erforderlich geworden[2]. Dies gilt umsomehr, als es zweifelhaft ist, ob Daten als Sachen im Sinne des § 303 StGB angesehen werden können. Selbst wenn diese Frage mit der h. M. bejaht wird[3], erscheint der Strafrahmen des § 303 StGB (Freiheitsstrafe bis zu 2 Jahren) angesichts der denkbaren Schäden als unzureichend. Daher ist der § 303 b StGB, der ebenso wie § 303 a StGB in den Entwürfen des 2. WiKG nicht enthalten war, in das Strafgesetzbuch aufgenommen worden. Ziel der Vorschrift ist es, Datenverarbeitungen, die in Wirtschaft und Verwaltung von wesentlicher Bedeutung sind, gegen bestimmte Sabotagehandlungen zu schützen[4].

I. Geschütztes Rechtsgut

1. § 303 b StGB schützt das Interesse von Wirtschaftsunternehmen und Behörden an einem störungsfreien Funktionieren ihrer Datenverarbeitung[5].

II. Schutzgegenstand

1. Schutzgegenstand ist „eine Datenverarbeitung". Der Begriff der Datenverarbeitung ist weit auszulegen. Er umfaßt nicht nur den einzelnen DV-Vorgang, sondern auch den weiteren Umgang mit Daten und deren Verwertung[6].

2. Die Datenverarbeitung muß für einen fremden Betrieb, ein fremdes Unternehmen oder für eine Behörde von wesentlicher Bedeutung sein.

a) Die in § 265 b Abs. 3 Nr. 1 StGB normierte Definition für „Betrieb" und „Unternehmen" ist im Hinblick auf den Schutzzweck des § 303 b StGB nicht übertragbar. § 265 b StGB schützt lediglich solche Gewerbebetriebe, die eine kaufmännische Einrichtung erfordern (§ 265 b Abs. 3 Nr. 1 StGB). Nach dem Willen des Gesetzgebers sollen aber auch kleine Handwerks-

[1] BT-Drucks. 10/5058/35
[2] Möhrenschlager, Manfred (Das neue Computerstrafrecht, wistra 86, 123 f.) S. 128
[3] vgl. SchSch-Stree (Schönke, Adolf; Schröder, Horst; Strafgesetzbuch-Kommentar 22. Auflage, München 1984) § 303 Rn 8 m. w. N
[4] BT-Drucks. 10/5058/35.
[5] Möhrenschlager, wistra 1986, 122, 141; Dreher in: (Dreher, Eduard; Tröndle, Adolf, Strafgesetzbuch mit Nebengesetzen 43. Auflage, München 1986) § 303 b Anm. 2
[6] BT-Drucks. 10/5058/35; Dreher § 303 b Rn 2

betriebe dem Schutzbereich der Norm unterfallen[7]. Um diesem Schutzzweck gerecht zu werden, erscheint die im Arbeitsrecht (insbesondere § 47 Abs. 1 BetrVerfG) verwandte Unterscheidung zwischen Betrieb und Unternehmen sachgerecht. Danach ist ein Betrieb als eine räumlich-technische Einheit aufzufassen, mit der ein bestimmter arbeitstechnischer Zweck verfolgt wird[8].

b) Ein Unternehmen ist demgegenüber eine organisatorische Einheit, die auf einer Verbindung personeller und sachlicher Mittel beruht[9]. Die Verfolgung eines wirtschaftlichen Zweckes muß nicht im Vordergrund stehen. Jeder erlaubte primäre Zweck reicht aus[10]. Es ist nicht einsehbar, warum z. B. karitative Organisationen, die gewöhnlich keine unmittelbar wirtschaftlichen Ziele verfolgen, keinen Strafrechtsschutz erhalten sollen.

c) Eine Behörde ist nach § 1 Abs. 4 VwVfG jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt. Unter den Begriff der Behörde fallen auch Verfassungsorgane (Bundespräsident, Bundestag, Bundesminister) sowie Gemeindeorgane oder auch Ausschüsse (z. B. Prüfungsausschuß, Untersuchungsausschuß etc.)[11]. Nach § 11 Abs. 1 Nr. 7 StGB ist im Strafrecht auch ein Gericht eine Behörde.

3. Einschränkend erfaßt § 303 b StGB nur eine Datenverarbeitung von wesentlicher Bedeutung[12]. Gemeint sind damit insbesondere solche Datenverarbeitungen in Großrechenanlagen bzw. Rechenzentren, die die für die Funktionsfähigkeit von Unternehmen wesentlichen Daten enthalten. Geschützt ist aber auch der einzige Personalcomputer eines Handwerksbetriebes[13]. Mit den Wesentlichkeitserfordernis scheidet die Norm von vornherein Fälle untergeordneter Bedeutung aus. Das sind beispielsweise Angriffe gegen einen Taschenrechner oder eine elektronische Büroschreibmaschine[14].

III. Tathandlung

§ 303 b StGB stellt das Stören einer Datenverarbeitung unter Strafe. Eine bloße Gefährdung ist für eine Strafbarkeit nach § 303 b StGB nicht ausreichend. Andererseits ist eine Störung des Betriebs, die z. B. § 316 b StGB verlangt, nicht erforderlich[15]. Eine Störung liegt vor, „wenn der reibungslose Ablauf der Datenverarbeitung nicht unerheblich beeinträchtigt ist"[16]. Die Störung kann zum einen durch eine Tat nach § 303 b Abs. 1 Nr. 1 StGB, zum anderen durch eine Tatmodalität nach § 303 b Abs. 1 Nr. 2 StGB geschehen.

1. Tatbestandsmerkmale des § 303 b Abs. 1 Nr. 1 StGB

Die Strafbarkeit gem. § 303 b Abs. 1 Nr. 1 StGB setzt eine Tat nach § 303 a StGB voraus.

a) Das geschützte Rechtsgut des § 303 a StGB ist das Interesse des Verwenders an der ungehinderten Nutzung der in den Daten enthaltenen Informationen[17].

b) Tatobjekt sind Daten im Sinne des § 202 a Abs. 2 StGB. Daten müssen demnach elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sein bzw. übermittelt werden. Untaugliche Tatobjekte sind allerdings Daten, an denen kein Verwendungsinteresse mehr besteht. Das von § 303 a StGB geschützte Rechtsgut kann in diesem Fall nicht veletzt werden.

c) Tathandlungen sind das Löschen, Unterdrücken, Unbrauchbarmachen und Verändern von Daten. Inhaltlich überschneiden sich diese Verhaltensweisen.

Auf diese Weise sollen alle nur erdenklichen Einwirkungen auf Daten erfaßt werden[18]. Daten sind gelöscht, wenn sie unwiederbringlich unkenntlich gemacht worden sind[19]. Das Unterdrücken von Daten ist deren Entziehung vor dem Zugriff des Berechtigten. Das Unbrauchbarmachen von Daten meint die Beeinträchtigung ihrer Funktionsfähigkeit mit der Konsequenz, daß sie nicht mehr ordnungsgemäß verwendet werden können. Daten sind verändert, wenn sie durch inhaltliche Umgestaltung einen neuen Informationsgehalt bzw. Aussagewert erhalten haben[20].

2. Tatbestandsmerkmale des § 303 b Abs. 1 Nr. 2 StGB

a) Der Begriff der Datenverarbeitungsanlage umfaßt alle zur maschinentechnischen Ausstattung gehörenden Komponenten (= Hardware). Hierzu gehören z. B. die Zentraleinheit, Ein- und Ausgabegeräte, sowie die Peripherie. Auch das Betriebssystem kann Bestandteil der Datenverarbeitungsanlage sein. Das trifft zu, wenn es sich im ROM (Read Only Memory) befindet. Muß es aber von Datenträgern in das RAM (Random Access Memory) eingeladen werden, so handelt es sich dabei um Software.

b) Datenträger sind alle Medien, die zur zumindest vorübergehenden Speicherung von Daten bestimmt

[7] Möhrenschlager, wistra 1986, 122, 141

[8] Brox, Hans (Handels- und Wertpapierrecht, 6. Auflage, München 1987) Rn. 154 a. E.

[9] Brox, Hans (Allgemeiner Teil des Bürgerlichen Gesetzbuches, 10. Auflage, Köln, Bonn, Berlin, München 1986) Rn 743

[10] Brox AT, Rn 743

[11] Maurer, Hartmut (Allgemeines Verwaltungsrecht, 3. Auflage, München 1983) S. 145

[12] BT-Drucks. 10/5058/35; Dreher § 303 b Rn 4; Schlüchter, Ellen (Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität, Heidelberg 1987) S. 76 f.

[13] Möhrenschlager, wistra 86, 122, 141; Dreher § 303 a Rn 4;

[14] BT-Drucks. 10/5058/35; Dreher § 303 b Rn 4; (vgl. dazu auch Teil B)

[15] BT-Drucks. 10/5058/35; Dreher § 303 b Rn 4

[16] BT-Drucks. 10/5058/35; Dreher § 303 b Rn 5; Achenbach, Hans (Das zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, NJW 86, S. 1835 ff.) S. 1838; vgl. dazu auch Teil B

[17] BT-Drucks. 10/5058/34; Dreher § 303 a Rn 2

[18] Dreher § 303 a Rn 2

[19] Dreher § 303 a Rn 5

[20] BT-Drucks. 10/5058/35; Dreher § 303 a Rn 6 f.

sind (z.B. Magnetplatten, Disketten und Magnetbänder)[21].

c) Die in § 303 b Abs. 1 Nr. 2 StGB aufgeführten Tatmodalitäten „zerstören", bzw. „beschädigen" sind wie in § 303 StGB aufzufassen[22]. Eine Datenverarbeitungsanlage oder ein Datenträger ist zerstört, wenn er in seiner Existenz vernichtet oder so wesentlich beschädigt ist, daß die bestimmungsgemäße Brauchbarkeit verlorengeht[23]. Eine Beschädigung liegt vor bei einer erheblichen Beeinträchtigung der Unversehrtheit oder der bestimmungsgemäßen Brauchbarkeit[24]. Dieses Merkmal ist zwar im Rahmen des § 303 StGB heftig umstritten. Der Meinungsstreit wird jedoch bei § 303 b Abs. 1 Nr. 2 StGB dadurch entschärft, daß zusätzliche Tathandlungen in Betracht kommen (Unbrauchbarmachen, Verändern, Beseitigen), die sich gegenseitig überschneiden.

d) Das Merkmal „Unbrauchbarmachen" ist einschlägig, wenn die Gebrauchsfähigkeit des Tatobjekts so stark eingeschränkt ist, daß es nicht mehr ordnungsgemäß verwendet werden kann[25].

e) Ein Beseitigen ist gegeben, wenn das Tatobjekt aus dem Verfügungsbereich des Berechtigten entfernt worden ist[26].

f) Ein Datenträger oder eine Datenverarbeitungsanlage ist verändert, wenn der Täter einen Zustand herbeiführt, der vom bisherigen Zustand abweicht[27].

3. Das Vorliegen einer Tathandlung nach § 303 b Abs. 1 Nr. 1 StGB bzw. § 303 b Abs. 1 Nr. 2 StGB ist nicht zwangsläufig gleichbedeutend mit der Störung einer Datenverarbeitung. Die Störung ist als Handlungserfolg vielmehr gesondert festzustellen. Dabei hat das nach § 303 b Abs. 1 StGB relevante Verhalten für die Störung ursächlich zu sein[28].

IV. Täter

Täter des § 303 b StGB kann zunächst jeder sein, dessen Tat sich nicht gegen die eigene Datenverarbeitung richtet[29]. Beschädigt jemand seine eigene Datenverarbeitungsanlage und wird dadurch gleichzeitig eine fremde Datenverarbeitung gestört, so kommt eine Strafbarkeit nach § 303 b Abs. 1 Nr. 2 StGB in Betracht[30]. Es ist daher für die Täterschaft zunächst zu prüfen, wem Eigentums-, Gebrauchs-, oder Verfügungsrechte an Hard- oder Software zustehen[31].

V. Vorsatz

Für eine Strafbarkeit nach § 303 b StGB reicht bedingter Vorsatz aus. Hinsichtlich der wesentlichen Bedeutung der Datenverarbeitung genügt die Kenntnis des Täters von den tatsächlichen Gegebenheiten, aus denen sich dies ergibt (sog. Parallelwertung in der Laiensphäre)[32].

VI. Deliktscharakter

Der Deliktscharakter des § 303 b StGB richtet sich nach der jeweiligen Tathandlung. § 303 b StGB beinhaltet drei verschiedene Möglichkeiten.

1. § 303 b Abs. 1 Nr. 1 StGB enthält eine Qualifikation zu § 303 a StGB[33].

2. Bei § 303 b Abs. 1 Nr. 2 StGB hat der Gesetzgeber auf das Merkmal „fremd" verzichtet. In bezug auf den Deliktscharakter besteht folgende Alternative.

a) § 303 b Abs. 1 Nr. 2 StGB ist zunächst eine qualifizierte Sachbeschädigung, wenn sich die Tathandlnng gegen eine fremde Datenverarbeitungsanlage oder einen fremden Datenträger richtet[34].

b) Bezieht sich die Tathandlung nach § 303 b Abs. 1 Nr. 2 StGB auf eine tätereigene Datenverarbeitungsanlage oder Datenträger, und wird dadurch die wesentliche Datenverarbeitung eines für den Täter fremden Unternehmens oder einer Behörde gestört, dann stellt § 303 b Abs. 1 Nr. 2 StGB ein selbständiges Verletzungsdelikt dar[35].

VII. Konkurrenzen

Neben den typischen Konkurrenzen mit §§ 303a und 303 StGB ist darüber hinaus u.a. auch Idealkonkurrenz mit §§ 87, 88, 109e, 242, 263a, 269, 304, 311, 316 b, 316 c I Nr. 2, 317 StGB möglich.

VIII. Strafantrag

§ 303 b ist gem. § 303 c StGB ein Antragsdelikt. Ausnahmsweise kann die Strafverfolgungsbehörde bei besonderem öffentlichen Interesse an der Strafverfolgung einschreiten.

Strafantragsberechtigt ist, wer durch die Tat unmittelbar verletzt ist. Gleichgültig ist, ob er Eigentümer, dinglich oder persönlich Berechtigter ist[37].

[21] Dreher § 303 b Rn 7
[22] BT-Drucks. 10/5058/35; Dreher § 303 b Rn 7
[23] Wessels, Johannes (Strafrecht, Besonderer Teil 2 Heidelberg 1986) § 1 I 3b; SchSch-Stree § 303 Rn 7
[24] BGHSt 13, 208; SchSch-Stree § 303 Rn 8 m.w.N.; Wessels BT 2 § 1 I 3b
[25] BT-Drucks. 10/5058/35; Dreher § 303 b Rn 7
[26] BT-Drucks. 10/5058/36; Dreher § 303 b Rn 7
[27] BT-Drucks. 10/5058/36; Dreher § 303 b Rn 7
[28] Schlüchter, S. 79 u. 80
[29] BT-Drucks. 10/5058/35; Dreher § 303 b Rn 8
[30] Die Bundesregierung war in diesem Punkt offen. Die Entscheidung über eine Strafbarkeit ist rechtspolitischer Art (vgl. Protokolle 71/42). In den Ausschußberatungen wurde eine Strafwürdigkeit dieses Falles schließlich bejaht (vgl. Protokolle 71/42 ff.)
[31] Dreher § 303 b Rn 8
[32] Dreher § 303 b Rn 9
[33] BT-Drucks. 10/5058/36; Dreher § 303 b Rn 11; Möhrenschlager, wistra 86, 122, 141
[34] BT-Drucks. 10/5058/36
[35] BT-Drucks. 10/5058/36; vgl. Prot. 71/ 43 u. 62
[36] Vgl. dazu auch Dreher § 303 b Rn 11
[37] Dreher § 303 c Rn 2

B. Rechtliche Probleme der Computersabotage gem. § 303 b StGB

I. Die wesentliche Bedeutung der Datenverarbeitung

Die Datenverarbeitung muß für das betroffene Unternehmen von wesentlicher Bedeutung sein. Der Rechtsausschuß hat diesen unbestimmten Rechtsbegriff in zweifacher Hinsicht präzisiert. Erstens zieht er die Grenzlinie zum strafrechtlichen Vorfeld des § 303 b StGB. Von einer wesentlichen Bedeutung der Datenverarbeitung könne dann keine Rede sein, wenn sich mit Hilfe von bloßen innerbetrieblichen Umstellungen die Funktion der Datenverarbeitung noch befriedigend ausüben lasse[38]. Deshalb fallen z.B. die mittels elektronischer Schreibmaschinen und Taschenrechner vorgenommenen Datenverarbeitungen nicht in den Schutzbereich der Norm. Im Umkehrschluß ergibt sich: Ist das Unternehmen ohne die Datenverarbeitung nicht mehr in der Lage, seine Aufgaben zufriedenstellend wahrzunehmen, dann hat die Datenverarbeitung eine wesentliche Bedeutung[39].

Zweitens sollen durch § 303 b StGB diejenigen Daten geschützt werden, „welche die für die Funktionsfähigkeit von Unternehmen bzw. Behörden zentralen Informationen enthalten"[40].

Abgestellt werden soll also auf den Informationsgehalt der Daten. Demgegenüber spricht das Gesetz von der Wesentlichkeit der Datenverarbeitung. Dieser scheinbare Widerspruch löst sich jedoch durch teleologische Reduktion auf. Die Datenverarbeitung kann dann nicht wesentlich sein, wenn die bearbeiteten Daten für das Unternehmen wertlos sind. Kommt umgekehrt den Daten eine erhebliche Bedeutung zu, so gilt dies auch für die Verarbeitung dieser Daten. Die wesentliche Bedeutung der Datenverarbeitung kann also nicht isoliert von den zu verarbeitenden Daten beurteilt werden. Das Gewicht der Daten ist dabei im Verhältnis zu den Aufgaben des Unternehmens zu bestimmen. Zu den in der Regel elementaren Aufgaben eines Unternehmens zählen jedenfalls Produktion, Absatz, Personalwesen, Beschaffungswesen, Finanzierung u. Forschung. Bei Behörden gelten die gesetzlich zugewiesenen Aufgaben. Diesbezügliche Daten(verarbeitungen) indizieren die wesentliche Bedeutung.

Als Synthese ergibt sich für die „wesentliche Bedeutung" der Datenverarbeitung folgende Prüfungsreihenfolge:

(1) Wird mit der Datenverarbeitung eine Aufgabe des Unternehmens erledigt?

(2) Kann das Unternehmen ohne nennenswerten Schaden auf diese Aufgabenerledigung verzichten?

(3) Wenn nicht: läßt sich die Aufgabe auch ohne eine Datenverarbeitung (z.B. durch bloßes Umdisponieren) noch effektiv bewältigen?

II. Die Störung einer Datenverarbeitung

Der objektive Tatbestand des § 303 b StGB ist erst dann erfüllt, wenn durch eine Handlung nach § 303 b Abs. 1 Nr. 1 oder § 303 b Abs. 1 Nr. 2 StGB eine Datenverarbeitung von wesentlicher Bedeutung gestört wird. Nach der Auffassung des Rechtsausschusses bedarf es für eine Störung einer „nicht unerheblichen Beeinträchtigung des reibungslosen Ablaufs der Datenverarbeitung"[41]. Zutreffend folgert der Ausschuß daraus, daß einerseits eine Störung des Betriebes insgesamt nicht erforderlich ist, daß aber andererseits eine bloße Gefährdung der Datenverarbeitung noch nicht ausreicht. Dieses „Grobraster" bietet indes nur eine Orientierungshilfe, was folgende Beispielsfälle verdeutlichen.

Fall 1: Kindergeldmanipulationen

Eine bestehende Datei von Kindergeldbezugsberechtigten wird von einem Programmierer mit Daten von nicht bezugsberechtigten Personen erweitert. Daraufhin erhalten diese Nichtberechtigten monatliche Kindergeldüberweisungen[42].

Fall 2: Rundungstrick

Ein Programmierer erstellte für den Computer eines Geldinstituts das Zinsberechnungsprogramm. Er hat es so gestaltet, daß die Zinsbeträge zwar genau auf 1/10-Pfennig-Beträge berechnet, anschließend aber immer auf ganze Pfennig-Beträge abgerundet werden. Die überschüssigen 1/10-Pfennig-Beträge läßt er automatisch auf sein eigenes Konto überweisen[43].

Fall 3: Kopierfall

In der Forschungsabteilung eines Elektronikkonzerns fertigt ein Mitarbeiter unberechtigt Kopien von gespeicherten Forschungsergebnissen an. Diese Kopien veräußert er an ein Konkurrenzunternehmen. Gleichzeitig verfälscht er einige auf Datenträgern erfaßte Testergebnisse, um das Forschungsprojekt zu verzögern[44].

Es fragt sich, ob bei diesen in der Praxis vorgekommenen Fallgestaltungen eine „nicht unerhebliche Beeinträchtigung des reibungslosen Ablaufs der Datenverarbeitung" bejaht werden muß.

1. Aufhebung der Funktionsfähigkeit

Tatbestandsmäßig sind jedenfalls diejenigen Handlungen nach § 303 b Abs. 1 Nr. 1 u. Nr. 2 StGB, die die Funktionsfähigkeit der Datenverarbeitungsanlage völlig aufheben. Dabei ist es gleichgültig, ob die Datenver-

[38] BT-Drucksachen 10/5058,35
[39] Schlüchter S. 79; aber auch § 316 b
[40] BT-Drucksachen 10/5058,35
[41] BT-Drucks. 10/5058/35
[42] Sieg, Rainer (Strafrechtlicher Schutz gegen Computerkriminalität, Jura 1986, 352f.) S. 354
[43] Fall nach Sieg, Jura 86, 352, 356
[44] Liebl, Karlhans; Grosch, Olaf (Datendiebstahl als Form der Computerkriminalität, CuR 3/85, 162f.) S. 163

arbeitungsanlage in ihrer Substanz verletzt wird oder ob die Funktionsfähigkeit auf andere Weise aufgehoben wird. Die Datenverarbeitung ist dann nicht nur in ihrem Ablauf beeinträchtigt, sondern ausgeschlossen. Bei der rechtlichen Beurteilung hat außer Betracht zu bleiben, daß eventuell eine weitere Anlage vorhanden ist, auf die im Störungsfall ausgewichen werden kann. Grund: Eine Betriebsstörung ist nicht erforderlich (s.o.). Damit sind folgende Fälle aus der Praxis problemlos unter den Tatbestand der Computersabotage zu subsumieren:

— Terroristen zünden im einbruchsicheren Rechenzentrum von MAN eine Bombe und verursachen Schäden in Millionenhöhe[45].
— ein Programmierer „erschießt" einen Computer[46].
— ein Datenfachmann schmettert Bierflaschen in den Computer seines Arbeitgebers[47].
— ein Programmierer gießt Brennspiritus in seinen Computer und zündet ihn an[48].
— Jemand zerstört Daten und Programme durch einen Magneten[49].
— ein Operator eines Rechenzentrums vertauscht Ein- und Ausgangsstecker am Zentralrechner, wodurch das gesamte System zusammenbricht[50].

In den ersten drei Beispielen ist die Datenverarbeitung durch Zerstörung bzw. Beschädigung der Datenverarbeitungsanlage gestört. Im vierten liegt ein Unbrauchbarmachen eines Datenträgers, im letzten Fall sowohl ein Unbrauchbarmachen als auch ein Verändern der Datenverarbeitungsanlage vor.

2. *Einschränkung der Funktionsfähigkeit*

Nicht so eindeutig zu bewerten sind Manipulationen, die nur den Ausfall einzelner Funktionen der Datenverarbeitungsanlage zur Folge haben.
Beispiele:
— Unterbrechung der Verbindung zum Drucker
— Zerstörung bzw. Beschädigung des Monitors

Hier ist zu berücksichtigen, daß sich die Datenverarbeitung dem Arbeitsablauf entsprechend auf die Eingabe-, Verarbeitungs- und Ausgabephase erstreckt[51]. Ist die Datenleitung zum Drucker unterbrochen, dann ist die Datenausgabe unmöglich. Folglich ist die Datenverarbeitung gestört. Erfordert die Datenverarbeitung einen Dialog mit dem Rechner, wie z.B. bei den sog. Expertensystemen[52], dann bedeutet der Ausfall des Monitors eine erhebliche Ablaufbeeinträchtigung. Da § 303 b StGB die Störung einer Datenverarbeitung von wesentlicher Bedeutung verlangt, ist der Blick auf alle von der manipulierten Datenverarbeitungsanlage ausgeführten Datenverarbeitungen zu richten. Wirkt sich die Funktionsbeeinträchtigung auf mindestens eine wesentliche Datenverarbeitung aus[53], liegt immer eine Störung vor. Bei Tathandlungen, die sich gegen die Hardware richten und deren Funktionsfähigkeit einschränken, ist davon regelmäßig auszugehen. Bei Funktionsbeeinträchtigungen durch Software, die ebenfalls denkbar sind, ist darüber hinaus zu prüfen, ob sie die gleiche Intensität erreichen wie Hardwarebeeinträchtigungen. So ist eine Störung der Datenverarbeitung z.B. dann zu verneinen, wenn durch Betätigen einer „Resetfunktion"[54] die volle Funktionsfähigkeit auf Dauer wiederhergestellt werden kann.

3. *Einflußnahme auf das Ergebnis der Datenverarbeitung*

Der eigentliche Schwerpunkt der Computermanipulationen besteht jedoch in der unberechtigten Beeinflussung des Ergebnisses eines Datenverarbeitungsvorganges[55]. In diesem Bereich sind die oben (vgl. B II) dargestellten Fälle 1 bis 3 anzusiedeln. Im Gegensatz zu den Funktionsbeeinträchtigungen ist die Besonderheit dieser Fallkonstellationen darin zu sehen, daß der reibungslose Ablauf des Datenverarbeitungsvorgangs nicht behindert wird. Diese Problematik hat auch der Rechtsausschuß gesehen und deshalb den Begriff der Datenverarbeitung nicht nur auf den einzelnen Datenverarbeitungsvorgang, sondern auch auf den weiteren Umgang mit den Daten, sowie deren Verwertung erstreckt[56]. Für diese weite Auslegung des Begriffs der Datenverarbeitung spricht, daß eine Datenverarbeitungsanlage, die „falsche" Resultate errechnet, weitaus größere Schäden verursachen kann als eine Anlage, die gar nicht oder nur teilweise funktioniert. Zudem wird eine Manipulation, die sich in „falschen" Ergebnissen niederschlägt, zumeist später entdeckt werden als der völlige Ausfall der Anlage. Für diese Wertung spricht auch die gesetzessystematische Stellung des § 303 b StGB bei den Sachbeschädigungsdelikten. Nach heute überwiegender Auffassung liegt der Tatbestand der Sachbeschädigung gem. § 303 StGB vor, wenn die Tathandlung zu einer erheblichen Beeinträchtigung der bestimmungsgemäßen Brauchbarkeit führt[57]. Sind die Resultate der Datenverarbeitung aus der Sicht des Betreibers infolge der Manipulation „falsch", so kann sie ihren Verwendungszweck nicht mehr erfüllen. Die Datenverarbeitung hat für ihren Betreiber u.U. keinen Gebrauchswert mehr.

Um dem Schutzzweck des § 303 b StGB gerecht zu werden und ein Leerlaufen der Norm gerade bei den

[45] Soyka, Joachim (Computer-Kriminalität München 1986) S. 88; ein ähnlicher Fall auch bei Sieg Jura 86, 352, 354
[46] Sieg Jura 86, 352, 354
[47] Sieg Jura 86, 352, 354
[48] Soyka, S. 83
[49] Beispiele bei: von zur Mühlen, Rainer (Computer-Kriminalität, Gefahren und Abwehrmaßnahmen, 1973) s. 97 u. 99
[50] Soyka, S. 86
[51] Vgl. Sieg Jura 86, 352, 354
[52] Computersysteme, die Laien im selbständigen „Ja/Nein - Dialog" das gespeicherte Fachwissen von Experten zur Lösung vielfältiger Probleme zur Verfügung stellen; zu jur. Expertensystemen vgl Lusti, Expertensysteme im Recht, IuR 2/86, 77 f.
[53] zum Begriff s.o. II. 1
[54] Systembefehl, der alle flüchtigen Speicher löscht und die Anlage in einen betriebsbereiten Zustand zurückversetzt
[55] Sieg Jura 86, 352, 354
[56] BT-Drucks. 10/5058/35
[57] BGHSt 13, 107; BGH NJW 1980, 601; Wessels BT 2 § 1 I 3 b

gefährlichsten Sabotagefällen zu verhindern, ist die weite Begriffsbestimmung des Rechtsausschusses angemessen.

Trotz dieser weiten Auslegung sind allerdings längst nicht alle Unklarheiten des Tatbestandes beseitigt.

a) Einflußnahme durch Erstellung eines neuen Programms

In dem oben geschilderten Fall 2 (Rundungstrick) wird zwar das Ergebnis der Datenverarbeitung unberechtigt beeinflußt, es fragt sich aber, ob überhaupt eine tatbestandsmäßige Handlung gegeben ist. Es müßten dazu gem. § 303 b Abs. 1 Nr. 1 StGB Daten verändert worden sein.

Das in Rede stehende Programm ist vom Täter komplett neu erstellt worden. Er hat damit keinen Einfluß auf vorhandene Daten genommen. Ebenso, wie die Herstellung einer fehlerhaften Sache keine Sachbeschädigung ist, ist die Erstellung eines Programmes, das lediglich falsche Rechenergebnisse erzeugt, nicht tatbestandsmäßig im Sinne des § 303 a StGB[58].

Allerdings könnte man stattdessen bei der Subsumtion unter das Merkmal „Daten verändern" auf den Zeitpunkt der Nutzung des Programms abstellen, genauer: auf den Zeitpunkt, zu dem die Bruchteilspfennigbeträge von den berechneten Zinsen abgezogen werden. Dieser Ansatz läßt sich jedenfalls nicht mit dem Argument verwerfen, es habe nicht der Täter selbst, sondern das von ihm erstellte Programm die Daten manipuliert. Dies ist allein eine Frage der Kausalität: Hätte der Täter nicht das Programm erstellt, so hätte dies auch keine Daten verändern können.

Fraglich ist aber, ob Daten im Sinne des § 202 a Abs. 2 verändert worden sind. Danach sind Daten nur solche, die (nicht unmittelbar wahrnehmbar) gespeichert sind oder übermittelt werden. Speichern im Sinne des § 202 a StGB heißt, Daten zum Zwecke ihrer Weiterverwendung zu erfassen, aufzunehmen oder aufzubewahren (vgl. § 2 Abs. 2 Nr. 1 BDSG)[59]. Daraus folgt, daß die Daten zumindest kurzfristig fixiert sein müssen. Es ist also eine gewisse Bestandsdauer der Daten erforderlich.

Im Fall 2 (Rundungstrick) existieren die beeinflußten Daten nur als Zwischenergebnisse eines Berechnungsvorgangs und dies auch nur für einen nicht mehr nachvollziehbaren, extrem kurzen Augenhlick. Das notwendige zeitliche Moment fehlt hier. Aus diesem Grund liegt keine Handlung nach § 303 a und damit auch keine Tathandlung nach § 303 b Abs. 1 Nr. 1 StGB vor.

Anders verhält es sich aber dann, wenn das Programm mittels einer Sabotagefunktion (vgl. dazu Teil C) auf schon existierende Daten zurückgreift, indem es diese löscht oder verändert[60]. Darüber hinaus kommt auch eine Strafbarkeit nach § 303 b Abs. 1 Nr. 2 StGB in Betracht, wenn sich die Manipulation in Form mechanischer Zerstörung oder Beschädigung auf die DV-Anlage oder einen Datenträger auswirkt[61].

b) Einflußnahme auf bestehende Programme oder Dateien

Die Erheblichkeit der Ablaufbeeinträchtigung kann unterschiedlich zu beurteilen sein, je nachdem ob Programme oder Dateien (wie in Fall 1 und 3) manipuliert werden.

aa) Wird ein Programmalgorithmus verändert, wirkt sich die Manipulation auf alle von diesem Programm zu verarbeitenden Daten aus. Eine erhebliche Ablaufbeeinträchtigung ist damit in der Regel gegeben.

bb) Richtet sich die Tathandlung gegen Dateidaten, so ist zu unterscheiden.

Wird eine gesamte Datei (z. B. durch Löschung oder Diebstahl) dem Zugriff des Berechtigten entzogen, können diese Daten nicht mehr verarbeitet werden. Die Datenverarbeitung ist also gestört. Danach sind folgende Fälle tatbestandsmäßig im Sinne des § 303 b Abs. 1 Nr. 1 bzw. Nr. 2 StGB:

— Löschen des Strafregisters durch Angestellte des kalifornischen Justizministeriums[62];
— Diebstahl von Datenträgern eines Wirtschaftsunternehmens, auf denen die Daten für ein Großprojekt im Ausland gespeichert waren[63].

Erhalten alle Dateidaten (z. B. durch Vorzeichenumkehr) einen anderen Aussagewert, wird diese Datei für den „Herrn der Daten" im Hinblick auf die weitere Verwertung unbrauchbar. Auch dann ist eine Störung zu bejahen.

Schwierig gestaltet sich die Beurteilung, wenn Daten hinzugefügt (Kindergeldfall), einzelne Daten verändert (Kopierfall) oder gelöscht werden. Diese Tathandlungen — auch das Hinzufügen neuer Daten[64] — werden von § 303 b Abs. 1 Nr. 1 StGB erfaßt. Ob dadurch aber die Datenverarbeitung gestört wird, läßt sich nicht einheitlich beantworten. Dies ist zum einen abhängig von Anzahl und Bedeutung der manipulierten Daten. Zum anderen ist auf den Zweck der Datei abzustellen. Die Zweckbestimmung ist dabei objektiv und nicht nach den subjektiven Vorstellungen des Betreibers vorzunehmen. Bewirkt die Datenveränderung gem. § 303 b Abs. 1 Nr. 1 StGB, daß dieser Zweck nicht mehr oder nur noch eingeschränkt erreicht werden kann, dann ist die weitere Verwertung der Daten erheblich beeinträchtigt. Im Fall 3 (Kopierfall) wurden einzelne Daten der Testergebnisse eines Forschungsprojekts verfälscht, um dessen Fortgang zu verzögern. Die Forschungsergebnisse können nunmehr, wenn überhaupt, nur noch eingeschränkt verwertet werden. Mithin ist die Datenverarbeitung gestört.

Wird demgegenüber (wie in Fall 1) eine Datei, deren Zweck die Erfassung aller Kindergeldbezugsberechtigten ist, um die Daten eines Nichtberechtigten erweitert, ist keine nachteilige Auswirkung auf die Zweckbestimmung der Datei zu konstatieren. Die Beeinträchti-

[58] Möhrenschlager, wistra, 86, 122, 142; Schlüchter, S. 77
[59] Dreher, § 202 a Rn 4
[60] Diesen Fall scheint Möhrenschlager in wistra 86, 122, 142 übersehen zu haben
[61] Möhrenschlager, wistra 86, 122, 142
[62] Soyka S. 85
[63] Steinke, Wolfgang (Kriminalität durch Beeinflußung von Rechnerabläufen, NStZ 1984, S. 295 f.) S. 296
[64] Möhrenschlager, wistra 86, 122, 141

gung der Datenverarbeitung ist unerheblich. Zu einer anderen Bewertung gelangt man nur dann, wenn man den eintretenden Vermögensnachteil für den Betreiber als taugliches Kriterium für eine Störung anerkennt. So wurde vor der Einführung des 2. WiKG die Computersabotage als Beeinträchtigung eines Datenverarbeitungssystems mit der Folge eines Vermögensnachteils definiert[65]. Tatbestandsmäßig wäre danach z.B. anch die Buchung von tatsächlich nicht erfolgten Zahlungen oder Warenlieferungen[66]. Die Praxis zeigt jedoch, daß nahezu jede Einflußnahme auf eine Datenverarbeitung einen Vermögensnaehteil für den Betreiber hervorruft[67]. Hinzu kommt, daß zum Schutz des Vermögens des Betreibers einer Datenverarbeitung der § 263 a StGB eingeführt worden ist. § 303 b StGB soll lediglich die Funktionsfähigkeit von Datenverarbeitungen schützen[68]. Mit der Einbeziehung des Gesichtspunktes „Vermögensschaden" käme dem § 303 b StGB im Bereich des Computerstrafrechts der Charakter eines Auffangtatbestandes zu. Folgerichtig hat daher der Rechtsausschuß den Aspekt des Vermögensnachteils nicht übernommen.

cc) Festzuhalten ist, daß die Einflußnahme auf einen Programmalgorithmus die Störung indiziert, während bei Dateibeeinträchtigungen jeder Einzelfall anhand der aufgeführten Kriterien gesondert zu nntersuchen ist.

4. Unbefugtes Anfertigen oder Sichverschaffen von Kopien

Anders gelagert ist die in Fall 3 (Kopierfall) ebenfalls dargestellte Problematik des unbefugten Anfertigens und Sichverschaffens von (Sicherungs-)Kopien, die anschließend vom Täter selbst oder von Dritten verwertet werden. Benützt der Täter einen eigenen Datenträger, dann ist allein eine Tathandlung nach § 303 b Abs. 1 Nr. 1 StGB — Daten unterdrücken — denkbar. Unterdrücken bedeutet, Daten dem Zugriff des Berechtigten zu entziehen, so daß dieser sie nicht mehr verwenden kann[69]. Fraglich ist, ob Daten unterdrückt sind, wenn nur ein Duplikat dem Zugriff des Berechtigten entzogen wird. Dieses thematisch zu § 303 a StGB gehörende Problem soll hier nicht vertieft werden.

Unterstellt, es sind Daten unterdrückt worden, ist zweifelhaft, ob dadurch eine Datenverarbeitung gestört ist. Sicherlich wird der Ablauf des Datenverarbeitungsvorgangs nicht angetastet. Folglich kann allenfalls die weitere Verwertung der Daten beeinträchtigt sein, obwohl die Originalversion noch vorhanden ist und diese planmäßig verwendet werden kann.

Stellt man darauf ab, daß ausschließlich der Berechtigte die Verwertungsbefugnis hat, ist bei der Datenverwertung durch Dritte die Datenverarbeitung gestört. Dennoch scheitert die Tatbestandsmäßigkeit dieses Verhaltens an dem Erfordernis der kausalen Verknüpfung von Handlung und Erfolg. Nicht die Anfertigung oder die Verschaffung der Kopie bewirkt die Störung der Datenverarbeitung, sondern erst die sich anschließende Verwertung der Kopie. Die Verwertung ist eine selbständige Ursacire, und wird von keiner Tatmodalität des § 303 b StGB erfaßt.

Allgemein erscheint zweifelhaft, inwiefern vorhandene Sicherungskopien, die für wichtige Daten üblicherweise angelegt werden, bei der Subsumtion unter das Merkmal „stören" zu berücksichtigen sind. Wird beispielsweise die Originalversion gelöscht, so könnte die Sicherungskopie anstelle des Originals genutzt werden. Es träte keine Störung der Datenverarbeitung ein, so daß allenfalls eine Strafbarkeit wegen Versuchs (§ 303 b Abs. 2 StGB) angenommen werden könnte. Hier darf aber nichts anderes gelten, als bei einer doppelt vorhandenen Datenverarbeitungsanlage (s.o). Da § 303 b StGB im Gegensatz zu § 315 b StGB keine Betriebsstörung verlangt, haben Sicherungskopien bei der rechtlichen Einordnung außer Betracht zu bleiben.

C. Computersabotage durch Sabotageprogramme

Der Tatbestand der Computersabotage kann durch verschiedene Tathandlungen verwirklicht werden. Häufig richtet sich ein Sabotageangriff unmittelbar gegen die Hardware. Wird dadurch das Rechnersystem in seiner Sachsubstanz beschädigt oder zerstört, so ist eine Sabotagehandlung offensichtlich[70]. Anders verhält es sich aber, wenn ein eigens zu Sabotagezwecken präpariertes Programm eingesetzt wird. Aufgrund moderner und intelligenter Programmiertechniken ist in einem solchen Fall das Erkennen einer strafbaren Handlung nahezu unmöglich geworden. Der folgende Teil versucht daher, die Möglichkeiten und Auswirkungen der Programmsabotage darzustellen.

Eine Sonderstellung innerhalb der Sabotageprogramme nehmen die sogenannten Computerviren ein; sie gehören, wie noch gezeigt wird, nur unter bestimmten Voraussetzungen zu den Sabotageprogrammen.

I. Sabotageprogramme

1. Begriff und Arten

Allen Sabotageprogrammen ist gemeinsam, daß sie einen Auslöser für einen Zerstörungserfolg enthalten. Dieser Auslöser wird durch den Eintritt einer bestimmten Bedingung, wie z.B. ein Datum oder die Eingabe eines Kennwortes, aktiviert. Ob die Bedingung eingetreten ist, wird durch das Programm in einer entsprechenden Routine ständig überprüft. Je nach dem, ob dieser Indikator innerhalb des EDV-Systems verfügbar ist, oder ob er noch gesondert von außeh eingebracht werden muß, ist zwischen aktiven und passiven Auslösern zu unterscheiden[71].

[65] vgl. Steinke NStZ 84, 295; Sieg Jura 86, 359

[66] vgl. die Fälle bei Steinke NStZ 84, 295, 296

[67] Möhrenschlager, wistra 86, 122, 140; Steinke NStZ 84, 295; Sieber, Ulrich (Computerkriminalität u. Strafrecht, 2. Auflage, Köln, Bonn, München 1980) S. 87

[68] Dreher § 303 b Rn 1

[69] BT-Drucks. 10/5058/35; Dreher § 303 a Rn 6

[70] vgl. die obigen Beispielsfälle unter B II 1

[71] Schmidt, Egon (Computerviren — was sie schaden was sie nutzen — Computerwoche (cw) v. 27. 3. 87, S. 32 ff. u. v. 3. 4. 87 S. 42 ff) cw v. 3. 4. 87, 42, dessen Beispiel sich auf Auslöser in einem Virusprogramm bezieht

a) Passive Auslöser sind solche, bei denen kein weiterer Eingriff des Täters mehr erforderlich ist, um den Zerstörungserfolg herbeizuführen. Sabotageprogramme, die solche Auslöser verwenden, sind in ihrer Wirkungsweise mit „Zeitbomben" vergleichbar[72]. Die folgenden Fälle zeigen die Verwendungsmöglichkeiten von Programmen mit „logischen Zeitbomben".

— Ein Computer-Experte drohte damit, daß sich das von ihm erstellte Computerprogramm „GURUGS 2001" in der Silvesternacht des Jahres 1984 selbständig zerstören werde, wenn man seinen Gehaltsforderungen nicht nachkomme. Da sein Arbeitgeber, die Bundeswehr, auf diese Forderungen nicht einging, wurde das Programm zum vorhergesagten Zeitpunkt gelöscht[73].

— In einem anderen, 1968 in Frankreich einschlägigen Fall, wurde zwei Jahre nach der Entlassung eines Programmierers bei dessen früherem Arbeitgeber die Löschung eines wichtigen Programms ausgelöst. Dreihundert Rechner-Terminals, die an den mit dem Programm arbeitenden Großrechner angeschlossen waren, fielen für mehrere Tage aus[74].

b) Im Gegensatz zu den passiven Auslösern bedürfen aktive Auslöser zur Entfaltung ihrer Wirkung noch einer besonderen Aktivierung von außen. Dies geschieht zumeist durch ein spezielles Codewort, dessen Eingabe auch ohne besondere Zugriffsberechtigung möglich ist.

— So kann ein in das Rechnersystem einer Reisegesellschaft eingebrachter Auslöser angesprochen werden, indem der ahnungslose Sachbearbeiter der Gesellschaft auf Veranlassung des Täters einen fiktiven Hotelnamen im Rechner abfragt[75].

Denkbar sind aber auch andere Beispiele für eine aktive Auslösung:

— In das Programm der Personalabteilung eines deutschen Unternehmens fügte ein Programmierer die Anweisung ein, den gesamten Personaldatenbestand zu löschen, sobald sein Name von der Personalliste gelöscht würde. Nach seiner Entlassung wurde die Löschung bestimmungsgemäß ausgelöst. Die Firma mußte das gesamte Datenbanksystem neu erstellen lassen[76].

2. Auswirkungen von Sabotageprogrammen

Die möglichen Auswirkungen eines Sabotageprogrammes auf das betroffene System sind mannigfaltig. Das Spektrum reicht von der Zerstörung der Hardware[77] bis zur Ausgabe optischer oder akustischer Signale. In den meisten Fällen wird die Sabotagehandlung aber in der Löschung oder Unkenntlichmachung der in Form von Programmen oder Daten gespeicherten Informationen bestehen. Während bei den häufig im Dauerbetrieb arbeitenden Großrechnern genügend Zeit zur Verfügung steht, zu der Dateien oder Programme unbeobachtet gelöscht werden können, ist ein PC in der Regel nur dann eingeschaltet, wenn er auch von einem Anwender genutzt wird. Wird in dessen Beisein eine Löschfunktion ausgelöst, so könnte er durch Unterbrechen der Stromzufuhr oder Entnahme der Diskette noch größere Schäden verhindern. Dies umgehen Sabotageprogramme für PCs aber dadurch, daß sie einfach diejenigen Bereiche auf dem Datenträger (Diskette oder Festplatte) überschreiben, die dessen Inhaltsverzeichnis (Directory) enthalten[78]. Die Daten sind danach zwar noch auf dem Datenträger vorhanden, sie sind aber selbst für einen sachkundigen Nutzer mit Hilfe entsprechender Zusatzprogramme kaum noch auffindbar. Da ein solcher Eingriff vom Betriebssystem innerhalb von Sekunden ausgeführt wird, ist er äußerst wirkungsvoll.

Ein Programm, das eine Sabotagefunktion in sich birgt, verhält sich wie jedes andere, normale Programm und fällt daher in der Regel nicht als Sabotageprogramm auf. Wird zu einem späteren Zeitpunkt die Sabotagefunktion ausgelöst, dann ist selten ein Zusammenhang zwischen der Tathandlung einer bestimmten Person und dem eingetretenen Erfolg herzustellen. Mit der Datenlöschung werden zumeist auch gleichzeitig alle Spuren der Manipulation beseitigt. Aus diesem Grunde bestehen für die Strafverfolgungsorgane große Probleme, Fälle von Programmsabotage zu erkennen oder gar zu beweisen[79].

II. Computerviren

1. Begriff, Eigenschaften und Möglichkeiten

Eine Sonderstellung nehmen im Zusammenhang mit Computersabotage die mit zunehmendem Interesse verfolgten Computerviren ein[80]. Hinter diesem Begriff verbirgt sich eine erstmals im Jahre 1983 von dem Amerikaner F. Cohen in einer Reihe von Experimenten untersuchte[81] besondere Art von kleinen und kleinsten Computerprogrammen. Diese Programme werden deshalb als „Viren" bezeichnet, weil sie ein wesentliches Merkmal mit biologischen Viren teilen: Sie können andere Programm infizieren und sich dadurch „virusartig" ausbreiten.

Computerviren zeichnen sich durch zwei Eigenschaften aus. So können sie Kopien ihres eigenen Programmcodes erzeugen und ihn in andere Computerprogramme einpflanzen, ohne die auf diese Weise „infizierten" Programme damit zu zerstören. Daneben

[72] so Soyka, S. 91
[73] Vgl. Sieg Jura 86, 352, 359
[74] Soyka, S. 94
[75] s.o.; so das fiktive Beispiel bei Schmidt, cw v. 3. 04. 87, 42, 45
[76] Fall nach Soyka, 94 mit weiteren Fällen
[77] wofür bisher kein Fall aus der Praxis nachgewiesen werden kann
[78] Krabel, Eckhard (Die Viren kommen ct (computing today) 4/87, 108 f.) S. 108
[79] Paul, Werner (Programmsabotage, Polizeiliche Ermittlungspraxis und Virusprogramme CuR 85, 52 f.) S. 52
[80] Schmidt, cw v. 27. 03. 87; Krabel ct 4/87, 108 f.; Paul, CuR 1985, 52; Soyka, S. 94; Piller, Ernst/Weißenbrunner, Ernst (Software-Schutz; Wien, New York 1986) S. 24; Experimente mit Computer-Viren (KES - Zeitschrift für Kommunikations- und EDV-Sicherheit 1987, 102–113)
[81] vgl. die Beschreibung dieser Versuche bei Schmidt, cw v. 27. 3. 87, 35; u. Cohen, Fred: Computer Virusses, Theory and Experiments, 1983

können sie zusätzliche, exakt vorherbestimmbare Funktionen wahrnehmen[82].

Aus dieser Definition ergibt sich, daß Virusprogramme selbst neutral sind; ihre bloße Existenz verursacht noch keine Schäden in den „Wirtsprogrammen". Viren können vielmehr auch zu nützlichen Zwecken Verwendung finden und verschiedene Hilfsfunktionen wahrnehmen (wie etwa das Komprimieren von Programmen zum Zwecke der Speichereinsparung)[83]. Zum Sabotageprogramm wird ein Virus erst dadurch, daß ihm als Zusatzfunktion ein „Sabotageauftrag" erteilt wird, indem es mit einem aktiven oder passiven Auslöser (s. o.) gekoppelt wird. Nun kann das Virus als Trägermittel für jede erdenkliche Sabotagefunktion in allen Bereichen eines Rechnersystems dienen.

Die von einem Virus erzeugten Viruskopien sind ihrerseits in der Lage, selbständig weitere Kopien zu generieren. Die besondere, von Computerviren ausgehende Gefahr, besteht daher in ihrer Fähigkeit zur raschen und unkontrollierbaren Weiterverbreitung. Hierdurch können unabsehbare Schäden verursacht werden.

Die Existenz von Viren in einem Rechnersystem kann in den seltensten Fällen erkannt werden[84]. Virusprogramme können zur unentdeckten Verfolgung ihrer Zweckbestimmung durch die unterschiedlichsten Tarnmaßnahmen geschützt sein. So ist ein Virus sehr klein, womit seine Existenz und Wirkung in der Regel nicht an der Inanspruchnahme meßbarer Rechen- oder Datenträgerzugriffszeit erkannt werden kann. Auch das Diagnostizieren eines Virus durch außerprogrammmäßige Datenträgerzugriffe ist nicht möglich. Viren werden über Datenträger nur dann weiterverbreitet, wenn im Programmablauf ohnehin ein Zugriff auf den Datenträger vorgesehen ist. Die Länge eines vom Virus infizierten Programmes ändert sich in der Regel durch den Virus-Befall nicht[85]. Eine weitere Tarnmaßnahme für Virusprogramme kann darin bestehen, daß sie sich während der Kopiertätigkeit selbständig umstrukturieren[86]. Virusprogramme können so konzipiert sein, daß sie nicht wahllos alle Programme oder Datenbestände befallen, sondern sich ihre „Wirtsprogramme" nach bestimmten Kriterien auswählen[87].

2. Arbeitsweise

Alle Virusprogramme arbeiten nach einem ähnlichen Prinzip. Wird ein mit einem Virus infiziertes „Wirtsprogramm" von einem Datenträger geladen und im Rechner gestartet, sorgt ein Sprungbefehl dafür, daß das als Unterprogramm konzipierte eigentliche Virusprogramm ausgeführt wird. Das Virusprogramm sucht nun auf einem der Datenträger ein anderes, noch nicht infiziertes Programm und schreibt dann in einen bestimmten Bereich dieses Programmes einen Sprungbefehl, der die Startadresse seiner späteren Kopie enthält. Die anschließend erzeugte Kopie wird danach an die zuvor bezeichnete Adresse geschrieben nnd das gefundene Programm auf diese Weise infiziert. Programmteile, die während dieses Vorgangs vom Virus verändert wurden und den ordnungsgemäßen Ablauf des Ursprungsprogramms stören könnten, werden vorher wieder restauriert. Die dazu erforderlichen Daten sind im Virus selbst zwischengespeichert worden. Im Anschluß an diese „Infektion" wird das ursprünglich gestartete Wirtsprogramm normal abgearbeitet. Die mit diesem Vorgang verbundene, geringfügige Verzögerung ist bei modernen Rechnern mit hoher Rechengeschwindigkeit fast nicht meßbar[88]. Wenn das neu infizierte Programm gestartet wird, wirkt es seinerseits als Virus und „verseucht" auf dieselbe Weise andere Programme[89].

Neben der „Infektion" anderer Programme durch den Zugriff auf Datenträger, können sich Viren auch ausschließlich über das RAM ausbreiten. Nach dem Start eines infizierten Programmes wird das Virus in einen freien, üblicherweise von Programmen nicht genutzten RAM-Bereich kopiert. Befindet es sich hier, ist es nicht aufzuspüren, es infiziert aber jedes weitere geladene oder gestartete Programm. Ein einfaches „RESET" reicht nicht aus, um das Umsichgreifen dieser Virusart zu bekämpfen; erst beim Ausschalten des Rechners wird das Virus im RAM gelöscht[90]. Das Auftreten eines solchen Virentyps kann insbesondere in Rechnersystemen, die im Dauerbetrieb arbeiten, fatale Folgen haben.

3. Erstellung und Verbreitung

Virusprogramme können in nahezu allen höheren Programmiersprachen geschrieben werden. Der hierzu erforderliche Programmalgorithmus kann von einem Programmierer mit elementaren Systemkenntnissen ohne besondere Probleme entwickelt werden[91]. Das Ausmaß der Ausbreitung von Virusprogrammen ist vom jeweiligen Rechnersystem und den dort getroffenen Sicherungsvorkehrungen abhängig. Dieser Unterschied wird beim Vergleich von Großrechenanlagen und PCs deutlich.

a) In Home- und Personal-Computern werden Viren zumeist durch die Verwendung von Datenträgern

[82] So die Def. von Dierstein, cw Nr. 37, 1985, zit. n. Schmidt, cw v. 27. 3. 87 m. w. N., der diese Fähigkeiten als „Reproduktion" und „Funktionalität" bezeichnet

[83] weitere Beispiele dazu bei: Hoffmeister, Frank (Ein Ansatz zur Abwehr von Computerviren; Referat beim 7. GI Fachgespräch über Rechenzentren, München 1987 in: Organisation und Betrieb der verteilten Datenverarbeitung, Berlin, Heidelberg, New York 1987, S. 101 f.) S. 104

[84] Vgl. bes. Hoffmeister, 101, 102 m. w. N.; Schmidt, cw v. 27. 03., 32, 35 u. v. 3. 04. 87, 42, 45

[85] Krabel, ct 4/87, 108, 109

[86] Chaos-Computer-Club (Hacker steigen um auf 68 000er, 68 000er 3/87, S. 14) S. 14

[87] Vgl. Die Beispiele bei Krabel ct 4/87 108, 109 und Schmidt, cw v. 27. 03. 87, 32, 33

[88] Vgl. u. a. Schmidt, cw v. 27. 03. 87, 32, 35

[89] Vgl. zum technischen Ablauf das Virusbeispiel bei Krabel ct 4/87, 108, 109

[90] Vgl. Krabel ct 4/87, S. 110

[91] Vgl. Piller S. 24; Schmidt FAZ v. 7. 01. 87; bes. auch Ripota, Peter (Die neue Seuche: Computerviren im Programm, P. M. Computerheft, 2/86, S. 71 ff.) S. 73; u. Krabel ct 4/87, 108 f. mit entsprechenden Algorithmusbeispielen