Computer-Viren – Herkunft, Begriff, Eigenschaften, Deliktsformen

Thomas Hofer

I. Beschreibung der Problematik

USA: Versicherung gegen Virus-Schäden

Seit mehreren Jahren schon versetzt der aus dem Sprachschatz der Biologie entliehene Begriff „Computer-Virus" Besitzer jeder Art von Rechnersystemen in Angst und Schrecken. Nicht zuletzt die ausführliche Berichterstattung über spektakuläre Fälle von Virenbefall in Rechnernetzen[1] verursachte bei vielen Anwendern, insbesondere bei denen des am weitesten verbreiteten Betriebssystems DOS, Rat- und Hilflosigkeit, wenn es darum geht, dem Phänomen wirksam zu begegnen. Bemerkenswert erscheint in diesem Zusammenhang, daß die Zahl der virusinfizierten Computer allein in Deutschland bereits auf 200.000 geschätzt wird.[2] In den USA wird bereits Versicherungsschutz gegen Schäden durch Computer-Viren angeboten.[3]

1984: Erster Viren-Report von Fred Cohen

Seitdem 1984 Fred Cohen (University of Southern California) erstmals einen umfangreicheren Bericht über sogenannte Computer-Viren erstellt hat,[4] ist durch diese Art des Computermißbrauchs bereits einiger Schaden verursacht worden.

Hohe Dunkelziffer bei Viren-Befall

Was Viren bisher tatsächlich alles angerichtet haben, ist wenig bekannt. Der Hamburger Professor und Leiter eines Virentestzentrums, Klaus Brunnstein, hält die Dunkelziffer in diesem Bereich für sehr hoch, da kein Unternehmen gern zugeben wird, Opfer eines Virus geworden zu sein – müßte man doch eingestehen, es mit der Sicherheit der Daten nicht so genau genommen oder Software aus zweifelhaften Quellen – sprich Raubkopien – eingesetzt zu haben. Geschäftspartner wären beunruhigt, der Ruf wäre ruiniert. Peinlich ist ein Virenbefall vor allem bei Software- und Systemhäusern – was in letzter Zeit anscheinend bei kleineren Firmen häufiger passierte, indem infizierte Disketten an Kunden ausgeliefert wurden.[5] Letztere sind dann einer Infektion ihrer Geräte erst recht schutzlos ausgeliefert, vertrauen sie doch gerade auf die Virenfreiheit der Original-Disketten. Namhafte große Softwarefirmen treffen zwar schon seit längerem entsprechende Schutzmaßnahmen, wurden aber von der Virengefahr zunächst auch völlig überrascht.

Schaden: Schätzungen und Prognosen

Schätzungen gehen denn auch von bis dato über 160 Mio. Mark Schaden durch Computer-Viren in Deutschland aus; in den kommenden zehn Jahren dürften es sogar 500 Mio. Mark werden[6].

Risikozonen: Schulen und Universitäten

In besonders hohem Maße gefährdet sind Schulen und Universitäten wegen der Vielzahl der an den Geräten tätigen Personen und der Tatsache, daß diese vielfach eigene Software mitbringen. Hinzu kommt, daß dort Computer in immer größerem Umfang zu lokalen PC-Netzen zusammengeschlossen werden. So können Viren, die über die Disketten-Laufwerke der Arbeitsstationen eingeschleust werden, den zentralen Server befallen und damit schnell ein ganzes Netzwerk lahmlegen.[7]

1 Im „Fall Morris" stürzten EDV-Anlagen durch Speicherkapazitätsüberlastung aufgrund des sogenannten INTERNET-Wurm-Programms ab; Morris wurde 1990 zu 5 Jahren Gefängnis und 250.000 $ Geldstrafe verurteilt. Es ließen sich noch mehr derartige Beispiele aufzählen; vgl. dazu die Nachweise bei Rombach, Killer-Viren als Kopierschutz, CR 1990, S. 101

2 Wirtschaftswoche 12/1991, S. 105

3 Gerdes, VW 1990, S. 249

4 Dissertation „Computer Viruses"

5 Vgl. obige Ausführungen zu verseuchten Treiberdisketten.

6 Vgl. die Studie von Bernd Schrum, Computer-Viren und ihre wirtschaftlichen Auswirkungen, FH Gießen/Friedberg (Quelle: CHIP 2/91, S. 196 f.).

7 Vgl. zur Problematik von Viren im Netzwerk auch die Aufsätze von Vieten, CHIP 3/91, S. 266 sowie Dehn/Arndt, Personal Computer 2/91, S. 120 f.

JurPC-Archiv: http://www.jurpc.de

II. Funktionsweise von „Computer-Viren"

Definition „Biologische Viren"

Biologische Viren werden definiert als „Erreger von Infektionskrankheiten bei Menschen, Tieren oder Bakterien" (lt. Brockhaus). Diese Merkmale von Bio-Viren lassen sich natürlich nicht auf Computer-Viren übertragen – die aus der Biologie entlehnten Bezeichnungen nehmen jedoch durchweg als tertium comparationis auf deren Eigenschaften Bezug[8].

Definition „Computer-Viren"

Eine sehr vereinfachte Defintion der Computer-Viren lautet daher:
„Ein Sabotage- bzw. Störprogramm, das die Eigenschaft besitzt, andere Programme derart zu verändern, daß diese nach der Manipulation eine Kopie des Viruscode enthalten, und irgendwelche Wirkungen hervorruft, die vom Ursprungsprogramm nicht beabsichtigt sind (i. d. R. destruktive)."
Allgemein kann gesagt werden, daß Viren i. d. R. ungewöhnlich kurze und einfache Programme sind, die wie jedes andere Programm (in einer höheren Programmiersprache wie z. B. Pascal) geschrieben wurden; sie benötigen auch keine besondere Sprache oder Codierung, wie mancherorts irrtümlich angenommen wird. Zu ihrer Entwicklung bedarf es in der Regel nur durchschnittlicher Programmierkenntnisse.
An dieser Stelle sei die folgende Anmerkung erlaubt:
Dies zeigt, daß Computer-Viren partout nichts „Elektronisches" an sich haben. Die Tatsache, daß Viren – weil sie Programme sind – in elektronischen Rechenanlagen ausgeführt werden, ändert daran nichts.

Computer-Viren bestehen aus 2 Komponenten:

Programme, die man als echte Viren[9] bezeichnen kann, bestehen grundsätzlich aus zumindest zwei, funktionell voneinander getrennten Komponenten – einem Vervielfältigungsteil und einem Effekt- oder Schadensteil.

1. Der Vervielfältigungsteil

„Sich vermehren" heißt für ein Programm ganz allgemein: Es kann Kopien von sich erzeugen. Entscheidend ist aber nicht die Tatsache, daß Kopien erzeugt werden, sondern wie.
Der Vervielfältigungsteil eines Computer-Virus umfaßt alle Funktionen, die für seine Weiterverbreitung erforderlich sind. Dies beinhaltet die Suche nach nichtinfizierten Programmen, Veränderungen solcher Programme, Installation im Speicher, eventuell auch Tarnung. Vermehrung ist somit beim Virusprogramm immer die Fähigkeit, andere Programme zu infizieren, das heißt, eine Kopie von sich selbst in ein anderes Programm einzufügen. Dieser einfache Mechanismus führt dazu, daß jedes einmal infizierte Programm sofort selbst den Virus weiterverbreitet, und zwar solange, bis alle erreichbaren Wirtsprogramme verseucht sind. Je mehr verseuchte Programme aufgerufen werden, desto schneller geht die Ausbreitung vonstatten.[10] Damit kann sich eine Infektion genau wie bei biologischen Viren lawinenartig in einem DV-System ausbreiten.

2. Der Effekt- bzw. Funktionsteil

Der Effekt- bzw. Funktionsteil eines Virus wird im Regelfall erst nach Abarbeitung des Vervielfältigungsteils aktiv. Fast immer ist in diesem Teil des Virus eine ganz eindeutige Auslösebedingung (Trigger) festgelegt, die gleich zu Beginn überprüft wird. Trifft sie nicht zu, endet die Abarbeitung des Schadensteils, und es passiert nichts Auffälliges. Dies erklärt auch, warum Virusinfektionen sehr oft längere Zeit unentdeckt bleiben können – das Virus „schläft", bis der festgelegte Zeitpunkt eintritt.[11]
Wird die Auslösebedingung jedoch wahr, tritt der eigentliche Sabotagecode in Aktion. Programmtechnisch ist ein Auslöser nichts anderes als eine Bedingung („if ... then"-Abfrage).
Der prinzipielle Aufbau des Virus-Programms wird durch diesen sehr einfachen Zusatz kaum verändert, dafür aber das verheerende Verhalten der Virusprogramme wesentlich verstärkt.[12]

---

8 Selbstverständlich gibt es mancherlei Einzelheiten, die auf die biologischen Vorbilder nicht passen. Aber es ist auch nicht der Sinn eines bildhaften Vergleichs, vollständige Übereinstimmung zwischen Bild und Urbild, sondern vielmehr den Bezug auf mindestens eine, wesentliche Gemeinsamkeit herzustellen.

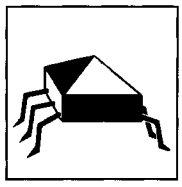
9 Vgl. zu den Erscheinungsformen von Computer-Viren und deren Abgrenzung im einzelnen Dierstein, Von Viren, trojanischen Pferden und logischen Bomben (I), NJW-CoR 4/90 S. 26 und Dehn/Paul: Vorbeugung bei Computer-Viren, CR 1989, S. 86 f.

10 Konsequenz: In einem ruhenden System kann sich kein Virusprogramm mehr fortpflanzen.

11 Als mögliche Auslösebedingungen sind bekannt geworden: Erreichen eines bestimmten Systemdatums, z. B. Freitag der 13., oder einer bestimmten Uhrzeit; Ausführen einer bestimmten Programmfunktion, z. B. Abspeichern; auch die Abwesenheit eines bestimmten Ereignisses kann Bedingung für das Auslösen einer bestimmten Folge sein.

12 Vgl. zum Einsatz als „logische Bombe" Rombach, CR 1990, S. 102

JurPC-Archiv: http://www.jurpc.de



Als bisher bekannte Schadensfolgen durch Virenbefall sind der Totalverlust aller Daten auf Festplatten oder Disketten durch Auslösen der Neuformatierung, aber auch subtilere Schäden, wie z. B. die Veränderung von Datenbeständen (Änderung von Zahlen in einer Tabellenkalkulation, Produktion falscher Rechenergebnisse[13], Änderung von Texten durch Einfügen fehlerhafter Zeichen), zu nennen. Andere Viren wiederum stellen sich vergleichsweise harmlos dar, indem sie z. B. den Rechner jeden Freitag verlangsamen, Buchstaben vom Bildschirm „fallen lassen", eine Musik spielen oder einen Ball auf dem Bildschirm umherttanzen lassen.

Bisher bekannte Schadensfolgen

Festzuhalten ist jedenfalls, daß nicht alle Viren von gleicher Gefährlichkeit für den Datenbestand des Benutzers sind.[14]

III. Herkunft und Verbreitung von Computer-Viren

1. Der Ursprung

Ursprünglich wurden Computer-Viren in den USA von angestellten Programmierern einiger Soft- und Hardwarefirmen entwickelt, die sich bei ihrem Arbeitgeber für schlechte Bezahlung, schlechte Arbeitsbedingungen oder Entlassung „rächen" wollten.[15]

Viren als „Rache" am Arbeitgeber

Die meisten Virenprogrammierer heute denken sich nichts „Böses" bei der Produktion eines Virus. Für sie sind diese rekursiven Programme faszinierende Spielereien, eine intellektuelle Herausforderung. Was nach deren Inverkehrbringen passiert, scheint ihnen egal zu sein; wer sich infiziert, ist ihrer Meinung nach selbst schuld.[16]

Nicht zuletzt sind Computer-Viren durch ihre schnelle Verbreitung und späte Erkennbarkeit auch für Wirtschafts- und Politkriminelle interessant; für viele Viren wurden als Herkunftsländer Ostblockstaaten, wie z. B. Bulgarien, aber auch Israel[17] entlarvt. Zumindest gibt es Anzeichen, daß Viren in immer größerem Ausmaß auch für verbrecherische Zwecke eingesetzt werden, wobei die Täter kaum Angst vor Entdeckung zu haben brauchen. Es ist davon auszugehen, daß die Verletzlichkeit der Computernetze bereits vom organisierten Verbrechen genutzt wird.

Computer-Viren und organisiertes Verbrechen

Selbst Militär und Geheimdienste sehen ihre Chancen. So soll das Pentagon im vergangenen Jahr öffentlich demjenigen, der ein akzeptables Konzept für einen militärisch nutzbaren Computervirus vorlegt, eine Belohnung von 50.000 $ versprochen und bei Funktionieren einen Auftrag in Höhe von 500.000 $ zur Realisierung des Konzepts in Aussicht gestellt haben.[18]

Pentagon soll Computer-Virus in Auftrag gegeben haben.

2. Das Einschleusen von Computer-Viren in fremde Rechner

Als erstes gerieten Public-Domain-Software, Shareware oder Raubkopien[19] aus dunklen Quellen in Verruf. Heute kann wohl davon ausgegangen werden, daß alle seriösen PD- und Shareware-Vertreiber ihr Angebot ständig auf Computer-Viren überprüfen, was nicht selten als werbeträchtiges Argument gegen Mitbewerber gebraucht wird.

Public Domain und Shareware

Selbstverständlich sind aber alle Disketten, die häufig kopiert werden, besonders gefährdet. So mußten in jüngster Zeit auch Käufer von bestimmten VGA-Grafikkarten und Mäusen (taiwanesischer Herkunft) die unangenehme Erfahrung machen, daß die beiliegenden Treiberdisketten virenverseucht waren. Nach Angaben des Virentestzentrums in Hamburg sind

Verseuchte Maustreiber aus Taiwan

13 Beispiel für die „Wirksamkeit" der neuen Viren-Generation ist der „dBase-Virus": Er verändert die Datendateien des weitverbreiteten Datenbankprogramms „dBase", das oftmals für die Bearbeitung wichtiger Finanzdaten verwendet wird, so, daß der Anwender anfangs keine Notiz von der Manipulation nimmt, denn auf dem Bildschirm erscheinen stets die korrekten Zahlen – die Berechnungen aber werden mit den manipulierten Daten ausgeführt.

14 Hilfe bei Virenbefall gewähren auf Anfrage die Redaktionen namhafter Computerzeitschriften (z. B. Computer Persönlich, CHIP) und die Virentestzentren der Universitäten Hamburg und Karlsruhe.

15 Laut einer Studie des amerikanischen Pioniers in der Virenforschung, Fred Cohen.

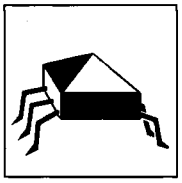
16 Wie Interviews mit entdeckten Virenprogrammierern gezeigt haben, vgl. CHIP 3/1990.

17 Zu einiger „Berühmtheit" hat es der sogenannte Israel- oder auch Jerusalem-Virus gebracht, der den Zweck hatte, 1988 am 40. Jahrestag des Bestehens Israels alle befallenen Programme zu löschen; hier wurde sogar ein politisch motivierter Anschlag vermutet; vgl. mc 7/1988, S. 75.

18 Gero v. Randow, CHIP 3/91, S. 25

19 Vor dem Hintergrund erheblicher Umsatzeinbußen durch das Anfertigen unautorisierter Kopien von Originalprogrammen kam die Softwareindustrie auf den Gedanken, „Killer-Viren" quasi als Kopierschutz einzusetzen, vgl. zu diesem Problemkreis insbesondere Rombach, CR 1990, S. 101 ff. u. 184 ff.

JurPC-Archiv: http://www.jurpc.de



Viren auf Treiberdisketten nicht ungewöhnlich, denn diese schleichen sich bei der massenhaften Produktion dieser Disketten schon einmal in der Kopieranstalt auf die Floppies, wenn lediglich die angelieferte Ausgangsdiskette befallen war.

Programme aus (privaten) Mailboxen

Erwähnung bedarf in diesem Zusammenhang auch der immer beliebter werdende Zugang zu Mailboxen per Modem. Da dort häufig PD-Software zum Download angeboten wird, ist das Risiko, verseuchte Programme zu erlangen, wegen der geringeren Sorgfalt der meist privaten Mailbox-Betreiber evident.

IV. Strafrechtliche Erfassung und Bewertung

1. Deliktsformen

Eine Strafbarkeit wegen des Verbreitens von Computer-Viren kann sich vor allem aus den nachträglich durch das 2. WiKG 1986 eingefügten §§ 303 a, 303 b StGB ergeben.

a) § 303 a StGB

§ 303 a StGB dient dem Schutz des Interesses an der Verwendbarkeit der in den gespeicherten Daten enthaltenen Informationen,[20] beziehungsweise hat nach anderer, im praktischen Ergebnis weitgehend gleicher Auffassung den Charakter eines spezialisierten Vermögensrechts[21].

Tatobjekt: Daten, unabhängig von ihrem Inhalt

Geschützt sind Daten i. S. § 202 a II StGB; hier werden alle Daten erfaßt, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Auf den Inhalt der Daten bzw. der darin enthaltenen Informationen kommt es nicht an,[22] deshalb besteht keine Notwendigkeit, zwischen Daten im eigentlichen Sinne und Computerprogrammen zu differenzieren[23].

Tathandlungen

Grundsätzlich liegt bei vorsätzlicher Installation eines Virus Strafbarkeit nach § 303 a StGB vor,[24] jedoch ist hier auf die Eigenart des speziellen Virusprogramms einzugehen:

Löschung

- Löschung: Darunter wird die irreversible physische Aufhebung ihrer Verkörperung verstanden, entsprechend der Zerstörung einer Sache bei Sachbeschädigung (§ 303 StGB).[25] Überschreibt ein Virus Daten, so liegt darin eine Löschung oder Veränderung i. S. § 303 a StGB. Wird durch ein Störprogramm ein Systemabsturz hervorgerufen, so werden dabei alle Daten im Arbeitsspeicher zerstört; also liegt darin ebenfalls eine Löschungshandlung.

Unterdrückung

- Unterdrückung: Diese besteht in einem Entzug der Zugriffsmöglichkeit des Berechtigten.[26] Der typische Fall der Unterdrückung wird durch Störprogramme hervorgerufen, die dem Benutzer den Zugriff auf Daten (auch Programme) unmöglich machen.[27] Löscht ein Virus Dateien durch Entfernung des Verzeichniseintrags, wie dies z. B. durch den DELETE-Befehl in MS-DOS geschieht, so liegt hierin zum einen eine Löschungshandlung durch Vernichten dieser Verzeichnisdaten, zum anderen eine Unterdrückung der eigentlichen Datei-Daten, da diese nur durch ein spezielles Programm rekonstruiert werden können.[28] Dasselbe gilt für die Zerstörung des Boot- oder des Partitionsektors beziehungsweise bei Neuformatieren der Platte.

Unbrauchbarmachung

- Unbrauchbarmachung: Allgemein versteht man hierunter Aufhebung der bestimmungsgemäßen Verwendbarkeit der Daten.[29]

Veränderung

- Veränderung: Diese Begehungsweise des § 303 a StGB erfaßt nicht nur die inhaltliche Umgestaltung wie in § 2 II Nr. 3 BDSG, sondern auch jegliche Veränderung der physisehen Gestalt.[30]

---

20 Dreher/Tröndle, StGB, 45. Auflage 1991, § 303 a Rdnr. 2

21 Welp, Datenveränderung (§ 303 a StGB), IuR 1988, S. 448 f.

22 So auch Welp, a. a. O., S. 445; vgl. DIN 44300.

23 So aber Gravenreuth, Juristisch relevante technische Fragen zur Beurteilung von Computerprogrammen, GRUR 1986, S. 727; dagegen aber LG Ulm in CR 1989, S. 825.

24 Gravenreuth, Computerviren, Hacker, Datenspione, Crasher und Cracker, NStZ 1989, S. 204

25 Welp, a. a. O., S. 434 f.

26 Gravenvreuth, a. a. O., S. 206

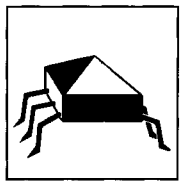
27 LG Ulm, CR 1989, S. 825 („Programmsperre")

28 Welp, a. a. O., S. 435

29 Dreher/Tröndle, a. a. O., § 303 a Rdnr. 7

30 Welp, a. a. O., S. 435 f.

JurPC-Archiv: http://www.jurpc.de



Die einzelnen Begehungsweisen überschneiden sich im Interesse eines vollständigen Rechtsschutzes.

Fraglich ist, ob von § 303 a StGB auch Computer-Viren erfaßt werden, die den Benutzer zwar mit mehr oder weniger humorvollen Wirkungen belästigen, aber nicht seine Daten beeinträchtigen. Diese Programme könnten durch das bloße Belegen von Speicherplatz bereits unter § 303 a StGB fallen. Es wäre durch die Veränderung der in den leeren Speicherzellen enthaltenen „Null-Information" zu begründen[31]. Jedoch bleibt durch die Löschbarkeit des Störprogrammes das ursprüngliche Interesse an der in leeren Speicherzellen enthaltenen Information gewahrt, nämlich die Verfügbarkeit des Speicherplatzes. Also wird das bloße Belegen von Speicherplatz durch solche Programme vom Rechtsschutzbereich des § 303 a StGB (vgl. 3.1) nicht erfaßt.

Computer-Viren, die lediglich „belästigen"

Zu Programmen, die durch systematisches Überfüllen des Speichers den Systembetrieb lahmlegen, siehe unten § 303 b StGB.

Für andere Störprogramme, die keine Computer-Viren sind, gelten diese Ausführungen entsprechend.

Das Tatbestandsmerkmal[32] „rechtswidrig" dient der tatbestandlichen Ausschließung aller ordnungsgemäßen Datenmanipulationen und verlangt somit einen Eingriff in fremde Rechtspositionen. Fraglich ist die Bestimmung dieses Merkmals[33]. Eine Einordnung nach dem Sachenrecht ist nicht möglich, da Daten keine Sachen i. S. des BGB sind. Auch der Erzeuger von Daten kann nicht als der Alleinberechtigte angesehen werden. Richtig ist es, als Berechtigte sowohl den zur Verfügung über die Daten Berechtigten als auch den vom Inhalt der Daten Betroffenen anzusehen.[34]

Rechtswidrigkeit als Tatbestandsmerkmal

Bedingter Vorsatz bezüglich der Merkmale des objektiven Tatbestandes genügt.[35] Der Versuch der Tat ist nach §§ 23 I, 12 II, 303 a II StGB strafbewehrt; fahrlässiges Handeln steht nicht unter Strafe. Nach § 303 c StGB ist Strafantrag erforderlich.

Der Versuch ist strafbar.

b) § 303 b StGB

§ 303 b StGB dient dem Schutz des Interesses von Wirtschaft und Behörden an einem störungsfreien Betrieb der Datenverarbeitung.[36] Computer-Viren können grundsätzlich den Tatbestand des § 303 b StGB erfüllen.[37] Auch hier ist jedoch auf die Eigenheiten des Virusprogramms abzustellen.

§ 303 b StGB schützt „eine Datenverarbeitung". Unter diesen weitgefaßten Begriff werden auch die Verarbeitung sowie die weitere Verwertung von Daten gefaßt[38].

Tatobjekt: Datenverarbeitung von Betrieb, Unternehmen oder Behörde

Es muß sich um die Datenverarbeitung eines Betriebs, Unternehmens oder einer Behörde handeln. Der Begriff der Behörde richtet sich nach § 1 IV VwVfG. Die Bezeichnungen „Betrieb" und „Unternehmen" sind bei § 303 b StGB im weiten Sinne als organisatorische Einheit aufzufassen, die nicht unbedingt kaufmännische Betriebe sein müssen.[39]

Der Betrieb oder das Unternehmen muß für den Täter fremd sein; er darf also keine Eigentums-, Gebrauchs- oder Verfügungsrechte an der Datenverarbeitung haben.[40] Demnach ist für einen gewöhnlichen Mitarbeiter der Betrieb, in dem er angestellt ist, fremd. Dies ist insofern bedeutsam, als gerade unzufriedene Mitarbeiter häufig Urheber von Störprogrammen sind[41].

Fremdheit von Betrieb oder Unternehmen

Die Datenverarbeitung muß von wesentlicher Bedeutung sein, das heißt, es muß sich um die Verwaltung von Daten handeln, die für den Arbeitsablauf grundlegend sind.[42]

---

31 vgl. Welp, a. a. O., S. 435, Fußnote 55

32 Dreher/Tröndle, a. a. O., § 303 a Rdnr. 9; Welp, a. a .O., S. 447, sieht hier ein allgemeines Deliktsmerkmal.

33 Aufgrund dieser Unbestimmtheit wird diese Norm als „mißglückt" (SK-Samson) oder „verfassungsrechtlich zweifelhaft" (Welp, S. 447) beurteilt.

34 Welp, S. 448; Dreher/Tröndle, a. a. O., § 303 a Rdnr. 9

35 Dreher/Tröndle, a. a. O., § 303 a Rdnr. 10

36 Dreher/Tröndle, a. a. O., § 303 b Rdnr. 2 m. w. N.

37 Dreher/Tröndle, a. a. O., § 303 b Rdnr. 7

38 BT-Drucks. 10/5058/35

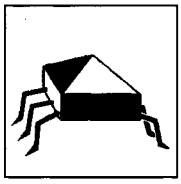
39 Volesky/Scholten, Computersabotage – Sabotageprogramme – Computerviren, IuR 1987, S. 281

40 Dreher/Tröndle, a. a. O., § 303 b Rdnr. 8

41 Bunge, Die größte Gefahr ist der ungetreue Mitarbeiter, Kriminalistik 1987, S. 78 ff.

42 vgl. Dreher/Tröndle, a. a. O., § 303 b Rdnr. 4

JurPC-Archiv: http://www.jurpc.de



Die Tat wird durch das Stören einer der oben erläuterten Datenverarbeitungsanlagen verübt. Möglichkeiten sind:

(1) § 303 b I Nr. 1 StGB: Die Störung kann durch eine Tat nach § 303 a StGB erreicht werden. § 303 b I Nr. 1 StGB ist insofern Qualifikation zu § 303 a StGB.[43]

(2) § 303 b I Nr. 2 StGB: Die Störung kann auch durch spezielle weitere, hier aufgeführte Handlungen erfolgen. Deren Tatobjekt ist eine Datenverarbeitungsanlage oder ein Datenträger. Unter Datenverarbeitungsanlage ist die gesamte Hardware eines Systems zu verstehen, also Recheneinheit, Peripherie und auch die im ROM (Read-Only-Memory) eines Rechners enthaltenen Informationen[44]. Als Datenträger kommen vor allem Magnetplatten (Festplatten, Disketten) oder Magnetbänder, aber auch EPROMS in Betracht. Es ist also zu differenzieren zwischen dem Tatobjekt der Störung und dem Objekt der folgenden Störungshandlungen:

Zerstörung
- Unter Zerstörung wird, wie bei der einfachen Sachbeschädigung nach § 303 StGB, eine substantielle Einwirkung verstanden.[45]

Beschädigung
- Beschädigung bedeutet erhebliche Einschränkung der Unversehrtheit.[46] In der Praxis sind zwar bisher noch keine Fälle bekanntgeworden, in denen ein Virus mechanische Schäden hervorgerufen hätte.[47] Denkbar ist dies jedoch, z. B. durch extreme Steuerungsbefehle an den Controller der Festplatte, oder Einbrennen des Bildschirms.[48]

Unbrauchbarmachung
- Unbrauchbarmachung ist die Aufhebung der ordnungsgemäßen Verwendbarkeit.[49] Hier ist besonders der Fall relevant, daß ein Virus durch explosionsartige Vervielfältigung Speicher oder Kommunikationsleitungen blockiert und dadurch eine Störung einer Datenverarbeitung herbeiführt.

Beseitigung
- Beseitigung ist das Entfernen aus dem Verfügungsbereich des Berechtigten[50] und kommt hier naturgemäß nicht in Betracht.

Veränderung
- Eine Veränderung liegt bei jeder Abweichung vom ursprünglichen Zustand vor.[51] Diese ist jedoch nur dann relevant, wenn sie die Wirkung der Anlage beeinflußt[52], was bereits durch die spezielleren Störhandlungstatbestände abgedeckt sein dürfte.

Strafantrag erforderlich

Bedingter Vorsatz bezüglich des objektiven Tatbestandes genügt; der Versuch ist strafbar, ein Fahrlässigkeitsdelikt besteht nicht; gemäß § 303 c StGB ist Strafantrag erforderlich.

c) Ergebnis

Computer-Viren, die keine schädlichen Auswirkungen haben, und auch nicht durch ihre Existenz oder Vervielfältigung die Datenverarbeitung blockieren, fallen nicht in den strafrechtlich relevanten Bereich.

2. Weitere Rechtsfragen

a) Urheberrechtliche Konsequenzen

Ein Computervirus kann gegen den Schutz urheberrechtlich geschützter Werke vor Beeinträchtigung verstoßen (§§ 14, 39 UrhG).

Infizierung urheberrechtlich geschützter Programme

Wird vom Täter bewußt ein urheberrechtlich geschütztes Programm infiziert und werden dadurch die Interessen des Urhebers gefährdet, ergeben sich hier keine Probleme.
Problematisch wird es jedoch, wenn ein solches Programm nicht direkt, sondern erst im Zuge der vom Täter nicht mehr kontrollierbaren Vervielfältigung befallen wird.
Ist dies vom Täter beabsichtigt, so muß ein urheberrechtlicher Eingriff bejaht werden.[53]

---

43 Dreher/Tröndle, a. a. O., § 303 b Rdnr. 6

44 Volesky/Scholten, a. a. O., S. 281

45 vgl. Wessels, Strafrecht BT Bd.2, 13. Aufl. 1990, § 1 I 3 b) m. w. N.

46 Schönke/Schröder-Stree, StGB, 23. Aufl. 1988, § 303 Rdnr. 8; Dreher/Tröndle, a. a. O., § 303 Rdnr. 5

47 Volesky/Scholten, a. a. O., S. 287

48 Gravenreuth, a. a. O., S. 202; Welp, a. a. O., S. 437

49 Dreher/Tröndle, a. a. O., § 303 b Rdnr. 7

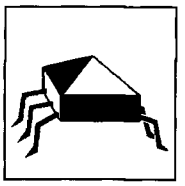
50 Dreher/Tröndle FN 49

51 Volesky/Scholten, a. a. O., S. 282

52 Gravenreuth, a. a. O., S. 204

53 Gravenreuth, GRUR 1986 S. 726

JurPC-Archiv: http://www.jurpc.de



Hat der Täter jedoch keine Kenntnis von den befallenen Programmen, wird die Auffassung vertreten, keinen urheberrechtlich relevanten Eingriff anzunehmen, da dieser zielgerichtetes Handeln voraussetzt.[54] Hier muß jedoch bedacht werden, daß das vom Täter bewußt gesetzte **R**isiko gerade in der unkontrollierbaren Ausbreitung liegt, so daß auch bei mehr oder minder zufällig getroffenen urheberrechtlich geschützten Programmen dem Berechtigten ein Anspruch auf Verbot der Beeinträchtigung zustehen sollte, zumal dieser in den meisten Fällen ohnehin nicht durchsetzbar sein dürfte, da die Feststellung des Täters beträchtliche Schwierigkeiten mit sich bringt[55].

3. **Rech**tsdogmatische Fragen

a) Schaffung eines Fahrlässigkeitsdelikts

Schwierige Ermittlungen und Beweislage

Die Möglichkeiten der Opfer von Computer-Viren – dies haben die Erfahrungen gezeigt –, sich mit Hilfe der Gerichte gegen die Hersteller von Computer-Viren zur Wehr zu setzen, geschweige denn, Schadensersatz zu bekommen, sind äußerst gering. Das fängt schon damit an, daß Virenprogrammierer eigentlich nie gefaßt werden können, denn der Verursacherkreis ist praktisch unbegrenzt, und selbst wenn der Täter ermittelt wird, gestaltet sich die Beweisführung mangels Informationen, mit denen der Ablauf oder die Umstände einer Infektion belegt werden können, sehr schwierig. Aus diesem Grund ist auch auf die – kriminalpolitische – Frage, ob neben den oben aufgeführten Vorsatz-Deliktsformen auch ein Fahrlässigkeitsdelikt wünschenswert wäre, einzugehen.

Der Täterkreis: Computerfreaks und unzufriedene Mitarbeiter

Hier hilft ein Blick auf die Struktur des Täterkreises weiter: Neben unzufriedenen Mitarbeitern[56] sind die Urheber von Computer-Viren hauptsächlich Computerfreaks, die in der Herstellung von Viren lediglich eine Art sportlicher Herausforderung sehen[57]. Außerdem steckt ein großes Gefährdungspotential in spielenden Systemverantwortlichen, die schädliche Auswirkungen provozieren, auch wenn sie das gar nicht wollen.[58] Ohne Fahrlässigkeitsdelikt kann also ein großer Teil der Urheberschaft von Virusprogrammen nicht erfaßt werden.

Mangelnde Fachkenntnis der Ermittlungsbeamten

Zudem gelingt es nur selten, den Verbreiter eines Virus ausfindig zu machen,[59] einerseits aus technischen Gründen, andererseits wegen mangelnder Fachkenntnis der Ermittlungsbeamten[60] und auch wegen des Schweigens betroffener Softwarehäuser aus Furcht vor Negativ-Werbung. Wenn dem Täter dann noch die Schutzbehauptung offensteht, er habe nur experimentieren wollen und dabei sei der Virus versehentlich in Umlauf gebracht worden, so kann der strafrechtliche Schutz nicht besonders effektiv ausfallen.

Demnach wäre die Schaffung eines Fahrlässigkeitsdelikts im Bereich der Computer-Viren durchaus wünschenswert.

b) Verbot von Virenforschung

Minnesota: Gesetz zur Bekämpfung und Herstellung von Viren

In den USA wird die Problematik so gravierend eingeschätzt, daß in Minnesota bereits ein Gesetz zur Bekämpfung der Herstellung und Verbreitung von Computer-Viren erlassen wurde.[61] Sogar dem Virenforscher Cohen wurden einige Experimente untersagt.[62]

Umstritten ist hier insbesondere, inwieweit die Veröffentlichung von Viren-Quellcodes zulässig sein soll.

Dies gilt nicht zuletzt auch für Anbieter von sogenannten Viren-Construction-Sets.[63]

Fraglich ist also, ob die Forschung im Bereich der Computer-Viren eingeschränkt oder gar untersagt werden sollte. Verfechter einer restriktiven Informationspolitik in diesem Bereich sehen hierin vor allem die Gefahr zur Nachahmung, andere wiederum halten es für zwin-

54 Gravenreuth, NStZ 1989 S. 203

55 Welp, a. a. O., S. 437/438; Gravenreuth GRUR 1986 S. 726

56 Vgl. Dehn/Paul, Vorbeugung bei Computerviren, CR 1989, S. 69 f.; Bunge, a. a. O., S. 78

57 Volesky/Scholten, a. a. O., S. 289

58 Stark hervorgehoben bei Dierstein, Von Viren, trojanischen Pferden und logischen Bomben, NJW-CoR 4/90, S. 9.

59 Sperber, Virusfieber, mc Juli 1988, S. 77

60 Werner, Die Computerkriminalität als neue Form der Wirtschaftskriminalität, RDV 1989, S. 221

61 CHIP 10/1989 Viren-Forum; CR 1989, S. 662 (Mitteilung)

62 Volesky/Scholten, a. a. O., S. 289

63 Werkzeuge zur Virenprogrammierung, vgl. Sperber a. a. O., S. 77

JurPC-Archiv: http://www.jurpc.de

gend erforderlich, daß zumindest die betroffenen Fachkreise – sprich alle in der Virenabwehr engangierten Programmierer, etc. – umgehend von den Strukturen jedes neuen Virus Kenntnis erlangen müssen. Für dieses Regelungsvakuum werden bereits Gesetzesvorlagen erarbeitet.[64]

Virenforschung und Art. 5 GG

Dies scheint im Hinblick auf das Grundrecht der Freiheit der Forschung nach Art. 5 III 1 GG nicht unbedenklich, denn das Grundgesetz gewährleistet die Freiheit von Wissenschaft und Forschung vorbehaltlos. Dieses Grundrecht kann demnach nur durch immanente Grundrechtsschranken, d. h. kollidierendes Verfassungsrecht, beschränkt werden.[65]
Mithin ist die Beschränkung der Virenforschung durch Gesetz als verfassungsrechtlich unzulässig anzusehen.
Demnach müßte die Freiheit der Virenforschung gegen unmittelbares Verfassungsrecht verstoßen.

Ein Vergleich mit der Gentechnologie

Im Bereich der Gentechnologie besteht eine Kollision mit anderem Verfassungsrecht – Gefährdung der Menschenwürde (Art. 1 GG) und des Lebens-, Gesundheits- und Persönlichkeitsschutzes (Art. 2 GG).[66] Dies gestattet eine Beschränkung der Forschung auf diesem Gebiet. Die Computer-Virenforschung gefährdet jedoch nicht persönliche, sondern „nur" vermögenswerte Bereiche, also scheidet eine Behandlung der Virenforschung analog der Gentechnologie aus. Eine existentielle Bedrohung anderweitiger verfassungsrechtlicher Güter durch eine freie Betätigung der Virenforschung ist nicht ersichtlich.
Also ist – anders als in den USA – nach deutschem Recht eine Einschränkung der Computer-Virenforschung unzulässig.

64 vgl. Gravenreuth, CHIP 1/91, S. 159

65 Pieroth/Schlink, Staatsrecht II – Grundrechte, 5. Aufl. 1989, Rdnr. 709, 713; BVerfGE 30, 191 f. (173)

66 Pieroth/Schlink, Fußnote 65

JurPC-Archiv: http://www.jurpc.de