Äquivalent erlaubt ist oder da es möglich ist, zu diesem anderen Ergebnis, von dem die Entscheidung spricht, über eine andere und anders geschriebene Software zu gelangen, als zur Nachahmung geeignet betrachten und ihren Urheber als Nachahmer durch Bereitstellung der Mittel? Man kann sich ohne Mühe die außerordentliche Behinderung vorstellen, die das für die Softwareindustrie bedeuten würde. Man müßte also das Patentrecht „neu" lesen?

14. - In Wirklichkeit zeigt die letztere Beobachtung ebenso wie die vorhergehenden, daß die scheinbar natürliche Aufnahme der Erfindungen der Informatik in das Recht des geistigen Eigentums mit der Begründung, daß es sich um „geistige Werke" handelt, nicht nur den Effekt hat, diesem Rechtsgebiet eine neue Dimension zu geben, sondern auch dazu führt, es von innen heraus zu verändern. Es geht um eine variable Transformation, die man diskutieren kann: aber das muß mit Gründen geschehen, soweit es sich darum handelt, einen alten Begriff wie den der Originalität neu zu durchdenken. Im Falle der Entscheidungen des Europäischen Patentamtes scheint diese Transformation jedoch eher unkontrolliert zu verlaufen.

Der Sicherheit im EDV-Bereich erfordert eine perfekte Kontrolle der Systeme. Die Rechtssicherheit im Bereich der Informatik beziehungsweise des geistigen Eigentums setzt eine perfekte Kontrolle bei der Normgestaltung voraus. Dazu sollte hier ein kleiner Beitrag geleistet werden[30].

(übersetzt von J. Müller)

30 Für eine Vertiefung vgl. M. Vivant, The Challenge of Computer Law, im Erscheinen bei Kluwer, oder auf Französisch „Le 'défi' du droit de l'informatique, im Erscheinen bei „Editions de l'Université Autonome de Mexico".

Zur Terminologie im Bereich softwaretechnischer Dysfunktionen

Michael Schneider*

Fragen der Datensicherheit erlangen zunehmende Relevanz für den juristischen Bereich. Aufgrund dieser Tatsache wird es auch für Juristen erforderlich, sich mit Phänomenen auseinanderzusetzen, die diese Sicherheit gefährden. Dabei treten allerdings beträchtliche terminologische Probleme auf, von denen nachfolgend einige aufgezeigt werden sollen.

I. Datensicherheit im Recht

Noch vor wenigen Jahren standen datenschutzrechtliche Fragen im Mittelpunkt der juristischen Auseinandersetzungen mit Informationstechnik. Inzwischen greift die Erkenntnis Raum, daß der Datensicherheit als technischem Datenschutz kein geringerer Stellenwert beizumessen ist. Die Sicherheit eines Systems ist eine der Grundvoraussetzungen für die Durchsetzung von Regeln über die Verarbeitung personenbezogener Daten mittels automatisierter Verfahren.

Die Palette sicherheitsrelevanter Probleme beschränkt sich jedoch keineswegs auf den Datenschutz. Je komplexer und offener installierte Systeme werden, desto höher ist auch die Gefahr unerlaubter Eingriffe. Gleichzeitig wächst die Abhängigkeit von der Funktionsfähigkeit der einmal aufgebauten Datenverarbeitungs-Infrastruktur - in vielen Lebensbereichen ist die Informationstechnik unverzichtbar geworden; Fehlfunktionen oder Systemausfälle können unübersehbare Schäden verursachen. Spektakuläre Fälle von Computerspionage und -sabotage der letzten Zeit vermitteln einen Eindruck davon, wie empfindlich sich Schadensereignisse für die Betroffenen auswirken können und welcher Stellenwert daher künftig allein Phänomenen aus dem Bereich der Computerkriminalität zukommen wird.

Doch auch in der Rechtspraxis ergeben sich immer häufiger Probleme, deren Lösung nur unter Berücksichtigung sicherheitstechnischer Aspekte möglich ist. Das Spektrum der rechtsrelevanten Fragestellungen erstreckt sich von der Konzeption vertrauenswürdiger Telematik-Dienste und der hierfür notwendigen rechtlichen Rahmenbedingungen über Fragen, die sich bei der Nutzung neuer Kommunikationssysteme ergeben[1], bis hin zu einer Vielzahl von Praxisproblemen, deren Bezug zur Datensicherheit erst auf den zweiten Blick offenkundig wird[2].

Desweiteren werden Juristen durch den praktischen Einsatz der Informationstechnik, und sei es nur durch die Inanspruchnahme von Mehrwertdiensten wie Online-Datenbanken oder Mailbox-Systemen, mit denselben Problemen konfrontiert, wie Angehörige anderer Berufsgruppen. Mit der Installation von Computern am Arbeitsplatz wird der einzelne außerdem - je nach seinem Kenntnisstand - Anwender, Programmierer, Daten-Archivar odar gar System-Manager in einer Person. Dementsprechend haben sich auch Juristen dem Risikopotential zu stellen, das mit dem Einsatz der von ihnen verwendeten Datenverarbeitunsanlagen verbunden ist. Potentielle Schadensereignisse müssen abgeschätzt, Defizite lokalisiert und gegen erkannte, nicht akzeptable Risiken geeignete Gegenmaßnahmen ergriffen werden.

* Michael Schneider ist Mitarbeiter der Gesellschaft für Mathematik und Datenverarbeitung (GMD), Arbeitsgruppe Rechtsinformatik, Bonn

1 Bei allen geplanten Diensten und Netzen - derzeit insbesondere dem ISDN -ist die Frage zu stellen, wie gut ihre Nutzer vor Schaden geschützt sein werden. Ein Teilnehmer kann beispielsweise geschädigt werden, indem eine Dienstleistung für ihn mit Verzögerung oder überhaupt nicht erbracht, ihr Ergebnis verfälscht, oder ihm eine Kommunikationsbeziehung zugerechnet wird, die ohne sein Wissen oder seine Billigung aufgebaut wurde. Vgl dazu: JA. Pfitzmann / B. Pfitzmann / M. Waidner; Datenschutz garantierende offene Kommunikationsnetze, Informatik-Spektrum 1988, S. 118

2 Als Beispiel sei an dieser Stelle nur die Frage genannt, ob die Hinterlegung von Software unter Insolvenzgesichtspunkten überhaupt zweckmäßig erscheint, wenn man berücksichtigt, daß ein Softwareproduzent sowohl Motive wie auch Möglichkeiten hat, derartige Maßnahmen zu unterminieren. Vgl. dazu auch: F. Hoffmeister / M. Schneider; Technische Möglichkeiten zur Sabotage im Rahmen der Softwarehinterlegung. In: Software in der Insolvenz; D.J. Hildebrand / Th. Hoene (Hrsg.), Stuttgart 1989, S. 52

II. Terminologische Defizite

Die Bewältigung sicherheitstechnischer Probleme scheitert allerdings oftmals an der Komplexität der zugrundeliegenden technischen wie rechtlichen Materie. Die in diesem Zusammenhang auftretenden Sprach-schwierigkeiten zwischen Juristen, Organisations-Fachleuten und Informatikern werden aufgrund terminologischer Inkonsistenzen noch verschärft.

Dies gilt insbesondere im Bereich der Software-Sicherheit, denn hier sind die Risiken besonders schwer einschätz- und beherrschbar. Daher ist es auch nicht gelungen, ein einheitliches Klassifikationssystem für Fehlfunktionen von Software zu etablieren. Das führt dazu, daß vergleichbare Fehler nicht selten unter verschiedene Begriffe subsumiert werden oder aber derselbe Terminus für unterschiedliche technische Sachverhalte Anwendung findet. Im Rahmen der Namensgebung kann bereits dem politischen oder gesellschaftlichen Umfeld eines Betroffenen entscheidende Bedeutung zukommen. So mag der eine für „Widerstandssoftware" halten, was andere als „logische Bombe" bezeichnen. Desweiteren könnte der Betreiber einer DV-Anlage nachträgliche Programm-Manipulationen, die der Überwachung der Anwender dienen, als legitime Einwirkung sehen, während sich die Überwachten von einem „Zimmermann-Virus" betroffen fühlen[3].

Besonderen Zuspruchs erfreuen sich bei der Benennung von Software-Fehlfunktionen Begriffe aus Immunologie und Parasitologie. Der Grund dafür liegt in dem Umstand, daß Datenverarbeitungssysteme eine Reihe von Parallelen zu komplexen biologischen Systemen aufweisen. Dementsprechend wurden softwaretechnische Dysfunktionen in den letzen Jahren zunehmend mit Begriffen wie „Läuse", „Wanzen", „Würmer", „Viren" und „Bakterien" belegt. Das Repertoire der Analogien wird durch historische Auseinandersetzungs-Strategien ergänzt; aus diesem Bereich stammen die Ausdrücke „Trojanische Pferde" und „Falltüren".

1. Etablierte Begriffe

Die Bezeichnung Bugs - der englische Name für „Wanzen", der aber im DV-Zusammenhang auch mit „Läuse" übersetzt wird - gehört bereits zu den klassischen Homonymen, welche die Informationstechnik hervorgebracht hat. Bugs sind Programm- oder Programmierfehler im engeren Sinne.

Wird eine semantische Manipulation oder zusätzlicher Programmcode gezielt eingebracht, bezeichnet man die so veränderte Software als Trojanisches Pferd. Der Begriff geht auf Dan Edwards zurück[4]; erhat sich als Bezeichnung für geheimgehaltene Modifikationen oder Ergänzungen eines Programms, das neben den erklärten Leistungen zusätzliche Funktionen eines Angreifers oder Saboteurs erfüllt, durchgesetzt[5]. Falltüren (Trap Doors) repräsentieren eine spezielle Form Trojanischer Pferde; sie dienen dazu, Sicherheitsmechanismen eines Rechnersystems zu unterminieren. Zu diesem Zweck werden Prozeduren implementiert, die bei späterer Ausführung in einem privilegierten Systemzustand zumindest für die Dauer einer Operation die Kontrolle über den Rechner ermöglichen[6]. Stößt ein potentieller Angreifer eine derartige Routine an, kann er unter Umständen nachträglich in ein System eindringen und dort beliebige Manipulationen vornehmen.

Gleichwohl kann man solche Veränderungen, die zumeist am Source-Code vorgenommen werden, nicht als Fehler im technischen Sinne bezeichnen, denn die Zielvorgaben des Software-Ingenieurs decken sich durchaus mit dem tatsächlichen Verhalten des Programms. Aus rechtlicher Sicht hingegen stellen sich Funktionen, die dem Benutzer nicht bekannt sind, sehr wohl als Mangel dar[7]. Eine Ausnahme von dieser Regel ist allenfalls dann gegeben, wenn die gerügte Manipulation nachträglich und auf der Ebene des Object-Code realisiert worden ist. Derartiges ist mittels sogenannter „Computerviren" ohne weiteres machbar.

Als Computerviren bezeichnet man Programme, die nicht nur Funktionen einbringen, die dem Benutzer des betroffenen Systems verborgen bleiben; ein zweites wesentliches Merkmal liegt in ihrer Fähigkeit, sich selbst zu reproduzieren[8]. Computerviren besitzen darüberhinaus die Eigenschaft, Software zu „infizieren", d.h. sie binden eine - gegebenenfalls modifizierte (mutierte) - Kopie ihrer selbst in andere Programme ein[9].

Mit den genannten Fähigkeiten erschließen Computerviren eine neue Dimension des Gefährdungspotentials durch Software-Manipulation; dementsprechend erfreut sich das Thema seit den Experimenten von Fred Cohen[10] einiger Popularität. Seither wird auch die Bezeichnung „Computervirus" durchgängig für dasselbe Phänomen verwendet.

2. Weitergehende Klassifikation selbstreproduzierender Programme

Allerdings ist die Eigenschaft der Autoreproduktion weder auf Computerviren beschränkt, noch wäre nur ein Programmtyp denkbar, der die für Viren typischen Merkmale aufweist. Daher wurden in der Vergangenheit verschiedene Versuche unternommen, selbstreproduzierende Programme zu klassifizieren. Die Ansätze dazu sind vielfältig. In jüngster Zeit hat man häufig versucht, alle denkbaren Varianten selbstreproduzierender Sabotageprogramme auf den Virus-Begriff abzubilden; im Zuge derartiger Bemühungen sind Audrücke wie "Bootsektor"-, „Hardware"-, „Link"- oder „Live and Die"-Viren entstanden.
Mitunter wurden auch weitere Fachtermini aus dem biologischen Umfeld herangezogen; die bekanntesten Beispiele hierfür sind „Bakterien" und „Würmer".

3 Der Begriff „Zimmermann-Virus" wurde gelegentlich im Rahmen politisch motivierter Auseinandersetzungen benutzt. Er bezeichnet Virus-Programme (vgl. dazu die Ausführungen unter IL), mit deren Hilfe nachvollziehbar gemacht werden könnte, wann und wie oft ein Anwender auf bestimmte Software zugreift.

4 R.R. Linde; Operating System Penetration. In: Computers and Security; C.T. Dinardo (Edt.), New Jersey 1978, S. 85

5 Dabei ist allerdings zu beachten, daß einige Autoren das gesamte Programm, andere nur den Teil, der den zusätzlichen Programmcode beinhaltet, als „Trojanisches Pferd" bezeichnen.

6 G. Weck; Datensicherheit; Stuttgart 1984, S. 27

7 Zur Abgrenzung des technischen und rechtlichen Fehlerbegriffs vgl.: R.B. Abel; Fehlerhafte Software, RDV 1987, S. 212

8 Ein Programm heißt selbstreproduzierend, wenn es in der Lage ist, ein Doppel von sich selbst zu erstellen.

9 Das „befallene" Programm kann damit als Trojanisches Pferd betrachtet werden.

10 F. Cohen; Computer Viruses - Theory and Experiments; in: Computer Security: A Global Challenge; J.H. Finch, E.G. Dougall (Edt.); North-Holland 1984, S. 143

Als Bakterien werden dabei Programme bezeichnet, die kein „Wirtsprogramm" benötigen, sich im Übrigen aber verhalten, wie Computerviren[11].

Die Bezeichnung Wurm steht in einigen Publikationen für Programme, die sich in verteilten Systemen oder Rechnernetzen ausbreiten[12]. An anderer Stelle wird der Begriff hingegen für jede Form eigenständiger, selbstreproduzierender Programme benutzt[13]. Die letztgenannte Definition deckt sich demnach hinsichtlich ihres Bedeutungsgehaltes weitgehend mit der des Bakteriums.

III. Fazit

Obwohl sich einige der unter (II.2.) genannten Begriffe auf den ersten Blick geradezu aufzudrängen scheinen, ist bei ihrer Verwendung doch solange Vorsicht geboten, wie keine Definition für sie verfügbar ist, die allgemein als verbindlich betrachtet wird.

Zwar ist die Begriffsbildung bei den sogenannten „Würmern" noch vergleichsweise weit fortgeschritten: Während die Bezeichnung Bakterium sowie Neologismen auf der Basis des Viren-Begriffs erst in neuerer Zeit Verwendung finden, wurde der Terminus „Wurm" bereits in den 70er Jahren geprägt. Eine zunehmende Zahl von Angriffen auf Datennetze, von denen einige besonders spektakuläre mittels selbstreproduzierender Programme vorgetragen wurden[14], ließ den Begriff schließlich in den Mittelpunkt des öffentlichen Interesses rücken.
Im juristischen Sprachgebrauch sollte man sich dennoch besondere Zurückhaltung auferlegen. Aus technischer Sicht mag man terminologische Defizite akzeptieren; im Rahmen der juristischen Bewertung softwaretechnischer Phänomene können sich sprachliche und rechtliche Probleme dann jedoch leicht potenzieren.

11 Th. Dehn / W. Paul; Vorbeugung bei Computerviren, CR 1989, S. 68(69)
12 Vgl. statt vieler: K. Brunnstein; Über Viren, Würmer und anderes seltsames Getier in Computer-Systemen: ein kleines „Informatik-Bestiarium", Angewandte Informatik 1987, S. 397(399)
13 G. Hoffmann; „Wurm" im INTERNET, DuD 1989, S.63(64)
14 Ein derartiges Programm führte im November 1988 beispielsweise zum Zusammenbruch des Datenverkehrs im ARPANET. Interessant an diesem Fall ist unter anderem, daß die Ausbreitung des Wurms vermutlich durch die Existenz einer „Falltür" begünstigt wurde. Vgl. dazu auch die ausführliche Schilderung in: S. Weirauch; Der INTERNET-Wurm. Ein Programm erobert 6000 vernetzte UNIX-Rechner in zwei Tagen, Datenschutz-Berater 12/88, S. 1

„Technische Möglichkeiten zur kriminellen Einflußnahme auf Daten und Datenverarbeitung" (Teil 2)

Carsten Zobel

aa) Verbindung von Rechnern

Soll in ein fremdes Computersystem eingedrungen werden, so ist zunächst Bedingung, daß es sich bei dem jeweiligen Rechner nicht um ein „stand-alone"-Gerät handelt; es muß Zugangsmöglichkeiten zum Rechner geben. Diese sind oft in Form von Datenleitungen vorhanden. Denn wie oben unter den Begriffen Datenfernverarbeitung und Datenfernübertragung angesprochen, ist es oftmals erforderlich, daß unterschiedliche Computer, die an unterschiedlichen Orten stehen, Daten miteinander austauschen, miteinander „kommunizieren". Für diese „Kommunikation" zwischen Computern stehen sogenannte Netze zur Verfügung. Eines davon ist beispielsweise das Fernsprechnetz der Deutschen Bundespost; für die Datenfernübertragung in der Bundesrepublik werden allerdings meistens die sogenannten DATEX-Netze der Post verwendet 1). Bei der Benutzung unterscheidet man das DATEX-L- und das DATEX-P-Netz[46]. Das bundesweit gespannte DATEX-P-Netz ist zusätzlich mit anderen europäischen Netzen verbunden; diese wiederum ermöglichen durch entsprechende Verbindungen Kontakte zu amerikanischen Datennetzen[47]. Fraglich könnte nun sein, wie sich ein Täter Zugang zu einem solchen Datennetz verschafft. Die einfachste Möglichkeit besteht darin, sich über das Telefonnetz mittels eines Telefons Zugang zum DATEX-P-Netz (und damit zu anderen Netzen) verschaffen[48]: Computer, die am DATEX-P-Netz angeschlossen sind (hosts), können unter ihrer „Telefonnummer" der sogenannten NUA (Network User Adress) angerufen werden[49]. Dazu ist allerdings noch erforderlich, daß die jeweils vom Computer zu sendenden oder zu empfangenen Daten so umgewandelt werden, daß sie übers Telefonnetz übertragen werden können. Denn im Computer liegen die Daten in digitaler Form vor (d.h. als Folge von fließendem / nicht-fließendem Strom), das Telefonnetz überträgt jedoch analoge Signale. Die Umwandlung von -vereinfacht formuliert- Computerdaten in Töne erledigt ein Akustikkoppler oder ein Modem[50].

46) Freiberg, Chip-Special, S. 20
47) ein Überblick über die Vielzahl von Netzen bei Ammann/Lehnhardt, S. 215; Stahl, Computer-Buch, S. 54 ff.
48) Freiberg, Chip-Special, S. 23
49) Freiberg, Chip-Special, S. 24 f.
50) zur Funktionsweise vgl. Obermair, Chip-Special, S. 11 ff.