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.

Mit einer technischen Minimalkonfiguration von Telefon, -anschlüß, einem Computer und einem Akustikkoppler kann sich ein Täter also Verbindungen zu weltweit arbeitenden EDV-Anlagen herstellen[51].

bb) Eindringen in fremde Rechner

Auch wenn über die eben beschriebene Weise eine Verbindung zu anderen Computern hergestellt werden kann, so wird ein Zugriff auf die von diesem Computer verwalteten Daten in der Regel noch nicht möglich sein, ohne daß zuvor eine Zugangssperre überwunden wird. Als gebräuchlichste und bekannteste Sicherung kommt hier vor allem ein Paßwort in Betracht[52]. In das System kann ein Täter nur dann eindringen, wenn er dieses Paßwort kennt. Das Problem, ein Paßwort zu erfahren, stellt sich regelmäßig nicht als technisches Problem dar. Es ist zwar denkbar, ein Programm zu schreiben, daß mögliche Paßwörter mittels „trial and error" herausfinden soll; die Wirksamkeit eines solchen Programmes wäre aber äußerst zweifelhaft. Zum einen bestehen unzählige Kombinationsmöglichkeiten[53], zum anderen kommt hinzu, daß meist nach 3 Fehlversuchseingaben die Verbindung unterbrochen wird, d.h. nach jeweils 3 Versuchen müßte der jeweilige Rechner wieder angewählt werden. In Hackerkreisen (und wohl auch bei Computerspionen) sind daher andere Methoden beliebt, sich Zugang zu anderen Rechnern zu verschaffen. Diese haben aber nichts mehr mit technischer Einflußnahme zu tun, sondern stellen rein „organisatorische" Probleme dar[54], auf die hier nicht näher einzugehen ist.

cc) Technische Einflußnahmen im fremden Rechner

Ist trotz der eben beschriebenen Probleme ein Täter in einen fremden Rechner eingedrungen[55], dürfte es je nach Intention unterschiedliche Ziele geben. Ein Saboteur wird versuchen Daten unbrauchbar zu machen, indem er sie ändert oder löscht. Ein Spion hingegen wird sich durch die Daten über bestimmte Dinge informieren. Zusätzlich wird er jedoch versuchen, durch sein Eindringen keine Spuren zu hinterlassen. Weiterhin wird er sich bemühen, andere Zugangsmöglichkeiten, d.h. andere Paßwörter zu erfahren.

(1) Verändern / Löschen von Daten

Zunächst muß zum oben Gesagten ergänzend hinzugefügt werden, daß Paßwörter nicht nur den Sinn haben, Unberechtigte vom Zugriff auf Daten auszuschließen. Auch die Zugriffsmöglichkeiten von Berechtigten können regelmäßig durch die Paßwörter eingeschränkt werden. Man spricht in diesem Zusammenhang von System-Privilegien[55]. Die Problematik sei vereinfacht an einem Beispiel dargestellt. Der Betreiber einer EDV-Anlage möchte, daß Sachbearbeiter X die gespeicherten Daten nur lesen, nicht aber ändern oder löschen darf. Für das Paßwort des X, z. B. „ABC", wird vom Verantwortlichen nun in einer Tabelle als Privilegkennung ein „R" (vom englischen „read") eingetragen. Wird das Paßwort „ABC" eingegeben, so prüft das Betriebssystem in der System-Tabelle die Privilegien des Benutzers und läßt nur die dort gefundenen Zugriffsweisen zu. Der Computersaboteur, der mittels des Paßwortes „ABC" in das System eingedrungen ist, hat so anfangs nur die Möglichkeit, Daten zu lesen. Da es ihm aber um das Ändern und Löschen geht, muß er das jeweilige Systemprivileg ändern. Dies ist technisch möglich oder nicht, je nachdem, was für ein Betriebssystem verwendet wird. Durch einen Fehler war eine solche Änderung im Betriebssystem VMS V4.2 beispielsweise durchführbar[56]. Allerdings sind für die Änderung detaillierte Kenntnisse des jeweiligen Betriebssystems nötig.

(2) Verdecken / Sichern des Zugangs

Ebenfalls recht detaillierte Kenntnisse des jeweils benutzten Betriebssystems sind notwendig, um das Eindringen in fremde Systeme zu verdecken, bzw. um das wiederholte Eindringen durch „Sammeln" von zusätzlichen Paßwörtern zu ermöglichen. Da die Verfahren sich im Detail bei unterschiedlichen Betriebssystemen unterscheiden, werden auch diese Fälle nur verallgemeinernd und vereinfacht dargestellt. Zum Verdecken von Spuren ist zu sagen, daß die jeweils sich „im Rechner befindlichen" Anwender durch Betriebssystem-Aufrufe angezeigt werden können. Einem Kenner des Betriebssystems kann es jedoch möglich sein, Änderungen vorzunehmen, die Bewirken, daß ein bestimmter Anwender nicht mehr angezeigt wird. Ein Beispiel soll die verdeutlichen: In einer Systemvariable stehen die Nummern 1, 3 und 7. In einer bestimmten Tabelle ist hinterlegt, daß sich hinter diesen Nummern die jeweiligen Paßwörter verbergen. Durch ein Systemprogramm können diese Informationen miteinander verknüpft und die Benutzer angezeigt werden. Der Täter, der nun in der Lage ist, „seine" Nummer aus der Systemvariable zu entfernen, wird bei einer eventuellen Kontrolle nicht angezeigt werden[57]. Um weitere Paßwörter zu erfahren, könnte der Täter zunächst die Anzeige der sogenannten Paßwortdatei bewirken. Dies ist eine Datei, in der die jeweiligen Paßwörter gespeichert sind und die vom System benötigt wird, um zu überprüfen, ob ein bestimmtes Paßwort zum Zugang berechtigt. Allerdings ist anzunehmen, daß die Paßwörter in dieser Datei verschlüsselt hinterlegt sind. Ist eine Entschlüsselung nicht möglich oder ist der technische Aufwand unverhältnismäßig hoch, werden sogenannte „Trojanische Pferde"[58] benutzt. Auch diese Form der technischen Einflußnahme sei hier nur sehr vereinfacht anhand eines Beispiels beschrieben. Möchte der berechtigte Benutzer X mit seinem Paßwort „ABC" in den Rechner „hinein", so wählt er diesen an. Der Rechner startet ein Log-In-Programm: Es erscheint eine Eingabemaske, eine Art Bildschirmformular, in die X sein Paßwort eingibt. Anschließend wird der Zugriff erteilt. Vertippt sich X bei der Eingabe, was leicht möglich ist, da diese nicht angezeigt wird, so erscheint eine Fehlermeldung und die Eingabeprozedur wiederholt sich. Dies kann sich nun ein Täter zunutze machen. Er schreibt ein Programm, das die gleiche Eingabemaske bietet, wie das System. Der Täter schleust dieses Programm in den Rechner ein und veranlaßt das Betriebs

51) Zur Vollständigkeit: Da ein DATEX-P-Zugang kostenpflichtig ist, benötigt der Täter zusätlich eine von der Bundespost (für 15 DM im Monat) vergebene NUI (Network User Identification); vgl. dazu auch B. II. 1) b) dd)
52) Leicht, iur 87, S. 50
53) ein achtstelliges Paßwort, daß sich nur aus den Ziffern 0 bis 9 zusammensetzt, läßt bereits 10^8 = 100.000.000 Kombinationsmöglichkeiten zu
54) Möglichkeiten Paßwörter zu erfahren sind im Ansatz dargestellt bei Ammann/Lehnhardt, insbesondere S. 84 („Sammeln" von Paßwörter auf Messen und Vorführungen) und S. 87 f. (Aushorchen von Mitarbeitern)
55) Stahl, Computer-Buch, S. 88 f.
56) Stahl, Computer-Buch, S. 88 f., dort auch die erforderlichen Betriebssystem-Befehle
57) zum Verändern von Systemvariablen vgl. Müller-Maguhn/Schrutzki, Computer-Buch, S. 39
58) Uepping, DVR 85, S. 343

system, sein Programm statt des Log-In-Programmes zu starten. Auch im Täterprogramm erfolgt zunächst die Abfrage wie beim „echten" Log-In-Programm. Allerdings wird das eingegebene Paßwort nun nicht verschlüsselt und mit der Paßwortdatei verglichen, sondern es wird in eine Datei des Täters geschrieben. Nach der Paßworteingabe wird die Fehlermeldung, die das Originalprogramm für Falscheingaben bereithält angezeigt; der Anwender wird regelmäßig glauben, sich vertippt zu haben. Anschließend wird das „echte" Log-In-Programm gestartet[59]. Der Täter kann nun die „gesammelten" Paßwörter aus seiner Datei lesen.

dd) Verwendung einer fremden NUI

Ein Problem nicht technischer Art sei hier nur vollständigkeitshalber kurz erwähnt, da es mit der eben beschriebenen Thematik eng zusammenhängt: die Verwendung fremder NUIs. Die NUI (Network User Identification) ist die Benutzerkennung, über die die Deutsche Bundespost die Gebühren für die Nutzung des DATEX-P-Netzes abrechnet. Sollte jemand die (eigentlich geheime) NUI eines anderen nutzen, so können beträchtliche Schäden entstehen[60].

2) Zerstörung von Daten

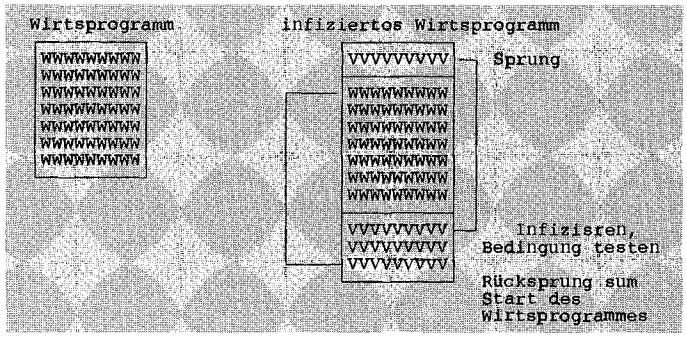
Eine besondere Form der technischen Einflußnahme auf Daten stellt die Zerstörung derselben durch speziell dafür geschriebene Programme dar. Bei diesen Programmen werden regelmäßig Sabotageprogramme und als eine Sonderform Virusprogramme (Computerviren) unterschieden[61].

a) Sabotageprogramme

Ein Sabotageprogramm ist ein Programm, das eine bestimmte Zerstörung hervorruft, sobald eine vom Programmierer festgelegte Bedingung erfüllt ist. Die ist programmtechnisch nicht sonderlich schwer zu bewältigen. So ist es beispielsweise möglich, daß in einem Programm ein Zählervariable verwendet wird, in der gespeichert ist, wie oft dieses Programm gestartet wird. Möchte der Programmierer, daß sein Programm höchstens dreimal gestartet werden kann, weil er es anderen nur zu Demonstrationszwecken überlassen hat, so braucht er beim dritten Aufruf nur eine entsprechende Programmroutine ablaufen zu lassen, die sein Programm vom Datenspeicher löscht. Diese Löschroutine kann allerdings auch andere Befehle enthalten; ein rachesüchtiger Programmierer könnte ebenso die Löschung anderer Daten veranlassen. Eine andere Möglichkeit bietet sich dem Programmierer über den Zeitvergleich. Bei vielen Computern werden Datum und Uhrzeit intern gespeichert; bei einigen Personal Computern müssen diese Daten beim Start eingegeben werden (das ist zwar nicht zwingend, vielfach erfordern es jedoch die eingesetzten Programme). Der Programmierer hat nun die Möglichkeit, das jeweilige Systemdatum abzufragen, es mit einem vorgegebenen Termin zu vergleichen und bei Übereinstimmung eine entsprechende Zerstörung von Daten einzuleiten[62],[63].

b) Computerviren[64]

Computerviren, auch die Bezeichnung Virusprogramme ist gebräuchlich, stellen -gegebenenfallseine Sonderform der Computersabotage dar[65].



Einnisten eines Virusprogrammes in einem Wirtsprogramm (vgl. Radelow/Merkl, Chip 7/88, S.88)

aa) Eigenschaften von Virusprogrammen

Computerviren sind Programme, die durch zwei typische Eigenschaften gekennzeichnet sind[66]: Die erste Eigenschaft ist die Fähigkeit, sich selbst zu kopieren und in andere Programme einzupflanzen (self reproduction). Die zweite Eigenschaft besteht darin, unter einer bestimmten vom Programmierer festgelegten Voraussetzung eine vorher definierte Aufgabe auszuführen (functionality). Besteht diese Eigenschaft in der Zerstörung/ Modifikation von Daten, so ist ein solches Programm den Fällen der Computersabotage zuzuordnen.

bb) Funktion von Virusprogrammen

Ein Virusprogramm wird gestartet durch den Aufruf des infizierten „Wirtsprogrammes". Es werden dann folgende Funktionen ausgeführt[67]: Zunächst werden auf einem Speichermedien bestimmte -vom Programmierer im Virusprogramm beschriebene- Programme gesucht. Der Virus überprüft zunächst, ob das gefundene Programm schon infiziert ist. Ist dies der Fall, dann wird geprüft, ob die Auslöse-Bedingung erfüllt ist. Ist dies der Fall wird die entsprechende Aufgabe, z. B. das Löschen von Daten, ausgeführt. Anderenfalls wird das gestartete „Wirtsprogramm" abgearbeitet. Das neu infizierte Programm wird nunmehr beim Starten den Virus wieder weiterverbreiten. Technisch anspruchsvoller sind Viren, die sich von ihrem „Wirtsprogramm" lösen und im Arbeitsspeichers (dem RAM) eines Computers „versteckt" werden. Die Vorgehensweise entspricht der oben dargestellten. Abweichend erfolgt bei diesen speicherresidenten Viren jedoch kein Zugriff auf Speichermedien, sondern die jeweils vom Anwender gestarteten Programme werden überprüft und gegebenenfalls infiziert. Durch den Fortfall des Zugriffs auf die Speichermedien ist dies Verfahren vor allem schneller.

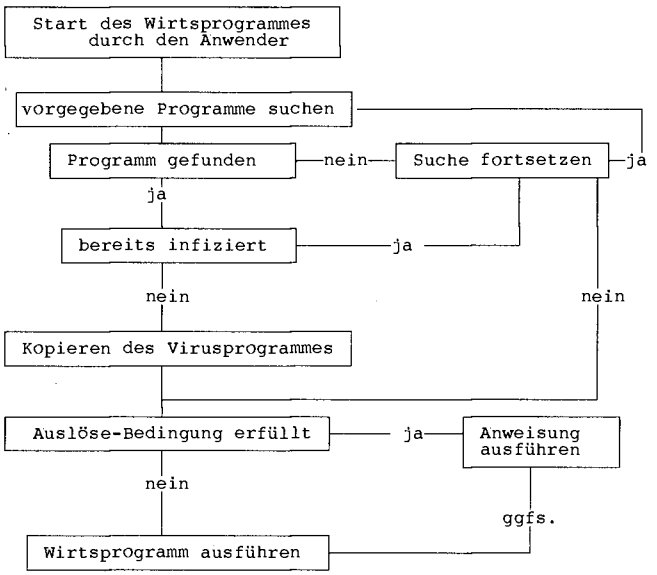
59) Sabotage—Müller-Maguhn/Schrutzki, Computer-Buch, S. 40
60) Fälle und Zahlen bei Lehnhardt, Computer-Buch, S. 101; Obermair, Chip-Special, S. 87
61) Volesky/Scholten, iur 87, S. 286 f.
62) So in den Fällen bei Sieg, Jura 86, S. 359 Volesky/Scholten, iur 87, S. 287
63) Da sich das Sabotageprogramm oftmals erst auswirkt, wenn der Täter zum externen Personenkreis gehört, scheint die systematische Einordnung an dieser Stelle sinnvoll.
64) vgl. ergänzend grafische Darstellung im Anhang
65) Volesky/Scholten, iur 87, S. 287
66) Lehnhardt, Computer-Buch, S. 77 Sperber, mc 7/88, S. 74 Volesky/Scholten, iur 87, S. 287 f.
67) Lehnhardt, Computer-Buch, S. 78 Volesky/Scholten, iur 87, S. 287

cc) Erstellung von Viren

Die Programmierung von Viren ist technisch relativ einfach, zumal selbst ungeübte Programmierer Virusprogramme aus Fachzeitschriften abtippen können[68]. Außerdem gibt es (zumindest ein) Programm, mit dessen Hilfe selbst derjenige, der keine Programmierkenntnisse besitzt, Computerviren erstellen kann[69].

dd) Verbreitung von Virusprogrammen

Eine Verbreitungsmöglichkeit besteht durch die Datenfernübertragung. Ein Virus kann nämlich so programmiert sein, daß er die Liste, in der die jeweils angeschlossenen Rechner gespeichert sind, liest und sich anschließend selbst an die so gefundenen Adressen „verschickt"[70]. Auch über Raubkopien oder kostenlos abgegebene Programme (sog. Public Domain Software) verbreiten sich Viren. Schließlich soll es auch vorkommen, daß sich Softwarehäuser durch das Einarbeiten von Computerviren in ihre kommerzielle Software vor Raubkopien schützen[71].



Funktion eines Virusprogrammes

2) Zusammenfassung

Da der externe Personenkreis das für den internen Personenkreis so vorteilhafte Wissen hinsichtlich der betrieblichen Organisation nicht hat, werden externe Täter eher auf Formen der technischen Einflußnahme zurückgreifen als Interne. Dabei sind Möglichkeiten der technischen Einflußnahme auf Daten und EDV für den externen Personenkreis grundsätzlich recht vielgestaltig. Inwieweit eine jeweilige Einflußmöglichkeit jedoch tatsächlich realisierbar ist, hängt wesentlich von einzelnen Schutzmechanismen ab.

```
IDENTIFICATION DIVISION.

PROGRAM-ID. RUNDUNGSTRICK.
AUTHOR. ZOBEL CARSTEN.
DATE-WRITTEN. 11-06-88.

ENVIRONMENT DIVISION.

CONFIGURATION SECTION.
SOURCE-COMPUTER. PC1512.
OBJECT-COMPUTER. PC1512.
SPECIAL-NAMES.
    DECIMAL-POINT IS COMMA.

DATA DIVISION.

WORKING-STORAGE SECTION.

77  AUSGANGSZINSEN                 PIC 99V999.
77  OFFIZIELLES-ZINS-KONTO         PIC 99999999V999.
77  KUNDEN-ZINS-KONTO              PIC 99999999V999.
77  TAETER-ZINS-KONTO              PIC 99999999V999.
01  ERTEILTE-ZINSGUTSCHRIFTEN.
    05  KUNDEN-ZINSEN              PIC 99V99.
    05  DRITTE-STELLE              PIC 9.
77  HILFS-VARIABLE                 PIC 9V999.
77  AUSGABE                        PIC ZZZ.ZZZ.ZZ9,999.

PROCEDURE DIVISION.

PROGRAMM-BEGINN.
    DISPLAY " " ERASE.
    MOVE 4,586 TO AUSGANGSZINSEN.
    PERFORM UMBUCHUNGS-ROUTINE.
    DISPLAY "Ergebnisse bei einem Duchlauf:"  LINE 5
                                              POSITION 1.
    MOVE OFFIZIELLES-ZINS-KONTO TO AUSGABE.
    DISPLAY "   Offizielles Zinskonto    : "  LINE 7
                                              POSITION 1.
    DISPLAY AUSGABE POSITION 0.
    MOVE KUNDEN-ZINS-KONTO TO AUSGABE.
    DISPLAY "   Kundenzinsen             : "  LINE 9
                                              POSITION 1.
    DISPLAY AUSGABE POSITION 0.
    MOVE TAETER-ZINS-KONTO TO AUSGABE.
    DISPLAY "   Taeterzinsen             : "  LINE 11
                                              POSITION 1.
    DISPLAY  AUSGABE POSITION 0.
PROGRAMM-ENDE.
    STOP RUN.

UMBUCHUNGS-ROUTINE.
    ADD AUSGANGSZINSEN TO OFFIZIELLES-ZINS-KONTO.
    MOVE AUSGANGSZINSEN TO ERTEILTE-ZINSGUTSCHRIFTEN.
    ADD KUNDEN-ZINSEN TO KUNDEN-ZINS-KONTO.
    DIVIDE DRITTE-STELLE BY 1000 GIVING HILFS-VARIABLE.
    ADD HILFS-VARIABLE TO TAETER-ZINS-KONTO.
```

COBOL-Programm zur Demonstration des Rundungstrick-Falles

68) Soft-Beispiele bei Krabel, c't 4/87, S. 108 ff.; Koziel/Leister, c't 7/88, S. 72 ff.
69) Radelow/Merkl, Chip 7/88, S. 84; Sperber, mc 7/88, S. 77
70) Sperber, mc 7/88, S. 76; Volesky/Scholten, iur 87, S. 288 aktuelles Beispiel in der FAZ vom 7.11.88 „Ein ‚Wurm' legte Tausende von Computern lahm"
71) Radelow/Merkl, Chip 7/88, S. 84