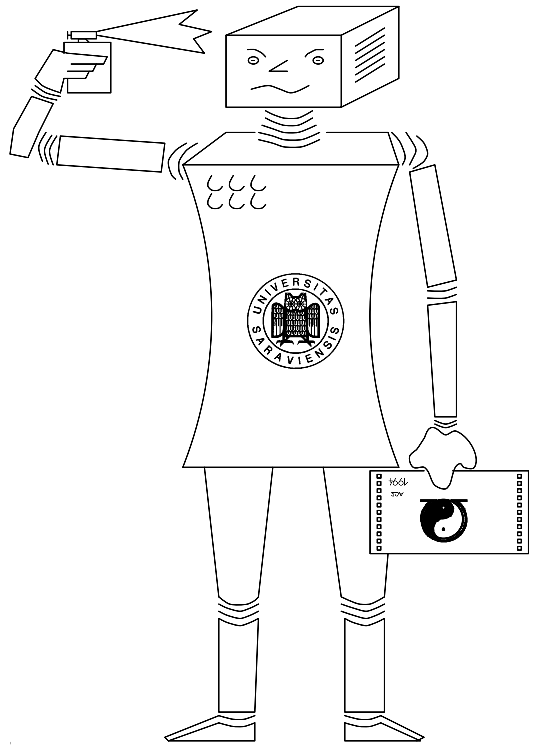
UNIVERSITÄT DES SAARLANDES
FACHBEREICH INFORMATIK
D-66041 SAARBRÜCKEN
GERMANY
WWW: http://js-sfbsun.cs.uni-sb.de/pub/www/



Beherrschbarkeit von Computersystemen

Manfred Kerber and Axel Präcklein (eds.)

Published as: Script of a seminar, Summer 1989, Fachbereich Informatik,
Universität Kaiserslautern, Kaiserslautern, Germany
The missing pictures can be sent on request.

Beherrschbarkeit von Computersystemen

Skript zum Seminar, Sommersemester 1989

Herausgeber:
Manfred Kerber, Axel Präcklein

Fachbereich Informatik, Universität Kaiserslautern
D-6750 Kaiserslautern, West Germany

Inhalt

Vorwort

Dieses Skript enthält die Vortragsausarbeitungen des Seminars „Beherrschbarkeit von Computersystemen“, das im Sommersemester 1989 vom Fachbereich Informatik der Universität Kaiserslautern veranstaltet wurde.

Das Seminar ist das vierte in einer Reihe, die von wissenschaftlichen Mitarbeitern und Studenten betreut wird. Die Idee dazu entstand bei der Arbeit im FIFF (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung).

Die elf Vorträge des Seminars behandeln sechs verschiedene Aspekte der Beherrschbarkeit von Computersystemen.

Ohne hinreichende Datenschutzgesetzgebung entwickelt die computerisierte Industriegesellschaft immer subtilere Überwachungsmechanismen. Der erste Vortrag erläutert die momentane rechtliche Lage im Hinblick auf die bundesdeutschen Datenschutzgesetze unter den gewachsenen technischen Möglichkeiten. Es wird ein historischer Rückblick gegeben und auf die sehr schwachen internationalen Regelungen eingegangen. Der zweite Vortrag behandelt die Sicherheitsgesetze und die polizeiliche Datenverarbeitung. Dabei werden die eigentlich erforderlichen Einschränkungen der Befugnisse von Polizei und Geheimdiensten den geplanten neuen Sicherheitsgesetzen gegenübergestellt.

Eine völlig neue Dimension der Überwachung am Arbeitsplatz entsteht durch die Nutzung der Möglichkeiten von Personalinformationssystemen. Sie erreichen Ausmaße, die das Bild vom gläsernen Arbeitnehmer beziehungsweise den Eindruck der totalen Überwachung des Menschen am Arbeitsplatz entstehen lassen. Im ersten der drei diesem Thema zugeordneten Vorträge werden die Personalinformationssysteme vorgestellt und geklärt, welche Daten dort gespeichert werden und was das für Folgen nach sich zieht. Dabei wird die Vorgehensweise der Arbeitgeber bei der Einführung dieser Systeme analysiert. Der nächste Vortrag beleuchtet die Folgen von Personalinformationssystemen für den einzelnen Arbeitnehmer. Schwerpunkte sind dabei der Rationalisierungseffekt, die Personalbeurteilung auch aufgrund von Tests sowie die Stellung des Betriebsarztes. Im letzten Vortrag des Themenbereichs ‚Personaldaten im Betrieb‘ werden die rechtlichen Handlungsmöglichkeiten des betrieblichen Datenschutzbeauftragten und des Betriebsrates im Bereich der Personalinformationssysteme dargelegt. Insbesondere werden Notwendigkeit und Möglichkeiten von Betriebsvereinbarungen diskutiert.

Computerkriminalität scheint auf den ersten Blick nicht jeden zu gefährden, doch dieser erste Blick trügt. Im ersten Vortrag dieses Blockes geht es um Computerviren. An Beispielen wird ihre Funktionsweise und die Anfälligkeit von vielen Systemen gegenüber Viren vorgestellt. Außerdem wird auf Herkunft und Schutzvorkehrungen gegen Viren eingegangen. Der zweite Vortrag umfaßt den Bereich Wirtschaftskriminalität. Insbesondere wird ausgearbeitet, was im Zusammenhang mit Rechnern an Sabotage, Spionage und Diebstahl möglich ist und ermöglicht wird. Dies hat zu einer Erweiterung der Strafgesetze geführt, da viele Paragraphen auf die neue Technik nicht anwendbar waren.

‚Sicherheit von und mit Computersystemen‘ ist der vorletzte Themenbereich überschrieben. Im ersten Vortrag werden Schutzmechanismen für Speicher, Prozesse und Dateien vorgestellt. Weiterhin wird auf die Probleme der Sicherheit von sensitiven Einzeldaten in statistischen Datenbanken eingegangen. Im zweiten Teil beschäftigt sich dieser Vortrag mit der Verschlüsselung und Entschlüsselung von Daten, wobei ein Überblick über die gängigen Methoden gegeben wird. Der zweite Vortrag führt die Begriffe Sicherheit und Zuverlässigkeit von Programmen ein, gibt einen Überblick über die Techniken, um Software so zu erstellen, daß sie möglichst sicher ist, und erläutert, welche Faktoren dazu führen, daß auch die so erstellten Computersysteme nie so sicher sein können, wie das in den Prospekten der Hersteller zu lesen ist. Der dritte Vortrag dieses Abschnitts macht uns mit Simulationsmethoden bekannt und erläutert, wie diese klassifiziert werden und wie die fünf Phasen einer Simulation ablaufen. Insbesondere wird auf die Probleme bei der wichtigen Validierungsphase eingegangen.

Der einzige Vortrag des letzten Block macht uns mit der tödlichsten Bedrohung bekannt, die von Computersystemen ausgeht, dem ‚Krieg aus Versehen'. Der Einsatz hochkomplexer computergestützter Frühwarn- und Entscheidungssysteme bringt enorme Gefahren mit sich. Es kommt dabei recht häufig zu Fehlalarmen bis zur höchsten Stufe, die teilweise auch dokumentiert sind. Zusammenfassend wird auf die Möglichkeiten zur Verhinderung eines solchen Krieges aus Versehen eingegangen. Desweiteren werden militärische Zukunftsprojekte wie SDI, präzisionsgelenkte Munition und Kampfroboter besprochen.

Die Teilnehmer des Seminars haben sich durchweg mit viel Engagement in die entsprechende Thematik eingearbeitet und gut aufbereitete Vorträge gehalten. In der an die Vorträge anschließenden Diskussion zeigte sich oft eine außergewöhnliche Detailkenntnis.

Hans-Jürgen Bürckert
Bernhard Gramlich
Manfred Kerber
Anne Mahn
Axel Präcklein
Detlef Schneider
Hans-Georg Schwinn
Rolf Socher-Ambrosius

Teil I

Datenschutz

Kapitel 1

Datenschutz – rechtliche Lage

Heiko Dotzauer

1.1 Woher kommt und was bedeutet eigentlich Datenschutz?

1.1.1 Historischer Abriß

In den USA gab es bereits Anfang bis Mitte der 60er Jahre die ersten Veröffentlichungen und die ersten öffentlichen Diskussionen über Datenschutz. Ausschlag dafür war der Vorschlag einer Kommission der Yale-Universität. Hierin wurde der Regierung der Aufbau einer **nationalen Datenbank** empfohlen. Dabei sollten aus den Datenbeständen mehrerer Großcomputer Bürgerdaten zusammmengeführt werden. Über jeden Einwohner würde dann ein persönlicher Datensatz angelegt, auf den die Behörden dann Zugriff von *der Wiege bis zum Grab* hätten [97]. Dieses Projekt wurde in der amerikanischen Öffentlichkeit sowie in den Ausschüssen des Senats und des Repräsentantenhauses sehr kontrovers erörtert. Die meisten der Argumente in der Diskussion, die damals formuliert wurden, werden auch heute noch, in gleicher oder ähnlicher Form, vorgebracht. Grob gesagt standen damals wie heute die Interessen der Statistiker und Budgetplaner dem Schutz der Individualrechte gegenüber. Im Laufe der Diskusion konkretisierten sich bereits die Anforderungen, denen ein ausreichender Datenschutz gerecht werden müßte. So forderte z.B. ein amerikanischer Rechtsprofessor eine unabhängige Überwachungsbehörde für Datenzentren, sowie ein prinzipielles Verbot der Speicherung „bestimmter Arten" von Daten [17, S.74]. Jahre später tauchten auch in der Bundesrepublik Pläne für eine „Superdatenbank" auf. Hierbei handelte es sich um ein sogenanntes **Informationsbankensystem**. Aus einem weitgehend gemeinsamen Datenbestand sollten sowohl Staat als auch Wissenschaft und Wirtschaft, sowie der einzelne Bürger Informationen gewinnen [17, S.75]. Dieses deutsche und auch das amerikanische Modell scheiterten. Jedoch ließen die Planungen, sowie die sich immer mehr häufenden Berichte über unmäßiges Datensammeln und Datentauschen (so speicherte z.B. in den USA ein Kreditinstitut Merkmale wie Homosexualität in ihren Kundendatenbeständen und gab diese auch weiter), schließlich den Ruf nach datenschutzrechtlichen Regelungen immer lauter werden. So begannen in der BRD bereits Ende der 60er Jahre die Vorbereitungen für ein bundesweites Datenschutzgesetz. Als weltweit erstes Land erließ dann 1970 Hessen ein Datenschutzgesetz für die Landesregierung. Im selben Jahr wurden in den USA und in Schweden jeweils ein Gesetz über Datenschutz im Kreditwesen verabschiedet. 1973 wurde, ebenfalls in Schweden, ein Datenschutzgesetz, das unter anderem auch die Einrichtung einer Dateninspektion vorsah, ratifiziert. Dieser Einbau des Datenschutzes in die rechtlichen Grundfeste hat sich seither immer weiter verbreitet (1988 der Privacy-Act in Australien), und zeigt sich auch gelegentlich schon im internationalen Bereich. So hat der Europarat 1981 ein Datenschutzabkommen „Zum Schutz des Einzelnen unter besonderer Berücksichtigung der automatisierten Verarbeitung personenbezogener Daten" ausgearbeitet, welches von der BRD 1985 ratifiziert wurde. Es hat sich also seit den (Alp-)Träumen von der „Superdatenbank" einiges getan, um den „Big Brother" im Zaum zu halten. Wie diese gesetzlichen Regelungen in der BRD zur Zeit aussehen, wie sie realisiert werden, und inwieweit sie den Anforderungen der modernen Informationsgesellschaft gerecht werden, wird im folgenden dargestellt bzw. untersucht. Vorweg jedoch erst einmal eine Begriffsbestimmung.

1.1.2 Begriffsbestimmung

Recht auf informationelle Selbstbestimmung bedeutet: Jeder soll grundsätzlich selbst entscheiden können, wie er sich der Öffentlichkeit gegenüber darstellen will, und ob und inwieweit von Dritten über seine persönlichen Daten verfügt werden kann. Unter **Datenschutz** verstehen wir: Regelungen für die Verarbeitung von personenbezogenen Daten. Erstes Ziel des Datenschutzes sollte der *Schutz des Rechtes auf informationelle Selbstbestimmung* sein. Unter **Datensicherung** faßt man zusammen: Technische Maßnahmen und Einrichtungen zum Schutz der Daten (DIN 44300). Im folgenden werden wir uns hauptsächlich mit Datenschutz befassen. **Bereichsspezifische Regelungen** sind: Gesetzliche Regelungen, die den Datenschutz in bestimmten, eng umgrenzten Bereichen regeln (z.B. im Arbeitsrecht, im Steuerrecht). **Automatisch betriebene Dateien** sind Datensammlungen, die durch automatisierte Verfahren, das heißt Verfahren, die mit Hilfe programmgesteuerter Geräte ablaufen, umgeordnet und ausgewertet werden.

1.2 Gegenwärtige Rechtslage

1.2.1 Datenschutz allgemein

Daten wurden schon lange vor dem Einsatz rechnergestützter Dateninformationssysteme gesammelt und ausgewertet. Die Gefahr des Mißbrauchs ist also nicht erst durch die modernen Systeme entstanden, sondern hat sich nur durch diese verstärkt. Es gab daher auch schon Vorschriften über die Handhabung personenbezogener Informationen, lange bevor der Begriff Datenschutz überhaupt existierte. Beispiele hierfür sind die ärztliche Schweigepflicht oder das Steuergeheimnis. Im folgenden interessieren uns jedoch hauptsächlich die speziell auf die *modernen Dateninformationssysteme* abgestimmten Datenschutzregelungen.

1.2.2 Struktur des Datenschutzrechts

Bei der Betrachtung des Datenschutz müssen wir drei Bereiche unterscheiden, den **öffentlichen**, den **privaten** und den **kirchlichen** Bereich. Neben den bereichsspezifischen Regelungen innerhalb der drei Gebiete gelten folgende Zuständigkeiten: Das **BundesDatenSchutzGesetz** regelt den Datenschutz im privaten Sektor und in der Bundesverwaltung. Die Länder regeln in den **LandesDatenSchutzGesetzen** jeweils den Datenschutz in der entsprechenden Landesverwaltung. Das BDSG und die LDatGe sind von ihrem Selbstverständnis her **Auffangnetze** und finden daher nur dann Anwendung, wenn keine einschlägigen spezielle Rechtsnormen anzuwenden sind. Das heißt: besteht in einem Sachverhalt Deckungsgleichheit zwischen Bundes(Landes)DSG und einer bereichsspezifischen Regelung, so findet das Bundes(Landes)DSG keine Anwendung. Sind die Sachverhalte nicht deckungsgleich, so finden beide Vorschriften Anwendung oder ergänzen sich.

Die Kirchen haben nach dem Grundgesetz das Recht, ihre Angelegenheiten „innerhalb der Schranken des für alle geltenden Gesetzes“ selbständig zu ordnen und zu verwalten (Art.140 GG in Verbindung mit Art.137 Abs.3 der Weimarer Reichsverfassung). Der Datenschutz wird als solche „eigene Angelegenheit“ angesehen. Daher hat der Gesetzgeber darüber keine staatlichen Vorschriften erlassen, sondern nur festgelegt, unter welchen Voraussetzungen die Behörden Daten an kirchliche Stellen übermitteln dürfen. Es existieren allerdings *kircheninterne Regelungen* im Kirchengesetz, sowie Anordnungen über den kirchlichen Datenschutz. Diese Regelungen sind sowohl bei der katholischen, als auch bei der evangelischen Kirche stark an das BDSG angelehnt.

1.2.3 Kontrollinstanzen des Datenschutzes

Zu jedem der oben angeführten drei Bereiche existieren außerdem **Kontrollinstanzen**, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt worden zu sein. Hierbei gilt für die Zuständigkeit:

- Der **Bundesbeauftragte für den Datenschutz** ist zuständig für die Behörden der Bundesverwaltung und die sonstigen öffentlichen Stellen des Bundes. (Dieses Amt bekleidet zur Zeit Dr. Einwag)

- Die **Landesbeauftragten für den Datenschutz** sind zuständig für die Behörden der Landesverwaltung und die sonstigen öffentlichen Stellen jeweils ihres Landes. (In Rheinland-Pfalz wird der Datenschutzbeauftragte zur Zeit noch durch die Datenschutzkommission ersetzt. Dies soll jedoch in der Novellierung des LDatG geändert werden.)
- Der **kirchliche Beauftragte für den Datenschutz** ist zuständig für die kirchlichen Verwaltungsstellen.
- Die **Aufsichtsbehörden der Länder** sind zuständig für alle nichtöffentlichen Stellen in ihrem örtlichen Zuständigkeitsbereich. (in Rheinland-Pfalz: Hier ist die oberste Aufsichtsbehörde das Ministerium des Innern und für Sport in Mainz, die regional zuständigen Aufsichtsbehörden sind die Bezirksregierungen Koblenz, Trier bzw. Rheinhessen-Pfalz. [85, S.60])

1.2.4 Die Bedeutung des Volkszählungsurteils für den Datenschutz

Mit dem Volkszählungsurteil des Bundesverfassungsgerichts setzten die Karlsruher Richter einen wichtigen Wegweiser für künftige Verfahrensweisen bei statistischen Erhebungen. Sie reagierten damit auf eine Vielzahl von Verfassungsklagen aus der Bevölkerung, die das Volkszählungsgesetz 83 betrafen. Dabei ging es vor allem um die Melderegisterberichtigung (Dabei sollten aus der Volksbefragung gewonnene Informationen zur „Auffrischung“ der Daten in den Melderegistern benutzt werden.) und um Datenlieferungen an die Gemeinden und Gemeindeverbände zu Zwecken, die nicht mehr in den Bereich der Statistik fielen (Umweltschutz, gemeindliche Planung, Vermessungswesen). Obwohl ein ausdrückliches „Nachteilsverbot“ verhindern sollte, daß aus den Angaben des Volkszählungsbogens gewonnene Erkenntnisse gegen den einzelnen Auskunftspflichtigen verwendet werden würden, hielt das Bundesverfassungsgericht diese Verfahrensweise nicht für zulässig. Nach seiner Auffassung verstieße dieses Vorgehen gegen die verfassungsrechtliche Festschreibung des Grundsatzes, daß statistische Einzelangaben nicht für Verwaltungsaufgaben ausgewertet werden dürfen. In Fortführung der Rechtsprechung zum Volkszählungsgesetz nahm das Bundesverfassungsgericht erstmals zu allen grundlegenden Problemen des Datenschutz Stellung und formulierte wesentliche Leitsätze. In diesen wurde das Recht auf informationelle Selbstbestimmung zum Ausgangspunkt jeglichen Datenschutzes erklärt. Jedoch wurde auch gesagt, daß die Herrschaft des einzelnen über „seine“ Daten unter dem Aspekt der Gemeinschaftsbezogenheit einschränkbar ist. Nach Ansicht des ehemaligen Bundesdatenschutzbeauftragten Hans Peter Bull ist „mit dem Volkszählungsurteil eine schwierige Phase in der Geschichte des Datenschutz zu einem guten Ende gekommen.“

1.3 Die wesentlichen Inhalte des BDSG

Das BDSG gliedert sich in **sechs Abschnitte**, die hier, mit ein paar erläuternden Worten, vorgestellt werden sollen. Dabei beinhaltet der erste Abschnitt die **allgemeinen Vorschriften**, der zweite betrifft den **Datenschutz im öffentlichen Bereich**, der dritte und vierte im **nichtöffentlichen Bereich**, der fünfte regelt die **Straf- und Bußgeldvorschriften** und der letzte schließlich die **Übergangs- u. Schlußvorschriften** [BDSG vom 27. Januar 1977 zuletzt geändert am 18. Februar 1986].

1.3.1 Allgemeine Vorschriften

Hier werden u.a. *Aufgabe und Gegenstand des Datenschutzes, sowie die Rechte des Betroffenen* aufgeführt:

§1 (1) „Aufgabe des Datenschutzes ist es, durch den **Schutz personenbezogener Daten** vor Mißbrauch bei ihrer **Speicherung, Übermittlung, Veränderung** und **Löschung** (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken.“

Neben diesem sind im ersten Abschnitt vor allem die §§2, 3 und 4 interessant. In §2 wird der Begriff **Datei** definiert, nämlich „eine gleichartig aufgebaute Sammlung von Daten, nach bestimmten Merkmalen erfaßt und geordnet, ..., **ungeachtet der dabei angewendeten Verfahren**“. Das BDSG legt sich also nicht auf die rechnergestützte Datenverarbeitung fest, sondern hat den Begriff Datei möglichst weit gefaßt. Dies ist ein wichtiges Detail, da dadurch ein eventueller Rückzug auf manuell geführte Dateien, um Datenschutzbestimmungen zu umgehen, von vorneherein ausgeschlossen werden soll. Jedoch scheint auch dieser, schon recht allgemein gehaltene Dateibegriff, noch nicht ausreichend zu sein, wie wir bei der Diskussion um die Novellierung des BDSG später sehen werden. In §3 wird die Zulässigkeit der Datenverarbeitung festgeschrieben. Danach ist die Verarbeitung personenbezogener Daten nur zulässig, wenn:

1. „es dieses Gesetz oder eine andere Rechtsvorschrift erlaubt oder“
2. „der Betroffene eingewilligt hat.“

Dies bedeutet, daß prinzipiell alles verboten ist, was nicht ausdrücklich erlaubt wird! Es gibt jedoch eine ganze Reihe von Erlaubnisnormen, und wir werden daher später sehen, was im Endeffekt wirklich verboten ist. In §4 wird schließlich gesagt, was nun die Rechte des Betroffenen, also im Normalfall des Bürgers, sind:

1. „**Auskunft** über die zu seiner Person gespeicherten Daten, ...“
2. „**Berichtigung** der zu seiner Person gespeicherten Daten, ...“
3. „**Sperrung** der zu seiner Person gespeicherten Daten, ...“
4. „**Löschung** der zu seiner Person gespeicherten Daten, ...“

(Anmerkung: die Rechte 2, 3 bzw. 4 treten jeweils dann in Kraft, wenn die Daten unrichtig sind, sich weder deren Richtigkeit noch deren Unrichtigkeit feststellen läßt, die Speicherung unzulässig war, oder nach Wegfall der ursprünglich erfüllten Voraussetzungen für die Speicherung.) Zum ersten Punkt, dem Recht auf Auskunft, läßt sich noch folgendes bemerken:

Der Landesbeauftragte für den Datenschutz führt ein Register über die automatisch betriebenen Dateien der Landesverwaltung, der Kreise, Ämter, Gemeinden und sonstigen öffentlichen Stellen. Es enthält Angaben darüber, welche Art von Daten erfaßt und an wen diese weitergegeben werden. Dieses Register ist für Jedermann zur Einsicht frei. Desgleichen wird bei der Aufsichtsbehörde für den Datenschutz ein Register über die nicht-öffentlichen Stellen, die Datenverarbeitung für fremde Zwecke betreiben (z.B. Auskunftsdateien, private Rechenzentren) geführt. Dieses enthält ebenfalls Angaben über die Art der von diesen Unternehmen verarbeiteten Daten und über die Empfänger der Daten. Auch dieses Register ist zur Einsichtnahme frei. Anhand dieser Register kann man feststellen, wo möglicherweise Daten über einen gespeichert sind. Den genauen Dateninhalt kann man dann gezielt durch Geltendmachung seines Auskunftsrechts gegenüber der entsprechenden Stelle erfragen. Einige Dateien sind von dieser Regelung ausgenommen, so z.B. Datensammlungen im Zusammenhang mit der Verbrechensbekämpfung und Steuerfahndung, sowie des Verfassungsschutzes. Auch dies ist ein weiterer Reibungspunkt, dem wir ebenfalls in der Novellierungsdiskussion wieder begegnen werden.

1.3.2 Datenverarbeitung der Behörden und sonstiger öffentlicher Stellen

Neben den Vorschriften über die **Datenverarbeitung bei Behörden** regelt dieser Abschnitt auch **Bestellung und Aufgabenbereich des Bundesbeauftragten für den Datenschutz**. Von besonderem Interesse sind in diesem 2. Teil des BDSG die §§9 bis 11, die die Datenspeicherung und Datenübermittlung betreffen. Darin heißt es unter anderem:

- „Das Speichern ... personenbezogener Daten ist zulässig, wenn es zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist.“ (§9, Abs.1)
- „Werden Daten beim Betroffenen auf Grund einer Rechtsvorschrift erhoben, dann ist er auf sie, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen.“ (§9, Abs.2)
- „Die Übermittlung personenbezogener Daten ... ist zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist.“ (§10)

Durch diese Paragraphen sollen vier wichtige Prinzipien verwirklicht werden. Im Einzelnen sind dies das der **Erforderlichkeit**, der **Zweckbindung**, der **Durchschaubarkeit** und der **informationellen Gewaltenteilung**. Es genügt nämlich nach §9.1 nicht, daß die Daten für die Aufgabenerfüllung förderlich sind, sondern sie müssen wirklich unverzichtbar sein (Prinzip der **Erforderlichkeit**). Ebenso wird durch diese Paragraphen das Sammeln von Daten für *noch nicht bestimmte Zwecke* untersagt (**Zweckbindung**). §9.2 verpflichtet die Behörden dazu dem Bürger mitzuteilen, aufgrund welcher Regelung er seine Daten preisgeben **muß** (z.B. Mikrozensus, Volkszählung, usw.), oder ob er sie nur freiwillig preisgeben **soll**. Damit wird der Sinn der Datenerhebung für den Befragten zumindest **durchschaubar**, wenn vielleicht auch nicht immer verständlich. Dadurch, daß jede Behörde nur die zu ihrem unmittelbaren Aufgabenbereich gehörigen Daten speichern und verarbeiten darf, wurde das wichtige Prinzip der **informationellen Gewaltenteilung** realisiert (Das Gegenstück dazu wäre eine bei einer Behörde untergebrachte zentrale Datenbank, die natürlich einen wesentlich umfangreicheren und detailierteren Datensatz pro Bürger hätte, vergleichbar dem Informationsbankensystem, von dem im ersten Kapitel die Rede war). Als Beispiel für eine Regelung, die das Prinzip der informationellen Gewaltenteilung realisiert, sei hier kurz folgendes angeführt: Die Verfassungsschutzämter, denen polizeiliche Befugnisse ausdrücklich untersagt sind, dürfen sich auch keine Daten von der Polizei verschaffen, die mittels solcher Befugnisse gewonnen wurden. Sie dürfen deshalb solche Daten auch nicht speichern [97, S.115]. Ein weiterer wichtiger Paragraph dieses Abschnittes ist §11. Er regelt den *Datentransfer von öffentlichen Stellen zu nicht-öffentlichen Stellen.* Dieser ist prinzipiell zulässig, wenn er „zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgabe erforderlich ist“ (z.B. bei der Vergabe eines Forschungsauftrages an ein privates Marktforschungsinstitut). Er ist aber auch gestattet, falls der „Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Unterliegen die personenbezogenen Daten einem Berufs- oder besonderem Amtsgeheimnis, ..., ist für die Zulässigkeit ferner erforderlich, daß die gleichen Voraussetzungen gegeben sind, unter denen sie die zur Verschwiegenheit verpflichtete Person übermitteln dürfte.“ Danach darf z.B. eine Gemeindeverwaltung die Anschriften von Einwohnern einem Adreßbuchverlag überlassen. Die Versorgungsämter jedoch dürfen Krankengeschichten, Befunde und Diagnosen nur weitergeben (z.B. an das Gesundheitsamt), wenn auch der Arzt zu einer solchen Weitergabe befugt bzw. verpflichtet wäre (z.B. bei einer besonders ansteckenden Krankheit nach dem Bundesseuchengesetz).

Die §§17-21 dieses Abschnittes regeln die Bestellung und den Aufgabenbereich des Bundesbeauftragten für den Datenschutz. Dieser gilt als besondere Kontrollinstanz, ist jedoch ohne Weisungsbefugnis. Nach §19.2 kontrolliert er *„... die Einhaltung der Vorschriften dieses Gesetzes* (BDSG) *sowie anderer Vorschriften über den Datenschutz“. „Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen“* (§17.4). Organisatorisch ist er der Bundesregierung zugeordnet, sein Amt liegt beim Bundesminister des Inneren. Er ist der Dienstaufsicht des Innenministers und der Rechtsaufsicht der Bundesregierung unterstellt (§17.5). Diese Dienstaufsicht betrifft jedoch nur das persönliche Rechtsverhältnis zum Bund, es wird also nicht kontrolliert wie der Beauftragte arbeitet, sondern geregelt werden lediglich seine gesetzlichen Ansprüche auf Gehalt, Urlaub usw. Die Unterstellung unter die Rechtsaufsicht der Bundesregierung bedeutet, daß bei Streit über die Rechtmäßigkeit von Amtshandlungen des Beauftragten die Bundesregierung ihre Rechtsauffassung verbindlich aussprechen kann, also keine gerichtliche Auseinandersetzung zwischen dem Beauftragten und der Regierung stattfinden soll. Vertritt jedoch der Bundesbeauftragte in einer Beanstandung eine Rechtsmeinung, die die Bundesregierung für rechtlich falsch hält, hat er auf jeden Fall das Recht, sie zu äußern. Rechtmäßigkeit bedeutet also nur Zulässigkeit und nicht etwa inhaltliche Richtigkeit. So ist es rechtmäßig, wenn (in einem fiktiven Fall) der Datenschutzbeauftragte etwa sagt, ein Betroffener habe das Recht, zu erfahren, was in einer Akte des MADs über ihn gespeichert sei. Nicht rechtmäßig aber wäre es, wenn der Beauftragte nach einer eventuellen Akteneinsichtnahme beim MAD diesen Inhalt dem Betroffenen mitteilen würde. Beanstandungen des Bundesbeauftragten sind für die Bundesregierung nicht verbindlich. Werden Vorschläge nicht beachtet, so bleibt ihm nur der Weg, sich an das Parlament und an die Öffentlichkeit zu wenden. Die fehlende Weisungsbefugnis ist jedoch keineswegs als ein Manko zu verstehen. So ist z.B. der frühere Datenschutzbeauftragte Hans-Peter Bull der Ansicht, daß *„die unabhängigen Datenschutzbeauftragten mit ihren Mitteln, vor allem der internen wie öffentlichen Erörterung der Probleme, mehr erreicht haben, als manche andere Stelle mit rechtlich viel stärkeren Befugnissen.“* [17, S.129]

Die Tätigkeit des Bundesbeauftragten für den Datenschutz wird teils durch Eingaben und Beschwerden von Bürgern ausgelöst, teils aus eigener Initiative systematisch geplant. Dabei ist von besonderem Interesse der §21 **über die Anrufung des Bundesbeauftragten für den Datenschutz:**

„Jedermann kann sich an den Bundesbeauftragten für den Datenschutz wenden, wenn er **der Ansicht ist**, bei der Verarbeitung seiner personenbezogenen Daten ... in seinen Rechten verletzt worden zu sein." Der Bürger soll also seine Meinung vorbringen, der Beauftragte muß daraufhin prüfen, ob diese Meinung rechtlich zutrifft. Hierbei ist es für den Bürger nicht nötig, irgendwelche begründeten oder gar bewiesenen Verdachtsmomente vorzubringen, es genügt, daß er der Ansicht ist, in seinen Rechten verletzt worden zu sein.

1.3.3 Datenverarbeitung nicht-öffentlicher Stellen

Bei den Datenschutzregeln für den nicht-öffentlichen Bereich werden grundsätzlich dieselben Prinzipien verwirklicht, wie bei denen für die öffentlichen Stellen. Allerdings wurden die Begriffe im Bereich der Zweckbindung etwas anders gefaßt. So heißt es hier in §23(25):

„Das Speichern (Verändern) personenbezogener Daten ist zulässig im Rahmen der **Zweckbestimmung eines Vetragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses** mit dem Betroffenen oder soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden." So dürfen z.B. Versicherungsgesellschaften Daten an ihre Rückversicherer übermitteln, da ja ein Vertragsverhältnis zwischen Versicherungsnehmer und Versicherungsinstitut besteht und außerdem die Weitergabe zur Wahrung der Interessen des Versicherers nötig sein kann. Auch ist es den speichernden Stellen prinzipiell erlaubt, Daten zur Auswertung an Forschungsinstitute weiterzugeben.

Das Auskunftsrecht im nicht-öffentlichen Bereich wird durch die Paragraphen 26(34) geregelt. Hier wird im Unterschied zum Auskunftsrecht bei öffentlichen Stellen den Betreibern der Dateien zusätzlich auferlegt, einen Betroffenen darüber zu informieren, wenn erstmals zu seiner Person Daten gespeichert werden.

1.3.4 Straf- und Bußgeldvorschriften

Die Straf- und Geldbußenandrohungen des BDSG sind mäßig. Die maximale Freiheitsstrafe, die danach verhängt werden kann, liegt bei zwei Jahren, das maximale Bußgeld bei fünfzigtausend DM. Der Gesetzgeber war beim Erlaß dieser Vorschriften wohl der Meinung, daß im Falle des Datenschutzes die Rechtfertigungspflicht gegenüber Vorgesetzten, Datenschutzbeauftragten und Öffentlichkeit ein besseres *Abschreckungsinstrument* darstellt, als die herkömmlichen Strafnormen. (Außerhalb des BDSG existieren allerdings seit einiger Zeit weiterreichende Strafnormen wie z.B. zum *Ausspähen von Daten (§202a StGB), zur Fälschung beweiserheblicher Daten (§269 StGB)* oder zur *Datenveränderung (§303a StGB).*

1.4 Schwachstellen des Datenschutzes, Novellierung des BDSGs

Im Jahre 1986 wurde von den Fraktionen der CDU/CSU und der FDP ein Gesetzesentwurf zur Änderung des Datenschutz-Rechts in den Deutschen Bundestag eingebracht. Eine parlamentarische Beratung des Entwurfs fand allerdings nicht statt. 1987 wurde dann ein weiterer Anlauf unternommen und eine leicht geänderte Neufassung dieses Entwurfs vorgestellt, die inhaltlich weitgehend und vielfach sogar wörtlich dem ersten Entwurf entsprach. Im letzten Jahr nun (1988) verabschiedete die Bundesregierung den Entwurf eines Artikelgesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes, in dem außer dem genannten Entwurf auch die Entwürfe der sogenannten Sicherheitsgesetze (Bundesverfassungsschutzrecht, MAD-Gesetz, BND-Gesetz) zusammengefaßt sind. Mit diesem Novellierungsentwurf sollen wesentliche Lücken im Datenschutzrecht gestopft werden. Er enthält jedoch auch eine ganze Reihe von Neuerungen, die nicht nur von Seiten der Opposition, sondern vor allem auch aus den Reihen der Datenschutzbeauftragten heraus, heftig kritisiert werden. Eine Auswahl der wichtigsten Themen des Entwurfs soll im nun folgenden kurz diskutiert werden.

1.4.1 Der Dateibegriff

Anstoß zur Kritik am bestehenden Datenschutzrecht gibt häufig der im BDSG definierte Begriff der Datei (vgl. oben). So bemängelte z.B. der Bundesdatenschutzbeauftragte Dr. Baumann in seinem 10. Bericht, daß dieser Begriff nicht auf neue Techniken, wie z.B. der Bildverarbeitung (Videoaufzeichnungen), vorbereitet sei. Ebenfalls nicht berücksichtigt sei die Entwicklung zu billigen Massenspeichern, die es heute erlaube, Dokumente wie Rechnungen oder Pläne, z.B. auf einer Bildplatte zu speichern. Die Datenorganisation könne dabei so gestaltet werden, daß der Dateibegriff des Gesetzes nicht erfüllt würde, das Gesetz also keine Anwendung fände, obwohl die Risiken für den Betroffenen zumindest vergleichbar seien.

Auch die Tatsache, daß Akten häufig nicht durch den Dateibegriff erfaßt werden, erregt Kritik. Der Bundesdatenschutzbeauftragte Dr. Einwag forderte die Miteinbeziehung von Akten unter den Dateibegriff, da es für den betroffenen Bürger keinen Unterschied mache, ob etwa unzulässig erhobene Daten in Dateien oder Akten erfaßt und daraus verarbeitet werden. Außerdem sei bei der modernen Kommunikations- und Informationstechnik eine nicht mehr trennbare Vermengung zwischen automatisierter Datenverarbeitung und Aktenbearbeitung gegeben. Nach dem Novellierungsentwurf soll nun der **Datenschutz für die Verarbeitung und Nutzung** (von personenbezogenen Daten) **außerhalb von Dateien** im **Verwaltungsverfahrensgesetz** geregelt werden. Diese Regelung stößt jedoch auf Kritik, da wesentliche Verwaltungsbereiche den Schutzvorschriften nicht unterliegen. So ist z.B. in der Finanzverwaltung, bei der Post, bei der Verfolgung von Straftaten und Ordnungswidrigkeiten und in weiten Bereichen der Sozialverwaltung das Verwaltungsverfahrensgesetz nicht gültig. Dr. Baumann ist hier der Ansicht, das eine Einbeziehung der Datenverarbeitung außerhalb von Dateien in das BDSG diese Schwierigkeit beseitigen und zugleich zur Rechtsvereinheitlichung beitragen würde.

1.4.2 Personal-Computer und Datennetze

Als völlig unzureichend stellt sich das derzeitige Datenschutz-Recht im Bezug auf den zunehmenden Einsatz der PCs heraus. Hier ist ein Benutzer häufig zugleich Programmierer, Datenverarbeiter und *Datenschützer*. Er ist relativ auf sich allein gestellt, und wird daher versuchen „seine Aufgaben“ möglichst effektiv zu lösen. Wer will da noch prüfen, ob der Benutzer für die jeweiligen Aufgaben auch nur die erforderlichen und nicht vielleicht auch ein paar nur nützliche Daten verarbeitet hat? Auch dem Datenmißbrauch für private oder sonstige Zwecke steht hier prinzipiell kaum noch etwas im Wege.

Ebenso werden die Entwicklung der Datenübertragung und der Bildung von Datennetzen, weder im bestehenden Datenschutz-Recht noch in der bevorstehenden Novellierung, ausreichend berücksichtigt. So wird noch nicht einmal verlangt, daß die datenverarbeitenden Stellen eine Übersicht über die interne Vernetzung und über die eingerichteten Datenübertragungsmöglichkeiten von und zu anderen Stellen führen müssen. Durch die technischen Möglichkeiten (Online-Verbindung) ist Verarbeitung von Daten aus fremden Beständen fast so einfach wie die eigener Daten. Auch hier fehlt es an Bestimmungen über die Weiterverarbeitung der so erhaltenen Daten.

1.4.3 Pauschales Auskunftsverweigerungsrecht bei BND und MAD

Dieses Verweigerungsrecht wird häufig im Widerspruch zu Artikel 19 Absatz 4 GG gesehen („Wird jemand durch die öffentliche Gewalt in seinen Rechten verletzt, so steht ihm der Rechtsweg offen“). Auch hier wäre eine Regelung besser, wie sie z.B. im Polizeibereich praktiziert wird, d.h. eine Abwägung des Interesses der Betroffenen an der Auskunftserteilung gegen die Geheimhaltungsinteressen der Behörden. Dies ist zumindest die Ansicht von Dr. Baumann und Dr. Einwag. Der Regierungsentwurf sieht für die Verfassungsschutzbehörden, den BND, den MAD und „andere Behörden des Bundesministeriums für Verteidigung“ weiterhin ein pauschales Auskunftsverweigerungsrecht ohne Begründungszwang vor.

Zum Abschluß dieses Kapitels hier noch ein paar Äußerungen von Datenschutz-Beauftragten zum Gesetzesentwurf. So schreibt z.B. Dr. Einwag im 11. Tätigkeitsbericht: *„Die von mir zu zahlreichen Regelungen des Entwurfs formulierte Kritik und meine Anregungen zu seiner Verbesserung im Sinne des Datenschutzgesetzes sind jedoch in keinem bedeutsamen Punkt aufgegriffen oder berücksichtigt worden.“* Zu einem ähnlich negativen Ausblick, diesmal in Bezug auf die Novellierung der Landesdatenschutzgesetze, gelangte auch die Landesbeauftragte für den Datenschutz in Baden-Württemberg Dr. Ruth Leutze. In ihrem Bericht meint sie abschließend: *„... wird* *sich die Landesregierung den umstrittenen Bundesentwurf ..., den nicht einmal das Bundeskabinett geschlossen trägt, zum Vorbild nehmen, oder wird sie ... einen Gesetzesentwurf konzipieren, der das Grundrecht auf Datenschutz ... umfassend sichert"*. Und Dr. Einwag noch einmal zusammenfassend: *„Im Ergebnis entspricht der Entwurf ... nicht den Erwartungen. Er erweckt insbesondere gegenüber vergleichbaren Länderregelungen den Eindruck, einer Besorgnis vor zu viel Datenschutz und vor der Kontrolltätigkeit des Bundesbeauftragten. Es ist dringend zu wünschen, daß die bestehenden Mängel im Laufe des Gesetzgebungsverfahrens noch behoben werden"*.

1.5 Datenschutz im internationalen Bereich

Die Internationalisierung wirtschaftlicher Tätigkeit und die Intensivierung internationaler Zusammenarbeit führen zu einem schnellen Anwachsen der Übermittlung von Daten über staatliche Grenzen. Obwohl nur ein Bruchteil dieser Daten personenbezogen ist, entsteht gerade beim Transfer ins Ausland die Gefahr der Beeinträchtigung des Rechts auf informationelle Selbstbestimmung. Dieser Gefahr wird sowohl auf nationaler, als auch auf internationaler Ebene zu begegnen versucht. Dabei haben die **nationalen Gesetzgeber** den grenzüberschreitenden Datenfluß höchst unterschiedlich geregelt: Einige Datenschutz-Gesetze gehen gar nicht auf ihn ein (USA, Neuseeland, Australien, Kanada), andere sehen gewisse materiellrechtliche Beschränkungen vor (BRD, Dänemark, Israel) oder erweitern den Anwendungsbereich ihres Datenschutz-Gesetzes über das nationale Territorium hinaus (Luxemburg, Österreich), wieder andere haben Lizenzierungsverfahren eingerichtet (Schweden, Norwegen). Die beiden für eine Normierung des Datenschutzrechts wohl interessantesten Modelle sind dabei das Lizenzierungssystem und das materiellrechtliche Modell.

- Beim **Lizenzierungssystem** bedarf der grenzüberschreitende Datenfluß einer Genehmigung durch die dafür zuständige Lizenzierungsbehörde. Dadurch wird der Datenexport (eventuell auch der Datenimport) grundsätzlich untersagt, kann aber durch eine Erlaubnis (Lizenz) im Einzelfall genehmigt werden. Dieses System wird durch das Erfordernis einer eigenen Behörde und des daraus resultierenden bürokratischen Aufwands in seiner Leistungsfähigkeit beeinträchtigt.
- Das **materiellrechtliche Modell** erlaubt die grenzüberschreitende Übermittlung personenbezogener Daten nur dann, wenn im Empfängerland Bestimmungen vorhanden sind, die den im Inland geltenden Prinzipien zum Schutz der Privatsphäre und zur Sicherung der Betroffenenrechte entsprechen. Der hauptsächliche Nachteil dieses Modells ist es, daß oft nur schwer feststellbar ist, ob die Voraussetzungen für einen Export erfüllt sind.

Die Schwierigkeiten der nationalstaatlichen Regelung haben die Datenschutz-Debatte schon relativ früh auf die Tagesordnung supranationaler Institutionen wie der OECD (Organisation für ökonomische Zusammenarbeit und Entwicklung), dem Europarat, der UNESCO und der Europäischen Gemeinschaft geführt. Jedoch konnten auch hier bislang keine entscheidenden Anstöße für eine Regelung des grenzüberschreitenden Datenflusses gegeben werden. Insbesondere die bereits verabschiedeten Übereinkommen der OECD und des Europarats bleiben hinter dem Niveau eines Großteils der nationalen Bestimmungen zurück. Der freie internationale Informationsfluß (*free flow*) wird in ihnen zu sehr gestärkt und die Bedrohung der Privatsphäre spielt lediglich eine untergeordnete Rolle. So darf ein Vertragsstaat nach der Europarats-Konvention nicht *„allein zum Zweck des Schutzes des Persönlichkeitsbereiches den grenzüberschreitenden Verkehr personenbezogener Daten in das Hoheitsgebiet eines anderen Vertragspartners"* verbieten, oder von einer besonderen Genehmigung abhängig machen. Jedoch sind Abweichungen hiervon zulässig, wenn z.B. eine Umgehung des nationalen Rechts verhindert werden soll. Das Europäische Parlament hingegen hat in einer *Entschließung zum Schutz der Rechte des Einzelnen angesichts der fortschreitenden technischen Entwicklung auf dem Gebiet der Datenverarbeitung* im März 1982 wesentlich strengere Bestimmungen gefordert, vor allem eine nationale Anmelde- und Genehmigungspflicht für den Betrieb von Datenbanken. Eine entsprechende Richtlinie der EG ist allerdings noch nicht beschlossen. Alles in allem verläuft also die internationale Harmonisierung des Datenschutzrechts etwas schleppend. Zwar haben inzwischen achtzehn von zwanzig Mitgliedern des Europarats die Konvention gezeichnet (außer der Schweiz und Liechtenstein), doch liegt die Anzahl der Mitgliedsstaaten, die die Konvention ratifiziert haben, erst bei acht (Österreich, Frankreich, BRD, Luxemburg, Norwegen, Spanien, Schweden, GB). „Von dem Ziel, in Europa –

und möglichst darüber hinaus – einen definierten Mindeststandard des Datenschutz zu garantieren und im gleichen Zuge spezifische Behinderungen des grenzüberschreitenden Datenverkehrs auszuschließen, sind wir damit nach wie vor weit entfernt“ [34].

1.6 Datenschutzrecht und neue Technologien

Anhand eines einzelnen Beispiels (des Funktelefons) soll nun noch kurz gezeigt werden, wie leicht es in unserem Zeitalter beständigen technischen Fortschritts möglich ist, daß sich Neuerungen rasant auf breiter Front durchsetzen, aber die zugehörigen datenschutzrechtlichen Regelungen nur langsam hinterherhinken. Das Beispiel wurde dem 11. Tätigkeitsbericht des Bundes-Datenschutz-Beauftragten entnommen [34, S.30].

Den Funktelefondienst der Deutschen Bundespost nutzen bislang etwa 130.000 Teilnehmer. Diese werden nicht anhand des Funkgerätes oder des Fahrzeuges, indem es installiert ist, erkannt, sondern durch Daten aus der sogenannten Berechtigungskarte, die zentral für die BRD erstellt und den Teilnehmern zugeschickt wird. Kennzeichnendes Merkmal für einen Teilnehmer am Funktelefondienst ist die Funktelefonnummer. Ein Teilnehmer wird über die Berechtigungskarte vom System erkannt, wenn die Karte in den Kartenleser des Funktelefons eingeführt wird, was den Vorgang des *Einbuchens* einleitet. Hierbei wird in der jeweilig zuständigen Funkvermittlungseinrichtung (FuVE) der DBP ein Datensatz angelegt, aus dem hervorgeht, daß dieser Teilnehmer „auf Empfang“ ist. Dabei wird auch die Nummer der Funkzelle gespeichert, in der sich der Teilnehmer gerade aufhält. Als Funkzelle wird dabei ein regionaler Bereich bezeichnet, der z.B. in Ballungsräumen recht klein sein kann, und daher den Standpunkt des Benutzers entsprechend genau beschreibt. Führt ein Teilnehmer nach erfolgreichem Einbuchen ein Gespräch, entsteht ein Verbindungsdatensatz, in dem nach Beendigung des Gespräches u. a. die folgenden Daten gespeichert bleiben:

- Funktelefonnummer,
- Rufnummer des angerufenen Teilnehmers,
- Angaben über Zeitpunkt, Dauer und Gebühreneinheiten des Gespräches,
- Angaben der Funkzellen, in denen die Verbindung aufgebaut und beendet wurde, sowie die
- Anzahl der Funkkanalwechsel.

Diese Registrierungen erfolgen, mit entsprechenden Einzelangaben, wie „Gesprächsdauer: 0 Sek.“, auch für Verbindungen, die z.B. wegen Nichtmelden des Angerufenen nicht zustande kamen. Für ankommende Gespräche wird ein ähnlicher Datensatz angelegt; lediglich die Telefonnummer des Anrufers fehlt. Die anfallenden Verbindungsdaten werden im Rechner der jeweils regional zuständigen FuVE auf Platten gespeichert. Diese Rechner sind durch ein bundesweites Datennetz miteinander verbunden, wodurch der Zugriff auf einen Teil der dort gespeicherten Daten einer Vielzahl weiterer Stellen eröffnet wird. Dr. Einwag stellte dazu fest: „Im Rahmen der Kontrolle konnte nicht abschließend geklärt werden, auf welche Daten die etwa 45 Datenterminals sowohl bei den Fernmeldeämtern im ganzen Bundesgebiet als auch beim Fernmeldetechnischen Zentralamt (FTZ) im einzelnen zugreifen können und mit welcher Aufgabenstellung die Erforderlichkeit des Zugriffs begründet wird. Insbesondere wurde nicht klar, durch welche Aufgabenzuweisungen an die entsprechenden Referate des FTZ die Erforderlichkeit des Zugriffs auf teilnehmerbezogene Daten begründet wird und auf welche Daten im einzelnen diese Zugriffsmöglichkeit sich erstreckt“. Das Funktelefon ist sicherlich nur eins von mehreren möglichen Beispielen (BTX, Videotext, ...) und betrifft auch „nur“ 130.000 Mitbürger direkt, trotzdem zeigt es, wie dringend notwendig neue Datenschutzregelungen gerade im Bereich der neuen Medien und Massenkommunikationsmittel sind.

1.7 Zusammenfassung

Abschließend kann man wohl sagen, daß der Datenschutz in der Bundesrepublik, und im wesentlich stärkerem Maße im internationalen Bereich, noch längst nicht den Anforderungen einer modernen Informationsgesellschaft gerecht wird. Gerade die heute rasant verlaufende Entwicklung der neuen Medien mit ihren immer größer werdenden und immer stärker verflochtenen Netzen machen neue Datenschutzregelungen und Datenschutzkontrollmöglichkeiten dringend erforderlich. Wenn wir auch nicht in der Gefahr eines „1984“ schweben, so sollten wir doch im nationalen wie auch im internationalen Bereich jede Tendenz zur Aufweichung der Individualrechte bereits in den Ansätzen erkennen und bekämpfen.

Kapitel 2

Sicherheitsgesetze – polizeiliche Datenverarbeitung

Paul Kandzia

2.1 Grundlagen

Grund- und Bürgerrechte, Recht auf informationelle Selbstbestimmung Die bisherigen Regelungen zum Verhältnis von Staat und Bürgern gehen von folgenden Grundsätzen aus:

- Der Staat tritt dem Bürger offen gegenüber. So dürfen Ermittlungsakten eingesehen werden, eine verdeckt agierende „GeStaPo“ sollte durch die Verfassung unbedingt vermieden werden.
- Privatsphäre und Kommunikation sind unverletzlich. Unerlaubtes Eindringen in die Intimsphäre gilt als Verletzung der Menschenwürde [64, S.91ff].
- Der Bürger entscheidet selbst, in welchem Umfang die Umwelt von seinem Denken und Handeln Kenntnis nimmt [64, S.99].

Polizei Es bestehen zwei grundsätzlich verschiedene Auffassungen:

- *klassischer Polizeibegriff*

  Die Polizei verfolgt Straftaten und wehrt **konkrete** Gefahren ab. Dabei können im Rahmen der Legalität Bürgerrechte außer Kraft gesetzt werden. Die Voraussetzungen dazu regelt die **polizeiliche Generalklausel**. Danach muß mindestens ein Anfangsverdacht gegen einen Störer bestehen und die Maßnahmen müssen „notwendig und verhältnismäßig“ sein [65, S.294].

- *erweiterter Polizeibegriff*

  H.Herold: „Die Polizei der Zukunft wird eine andere, höherstufige, mit einer gesellschaftssanitären Aufgabe sein.“ [10, S.90] Idee: Existieren genug Informationen, kann die Polizei (mit soziologischen Methoden) gefährliche Tendenzen vor dem Verbrechen erkennen und gegensteuern oder nach dem Verbrechen sofort auf Daten potentiell Verdächtiger zugreifen. Dazu ist die umfassende Sammlung von Daten weiter Bevölkerungskreise ohne konkreten Anlaß nötig.

  Dieser Ansatz kollidiert massiv mit den Grundlagen des Rechtsstaats. Es gibt sogar ein Gerichtsurteil, das das zugrundeliegende Menschenbild („Jeder wird potentiell irgendwann verdächtig“) als grundrechtswidrig klarstellt [45, S.327].

Die Polizei ist föderativ. Die eigentliche Strafverfolgung übernehmen die Landeskriminalämter (**LKA**s), das Bundeskriminalamt (**BKA**) ist für die Koordination und zentrale Aufgaben der Datenverarbeitung zuständig. Ferner unterhält das BKA eine Abteilung für Staatschutz. Dieses **BKA-St** dient zur Verfolgung von Angriffen auf Leib und Leben der Staatsorgane [65, S.311].

Geheimdienste Dies sind militärischer Abschirmdienst (**MAD**), Bundesnachrichtendienst (**BND**) und Bundesamt (Landesämter) für Verfassungsschutz (**BfV, LfV**). Sie unterstehen dem Verteidigungsminister bzw. dem Bundeskanzleramt. Die Aufgabe des BfV ist die Information der Regierung über staatsgefährdende Tätigkeit. Die Geheimdienste haben keine Vollzugsgewalt, dürfen aber, im Gegensatz zur Polizei, „nachrichtendienstliche Mittel“ (z.B. sog. „Wanzen“ zum Abhören des Fernsprechverkehrs) anwenden und damit das Post- und Fernmeldegeheimnis brechen. Zwischen Polizei und Nachrichtendiensten gilt deshalb das **Trennungsgebot**. Dieses hat Verfassungsrang [45, S.337]. Andererseits ist durch die Nähe der Aufgabengebiete – besonders BfV und BKA-St – der Wunsch nach Informationsaustausch auf beiden Seiten vorhanden.

Die rechtliche Grundlage für geheimdienstliche Tätigkeit überhaupt ist umstritten. So gibt es nach [64, S.165] keine gesetzliche Grundlage für BND und MAD.

2.2 Entwicklung der polizeilichen DV bis 1980

2.2.1 Die Polizeireform Anfang der 70er Jahre

Unter dem Begriff „Polizeireform“ versteht man ein von der sozialliberalen Koalition eingeführtes Programm zur Neuordnung der Polizei. Dieses umfaßte:

- Rationalisierung der Organisation, Straffung des Informationsflusses
- Dazu Einführung und Nutzung der EDV (1972)
- Die Zentralinstanzen LKAs und BKA wurden gestärkt, die Organisation auf technische Informationssysteme hin orientiert [63, S.218].
- Einführung des Begriffes „präventive Verbrechensbekämpfung“. Ausdrücklich forderte BKA-Präsident Horst Herold (seit 1972 im Amt) die „umfassende Erhebung aller sich auf das Verbrechen und den Verbrecher beziehenden Daten in einer systematischen, maschinengerechten Form“ und die Zusammenfassung sämtlicher staatlicher Institutionen zu einem Informationsverbund, auf den die Polizei Zugriff hat [89, S.278]. Die Polizei sollte Ursachen gesellschaftswidrigen Verhaltens erforschen und diese zusammen mit anderen Stellen ausräumen [63, S.219].

  Die konsequente Durchführung dieses Konzepts bedeutet, daß von der Polizei Funktionen übernommen werden, die ihr von der Aufgabenbeschreibung her überhaupt nicht zustehen. Damit werden elementare Prinzipien des Rechtsstaats – wie Gewaltenteilung – aufgegeben. Als gesetzliche Regelung führte man Begriffe wie „allgemeine Gefahrenvorsorge“ oder „vorbeugende Verbrechensbekämpfung“ ein. Die eigentlichen Bestimmungen fanden sich in internen Richtlinien.

2.2.2 Das INPOL-System bis 1980

INPOL umfaßt als Oberbegriff alle EDV-Anwendungen der Polizei in Bund und Ländern, die gemeinsam geplant und genutzt werden. Vorgesehen war auch, diese untereinander umfassend zu vernetzen. Dieser Verbund ist in Hard- und Software nicht einheitlich. Die wichtigsten Konzepte sind:

- **ZPI** (zentraler Personenindex)

  Diese auf Landes- und Bundesrechnern voll parallel geführte Datei sollte alle Personen, die in einer beliebigen INPOL-Datei gespeichert sind, zusammenführen. Alle Teilnehmer haben Zugriff. 1981 waren im ZPI zwei Millionen Personen aufgeführt.

- **PIOS** (Personen, Institutionen, Objekte, Sachen)

  Diese Datenbanksysteme gibt es seit 1975 auf dem BKA-Rechner mit Zugriff der Landesrechner, zunächst für den Bereich Terrorismus (PIOS-Te). Neu war eine netzartige Struktur und die Möglichkeit zur Eingabe von Freitext. Rechtlich neu war die explizite Aufnahme sogenannter „anderer Personen“, also auch Unverdächtiger.

Als Ziele dieser Konzeption gelten:

Auswertbarkeit fragmentarischer und noch nicht bewerteter Information, Anreicherung von Information und Verdeutlichung von Beziehungen, Verknüpfung von Information unterschiedlicher Ermittlungen.

So bekommt die elektronische Datenverarbeitung eine neue Bedeutung als „Verdachtschöpfungsmoment“.

Außerdem sollte PIOS Analysen und Querschnittsauswertungen ermöglichen. [64]

1980 bestanden PIOS-Dateien zu den Komplexen Rauschgift, Terrorismus, und Vorbereitung von Staatsgefährdung.

- **SPUDOK** (Spurendokumentation)

  SPUDOKS haben eine ähnliche Struktur wie PIOS. Sie sollen temporär Material sammeln, nach vorläufigem Abschluß einer Ermittlung werden relevante Daten an das entsprechende PIOS-System weitergegeben (Filterfunktion).

2.3 Charakterisierung des Umgangs mit personenbezogenen Daten bei der Polizei

Wie das Konzept der Prävention erwarten läßt, wurde sehr weitgehend Material gesammelt. Die Bindung einer Speicherung an bestimmte Straftaten und der Rechtsgrundsatz des Verdachts verschwanden zunehmend. Bereinigung der Daten nach Alter (Datenschutz!) oder Relevanz (Effizienz!) fand kaum statt.

So fand sich noch im Jahre 1982 eine Notierung über einen **ungeklärten Verdacht** auf Lagerung und Gebrauch von Sprengstoff aus dem Jahr 1953. [17, S.224]

Etwas Statistik: 1975/76 wurden 1.350.000 Datensätze neu in den ZPI aufgenommen, aber nur 25.000 gelöscht. Vorschläge zur automatischen Löschung nach Fristen setzten sich nicht durch [63, S.232].

Die Rechtsnormen sind bewußt weit gefaßt. So gilt jede Straftat mit politischem Motiv als Staatsschutzdelikt, z.B. „wildes Plakatieren“ - mit entsprechender Speicherung und u.U. Weitergabe.

Der Datenschutz wurde dabei vernachlässigt. 1984 arbeiteten an der Kontrolle der Sicherheitsbehörden beim Bundesbeauftragten für Datenschutz gerade vier Beamte – dagegen waren in dem betreffenden Bereich mehrere 10.000 Mitarbeiter mit der Erfassung und Auswertung personenbezogener Daten beschäftigt [17, S.220].

2.4 Probleme mit dem INPOL-System

Ende der 70er Jahre kam die schnelle Entwicklung zu immer weitgehenderer polizeilicher Datenerfassung zum Stehen. Im Wesentlichen entstanden folgende Probleme:

- **technische Grenzen**

  Als ungünstig erwies sich die sehr unterschiedliche Hardware: Zwei Siemens und eine IBM Baureihe wurden mit 10 verschiedenen Betriebs- und DB-Systemen verwendet. Daher ließ sich der Rechner-Rechner Verbund nicht voll verwirklichen. Die sternförmige Anordnung der LKA-Rechner um den zentralen BKA-Rechner führte zur Überlastung des Zentralrechners.

- **Probleme bei den Benutzern**

  Die starke Veränderung der Arbeitsabläufe durch die EDV-Einführung führte zu einer Überforderung der Sachbearbeiter. Diese reagierten mit laxer Handhabung bei Einstellungs- und Abfragevorgängen. So waren viele Eingaben unbrauchbar. Ein Beispiel: Aus der Meldung „Knarre mit Nüssen gestohlen“ (also ein Steckschlüssel mit Einsätzen) erstellte ein Sachbearbeiter die Eingabe „Diebstahl eines Gewehrs mit Munition“.

- **Konzeption**

  Die Dateneinstellung erfolgte auf Rechnerseite unverarbeitet, d.h. Effizienz und Erfolg des Systems hing vom Geschick der Benutzer ab. Man hatte eine einfache Struktur, die für kleinere Datenmengen (z.B. Fahndungsdatei) geeignet war, auf große, komplexe Konzepte (wie PIOS) übertragen. Eine nachträgliche Umstrukturierung war nicht mehr möglich, daher stieß INPOL an seine Grenzen [63, S.233].

So hatte sich die im letzten Absatz geschilderte Entwicklung, die für den Datenschutz sehr gefährlich war, vorerst totgelaufen. Als Konsequenz entwarf 1981 die Innenministerkonferenz ein Konzept zur Fortentwicklung von INPOL.

Bewertung der INPOL-Entwicklung

- Die Idee der Prävention und polizeiliches Sicherheitsdenken bergen die Gefahr überwachungsstaatlicher Züge. Grundlagen des Rechtsstaates, darunter Datenschutz, werden mißachtet.

  Es ist falsch, von den Sicherheitsbehörden Selbstbeschränkung bei der Arbeit mit personenbezogenen Daten zu erwarten.

- Die Entwicklung wurde durch interne Gründe gebremst, nicht etwa aus grundsätzlichen Erwägungen und entsprechender gesetzlicher Regelung.

- In einem pluralistischen System muß die Beschränkung einseitiger Kräfte durch die Gegenkräfte erfolgen. In diesem Zusammenhang sind das Gesetzgebung und kontrollierende Organe. Diese Meinung vertritt auch die Polizei selbst [89, S.279]. Leider kommen die Verantwortlichen ihrer Aufgabe völlig unzulänglich nach, versuchen sogar eher, gängige Praxis nachträglich zu legalisieren. Dies ist Inhalt des nächsten Abschnitts.

2.5 Neuerungen bei INPOL seit 1980

- Aufgrund der schlechten Erfahrungen ging man zu stärkerer Dezentralisierung über. Man unterscheidet heute INPOL-Bund und INPOL-Land, hierbei werden Daten, die nur regional relevant sind, den Ländersystemen zugeordnet. Deren Dateien sind nach außen abgeschottet. Es ist also nicht mehr möglich, über eine Zentralinstanz auf alle Datensätze zuzugreifen. Diese Option hatte sich ohnehin als eher effektivitätshemmend erwiesen [63, S.236].

- Der ZPI wird zu **KAN** (Kriminalaktennachweis)

  Nur noch Täter und Verdächtige mit überregionaler Bedeutung werden aufgenommen, für den Rest sind Länderdateien zuständig. 1986 hatte der KAN 63.500 Einträge [63, S.237].

- **PIOS/SPUDOK** gewinnen an Bedeutung und ersetzen teilweise Funktionen des alten ZPI. Seit 1986 existiert **APIS** (Arbeitsdatei PIOS innere Sicherheit) als Verbund von BKA und LKAs im Bereich polizeilicher Staatsschutz. Hier wurden BKA-St-Daten mit den alten PIOS-Te Beständen zusammengeführt. Obwohl das PIOS-Prinzip nur bei schweren Delikten gerechtfertigt ist, ist APIS real „ein Register politisch motivierter Daten geringer Bedeutung“. (1987: 70 v.H. Bagatellfälle, z.B. Schüler bemalt Wand) [92, S.147]

- Neue Verfahren der Datenerhebung sind:

  technische Mittel

  Mit diesen ist es möglich, ohne in der Wohnung installierte Sender jedes dort gesprochene Wort und u.U. auch optische Vorgänge aufzunehmen. Es gab bereits Anwendungen [90, S.263].

  maschinenlesbarer Personalausweis

  Er erlaubt Massenkontrollen an speziell eingerichteten Stellen im Inland, z.B. zur Schleppnetzfahndung.

- Es besteht die Tendenz, auf andere Dateien auszuweichen. Diese sind oft aktueller und besser gegliedert [63, S.238].

Die Mentalität der Sicherheitsbehörden hat sich leider nicht geändert. So waren in Berlin 1985 in einem „zentralen Informationssystem Verbrechensbekämpfung“ rund **1,32 Millionen Datensätze** vorhanden. Der Innensenator nannte als Rechtsgrundlage die Strafprozeßordnung, d.h. es muß für jeden Eintrag eine konkrete Gefahr, Beschuldigteneigenschaft oder Wiederholungsgefahr vorliegen [89, S.280]!

2.5.1 Starker Informationsaustausch BKA-Verfassungsschutz

Wie zu erwarten, besteht ein starkes Interesse an Datenübermittlung zwischen diesen Behörden. Das wird an solchen Beobachtungen deutlich:

- Das BKA speichert doppelt so viele Fälle in **NADIS** (nachrichtendienstliches Informationssystem, System des Verfassungsschutzes) wie in APIS. Somit benutzt das BKA NADIS als eine Art „Auffangdatei" für leichtere Fälle [34, S.64].
- Ungesetzliche routinemäßige Übermittlung fand statt [34, S.65]. So gilt Weitergabe auf Sachbearbeiterebene trotz abgelehntem Amtshilfeersuchen als „nicht außergewöhnlich" [64, S.198].
- Der Bundesinnenminister wertet den Umfang solcher Übermittlungen, die in diesem Maß vom Trennungsgebot her sicher nicht vorgesehen sind, gerade als Anzeichen für die Notwendigkeit eines umfassenden Austauschs. [34, S.65]

2.6 Die aktuelle Diskussion – neue Sicherheitsgesetze

2.6.1 Forderungen des Datenschutzes an gesetzliche Regelungen

- **Normenklarheit**

  Der Bürger muß das Maß staatlicher Eingriffe erkennen können, die Grenze zwischen legaler politischer Betätigung und verfassungsfeindlicher Aktion muß deutlich sein [50, S.7].

  Die Datenverarbeitung der Behörden muß verfahrensrechtlich klar geregelt werden, insbesondere **Aufklärungs-, Auskunfts- und Löschungspflichten**. Die Referenz auf das Erforderlichkeitsprinzip hat sich als unzureichend erwiesen. Dies folgt aus dem Volkszählungsurteil und Ähnlichem.
- Das **Trennungsgebot** muß auf informationeller Ebene strikt eingehalten werden, Amtshilfe kann nur eine exakt geregelte Ausnahme sein.

2.6.2 Neue Sicherheitsgesetze

Seit 1986 liegen verschiedene konkrete Vorschläge in Form von Musterentwürfen vor. Betrachtet werden hier:

- Bundesverfassungsschutzgesetz
- Verfassungsschutzmitteilungsgesetz
- Einheitliches Polizeigesetz des Bundes und der Länder
- Bundesdatenschutzgesetz

Die wichtigsten Kritikpunkte sind den unterschiedlichen Entwürfen gemeinsam. Die folgenden Punkte legalisieren nicht-rechtsstaatliche oder datenschutzfeindliche Verfahren oder ermöglichen diese. Beispielhaft werden Forderungen von Datenschützern im Zitat den entsprechenden Passagen der Entwürfe gegenübergestellt.

1. Die präventive Arbeit der Polizei wird ausdrücklich in die Aufgabenbeschreibung übernommen: „Sie hat auch für die Verfolgung von Straftaten vorzusorgen und Straftaten zu verhüten (vorbeugende Bekämpfung von Straftaten) sowie Vorbereitungen zu treffen, um künftige Straftaten abwehren zu können". [19, S.2] Damit darf sie auch gegen Personen Eingriffe vornehmen, die keine Störer sind, insbesondere darf sie Daten sammeln [50, S.10]. Diese Formulierung der Aufgabenbeschreibung gilt als zu weitgehend. „Insbesondere fehlt es an einer genauen Festlegung, bei welchen Delikten die Polizei vorbeugend tätig werden darf." [93, S.41]

   Zur Datenerhebung selbst sagt der Entwurf:

   „Die Polizei kann personenbezogene Daten von

(a) Personen, bei denen Anhaltspunkte bestehen, daß sie künftig Straftaten begehen,

(b) Kontakt- oder Begleitpersonen der in Nr.1 genannten Personen, ...

erheben, soweit dies aufgrund tatsächlicher **Anhaltspunkte erfahrungsgemäß** zur vorbeugenden Bekämpfung von Straftaten /mit erheblicher Bedeutung/ erforderlich ist.“ [19, S.6]

(Anmerkung: Die Schreibweise „/.../“ ist direkt aus dem Entwurf übernommen und kennzeichnet offensichtlich Alternativvorschläge und optionale Einfügungen.) Eine entsprechende Begründung ließe sich wohl immer finden.

„Die Polizei kann personenbezogene Daten, auch durch Bild- oder Tonaufnahme, bei oder im Zusammenhang mit öffentlichen Versammlungen erheben, wenn tatsächliche Anhaltspunkte die **Annahme rechtfertigen**, daß erhebliche Gefahren für die öffentliche Sicherheit und Ordnung entstehen.“ [19, S.7]

Diese Vorschrift erlaubt u.a. Massenkontrollen mit Hilfe des maschinenlesbaren Personalausweises, die sich ja auf mehr oder weniger Unbeteiligte beziehen. Aber „allenfalls bei Anhaltspunkten ... für bestimmte Straftaten, die in einem Katalog zu definieren wären, können so umfassende Maßnahmen in Betracht kommen.“ [93, S.44]

2. Das Trennungsgebot wird explizit und faktisch aufgehoben.

   - Der alte Paragraph zur Trennung fehlt im Entwurf.
   - Die Befugnisse von BKA und BfV sind bis in Details identisch

     „Besondere Formen der Datenerhebung“ werden der Polizei erlaubt, vor allem

     – längerfristige Observation
     – verdeckter Einsatz technischer Mittel
     – Under Cover Agents und V-Leute

     Bisher waren dies Privilegien der Geheimdienste, nämlich die „nachrichtendienstlichen Mittel“. Die legalen Anlässe zum Einsatz dieser Mittel sind viel weiter gefaßt als für „konventionelle Wanzen“ nach dem Post- und Fernmeldegeheimnis. Nach [90, S.268] dient nur noch das Verhältnismäßigkeitsgebot als Grenze, auch ist die Anwendung eigenmächtig (ohne richterlichen Beschluß) möglich.

     „Außer bei Gefahr im Verzug erfolgt die Anordnung der Maßnahme durch den Behördenleiter /Leiter der Dienststelle/ oder einen von ihm beauftragten Beamten.“ [19, S.9]

     Nach Meinung der Rheinland-Pfälzischen Datenschutzkomission sind für „diese besonderen Fahndungsmethoden Straftatenkataloge mit enumerativer Aufzählung erforderlich; sie sind den jeweiligen Fahndungsmethoden gesondert anzupaßen.“ [27, S.82] Aber dies ist im Entwurf nicht vorgesehen.

     Umgekehrt werden auch die Befugnisse des Verfassungsschutzes erweitert. Er darf jetzt auch direkt **personenbezogene** Daten sammeln - statt nur über **Bestrebungen** - und zwar sogar über selber nicht extremistische Personen. Die sogenannten „nachrichtendienstlichen“ Mittel werden nicht weiter definiert.

     Der Datenaustausch ist weitgehend frei. Dieser ist nämlich immer dann erlaubt, wenn es „Anhaltspunkte gibt, daß die Information zur Erfüllung gesetzlicher Aufgaben erforderlich ist“ [50, S.9].

3. Da die Neuerungen mit den bisherigen Datenschutzgesetzen kollidieren, werden diese angeglichen.

   - **Speicherungsdauer unklar**

     Beim Verfassungsschutz verbleiben Daten „für das für seine Aufgabenerfüllung erforderliche Maß“ [50, S.8], bei der Polizei werden sie gelöscht, „wenn nicht mehr erforderlich“ [19, S.22]
   - **Auskunftspflichten** gibt es für die Nachrichtendienste gar nicht, für die Polizei bei „Abwägung mit öffentlichem Interesse“.
   - **Übermittlung** von und zu anderen öffentlichen Stellen ist weitgehend frei.

     So erhält die Polizei Daten, „soweit dies zur Erfüllung polizeilicher Aufgaben erforderlich **erscheint**. Auf Ersuchen sind die Daten zu übermitteln ...“ [19, S.18] Eine Begründung wird nicht gefordert! Damit kann die Polizei auf andere Dateien ausweichen.

- **Zweckbindung** für Sicherheitsdienste aufgehoben

  Das Speichern, Verändern und Benutzen vorhandener Daten ist auch dann zulässig, wenn nach einer anderen Rechtsvorschrift die Daten erhoben werden dürften. Genau so ein Vorgehen soll aber das Prinzip der Zweckbindung verhindern.
- Die Rechte des **Datenschutzbeauftragten** werden eingeschränkt. So darf er keine polizeilichen **Akten** mehr prüfen, sondern nur noch **Dateien**. Dazu sollte man bedenken, daß bereits Daten gelöscht wurden, die zugehörigen Akten allerdings nicht [27, S.13]. Die Öffentlichkeit als letzte Kontrollinstanz wird ebenfalls zurückgedrängt, der Datenschutzbericht soll nur noch zweijährig erscheinen.

Erwartungsgemäß lautet das Urteil des Bundesbeauftragten für Datenschutz:

„Insgesamt werden die in der Begründung des Entwurfs genannten Ziele der beabsichtigten Weiterentwicklung des Bundesdatenschutzgesetzes nicht erreicht. Der Entwurf entspricht daher nicht den Erwartungen an ein zeitgemäßes Datenschutzrecht als Ausprägung des verfassungsrechtlich garantierten Rechts des Bürgers auf informationelle Selbstbestimmung.“ [34, S.97]

Fazit Es wird deutlich, daß sich der Standpunkt des Datenschutzes und liberale Prinzipien des Rechtsstaates nicht durchsetzen konnten. Stattdessen überläßt der Entwurf die Verantwortung über die Formen der DV der Sicherheitsdienste den betreffenden Behörden selber, indem er keine klaren Bestimmungen schafft, sondern extensiv schwammige Formulierungen wie „Erforderlichkeit“ und „Anhaltspunkte“ verwendet. Dies sollte nach den bisherigen Erfahrungen eigentlich nicht mehr vorkommen. So übertreibt Prof. Spiros Simitis, der hessische Datenschutzbeauftragte, wohl nicht, wenn er zu den Entwürfen äußerte, daß „zum ersten Male in der Geschichte der Bundesrepublik das Tor zur Geheimpolizei offenstünde“ [50, S.5]. Erschreckend ist auch, wie versucht wird, weitreichende Eingriffe zu verharmlosen. So steht in der Begründung, die Regelung zur Auskunftserteilung der Sicherheitsdienste an den Bürger bleibe erhalten. Diese Regelung legt aber gerade fest, daß die Dienste nicht zur Auskunftserteilung verpflichtet sind [21, S.49]

2.7 Die Genomanalyse

In den vorangegangenen Abschnitten sollte unter anderem deutlich werden, wie Datenschutz in ein Umfeld eingebunden ist, auf das politische, gesellschaftliche und technische Entwicklungen einwirken. Somit kann er nur erfolgreich durchgesetzt werden, wenn alle diese Einflüsse laufend beobachtet werden. Die Datenschutzentwicklung muß schritthaltend erfolgen.

So stellt Simitis in [93] innerhalb des Bereiches „Gesundheitswesen“ folgende Überlegungen zur Neuentwicklung Genomanalyse an, die hier kurz dargelegt werden sollen.

2.7.1 Grundsätzliche Probleme

- In manchen Bundesländern fehlen trotz Vorschlägen der Beauftragten immer noch spezielle gesetzliche Vorschriften zur Behandlung von Patientendaten in Krankenhäusern.
- Diese sind öffentlich–rechtliche **Wettbewerbsunternehmen**, daher gelten bezüglich **Behandlungsaufgaben** die Regelungen des Bundesdatenschutzgesetzes für den Privatbereich. Diese sind aber noch nicht an das Recht auf informationelle Selbstbestimmung angepaßt. Damit unterliegen sensible Patientendaten „einem geringeren Schutz als z.B. die Hundesteuerdaten.“ [93, S.65]
- Parallel dazu kommen Bestimmungen der Landesdatenschutzgesetze in den Bereichen **Arbeitnehmerschutz** und **Forschung** zur Anwendung. In der Praxis führt dies zu großen Schwierigkeiten in der Handhabung.
- Es besteht also auch hier ein starker Regelungsbedarf!

2.7.2 Datenschutzprobleme der Genomanalyse

Seit 1988 hat sich die Diskussion über zukünftige Auswirkungen der Genomanalyse intensiviert. Umstritten sind vor allem folgende existierende oder im Entwurf befindliche Verfahren:

- genetische Analysen in Strafverfahren

  Als Anwendungen sind reine Identifikationen, aber auch genetische Täterprofile aus Blutresten o.ä. am Tatort denkbar.

- humangenetische Beratung

- pränatale Diagnostik

  Es lassen sich schon vor der Geburt durch Entnahme von Zellen am Fötus statistische Aussagen über das zukünftige Ausbrechen genetisch bedingter Krankheiten machen.

- Neugeborenenscreening

  Hierunter versteht man Reihenuntersuchungen auf genetische Disposition am Neugeborenen.

- Anwendung im Zusammenhang mit Versicherungsverträgen

In allen Fällen werden äußerst sensible Daten erhoben. Die Kenntnis und Verwendung dieser Information kann gravierende Folgen für den Betroffenen haben. Daher reicht es nicht aus, diesen nur vor Mißbrauch zu schützen, sondern die Bedingungen für die Erhebung sind vorab zu klären und gesetzlich zu regeln. Da bisher aber über diese Fragen noch kein gesellschaftlicher Konsens besteht, ist der Aufbau sensibler genetischer Datensammlungen nicht akzeptabel. Erfahrungsgemäß sind ja bestehende Sammlungen sehr schwer nachträglich einzuschränken (siehe polizeiliche Datenverarbeitung).

Regelungsdefizite bestehen nicht nur in den Krankenhäusern (siehe oben), sondern auch bei:

- Gesundheitsämtern

  Diese arbeiten auf der Grundlage von Gesetzen aus den Jahren 1934 und 1935 ohne klare Aufgaben- und Befugnisnormen.

- Arbeitnehmerschutz

  Es besteht die Gefahr der Ausgrenzung weiter Personenkreise aus dem Erwerbsleben. Der Schutz vor Gefährdung durch Chemikalien o.ä. könnte durch Auswählen „resistenter" Arbeiter verringert werden.

  Simitis schlägt daher vor: Untersuchungen auf Disposition sind grundsätzlich zu untersagen (Analysen nur in Einzelfällen mit besonderer Genehmigung). Die erhobenen Daten dürfen nicht in Personalinformationssysteme eingegeben werden.

- Polizei

  In Großbritannien gab es schon Anwendungen zur Identifikation (1987). Dabei stellt sich die Frage nach dem anfallenden Informationsüberschuß, der u.U. Einblick in die Persönlichkeit Unschuldiger erlaubt.

Recht auf Nichtwissen Bisher ging es eigentlich immer darum, die Information Betroffener über Speicherung personenbezogener Information sicherzustellen. Völlig neu dagegen ist der Aspekt, daß jeder das Recht hat, unbelastet von der Kenntnis einer (eventuell) später ausbrechenden Krankheit zu leben („Recht auf Nichtwissen"). Falls solche Daten jedoch erst einmal existieren, muß der Betroffene auch informiert werden. Dieser Konflikt kann nur dadurch aufgelöst werden, daß entsprechende Daten gar nicht erst erhoben werden.

2.8 Zusammenfassung und abschließende Wertung

An den beiden Beispielen dieses Kapitels wurde deutlich, daß die Möglichkeiten der EDV, besonders der schnelle Zugriff auf große Datenmengen und ihre einfache Handhabung auch auf engem Raum, Behörden anregt, diese zur Verwaltung der Bürger zu nutzen. Dabei tritt dann leicht der Aspekt in den Vordergrund, Menschen als „Verwaltungsobjekte" zu betrachten, deren Wohl am besten von den betreffenden Staatsorganen „von oben" geregelt wird, gerade weil dort ja sämtliche Informationen zusammengeführt werden. Also müßten deren Entscheidungen notwendig besonders objektiv und damit richtig sein. Zumindest dient solch eine Argumentation oft als Begründung zu Datenerhebungen (z.B. Volkszählung). Verdrängt wird aber der Mensch als selbständig handelnder, sein Schicksal mitbestimmender, individueller „Staatsbürger" im Sinne des Grundgesetzes, der ursprüngliche „Souverän" der Demokratie. Es geht also um fundamentale Bestandteile menschlichen Zusammenlebens, Werte, die immer über den Interessen effektiver Verwaltung stehen sollten. Um diese zu schützen wurde das Recht auf informationelle Selbstbestimmung geschaffen, hier liegt die immer wichtiger werdende Aufgabe des Datenschutzes, und jeder Bürger sollte selber für die Bewahrung solcher Rechte eintreten.

Teil II

Personaldaten im Betrieb

Kapitel 3

Technische Möglichkeiten von Personalinformationssystemen

Jens Dupont

3.1 Funktion und Aufbau

3.1.1 Was ist ein Personalinformationssystem (PIS)?

Ein PIS ist eine jederzeit erweiterbare Sammlung von Personaldaten auf einem Datenträger. Es dient dem Zweck der effektiven Nutzung und Kontrolle menschlicher Arbeitskraft. Als Datenträger dienten früher zum Beispiel Karteikarten oder Aktenordner. Spricht man jedoch heute von einem PIS, sind alle computergestützten Systeme zu verstehen, die Personaldaten maschinell erfassen, speichern, verarbeiten, auswerten, übertragen, verknüpfen und sie über Bildschirmgeräte oder Druckausgaben abrufen [52].

3.1.2 Struktur von PISen

Als Grundlage und Ausgangspunkt für die eigentliche Implementierung dient die Aufgabenspezifikation. In ihr werden systematisch die durch das PIS zu lösenden Aufgaben dargestellt und in Teilaufgaben strukturiert.

Ein PIS läßt sich grob in 3 Subsysteme strukturieren (Abbildung 3.1).

Ein Subsystem ist das Methodensystem. Es beinhaltet Methoden und Algorithmen, auf die zur Lösung der in der Aufgabenspezifikation dargestellten Aufgaben zugegriffen werden kann. Das können statistische Aufbereitungen, Auswertungen oder ähnliches sein.

Das zweite Subsystem ist das eigentliche Datensystem. Es unterteilt sich in eine Personal- und eine Arbeitsplatzdatenbank. Diese Datenbanken liefern die Daten, auf denen das Methodensystem arbeitet. Das sind in der Personaldatenbank Daten über den Personalbestand, Personalveränderungen usw.; in der Arbeitsplatzdatenbank Daten über Arbeitsplatzmerkmale oder Tätigkeitsbereiche.

Desweiteren gehört zu einem PIS ein System zur Ein- und Ausgabe von Daten. Das sind z.B. Terminals, Drucker, usw. [44].

3.1.3 Aufgaben eines PIS

Bei der Aufgabenspezifikation richtet man sich im wesentlichen nach den betrieblichen Aufgaben, die vom Personalbereich gelöst werden, und versucht, diese mit Hilfe des Rechners zu erledigen. Man unterscheidet Kern- und Uraufgaben. Bei den Kernaufgaben handelt es sich um die „typischen“ personalwirtschaftlichen Aufgaben wie:

Abbildung 3.1: Personalinformationssysteme mit Personal- und Arbeitsplatzdatenbank

- Ermitteln des Personalbedarfs
- Beschaffen des Personals
- Einsetzen des Personals

- Erhalten des Personals (Lohnabrechnung)
- Entwickeln des Personals
- Freistellen des Personals (Bestimmen der Freistellungsart, Auswählen der aufzulösenden Verhältnisse, Auflösen der Arbeitsverhältnisse)

Uraufgaben dienen zur Datenerhebung für die Kernaufgaben. Sie zielen auf die Erfassung von Daten aus dem betrieblichen und überbetrieblichen Bereich ab. (z.B. Erforschen des Arbeitsmarktes, Auswerten des betrieblichen Leistungsprozesses oder Durchführen von Leistungsbewertungen und Mitarbeiterbeurteilungen.) Tröstlich ist, daß sich das Gros dieser Aufgaben noch nicht von Rechnern lösen läßt, da sie nicht oder nur teilweise algorithmisierbar sind oder dies nur unter Annahme großer Einschränkungen möglich ist. Der Trend geht allerdings dahin, nicht algorithmisierbare Probleme so zu formalisieren, daß sie zumindest teilweise berechnet werden können. Die Lohnabrechnung kann vollständig auf dem Rechner erfolgen [44].

3.2 Datenbestände

3.2.1 Art und Umfang von Daten

In modernen PISen werden eine Fülle von Daten gespeichert und verarbeitet. Man unterscheidet zwischen Arbeitnehmerdaten, die sich auf den einzelnen Angestellten beziehen, und Arbeitsplatzdaten, die den Arbeitsplatz und sein Umfeld beschreiben.

3.2.1.1 Was sind Arbeitnehmerdaten?

Als Arbeitnehmerdaten werden identifizierende und persönliche Daten gespeichert.

Identifizierende Daten sind Daten, die zur Erkennung des Arbeitnehmers und zu seiner Auffindung in Dateien dienen. Dazu gehört als wichtigstes Datum die Personalnummer. Weitere Daten sind z.B.

- Name, Geschlecht, Geburtsdatum, Geburtsort, Familienstand, Anrede
- Wohnort, Adresse, Telefonnummer (privat/intern)
- Rentenversicherungsnummer, Lohnsteuerschlüssel, Krankenkassenschlüssel, Angaben zur Sozialversicherung [25]

Persönliche Daten dienen zur Beurteilung eines Arbeitnehmers. Dazu gehören:

- **Kenntnis-Merkmale:** Schul-und Fachausbildung, Führerschein, Fremdsprachen, innerbetriebliche Weiterbildung
- **Körperlich-gesundheitliche Daten:** Seh- und Hörvermögen, Belastbarkeit der Gliedmaßen, Muskelbelastbarkeit, Maskenverträglichkeit, Allergien
- **Geistige Merkmale:** Auffassungsgabe, mündliche/schriftliche Ausdrucksfähigkeit, praktische Anstelligkeit, technisches Verständnis
- **Arbeits- und Gemeinschaftsverhalten:** Kontaktfähigkeit, Arbeitstempo, Verantwortungsbereitschaft, Ausdauer
- **Sensomotorische und psychische Merkmale:** Konzentrationsfähigkeit, Reaktionsvermögen, Monotoniefestigkeit
- **Lohn- und Gehaltsdaten:** Arbeitsplatz-, leistungs-, qualifikationsunabhängige Lohnbestandteile, Kündigungsschutz
- **Interessen:** Hobbys, Teilnahme am Betriebssport [52]

3.2.1.2 Was sind Arbeitsplatzdaten?

Arbeitsplatzdaten sind alle Daten, die mit dem Arbeitsplatz und seinem Umfeld im Zusammenhang stehen. Dazu gehören:

- **Identifizierende Merkmale:** Arbeitsplatznummer, Ort des Arbeitsplatzes
- **Allgemeine beschreibende Merkmale:** Telefonnummer, Funktionsbezeichnung, Funktionszulagen, Anforderung an Kenntnisse
- **Physische und psychische Anforderungen:** Klimabedingungen, Lärm, Staub, Gasbelästigung, Lichtverhältnisse

Die Liste dieser Daten ließe sich beliebig weiterführen. Im Schnitt werden in PISen zwischen 200 und 350 Arbeitnehmerdaten und etwa 250 Arbeitsplatzdaten gespeichert, oft jedoch mehr als 2000 Einzelangaben pro Arbeitnehmer. So stellt zum Beispiel das PIS PAISY theoretisch bis zu 2.500 kByte Speicherplatz pro Arbeitnehmer bereit. Das entspricht ca. 600 dichtbeschriebenen Schreibmaschinenseiten [84, 25].

3.2.2 Datenquellen und Erfassungsmethoden

Die Informationslieferanten für PISe unterteilt man im wesentlichen in zwei Gruppen: die automatisierten Datenquellen und die herkömmlichen nicht automatisierten Datenquellen. Zu den letzteren zählen z.B. Bewerbungsunterlagen, Personalfragebogen, Befragungen des Vorgesetzten und der Mitarbeiter, standardisierte Beurteilungsverfahren, Arbeitsplatz- und Arbeitsablaufuntersuchungen.
Diese Daten konnten prinzipiell schon immer erfaßt werden. Das eigentlich Neue an computergestützten PISen ist hier nur die Geschwindigkeit der Datenabfrage und -verarbeitung. Zu den vorhandenen Daten addieren sich nun aber noch Daten aus automatisierten Quellen, deren Verwaltungsaufwand ohne Rechner nicht zu bewältigen wäre. Die häufigsten computergestützten Erfassungs-, Be- und Verarbeitungssysteme sind:

3.2.2.1 Arbeitszeiterfassungssysteme

Zeiterfassungssyteme sind häufig kleine PISe, die neben personenidentifizierenden Daten, Daten über Jahresurlaub, bezahlte oder unbezahlte Sonderurlaube, Überstunden, lohnfortzahlungspflichtige Zeiten (Krankheit, Mutterschutz) speichern und verarbeiten. Nebenbei werden dann noch Beginn und Ende der täglichen Arbeits- und Arbeitsunterbrechungszeit minutiös erfaßt. Für die Lohnabrechnung können so monatliche Zeitkonten aufgestellt werden. Desweiteren lassen sich Fehlzeitenstatistiken, Statistiken über Verletzung von Kern- und Rahmenzeiten oder Verspätungen erstellen.

3.2.2.2 Betriebsdatenerfassungssysteme

Betriebsdaten sind alle über den Arbeits- bzw. Produktionsprozeß selbst erhobenen Informationen wie z.B. Beginn, Ende und Unterbrechung eines Arbeitsgangs, Art des Auftrags, belegte Maschine, Stillstand und Grund der Störung, verbrauchtes Material, usw. Diese Informationen werden in einer Betriebsmittel- und einer Auftragsdatei gespeichert. Erstere enthält alle Kapazitätsangaben über Maschinen bzw. Anlagen. Letztere beschreibt die zu bearbeitenden Aufträge bis hin zu den kleinsten sich wiederholenden Einheiten, den Arbeitsgängen. Die weitestgehende Form ist die lückenlose, zeitgenaue Erfassung aller Arbeitsgänge mit Beginn- und Ende-Zeitangabe der Bearbeitung. Die gespeicherte Datenbasis ermöglicht dem System die Lösung einer Reihe von Aufgaben:

- Feststellung des augenblicklichen Bearbeitungsstandes eines Auftrags
- Anzeigen aller Arbeiten, die sich seit einer bestimmten Anzahl von Stunden an einer bestimmten Fertigungsstelle befinden
- Anzeige verspäteter Aufträge
- Anzeige abweichender Zeiten für ausgewählte Arbeitsgänge
- Statistik von Störgründen [52]

3.2.2.3 Telefonüberwachungssysteme

Sie ermöglichen die Speicherung von Informationen über geführte Gespräche wie z.B.

- Datum des Gesprächs
- Uhrzeit
- Zielort
- Nummer des angerufenen Teilnehmers
- Gesprächsdauer
- Anzahl der Gebühreneinheiten
- Kosten des Gesprächs
- Nebenstellnummer
- Kennzeichnung (privat/dienstlich) [52]

3.2.2.4 Zugangskontrollsysteme

Sie erfordern die Einführung eines computerlesbaren Werksausweises, auf dem Personalnummer und Zugangsberechtigung eingetragen sind. Speichert das Ausweislesegerät nun den Zeitpunkt der Identifizierung, kann der Weg eines Arbeitnehmers und seine Aufenthaltsdauer an bestimmten Orten zumindest grob nachvollzogen werden.

Weitere Datenquellen sind: Die automatische Kantinenabrechnung, anhand der Eßgewohnheiten des Arbeitnehmers erfaßt werden können; die bargeldlose Benzinabrechnung an der betriebseigenen Tankstelle, mit der das Fahrverhalten überblickt werden kann; die Datenbanken des Werkschutzes und des werksärztlichen Dienstes. Bei Arbeiten an Bildschirmgeräten ist es möglich, Hintergrundprogramme zu installieren, die z.B. die Zahl der Anschläge, Unterbrechungszeiten o.ä. ermitteln.

Neben den genannten internen Datenquellen gibt es noch einige externe:

- Auskünfte früherer Arbeitgeber
- Mitteilungen von behördlichen Stellen [25, 52]

3.3 Möglichkeiten der Datenverarbeitung

3.3.1 Profilmethode

Bei der Profilmethode handelt es sich um einen systematischen Vergleich von Personal- und Arbeitsplatzdaten. Mit Hilfe der Arbeitsplatzdaten wird für einen Arbeitsplatz ein Anforderungsprofil erstellt, das dann mit dem Qualifikationsprofil des Arbeitnehmers oder Bewerbers verglichen wird. Auf diese Weise läßt sich für jeden Arbeitnehmer der geeignete Arbeitsplatz oder für jeden Arbeitsplatz der geeignete Arbeitnehmer finden.

Diese an sich sehr objektive Form der Arbeitsplatzverteilung birgt jedoch eine gewisse Problematik. Sehr oft werden beim Erstellen des Qualifikationsprofils medizinische und psychologische Merkmale verwendet, so daß minimale gesundheitliche Beeinträchtigungen ohne Bezug zur angestrebten Tätigkeit die Ablehnung eines Bewerbers zur Folge haben können. Der Mensch degeneriert zu einem Gegenstand mit bestimmten Eigenschaften, bei dem Motivation und Leistungsbereitschaft keine Beachtung finden. Der persönliche Eindruck des Arbeitnehmers zählt wenig, da sein objektiver Datenschatten für oder gegen ihn spricht. Viele dieser Daten sind jedoch nicht objektiv, da es für ihre Erfassung keine wissenschaftlich fundierten Messungen gibt. Zudem ist die Pflege der Daten ein Problem, da der Computer falsche oder veraltete Daten nicht „vergißt“. Aus diesen Gründen birgt die Profilmethode immer die Gefahr unberechtigter Benachteiligung und sozialer Diskriminierung [44, 52].

3.3.2 Möglichkeiten der Leistungsbeurteilung und Kontrolle

Die Einführung von Rechnern bewirkt, daß sich Daten in beliebiger Menge speichern, verknüpfen und anonym am Bildschirm abfragen lassen. Die meisten PISe bieten leicht erlernbare Benutzersprachen an. So ist es auch für einen nicht EDV-geschulten Personalchef kein Problem, sich z.B. zwecks Personalselektion eine Liste aller Arbeitnehmer über 50 Jahren mit mehr als 10 Fehltagen im Jahr ausdrucken zu lassen, wobei Montage und Freitage besonders gekennzeichnet werden. Diese Informationen sind für ihn innerhalb von Sekunden verfügbar.

Ein Beispiel aus der Praxis einer Kölner Firma verdeutlicht die Möglichkeiten der Verknüpfung von Daten. „So hatte ein Arbeitnehmer an einem Montag den nahezu leeren Tank seines Privat-Pkw an der firmeneigenen Zapfsäule mit Benzin gefüllt. Die Abrechnung erfolgte in diesem Betrieb automatisch am Monatsende über die Lohn- und Gehaltsabrechnung. In den darauffolgenden drei Arbeitstagen war der Arbeitnehmer laut ärztlicher Bescheinigung arbeitsunfähig erkrankt. Am Freitag nahm er seine Arbeit wieder auf. Nach Feierabend füllte er den wiederum fast leeren Tank seines Pkw auf. Dieser Umstand hatte Konsequenzen. Nach Erstellung der fälligen Lohn- und Gehaltsabrechnung wurde der Arbeitnehmer zu einem sogenannten Personalgespräch gebeten, in dem ihm vorgehalten wurde, daß er offensichtlich Zeiten seiner Arbeitsunfähigkeit dazu benutzte, Privatfahrten zu unternehmen. Die Lohnfortzahlung für die drei Krankheitstage wurde verweigert; eine Abmahnung sollte erteilt werden. Erst die Einschaltung des Betriebsrates führte in diesem Fall zur Rehabilitierung des Arbeitnehmers.“

Auch die Verknüpfung ‚harmloser‘ Daten kann zu erstaunlichen Ergebnissen und zur Entscheidungsgrundlage bei Bewerbungen dienen. In einem Fall wurde aus den Daten Familienstand, Vermögensbildung und Art der Vermögensbildung auf „mangelnde Eignung für kaufmännische Tätigkeiten“ sowie „Mangel an allgemeiner Vertrauenswürdigkeit“ geschlossen [52].

3.3.3 Folgen computergestützter PISe

Aus der fast unbegrenzten Speicherkapazität und Verknüpfbarkeit der Daten ergeben sich verschiedene Gefahren für den Arbeitnehmer:

- Langzeitüberwachung durch Langzeitspeicherung der persönlichen Daten
- Einmal gespeicherte Daten werden zu den unterschiedlichsten, nicht mehr mit der eigentlichen Erhebung in Verbindung stehenden Zwecken verwendet
- Verlust des Kontextes, da die Zusammenhänge, die bei der Entstehung eines Datums von Bedeutung sind, nicht mitgespeichert werden
- Gezielte Auslese von Arbeitnehmern nach nur bedingt durchschaubaren Auswahlkriterien
- Breitere Grundlagen, bei geringem Aufwand für eine schnelle und handhabbare Praxis von ‚schwarzen Listen‘
- Schnellere und umfangreichere Möglichkeit des Informationsaustausches zwischen Arbeitgebern
- Totale Überwachung der Leistung und des persönlichen Verhaltens der Arbeitnehmer
- Abbau der noch verbleibenden, der Regeneration dienenden Freiräume
- Erhöhter Leistungsdruck
- Größere Transparenz der Persönlichkeitsstruktur für den Arbeitgeber [25]

3.4 PISe in der betrieblichen Realität

3.4.1 Einführungsgründe

Trotz der Gefahren und Risiken, die sich bei der Einführung von PISen für den Arbeitnehmer ergeben, gibt es hauptsächlich für den Arbeitgeber eine Reihe gute Gründe ein PIS zu installieren. Diese liegen vor allem im Bereich der Flexibilität und der Verbesserung der Datenbasis des Betriebs.

Im einzelnen wurden auf eine Umfrage von Kilian (1981) folgende Argumente genannt. „Der absolut ... häufigste Grund war, eine Vergleichbarkeit und Vereinheitlichung im Konzern zu erzielen. An zweiter Stelle standen der Wunsch, durch das PIS die Genauigkeit, Umfassendheit und Aktualität der Personalplanung für die Unternehmensleitung zu erreichen sowie den Arbeitsablauf im Personalbereich zu rationalisieren.“ Dazu kamen Argumente wie:

- Kostenreduzierung
- schnellere Reaktion auf gesetzliche Änderungen
- schnellerer Zugriff für tarifpolitische Überlegungen
- schnellere zieladäquate Entscheidungsfindung für die Geschäftsleitung
- einfachere Verwaltung der zunehmenden Datenfülle und der gesetzlichen Erfordernisse

Für den Arbeitnehmer bleiben nur einige stark zu relativierende Vorteile. Dazu gehört die zeitliche Entlastung von Routinearbeiten, die u.U. mit Personalabbau einhergeht. Dazu gehört die Möglichkeit einen geeigneteren Arbeitsplatz zu finden, und eine gewisse Sicherheit des Arbeitsplatzes aufgrund wirtschaftlicher Vorteile für den Gesamtbetrieb [57].

3.4.2 Einführungsstrategien

Um dem Arbeitnehmer die Einführung von PISen schmackhaft zu machen, bedient sich der Arbeitgeber im Wesentlichen zweier Methoden.

Eine Methode ist eine Art ‚Salamitaktik‘, bei der Systeme stückweise nach einer Gewöhnungszeit eingeführt und erst später miteinander verbunden werden. So dient zum Beispiel die arbeitnehmerfreundliche Gleitzeit oft dazu, einen computerlesbaren Ausweis einzuführen, um den erhöhten Verwaltungsaufwand abzufangen. Mit diesem Ausweis kann später die automatische Kantinenabrechnung erfolgen oder das Tanken an der betriebseigenen Tankstelle organisiert werden.

„Oft erfolgt der Einstieg mit der Begründung des Unternehmens ‚wir wollen doch nur abrechnen‘. ... Zu diesem Zweck werden natürlich Daten zu Banken transferiert, Daten mit Krankenkassen ausgetauscht usw.“

Eine andere Methode besteht darin, die Konsequenzen von PISen systematisch zu verharmlosen. „Es wird der Eindruck erweckt, das System wird nur eingeführt, um den Beschäftigten die Arbeit zu erleichtern und mehr Gerechtigkeit durch ‚Objektivierung der Entscheidungsfindung‘ durch den Computer zu ereichen.“ Diese Verharmlosung ging in einigen Fällen so weit die Verfügung über umfassende Daten mit der sozialen Betreuung der Beschäftigten gleichzusetzen [52].

3.4.3 Kontrollmöglichkeiten durch den Betriebsrat

Die Kontrolle eines PIS durch den Betriebrat ist relativ schwierig. Trotzdem lassen sich einige Grundsätze angeben.

- Je früher die Kontrolle ansetzt, desto effektiver wirkt sie sich aus. Konkret heißt das, daß eine Kontrolle bei der Planung des PIS effektiver ist als eine Kontrolle der Verwirklichung. Die Kontrolle der Eingabe von Personalinformationen ist effektiver als die Kontrolle ihrer Verarbeitung.

- Je weniger Personalinformationen gespeichert werden und je konkreter ihr Verwendungszweck festgelegt wird, desto besser läßt sich ihre Verarbeitung nachvollziehen.
- Personalinformationen sollten transparent verarbeitet werden. Dies kann mit organisatorischen Maßnahmen wie lesbaren Computerausdrucken, dokumentierten Programmen, Einführung von Zugriffsrechten, der Vereinbarung von Zwangsprotokollen für bestimmte Datenläufe zumindest teilweise erreicht werden.
- Es sind rechtliche Regelungen notwendig, die Informationshaushalt und -verkehr regeln und transparent halten.
- Es ist notwendig, bestimmte Datenbestände voneinander zu trennen, z.B. Personaldaten und Betriebsdaten.
- Daten sollten so ungenau wie möglich gehalten werden; z.B. ist es möglich, nur kumulierte Daten bei Zeitabläufen zu speichern.

Die meisten Maßnahmen machen einen Mißbrauch zwar nicht unmöglich, erschweren ihn aber zumindest. In der betrieblichen Realität ist es jedoch oft schwierig, nur einige der genannten Möglichkeiten durchzusetzen [57, 52].

3.4.4 PAISY bei der Adam Opel AG

„‚PAISY‘ ist die verharmlosende und verniedlichende Abkürzung für das **P**ersonal-**A**brechnungs- und **I**nformations-**SY**stem, das ... bis 1971 von der Lammert Unternehmensberatung GmbH, Bremen, entwickelt wurde. PAISY ist bei Unternehmen aller Größenordnungen und Branchen im Einsatz“, da es einige entscheidende Vorteile gegenüber anderen Systemen besitzt.

- PAISY verursacht nur ca. 10-20 Prozent der Kosten, die bei einer vergleichbaren Eigenentwicklung zu erwarten wären.
- Es läßt sich in kurzer Zeit, im Schnitt innerhalb von einem viertel bis einem halben Jahr, einführen und ist unproblematisch in der Handhabung.
- Das System erfordert ein Minimum an laufender Systempflege und Wartung.

PAISY besteht aus drei Hauptkomponenten: dem Personaldatenbanksystem, dem Personalabrechnungssystem und dem Personalinformationssystem. Abrechnungs- und Informationssystem greifen auf die zentrale Datenbank zu, wobei das Abrechnungssystem standardmäßig alle Funktionen einer traditionellen Finanz- und Lohnbuchhaltung anbietet. Das Informationssystem ist für die Ein- und Ausgabe bzw. Abfrage von Daten zuständig. Zu diesem Zweck stellt es eine leicht erlernbare Benutzersprache zur Verfügung, die unmittelbare Abfragen an einzelne Dateien erlaubt.

Die Einführung von PAISY bei der Adam Opel AG war durch eine stark verharmlosende Strategie von seiten der Geschäftsleitung gekennzeichnet. „PAISY diene primär nur der verbesserten Abrechnung und sollte Auflagen der Sozialversicherungsträger erfüllen. Tatsächlich war aber auch eine personenbezogene Fehlzeitenauswertung (Krankenverfolgung) geplant.“ Nach knapp zwei Jahren Arbeitskampf und dem Einschalten einer Einigungsstelle kam es durch Spruch der Einigungsstelle am 9.7.82 zu folgendem Ergebnis.

Erstmals wurde in einem Großunternehmen die Mitbestimmungs- und Kontrollrechte des Betriebsrates bei Personalinformationssystemen anerkannt. Außerdem war ein Verbot von Profilvergleichen und Verknüpfungen der Personaldaten mit anderen Datenbeständen vorgesehen. Im Juni 83 kam es dazu noch zu einem Verbot personenbezogener Verarbeitung von Krankheitsdaten.

Trotz der Einführung von PAISY und der teilweisen Nichtbeachtung der Betriebsvereinbarung durch die Unternehmungsleitung in der Folgezeit, muß dieser Arbeitskampf positiv beurteilt werden, vergleicht man ihn mit den Ergebnissen bei der Einführung von ISA bei der Daimler Benz AG [12].

3.4.5 ISA bei der Daimler Benz AG

„Bei Daimler-Benz wurde das zunächt nur für den Arbeitsbereich geplante PIS ISA (Informationssystem Arbeitseinsatz und Arbeitsplatzplanung) erstmals im August 1978 der Kommission für Arbeitsgestaltung des Gesamtbetriebsrats vorgestellt. Im Hinblick auf die Schwerpunktsetzung auf Anforderungs- und Eignungsprofile, auf den Profilabgleich, für die Personaleinsatzplanung und auf die generellen Ziele, entspricht ISA dem klassischen Konzept von PIS. Es beinhaltet 220 Mitarbeiterdaten und 330 Arbeitsplatzdaten und sieht den Profilabgleich für Personalplanungsmaßnahmen und die Vorentscheidung personeller Entscheidungen vor."

Im folgenden Arbeitskampf wurden dem Betriebsrat keine Mitbestimmungsrechte eingeräumt. Es wurden Vereinbarungen getroffen, ihn umfassend über das System und geplante Änderungen zu unterrichten. Desweiteren wurde von seiten der Geschäftsleitung auf den automatisierten Profilabgleich bei Einzelarbeitsplätzen verzichtet, und teilweise und vorübergehende Anonymisierung von Gesundheitsdaten zugesichert.

Neben ISA wurde in den Jahren 1981/1982 ein Komm- und Gehzeiterfassungssystem, ein System der bargeldlosen Kantinenabrechnung sowie Zugangskontrollsysteme in einigen Bereichen eingeführt. Für diese Systeme war die Einführung eines computerlesbaren Werksausweises Voraussetzung. Ein Betriebsdatenerfassungssystem war 1984 in Planung [12, 81].

3.5 Stand und Trends bei PISen

3.5.1 Entwicklungsstand

Eine Umfrage von Kilian 1981 in deutschen Großunternehmen ergab, daß bereits 55,2 Prozent der Unternehmen ein PIS teilweise und 23,9 Prozent voll einsetzen. Ca. 44 Prozent dieser Unternehmen erledigten die Bereiche Personalstatistik und -verwaltung voll automatisiert, nur 9 Prozent die wesentlichen administrativen und dispositiven Aufgaben. Bei 98,5 Prozent aller Betriebe, die ein PIS einsetzen, verläuft die Lohn- und Gehaltsabrechnung automatisiert, aber nur bei 3 Prozent vollautomatisch.

Grundsätzlich werden Aufgaben, die einfach formalisierbar sind, in den meisten Betrieben von PISen erledigt. Dazu gehören die Erstellung verschiedenster Statistiken (Fehlzeitenstatistiken, Personalinformationsstatistiken 94 Prozent), Ermittlung verschiedener Formen der Lohnzahlung, Zeiterfassung (Urlaubsermittlung 94 Prozent, Terminüberwachung 64,2 Prozent u.ä.). Eine automatisierte Leistungsbewertung und Leistungsbeurteilung findet in über der Hälfte aller Betriebe statt; Personalfindung aufgrund eines Profilabgleichs nur in knapp 20 Prozent der befragten Unternehmen. Schwer formalisierbare planerische Entscheidungen werden nur sehr selten vom Rechner gelöst. So findet in keinem Betrieb eine maschinelle Arbeitsmarktforschung statt. Jedoch wird in immerhin 7,5 Prozent aller Betriebe der Freistellungsplan vom PIS bestimmt und mit Versetzungsanregungen abgeglichen [57].

3.5.2 Trends

„Die zukünftige Entwicklung wird entscheidend geprägt sein durch das Zusammenwachsen verschiedener Informationssysteme im Betrieb zu einem zentralen Management-Informationssystem (MIS, Abbildung 3.2) und durch die Tendenz der Entwicklung von überbetrieblichen Informationsnetzwerken."

„Bei MISen handelt es sich um Konzepte für Informations- und Kommunikationsysteme, die alle Unternehmensbereiche durchdringen." Sie sollen sowohl Sachbearbeiter auf der untersten Ebene als auch das Top-Management unterstützen. Die Entwicklung dieser Systeme scheiterte bisher an der mangelnden Formalisierbarkeit betrieblicher Vorgänge als auch an fehlenden technischen Voraussetzungen. Die technischen Vorausetzungen werden irgendwann gegeben sein. Durch die Entwicklung von Informationssystemen der Produktion, der Produktionswirtschaft, des Marketings und durch ihre Verknüpfung in zentralen Datenbanken wird auch die Entwicklung von MISen wahrscheinlicher. Ein umfassendes PIS ist dann nur noch ein Baustein der Kontrolle unter vielen.

Mit überbetrieblichen Netzwerken sind Netzwerke gemeint, die Zugriff auf weltweit verteilte Datenbanken ermöglichen. Mit ihrer Hilfe ist es möglich über Unternehmensgrenzen hinweg Daten von Beschäftigten zu übertragen und zu verarbeiten, unkontrollierbar von Management und Betriebsrat.

Als Folgen sind heute schon zu verzeichnen:

Abbildung 3.2: Das Personalinformationssystem als wesentlicher Bestandteil des MIS

- In Branchendatenbanken werden Informationen über vergleichbare Leistungsdaten gespeichert.
- Internationale Vergleiche von Beschäftigtendaten und z.B. Sozialleistungsdaten werden zur Verlagerung von Produktionsstätten herangezogen.
- Die gleichen Vergleichsdaten werden herangezogen, um Beschäftigte gegeneinander auszuspielen und Druck auf Einkommen und Leistung auszuüben [52].

Kapitel 4

Der gläserne Arbeitnehmer

Thomas Collet

4.1 Personalinformationssysteme

Definition

Ein Personalinformationssystem ist jedes computergestützte Informationssystem, das Arbeitnehmerdaten oder Arbeitsplatzdaten erfaßt, verarbeitet oder weiterleitet. Personalinformationssysteme werden i.a. zur Rationalisierung in Personalabteilungen eingesetzt [25, Kap.2].

Folgen eines computergestützten Personalinformationssystems

Durchschnittlich 2000 Einzelangaben pro Arbeitnehmer werden durch PISe verarbeitet. Der Inhalt eines solchen Systems vermittelt ein nahezu geschlossenes Bild über Leistungs- und Einsatzfähigkeit sowie das Verhalten eines jeden Betroffenen. Dadurch ist der Arbeitgeber in der Lage, sich ein Bild über Stärken und Schwächen seiner Arbeitnehmer zu machen. Unterstützt durch ein PIS wird er nur diejenigen einstellen bzw. weiterbeschäftigen, deren Arbeitsprofil und persönliches Profil weitgehend übereinstimmen.

Die Gefahren und Folgen, die dadurch für den Arbeitnehmer entstehen, sind folgende:

- Langzeitüberwachung durch Langzeitspeicherung persönlicher Daten
- Einmal gespeicherte Daten können zu den unterschiedlichsten, nicht mehr mit der eigentlichen Erhebung in Verbindung stehenden Zwecken benutzt werden
- Verlust des Kontextes, da die Zusammenhänge, die bei der Entstehung eines Datums von Bedeutung sind, nicht mitgespeichert werden
- Gezielte Auslese von Arbeitnehmern nach nur bedingt durchschaubaren Auswahlkriterien
- Breitere Grundlagen bei geringerem Aufwand für eine schnelle und handhabbare Praxis von „schwarzen Listen"
- Schnellere und umfangreichere Möglichkeit des Informationsaustausches zwischen Arbeitgebern
- Totale Überwachung der Leistungen und des persönlichen Verhaltens der Arbeitnehmer
- Gefahr des Abbaus der heute noch verbleibenden, der Regeneration dienenden Freiräume
- Erhöhter Leistungsdruck
- Größere Transparenz der Persönlichkeitsstruktur für den Arbeitgeber [25, Kap.8]

4.2 Rationalisierung

4.2.1 Tendenzen

In Abkehr von den umfassenden Informationssystem-Konzepten, die im Management Verwendung finden, werden *Teilinformationssysteme* für einzelne betriebliche Funktionsbereiche entwickelt. Die Personaldatenverarbeitung wird dabei über reine Verwaltungs- und Abrechnungsaufgaben hinaus zu weiterreichenden Planungszwecken eingesetzt. Dieser Einsatz findet in zunehmendem Maße auch auf Konzernebene statt, obwohl er durch ständig sinkende Hardware-Kosten und effizientere Programme auch für mittlere und kleinere Unternehmen interessant wird. Der Trend geht dahin, komplette Programmpakete bei Softwarefirmen günstig zu kaufen, statt langwierige und kostspielige Eigenentwicklung zu betreiben.

4.2.2 Der Rationalisierungseffekt

Personalinformationssysteme stellen Rationalisierungsmaßnahmen dar, die ökonomischen Nutzerwartungen zu entsprechen haben. Dadurch wird ein doppelter Rationalisierungseffekt erzielt: zum einen in der Personalabteilung selbst, zum anderen im Produktionsbereich.

Während durchschnittlich 25-30 Prozent aller Büroarbeitsplätze als automatisierbar eingestuft werden, gilt für die Automatisierbarkeit von Tätigkeiten in der Personalverwaltung ein langfristiger Schätzwert von 80 Prozent. Betroffen sind hauptsächlich Routinearbeiten wie die Datenerfassung und Belegerstellung für Lohn- und Gehaltsabrechnungen. Durch die Einführung eines PIS ist in der Personalabteilung innerhalb von vier Jahren eine Kostensenkung von 30 Prozent möglich. Im Bereich der öffentlichen Verwaltung lassen sich Personalbedarf und -kosten sogar bis zu 50 Prozent kürzen.

Für den Produktionsbereich ergibt sich die Rationalisierung erst durch Auswertung und Analyse betrieblicher und personenbezogener Daten. Dazu wird der Produktionsablauf nach arbeitswissenschaftlichen Kriterien strukturiert, in kleinste, datengerechte Arbeitsschritte zerlegt und jeder Arbeitsplatz mit zahlreichen Merkmalen in der Arbeitsdatenbank gespeichert. So können Anforderungsprofile einzelner Arbeitsplätze mit den Persönlichkeitsprofilen der Arbeitnehmer verglichen werden und die Idee vom *arbeitsplatzgerechten Beschäftigten* wird Realität. In Verbindung mit Gesundheitsdaten, Fehlzeitstatistiken und anderen Auswertungen entsteht auf diese Weise eine Rastersuche, als deren Ergebnis „olympiareife Mannschaften“ aus gesunden, starken und angepaßten Mitarbeitern in den Betrieben übrigbleiben. Eine Verschärfung dieser Situation ist bei diesem erhöhten Rationalisierungsdruck durch krisenhafte Entwicklungen des Wirtschaftssystems zu erwarten.

Insgesamt sind durch die Rationalisierung mit Hilfe der neuen Technologien bis 1990 in der Bundesrepublik Deutschland 3 bis 3,5 Millionen Arbeitsplätze gefährdet, wovon 2,5 Milllionen Arbeitsplätze den neuen Informations- und Kommunikationstechniken zugerechnet werden. Ein großer Teil dieser Rationalisierungsauswirkungen dürfte auf den Einsatz von PISen zurückzuführen sein.

4.2.3 Soziale Auswirkungen und Gefährdungen für den Arbeitnehmer

Die sozialen Auswirkungen und Gefahren der Rationalisierung durch PISe ergeben sich aus dem interessenbezogenen Technikeinsatz der Arbeitnehmer durch den Arbeitgeber. Die Standardisierung der Arbeitsabläufe, die effektiv erst durch ein PIS ermöglicht wird, führt zur Entwertung von im Laufe der Zeit angesammelter Berufserfahrung und damit zur Dequalifizierung des Arbeitnehmers, in deren Folge es oft zu Herabsetzungen in niedrigere Lohngruppen kommt.

Auch wird mit Hilfe eines PISes eine gezielte Auslese anhand von durch die Unternehmensleitung definierten Kriterien möglich, so daß Entlassungen mit Hilfe des Computers schnell und effizient durchgeführt werden können. Durch die Langzeitspeicherung von Leistungs- und Verhaltensdaten sowie durch freie Datenverknüpfbarkeit und den Verlust des Erziehungskontextes entstehen sogenannte *Datenschatten*, d.h. Daten von ehemaligen Mitarbeitern sind noch im PIS gespeichert bzw. überholte Daten von Mitarbeitern wurden noch nicht gelöscht. So wird der Arbeitnehmer zum **gläsernen Menschen** mit für den Arbeitgeber transparenter Persönlichkeitsstruktur.

Doch nicht nur während der Arbeitszeit ist der Arbeitnehmer durch ein PIS gefährdet, auch seine Freizeit wird mehr und mehr in Mitleidenschaft gezogen, da durch die Ermittlung von Leistungsreserven und zunehmende

Reduzierung der „unproduktiven“ Zeit eine Arbeitsverdichtung und somit eine Erhöhung des Leistungsdrucks stattfindet, die mittelfristig auf den Abbau der noch verbliebenen Freiräume abzielt.

Neben diesen direkten Gefahren ist der Arbeitnehmer durch die Existenz eines PISes in seinem Betrieb aber auch indirekt gefährdet, da der Betriebsrat die Rechte des Arbeitnehmers nicht mehr in dem Umfang wahren kann, wie das ohne ein PIS möglich war. So werden Entscheidungen auf Betriebsebene, die Änderungen oder den Ausbau des PISes zum Inhalt haben und mittelbar zu noch umfassenderer Kontrolle des Arbeitnehmers führen, ohne Mitspracherecht des Betriebsrates getroffen, Informationen werden ihm vorenthalten und der kontrollierende Zugriff auf das PIS erschwert, wenn nicht gar verweigert.

Insgesamt erhöht die Anwendung von PISen in Verbindung mit Profilvergleichen die Häufigkeit innerbetrieblicher Umsetzungen und verstärkt so die soziale Isolation des Arbeitnehmers [12, Kap.CI].

4.3 Testverfahren

4.3.1 Aufgaben und Kriterien eines Tests

Bestimmung des Eigenpotentials durch psychologische Untersuchungen

Der Mensch ist durch seine Komplexität nicht als Einheit erfaßbar. Deshalb wird eine Vielzahl psychologischer Testverfahren angewendet, die dazu bestimmt sind, spezielle menschliche Fähigkeiten in ihren Ausprägungen zu erfassen. Der Test bildet eine „... Verhaltensprobe, die möglichst exakt eine Teilfunktion der Persönlichkeit erfassen soll ...“. Nach der Analyse der verschiedenen Persönlichkeitselemente werden diese meist wieder zu einer Einheit zusammengefügt.

Aber ein Unternehmen nutzt nur einen bestimmten Teil des individuellen Eignungspotentials eines Mitarbeiters. Deshalb richtet sich die Fragestellung bei einer Beurteilung nicht primär an die Erfassung der Gesamtpersönlichkeit, sondern an die Ermittlung der durch das Unternehmen nutzbaren individuellen Eignungen.

Solche Testverfahren finden immer stärkere Anwendung in der *Personalbeurteilung*.

Zuverlässigkeit der Testverfahren

Ein Test wird zuverlässige und genaue Resultate liefern, wenn folgende drei, voneinander abhängige Kriterien erfüllt sind:

1. große *Streuung* der Resultate
2. normale bzw. regelmäßige *Verteilung* der Resultate
3. *gleichartige Resultate* einer Testperson, wenn der Test mehrmals angewendet wird.

Aussageumfang eines Tests

- Ein Test kann die Stellung eines Einzelnen innerhalb einer Gruppe von Personen in Bezug auf ein bestimmtes Persönlichkeitsmerkmal feststellen.
- Er kann den Grad der Ausprägung eines Persönlichkeitsmerkmales bestimmen. Das bedeutet, er kann eine Auslese nach einem bestimmten vorgegebenen Merkmal erzielen.
- Er kann das Profil einer Persönlichkeit sichtbar machen.
- Er kann Veränderungen eines Merkmales innerhalb einer Zeitspanne aufzeigen.
- Er kann Prognosen über das zukünftige Verhalten einer Person aufstellen.

Testgütekriterien:

Testgütekriterien dienen dazu, einen Test anhand gleicher und vergleichbarer Forderungen beurteilen zu können. Sie sind somit Grundforderungen, die jeder Test erfüllen sollte.

Hauptgütekriterien sind *Objektivität*, *Reliabilität* und *Validität*. Zu den Nebengütekriterien zählen *Normierung*, *Vergleichbarkeit*, *Wirtschaftlichkeit* und *Nützlichkeit*.

1. **Objektivität**

   Ein Test kann als objektiv bezeichnet werden, wenn verschiedene Auswerter unabhängig voneinander zu übereinstimmenden Aussagen gelangen. Es lassen sich verschiedenartige Aspekte bei der Objektivität von Tests unterscheiden:

   (a) *Durchführungsobjektivität* liegt vor, wenn eine Testperson trotz unbewußter oder bewußter Verhaltensveränderungen der Untersuchenden während des Testvorganges unbeeinflußt bleibt.

   (b) Die *Auswertungsobjektivität* beschäftigt sich mit der Auswertung des aufgezeichneten Testverhaltens. Handelt es sich um Testaufgaben, bei denen einzelne Antworten in eine Bewertungsskala einbezogen sind, so ist völlige Auswertungsobjektivität garantiert.

   (c) Die *Interpretationsobjektivität* sagt aus, in wieweit die Testergebnisse von der Person des Auswerters abhängig sind. Gelangen mehrere Untersucher bei der Auswertung eines Tests zu gleichen Ergebnissen, so läßt sich von absoluter Interpretationsobjektivität sprechen.

2. **Reliabilität**

   Sie beschreibt die Genauigkeit eines Tests. Ergibt sich für die Testperson bei mehrfacher Wiederholung eines Tests das gleiche Ergebnis, so wird der Test als vollständig reliabel oder auch als stabil bezeichnet.

3. **Validität**

   Sie gibt den diagnostischen Wert bzw. den Genauigkeitsgrad an, mit welchem der jeweilige Test die zu erfassende Eignung, Fähigkeit oder Verhaltensweise tatsächlich mißt. Validität ist demzufolge ein Maß für die Treffsicherheit, das heißt, sie gibt an, wie gut ein Test tatsächlich das ermittelt, was er ermitteln soll. Zum Beispiel ist ein Intelligenztest dann valide oder gültig, wenn er ausschließlich nur die Intelligenz eines Probanden mißt und nicht etwa seine Vorbildung, Geschicklichkeit oder ähnliches.

   Es werden verschiedene Aspekte der Validität betrachtet:

   (a) *Inhaltsvalidität*: Die Aufgaben eines Tests müssen eine repräsentative Stichprobe aller möglichen Aufgaben bilden, die das Persönlichkeitsmerkmal umfassen.

   (b) *Übereinstimmungsvalidität*: Hier vergleicht man die Testergebnisse mit einem zeitlich konsistenten Kriterium. Im allgemeinen erfolgt ein Vergleich mit einem bereits vorhandenen, validen Testverfahren, das ein ähnliches Persönlichkeitsmerkmal überprüft.

   (c) *Vorhersagevalidität*: Das Testergebnis wird mit Leistungen verglichen, die der Proband voraussichtlich in der Zukunft erbringen wird. Dazu werden Vergleichsdaten anderer Probanden herangezogen. So werden die Ergebnisse eines Vorschultests mit den Leistungen im zweiten oder dritten Schuljahr verglichen.

   (d) *Konstruktvalidität*: Hierbei wird geprüft, ob die Testergebnisse zu erwartende Verhaltensweisen der Testpersonen bestätigen. Es wird festgestellt, ob die Antworten auf einzelne Testfragen dem entsprechen, was aufgrund allgemeiner psychologischer Erkenntnisse erwartet werden darf.

4. **Wirtschaftlichkeit**

   Hier gibt es zwei unterschiedliche Aspekte: Ein Aspekt prüft bei Vorlage mehrerer alternativer Testverfahren, welches das geeignetere ist, ein anderer richtet sich auf die Relation zwischen zusätzlich gewonnener Information und dem dafür erforderlichen Mehraufwand, der im Testverfahren notwendig wird. Diese Beurteilung unterliegt einzig subjektiven Kriterien, die durch persönlichen Erfahrungswert zur Verfügung stehen.

5. **Normierung**

   Die Normierung eines Tests gibt an, wie die Testergebnisse einer Testperson in ein Bewertungssystem einzuordnen sind.

4.3.2 Psychologische Testverfahren

Die psychologischen Testverfahren lassen sich in *psychometrische* und *projektive* Verfahren unterscheiden.

Psychometrische Tests bestimmen möglichst genau und objektiv die Ausprägung einer bestimmten Eigenschaft. Das Verfahren geht davon aus, daß eine Fähigkeit in ihrer Ausprägung durch den jeweiligen *Leistungsgrad* ermittelt werden kann. Jedem psychometrischen Test unterliegt ein feststehendes Bezugssystem, nach dessen einheitlicher Bewertungsskala die Testleistung des Probanden gemessen und eingestuft wird.

Projektive Tests orientieren sich nicht nur an einer speziellen Fähigkeit, sondern versuchen, das gesamte Individuum zu erfassen. Deshalb werden sie auch als *Persönlichkeitstests* bezeichnet. Die Gruppe der projektiven Verfahren lassen sich in *affektive* und *strukturale* Tests aufgliedern. Die affektiven Tests sind darauf ausgerichtet, Phantasie, Gefühl, Wunschvorstellungen und Denkvorgänge als Ausdruck bestimmter Eigenschaften zu deuten. Strukturale Verfahren erfassen unbewußte Äußerungen wie Mimik, Bewegung und andere physische Aktivitäten, aus denen auf Charaktereigenschaften geschlossen werden kann.

Auswahl der Verfahren

Projektive Tests genügen nur in begrenztem Maße der Forderung nach Objektivierung, die in der Personalbeurteilung gestellt wird. Dies resultiert im wesentlichen aus zu geringer Objektivität, Reliabilität und Validität. Aber nicht nur unter dem Gesichtspunkt der Testgütekriterien sind Bedenken gegen projektive Verfahren anzumelden, vielmehr ergeben sich diese auch aus rechtlicher Sicht. Projektive Tests sind so konzipiert, daß sie die gesamte Persönlichkeit eines Menschen erfassen und seine charakterlichen Merkmale offenlegen. Sie erfassen damit mehr als nur das betrieblich nutzbare, individuelle Eignungspotential und stellen durch die Offenlegung der charakterlichen Merkmale einen verfassungsrechtlich unzulässigen Eingriff in die Intimsphäre des Einzelnen dar. Denn das Grundrecht gewährt in Art.1 und 2 des Grundgesetzes das Recht auf den Schutz der ureigensten Intimsphäre. Testverfahren, die in diesen Intimbereich eindringen, stehen so im Widerspruch zu den Gesetzen.

Die psychometrischen Eignungsuntersuchungen dürfen nach geltendem Recht nur auf solche Eigenschaften bezogen werden, die im Rahmen des betrieblichen Anforderungsspektrum benötigt werden.

Ziel von Tests ist es, einen numerischen Ausdruck für die spezifische Eignungsausprägung einer Testperson zu erhalten (z.B. IQ). Diese Forderung wird im wesentlichen durch psychometrische und nur in sehr geringem Umfang durch projektive Tests erfüllt. Daher werden projektive Tests innerhalb der betrieblichen Personalbeurteilung kaum verwendet [58, Kap.3.3].

4.3.3 Kritik zu Testanwendungen

Grundsätzliche Probleme von Tests

Einem Test kann kaum die alleinige Verantwortung für eine Entscheidung zugestanden werden, dennoch wird er den Entscheidungsprozeß nicht unerheblich beeinflussen. Dieser Einfluß wird häufig überschätzt, doch es ist verständlich, wenn sich selbst bei richtiger Gewichtung des Testergebnisse möglicherweise emotional bedingte Antipathien einschleichen. Außerdem darf nie vergessen werden, daß es sich um Menschen handelt, über die mittels eines Tests entschieden werden soll, und damit um möglicherweise weitreichende Konsequenzen im Leben des Betroffenen. So ist es durchaus zu verstehen, wenn auf Testverfahren mit einem gewissen Mißtrauen reagiert wird.

Methodische und technische Einwände

Zu dieser Gruppe von Einwänden zählen alle kritischen Äußerungen, die sich mit der technischen Qualität, d.h. mit dem Grad der Erfüllung der oben genannten Gütekriterien beschäftigen. Dies geschieht unabhängig davon, ob sich die Kritik an einzelne Testaufgaben oder an den Test als Ganzes richtet.

Denn ein Test kann nur dann qualitativ gut sein, wenn er bezüglich Validität und Reliabilität möglichst gute Werte liefert.

Ethische Einwände

1. *Verletzung der Vertraulichkeit*

   Es muß zwischen der Untersuchung zu Forschungszwecken, die anonym oder nicht-anonym sein kann, und der Notwendigkeit einer Untersuchung im Auftrag einer Person oder Instutition unterschieden werden.

   Im ersten Fall ist der Untersuchende meist nur an bestimmten Phänomenen und ihren Zusammenhängen interessiert, nicht aber an der Person des Untersuchten.

   Im zweiten Fall entstehen Gefahren: Falls ein Psychologe dem Auftraggeber berichtet, erhält dieser als Nichtpsychologe Einblick in Fragebogenantworten und deren Auswertung, sowie in den daraus resultierenden Befund. Dies muß vermieden werden. Eine zweite Gefahr stellt die Geheimhaltung gegenüber dem Untersuchten dar. Der Proband muß über das Ziel der Untersuchung informiert werden, man darf ihm die Ergebnisse aber nicht ohne psychologische Beratung mitteilen.

2. *Selektion*

   Das Problem der Selektion ist die Auswahl eines oder mehrerer Kandidaten unter Zuhilfenahme von Testergebnissen. Es tritt vor allem bei *indirekten Testverfahren* auf, die für den Probanden undurchschaubar konstruiert werden, um so Ablehnung oder Falschaussagen seitens des Probanden zu verhindern.

   Eine Selektion kann entweder durch ein möglichst objektives Testverfahren oder durch Gespräche mit dem Personalchef realisiert werden. Alternativ dazu wäre das Losverfahren denkbar, doch wird es wegen fehlender Berücksichtigung der Fähigkeiten eines Bewerbers selten angewendet.

3. *Eindringen in die Privatsphäre*

   Man kann mit jedem Test in die Privatsphäre eines Probanden eindringen, dies gilt nicht nur für Persönlichkeitstests, sondern auch für Begabungs- und Kenntnistests.

4. *Diskriminierung*

   Um Diskriminierung zu vermeiden, ist es wichtig, daß bei der Normierung eines Tests nicht einfach die Ergebnisse einer Population empirisch auf eine andere Population übertragen werden. Die Normen sollten grundsätzlich anhand einer Stichprobe ermittelt und nie aufgrund reiner Erfahrungswerte festgesetzt werden.

5. *Testeinsatz im Betrieb*

   Beim Einsatz von Tests in Betrieben muß vor allem eine umfassende Information der betroffenen Arbeitnehmer erfolgen. Sie müssen über Sinn und Zweck der Testuntersuchung aufgeklärt werden [18, Kap.7].

4.4 Personalbeurteilung, Auswahl

4.4.1 Personalbeurteilung

Bestimmung des qualitativen Personalangebots

Die Erfassung und Speicherung der Personaldaten sowie die Beurteilung eines Arbeitnehmers beginnt bei den Einstellungsuntersuchungen, wird fortgesetzt in unternehmensindividuellen Aus- und Fortbildungsprogrammen und zur Unterstützung von innerbetrieblichen Personalumbesetzungen und endet erst mit dem Ausscheiden eines Mitarbeiters.

Die *Personalbeurteilung* stellt im wesentlichen eine stichtagsbezogene Betrachtung dar. Obwohl sie sich mit einem längeren Zeitraum und den darin ausgeübten Tätigkeiten befaßt, ist ihre Aussage in der Regel nur auf die letzthin gezeigten Leistungen bezogen. Deshalb stellen Personalbeurteilungen zwar einen bedeutenden, aber eben nur einen Aspekt des vorhandenen Eignungspotentials eines Mitarbeiters dar.

Man unterscheidet zwischen zwei Sichten der Personalbeurteilung, nämlich der Sicht der *Verwendungsmöglichkeit* eines Mitarbeiters und derjenigen der tatsächlich erbrachten *Leistung* in einem Tätigkeitsbereich.

Die **Verwendungsbeurteilung** macht Aussagen über die Eignung des Mitarbeiters in bestimmten Bereichen, sie dient als Grundlage für Einsatzplanung, Aus- und Fortbildungsplanung und die Personalführung.

Die **Leistungsbeurteilung** erfaßt erbrachte und beobachtete Arbeitsergebnisse des Mitarbeiters. Sie ist darauf ausgerichtet, eine möglichst objektive Basis für ein Entlohnungssystem zu bilden. Leistungsbeurteilungen sind analytische, auf Einzelmerkmale bezogene Verfahren zur Leistungserfassung und Leistungsbewertung, die das Leistungsergebnis und das leistungsrelevante Verhalten einbeziehen. Die wesentlichen Determinanten dabei sind Arbeit, Körper, Geist und Charakter. Die Leistungsbeurteilung wird in 75 Prozent aller Unternehmen in die Personaldatenbank eingespeichert.

Beurteilungszyklus, Rhythmus von Personalbeurteilungen

Die Beurteilung von Mitarbeitern sollte ein kontinuierlicher Prozeß sein, doch muß dabei beachtet werden, daß sich daraus ein Arbeitsaufwand ergäbe, der in keinem vertretbaren Verhältnis zu der zusätzlich gewonnen Information stehen würde.

Deshalb erfolgen Personalbeurteilungen in regelmäßigen Abständen, die umso kleiner werden müssen, je öfter sich die zugrundegelegte Aufgabenstruktur und die daraus resultierenden Anforderungen einer Stelle ändern. Aber aus zu kurz aufeinanderfolgenden Beurteilungszyklen sind keine bedeutenden Aufschlüsse zu erwarten, da die Ergebnisse nur geringfügig variieren. Deshalb wird in der überwiegenden Zahl von Veröffentlichungen als Richtmaß für regelmäßig anfallende Personalbeurteilungen ein Zeitraum von einem Jahr genannt (Regelbeurteilung). Neben den regelmäßig anfallenden Personalbeurteilungen werden bei bestimmten personalpolitischen Anlässen (Einstellung, Ausbildung, Fortbildung, Versetzung, ...) Sonderbeurteilungen vorgenommen [58, Kap.3.5].

4.4.2 Datenprofile

Zur Objektivierung von Personalentscheidungen schlägt die Personalwirtschaftslehre vor, Fähigkeits- und Anforderungsprofile zu erstellen und diese abzugleichen. Das aus der Arbeitsanalyse gewonnene *Anforderungsprofil* sowie das aus der Eignungsanalyse gewonnene *Fähigkeitsprofil* sind Voraussetzungen aller personalpolitischen Dispositionen und Grundlage der Personalplanung.

Die *Arbeitsanalyse* liefert alle Daten und Angaben für eine Stellenbeschreibung. Dadurch ist sie Grundlage des Begriffs „Planstelle" und Teil des Stellenplans. Man unterscheidet bei der Arbeitsanalyse zwischen zwei Analyseverfahren: den *mathematisch-statistischen Verfahren* und der *Profilmethode*.

Die **mathematisch-statistischen Verfahren** gehen vom *Arbeitserfolg* aus und basieren auf Angaben der Arbeitsquantität und -qualität. Die für die meisten Arbeitsplätze notwendige Beurteilung des Arbeitserfolgs durch den Vorgesetzten schließt subjektive Elemente mit ein und kann bei Pauschalbewertungen zu Beurteilungsfehlern führen.

Demgegenüber strebt die **Profilmethode** ein *Anforderungsprofil* an, dessen Struktur es gestattet, alle im Unternehmen vorhandenen Arbeitsplätze in ein einheitliches Schema zu fassen. Sie ermöglicht einen direkten Vergleich des Arbeitsplatzprofils mit den Fähigkeiten einer Person. Anstatt des meist subjektiv beurteilten Arbeitserfolges wird eine Vielzahl von Arbeitsplatzbedingungen meßtechnisch bestimmt oder durch Bewertungsskalen weitgehend objektiv und reproduzierbar ermittelt. Gegenüber anderen Methoden hat die Profilmethode den Vorteil, daß ihr Verfahrensablauf und ihre Ergebnisse auch für Personenkreise, die sich nur selten damit beschäftigen, leicht verständlich sind.

Gefahren der Profilmethode werden zum einen darin gesehen, daß trotz einheitlicher Definitionen von Anforderungs- und Fähigkeitsmerkmalen die Messung durchaus mit unterschiedlichen Maßstäben erfolgen kann, was die Werte nur bedingt vergleichbar macht. Schwierigkeiten tauchen auch bei der Zuordnung von Fähigkeitsmerkmalen zu den Anforderungsmerkmalen auf. Zum anderen nimmt das Volumen an personenbezogenen Arbeitnehmerdaten analog der Staffelung der Arbeitsplatzprofile zu, wodurch sich die potentiellen Mißbrauchsmöglichkeiten erhöhen. Zum Beispiel läßt sich aus differenzierten Eignungsbeschränkungen der allgemeine Gesundheitszustand eines Arbeitnehmers indirekt erschließen. Außerdem erleichtert die Existenz großer Datenmengen über einen Arbeitnehmer formal-rationale Personalentscheidungen, die den Anschein der Zwangsläufigkeit erwecken. Doch hängt die Rationalität der Entscheidungen grundsätzlich von der Qualität der Verarbeitungsprogramme ab.

Kritisch bemerkt werden soll noch, daß die Personaleinsatzplanung aufgrund der Ergebnisse von Profilabgleichen notwendig solche Beschäftigungsgruppen markieren, für die ohnehin schon eine schwierige Arbeitsmarktsituation besteht (ältere und kranke Arbeitnehmer, sowie Frauen) [57, Kap.6].

Abbildung 4.1: Anforderungsprofil

4.4.3 Personalauswahl aufgrund von Anforderungsprofilen

Für die Personalauswahl ist es wichtig zu wissen, welche Anforderungen ein zu besetzender Arbeitsplatz stellt. Deshalb werden unter der *Anforderungsart* all diejenigen Eigenschaften eines Arbeitsplatzes erfaßt, die diesen charakterisieren und aus denen abgeleitet werden kann, welche Kenntnisse und Fähigkeiten ein Bewerber auf diesen Arbeitsplatz haben muß. Mit Hilfe der Anforderungsart kann zum Beispiel festgestellt werden, ob es in bestimmten Bereichen der Produktion Stellen gibt, die ohne besondere Vorkenntnisse nach kürzester Anlernzeit vollwertig ausgeführt werden können. Jede Anforderungsart muß dabei einer genauen Analyse unterzogen werden, in denen neben Höchst- und Mindestanforderungen vor allem zeitliche Aspekte zu berücksichtigen sind: Da Arbeitsplätze aufgrund langfristiger Überlegungen konzipiert werden, ist davon auszugehen, daß sich die Unternehmen bemühen, diese möglichst auch unter langfristigen Gesichtspunkten zu besetzen. Im Rahmen dieser Zielsetzung sind für jede Stellenanforderung Schwellenwerte zu definieren, die eine langfristige Unter- bzw. Obergrenze bilden. Hierbei handelt es sich um Mindest- und Höchstanforderungen, die eine Arbeitskraft in beiden Richtungen nicht überschreiten sollte, da in jedem Fall eine unzumutbare Beeinträchtigung der Leistungsfähigkeit auftritt. Innerhalb dieses Intervalls liegt die *Normalanforderung*, die eine Arbeitskraft bei eignungsgerechtem Einsatz möglichst erbringen soll.

Die Ausprägung der Anforderungsart wird mit einem numerischen Wert zwischen 0 (keine Ausprägung in der Anforderungsart) und 9 (höchste Anforderung in der Anforderungsart) wiedergegeben. In Abbildung 4.1 sind die Grenzen, zwischen denen die Anforderungsart bei langfristiger und kurzfristiger Betrachtungsweise variieren kann, graphisch erläutert. Jeder Mitarbeiter eines Betriebes hat ein bestimmtes Anforderungsprofil mit einem Wert zwischen 0 und 9. Während des Prozesses der Stellenanalyse werden für jedes Anforderungsprofil lang- und kurzfristige Mindest- und Höchstanforderungen ermittelt. Liegt das Eignungsprofil eines Stellenbewerbers innerhalb dieser Werte, so tritt er in die Gruppe der engeren Stellenbewerber ein. Genügt das Eignungsprofil des Stellenbewerbers diesen Anforderungen nicht, so wird es mit den kurzfristigen Anforderungen verglichen, um bei Mangel an qualifiziertem Personal eventuell eine kurzfristige Stelle zu besetzen. Werden auch hier die erforderlichen Grenzen nicht eingehalten, so scheidet der Mitarbeiter grundsätzlich aus dem Kreis der Bewerber um eine Stelle aus.

4.4.4 Personalbespitzelung

Personalbespitzelung kann durch ein PIS erfolgen, da es große Datenmengen von Arbeitnehmern speichert und diese unter Umständen leicht zugänglich macht. Solche Daten können z.B. gespeicherte Telefonnummern sein, die ein Mitarbeiter während eines Tages aus beliebigen Gründen gewählt hat.

Personalbespitzelungen treten in Betrieben praktisch jeden Tag auf, da der Arbeitnehmer durch Abstempeln von Arbeitsbeginn und Arbeitsende an Stechuhren, durch Zugangskontrollen per Ausweis für bestimmte Räumlichkeiten, aber auch durch Kameraüberwachung ständig überwacht wird.

Besonders gefährdet in Bezug auf Personalbespitzelungen sind Personen, die Geheimnisträger für einen Betrieb sind.

Rechtliche Möglichkeiten gegen Personalbespitzelungen

Zuerst muß festgestellt werden, welche und wieviele Geräte der verschiedenen systemtechnologischen Arten, die zu Überwachungszwecken eingesetzt werden können, bereits eingeführt sind. Dabei bedürfen Personaldatensysteme zu ihrer Einführung eines ein- bis zehnjährigen Zeitraumes.

Die Personaldatenverarbeitung ist unselbständiger Bestandteil übergreifender Technologie- und Organisationsplanungen eines Betriebes. Ohne Kenntnis des gesamten Sollkonzepts ist es für die Betroffenen unmöglich, die scheinbar völlig isoliert und unzusammenhängend eingeführten Einzeltechnologien einzuschätzen. Um dies dennoch zu erreichen, muß ein Technologie-Arbeitskreis gegründet werden, der das technische Wissen für Betriebs- und Personalräte beschafft und aufbereitet, den Informationsaustausch in technischen Fragen inner- und außerbetrieblich organisiert, sowie den Kontakt zur zuständigen Gewerkschaft sucht. Von Arbeitgeberseite her sollte die Belegschaft über technische Entwicklungen im Betrieb, ihre Auswirkungen auf die Beschäftigten sowie über mögliche Gegenwehr und Alternativen unterrichtet und durch konstruktive Mitbestimmung in den Betrieb eingebunden werden. Denn erst im kollektiven Zusammenhang ist individuelle Wahrung der Rechte möglich, da es sich bei der Einführung der neuen Technologien um transindividuelle Zusammenhänge handelt [96, S.17ff].

4.5 Stellung des Betriebsarztes

4.5.1 Aufgaben und Pflichten des Betriebsarztes

Ein Betriebsarzt steht sowohl mit der Betriebsleitung, als auch mit den Arbeitnehmern in Kontakt. Einerseits berät er den Arbeitgeber in Fragen des Arbeits- und Gesundheitsschutzes sowie der Unfallverhütung, andererseits führt er Einstellungs- und Reihenuntersuchungen an Arbeitnehmern durch, deren Ergebnisse er erfaßt und auswertet.

Die dabei zustandekommenden medizinischen Informationen unterliegen der ärztlichen Schweigepflicht, allerdings muß der Betriebsarzt dem Arbeitgeber auf Verlangen das Ergebnis einer arbeitsmedizinischen Untersuchung mitteilen. Dies geschieht entweder in zweigliedriger Form („geeignet“, „nicht geeignet“) oder in dreigliedriger Form („geeignet“, „bedingt geeignet“, „nicht geeignet“). Heute werden etwa 70 Prozent aller Arbeitnehmer von betriebseigenen Ärzten arbeitsmedizinisch untersucht, doch besitzen viele Unternehmen (insbesondere Großunternehmen) keine betriebsärztlichen Zentren, so daß nicht gewährleistet ist, daß Einstellungs- und Reihenuntersuchungen stattfinden, obwohl verschiedene Untersuchungen zwingend vorgeschrieben sind.

4.5.2 Rechnergestützte Funktionen des Betriebsarztes

Der Computer des Betriebsarztes übernimmt größtenteils administrative Aufgaben. Dazu gehören die Terminvergabe für erforderliche Untersuchungen und die Dokumentation von verschiedenen Ereignissen wie zum Beispiel ärztliche Maßnahmen, krankheitsbedingte Abwesenheit, Krankheitsgeschichte oder Krankheitsgründe. Einen geringen Teil des Einsatzes von Computern nehmen Auswertungsprogramme ein (z.B. Ergebnisse von Einstellungen). Das ist darauf zurückzuführen, daß die Zielsetzung der Auswertungen stark von den Bedürfnissen des jeweiligen Unternehmens abhängt und deshalb standardisierte Auswertungsprogramme fehlen.

Bei den meisten Unternehmen erhalten die Personalabteilungen nur Eignungsaussagen über einen Arbeitnehmer. In einigen Betrieben dagegen werden ihnen zudem noch einzelne Befund-, Diagnose- oder Therapiedaten geliefert.

Die Übermittlung *aller* Gesundheitsdaten an die Personalabteilung darf jedoch nicht erfolgen.

4.5.3 Zugriff auf arbeitsmedizinische Daten

In vielen Fällen haben Sachbearbeiter der Personalabteilung Zugriff auf Gesundheitsdaten, die in betriebseigenen PISen gespeichert sind. Für medizinische Eignungsaussagen ist dies auch notwendig. Doch müssen für solche sensiblen Daten besondere Sicherheitsvorkehrungen getroffen werden.

In vielen Betrieben läßt sich der Umgang mit arbeitsmedizinischen Gesundheitsdaten nur sehr schwer oder auch gar nicht mit der Wahrung des Arztgeheimnisses und des Rechts des Arbeitnehmers auf Schutz seiner persönlichen Daten in Einklang bringen. Die meisten auftretenden Probleme beruhen jedoch nicht auf bewußt rechtswidrigem Verhalten der Unternehmen, sondern auf unpräzisen gesetzlichen Regelungen, die bisher noch nicht auf die Voraussetzungen und Folgen einer automatisierten Datenverarbeitung in Großunternehmen zugeschnitten sind.

Unzulässig ist es, wenn der Betriebsarzt Gesundheitsdaten von Arbeitnehmern nicht in sein eigenes Informationssystem, sondern in das PIS des Unternehmens einspeichert.

4.5.4 Änderungen des Arbeitssicherheitsgesetzes

Folgende Verbesserungsvorschläge gibt es:

- Es ist eine neue Vorschrift einzuführen, wonach der Betriebsarzt das Recht hat, die von ihm erhobenen arbeitsmedizinischen Daten zu speichern und zu verarbeiten. Speicherung und Verarbeitung müssen innerhalb eines *seiner* Verantwortung unterliegenden Informationssystems erfolgen und dürfen organisatorisch nicht mit einem betrieblichen Teilinformationssystem verkoppelt werden.

- Befund-, Diagnose- und Therapiedaten dürfen vom Betriebsarzt nicht an das Unternehmen weitergegeben werden. Eine Mitteilung des Betriebsarztes an das Unternehmen darf weder direkte Angaben über Krankheiten enthalten, noch indirekte Merkmale, die den Schluß auf Krankheiten zulassen.

- Eine neue Vorschrift im Arbeitssicherheitsgesetz sollte sicherstellen, daß arbeitsmedizinische Eignungsaussagen für die Personalabteilung nicht allgemein zugänglich sind.

- Eine weitere Vorschrift sollte die beschränkte Verwendbarkeit arbeitsmedizinischer Eignungsaussagen für Entscheidungen zum Schutz der Arbeitnehmer klarstellen [57, Kap.5].

Kapitel 5

Rechtliche Handlungsmöglichkeiten

Monika Keil

5.1 Einleitung

Die in den vorherigen Kapiteln geschilderten Beispiele zeigen, welche Gefahren vom Computereinsatz für die Arbeitnehmer ausgehen. Vom Anspruch her soll das Bundesdatenschutzgesetz (BDSG), wie auch die allein für den öffentlichen Bereich der Länder geltenden Landesdatenschutzgesetze, einer Beeinträchtigung schutzwürdiger Belange entgegenwirken. Ob und wieweit dies tatsächlich der Fall ist, wird sich im folgenden zeigen. Als erstes werden die vorhandenen Kontrollorgane erläutert.

5.2 Bestellung und Aufgaben des betrieblichen Datenschutzbeauftragten

5.2.1 Bestellung des betrieblichen Datenschutzbeauftragten

Der Datenschutzbeauftragte muß bestellt werden, wenn entweder bei automatischer Datenverarbeitung von personenbezogenen Daten in der Regel mindestens fünf Arbeitnehmer oder bei nicht automatischer Datenverarbeitung in der Regel mindestens zwanzig Arbeitnehmer ständig beschäftigt sind. Gezählt werden nur Arbeitnehmer des datenverarbeitenden Betriebs, dagegen nicht freie Mitarbeiter oder Leiharbeitskräfte. Die Personenzahl für jedes der beiden Verfahren wird getrennt ermittelt für das gesamte Unternehmen, also beispielsweise nicht je Niederlassung. Allerdings kann nicht ohne weiteres eine effektive Kontrolle des Arbeitgebers in Datenschutzangelegenheiten erwartet werden, da der Datenschutzbeauftragte vom Arbeitgeber zu bestellen ist und diesem rechenschaftspflichtig ist.

Die Bestellung des Datenschutzbeauftragten ist mitbestimmungspflichtig, falls der bestellte Angestellte aufgrund seiner anderen Aufgaben nicht zum Personenkreis der leitenden Angestellten gehört oder es sich nicht um einen externen Datenschutzbeauftragten (Rechtsanwalt) handelt. Der Datenschutzbeauftragte ist von dieser Tätigkeit her kein leitender Angestellter [30].

5.2.2 Aufgaben des betrieblichen Datenschutzbeauftragten

Der einzelne Arbeitnehmer wird oft genug überfordert sein, wenn er allein seine Datenschutzrechte wahrnehmen will. Aufgrund dieser Tatsache ist dem Datenschutzbeauftragten vom Gesetzgeber die Aufgabe übertragen worden, die Ausführung des BDSG sowie anderer Vorschriften über den Datenschutz im Rahmen der ihm gesetzlich eingeräumten Befugnisse sicherzustellen, das heißt auch gegen den Willen der Geschäftsleitung. Er ist bei der Anwendung auf seinem Gebiet weisungsfrei, was bedeutet, daß er zu keiner anderen Beurteilung gezwungen werden darf. Wegen der Erfüllung seiner Aufgaben darf der Datenschutzbeauftragte nicht benachteiligt werden, woraus sich auch ein gewisser Kündigungsschutz für ihn ergibt.

Der Datenschutzbeauftragte soll weiterhin die zu den Aufgaben einer Geschäftsleitung gehörende Kontrollfunktion übernehmen und die richtige Anwendung der gesetzlichen Vorschrift durch seine Fachkunde unterstützen.

5.2.2.1 Einzelaufgaben

1. Laufendes Führen von Übersichten:
   - Art der gespeicherten personenbezogenen Daten
   - Geschäftszweck und Ziele, zu deren Erfüllung die Kenntnis der gespeicherten personenbezogenen Daten erforderlich ist
   - regelmäßige Empfänger von weitergegebenen gespeicherten personenbezogenen Daten
   - Beschreibung der EDV-Anlagen (gegebenenfalls nur Typenbezeichnung)
2. Überwachung der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen
3. Vertrautmachen der bei der Verarbeitung geschützter Daten tätigen Personen mit den für ihren Bereich zutreffenden Datenschutzvorschriften
4. Beratende Funktion bei der Personenauswahl für den Bereich der Verarbeitung von personenbezogenen Daten

5.2.2.2 Laufende innerbetriebliche Aufgaben

1. Prüfen der Zulässigkeit der Verarbeitung personenbezogener Daten in manuellen und automatischen Verfahren, und zwar in allen Phasen
2. Prüfen der Einhaltung der Richtlinien zur Durchführung der betrieblichen Datenschutzgrundsätze, des Auskunftsverfahrens, von Sperrungen sowie Auswahl und Kontrolle von Dienstleistungsunternehmen
3. Führen von Datenregistern aller personenbezogener Daten unter Berücksichtigung der jeweils vorrangigen Rechtsvorschrift (z.B. Zugriffsrechte, Zuständigkeit, Aufbewahrungsart, Geschäftszwecke, regelmäßige Empfänger)
4. Durchführen von Kontrollen, um die ordnungsgemäße Anwendung von Datenverarbeitungsprogrammen im Bereich personenbezogener Daten garantieren zu können
5. Verfolgung und Auswertung von Datenschutzverletzungen sowie von Beschwerden der Betroffenen
6. Durchführung angemessener und zielgruppenorientierter Ausbildung im Datenschutzrecht
7. Periodische Berichtserstattung an die Geschäftsleitung über Durchführung des BDSG (möglichst in schriftlicher Form) [30]

5.2.3 Rechte des Betriebsrates

Im folgenden sollen die wichtigsten Rechte des Betriebsrates aufgezeigt werden, die es ihm gestatten, den Datenschutz der Arbeitnehmer im Betrieb mitzugestalten.

Überwachungsrecht

Der Betriebsrat hat darüber zu wachen, daß die im Betrieb zugunsten der Arbeitnehmer geltenden Gesetze und anderen Rechtsgrundlagen eingehalten werden.

Die Mitbestimmung bei der Fassung von Personalfragebögen

Es muß eingehend überprüft werden, ob die vom Arbeitgeber erfragten Informationen über die Person des Arbeitnehmers von der Zweckbestimmung des Arbeitsverhältnisses her gerechtfertigt sind. Den Nachweis dafür hat der Arbeitgeber zu führen.

Mitbestimmung bei der Erstellung von Beurteilungsgrundsätzen

Werden anhand der Grundsätze Beurteilungen vorgenommen und Daten erhoben, so unterliegt auch deren Verwendung der Zustimmung des Betriebsrates.

Informationsrecht

Der Betriebsrat kann sich eines Sachverständigen bedienen, der auch ein Arbeitnehmer sein kann [4].

Recht zur Teilnahme an Schulungen

Der Betriebsrat darf sich dabei auch über die Auswirkung der PIS auf die Arbeitnehmer unterrichten lassen, wobei die Kosten der Arbeitgeber zu tragen hat [26].

5.2.4 Aufgaben der Aufsichtsbehörde

Die ab 1.1.1978 bei den einzelnen Bundesländern durch Landesrecht eingerichtete Aufsichtsbehörde wird nur auf Antrag im Bereich des BDSG tätig. Sie hat von Amts wegen die Ausführung des BDSG und des Betriebsverfassungsgesetzes zu überwachen.

Prüfung bei datenverarbeitenden Betrieben

Die Aufsichtsbehörde führt eine Überprüfung durch, wenn ihr ein Betroffener eine Verletzung seiner Schutzrechte begründet darlegt. Stellt die Aufsichtsbehörde einen Verstoß fest, dann kann sie den Betrieb um Abhilfe bitten. Falls der Betrieb hierzu nicht bereit ist, kann die Aufsichtsbehörde den Betroffene entsprechend informieren, damit er seine Rechte gegenüber dem datenverarbeitenden Betrieb verfolgen und gegebenenfalls einen Antrag auf Strafverfolgung stellen kann.

Unterstützung des Datenschutzbeauftragten

Wenn sich der Datenschutzbeauftragte an die Aufsichtsbehörde wendet, muß sie ihn weitgehend unterstützen. Die mit der Überprüfung beauftragten Personen der Aufsichtsbehörde erhalten bei Beschwerde eines Betroffenen, oder für den Fall, daß der Datenschutzbeauftragte um Unterstützung gebeten hat, weitgehende Rechte. So dürfen z.B. das Betriebsgrundstück und Geschäftsräume betreten werden, um dort Prüfungen und Besichtigungen vorzunehmen. Dabei können sie geschäftliche Unterlagen einsehen, und zwar nur soweit dies erforderlich ist. Führt die Behörde Testläufe durch, um Datenverarbeitungsprogramme zu prüfen, dann hat der überprüfte Betrieb einen Anspruch auf Kostenerstattung [30].

5.2.5 Verhältnis zwischen den Kontrollorganen

Der Datenschutzbeauftragte ist verpflichtet, dem Betriebsrat seine Informationen über Ziel und Zweck der Datenverarbeitung auszuhändigen. Allerdings ist es ihm nicht gestattet, Dateien und Daten des Betriebsrates zu kontrollieren, da er nach dem BDSG eindeutig ein Mann des Unternehmens ist und somit keiner Schweigepflicht gegenüber dem Arbeitgeber unterliegt. Der Betriebsrat kann sich nicht direkt an die Aufsichtsbehörde wenden, wenn er Verstöße gegen das BDSG feststellt. Hierzu ist grundsätzlich nur der betroffene Arbeitnehmer oder der betriebliche Datenschutzbeauftragte befugt. Allerdings kann der Arbeitnehmer seinen Betriebsrat bevollmächtigen, die Aufsichtsbehörde einzuschalten [26].

5.3 Betriebsvereinbarung

5.3.1 Grundsätze einer Betriebsvereinbarung zu PIS

Zur Verstärkung des gesetzlichen Datenschutzes zu Gunsten der Arbeitnehmer beim Einsatz von PISen kann die Möglichkeit des Abschlusses einer Betriebsvereinbarung zwischen Betriebsinhaber und Betriebsrat ins Auge gefaßt werden, wobei in den meisten Fällen der jeweilige Gesamtbetriebsrat zuständig sein würde. Allerdings helfen Muster-Betriebsvereinbarungen, die nur von der Gewerkschaft eingeholt wurden und nicht auf die jeweiligen betrieblichen Zwecke ausgerichtet sind, in keinster Weise. Aufgrund dieser Tatsache sollen nur Grundsätze für Betriebsvereinbarungen zu PIS in Form einer Gliederung und Problemfragen herangezogen werden. Ein Grundsatzkatalog, für solch eine freiwillige Betriebsvereinbarung wurde bereits beispielhaft erarbeitet. Nachfolgend werden die wichtigsten Punkte erläutert:

5.3.1.1 1. Zielsetzung

Hier sollte bezüglich des Gesamtsystems und der einzelnen Daten eine konkrete Bestimmung vorgenommen werden. Als Zwecke sollten nur Lohn- und Gehaltsabrechnung, Werksrentenabrechnung, andere spezielle Teilabrechnungen (z.B. Jubiläumsgelder) und Übermittlung an öffentliche Träger (z.B. Sozialversicherungen) erscheinen. Dabei sollten natürlich die Interessen der Arbeitnehmer im Vordergrund stehen. Außerdem sollten Forderungen zur Beteiligung von Betriebsrat und Arbeitnehmer z.B. bei Gestaltungszielen erwähnt werden.

5.3.1.2 2. Geltungsbereich, Gegenstand

Sachlicher und personeller Geltungsbereich der Vereinbarung sollten festgehalten werden. Mit dem sachlichen Geltungsbereich sind alle Computeranwendungen im weitesten Sinne gemeint, auf die sich die Betriebsvereinbarung bezieht. Weiterhin sollte eine Öffnungsklausel enthalten sein, wodurch gewährleistet werden soll, daß die abgeschlossene Rahmenbetriebsvereinbarung nicht als Zustimmung zu der Nutzung aller weiteren Einzelsysteme verstanden werden kann.

5.3.1.3 3. Rationalisierungsschutz

Der umfassende Schutz vor Entlassungen ist der zentrale Punkt der Vereinbarung. Die Beweislast, daß auch zeitversetzte Rationalisierungsmaßnahmen nicht im Zusammenhang mit der Einführung des EDV-Systems stehen, sollten möglichst bei der Geschäftsleitung liegen.

5.3.1.4 4. Bestandsverzeichnis

Der Betriebsrat sollte das vollständige, aktuelle Bestandsverzeichnis aller technischen Geräte, der genutzten System- und Anwendungsprogramme einschließlich des Dateiaufbaus mit Datenformaten erhalten. Außerdem sollten ihm alle Geräteschnittstellen sowie Verknüpfungsmöglichkeiten und die vorgesehene Verarbeitung und Auswertung der gespeicherten Daten zugängig gemacht werden. Nur so ist eine Überprüfung der Einhaltung der Rahmenbetriebsvereinbarung möglich.

5.3.1.5 5. Beteiligung der Interessenvertretungen

Obwohl die Informationsrechte des Betriebrates im Betriebsverfassungsgesetz eindeutig festgelegt sind, sieht es in der Realität ganz anders aus. Aus diesem Grund sollte es in der Betriebsvereinbarung nochmal ausdrücklich erwähnt werden, daß die Geschäftsleitung bei der Planung von Rationalisierungsmaßnahmen dem Betriebsrat das zugrundeliegende Phasenkonzept zugängig macht.
Die folgenden Schritte tauchen bei mehr oder weniger allen Planungskonzepten für PISe auf:

- Projektantrag
- Ist-Analyse
- Grobplanung
- Detailplanung
- Systemauswahl und -anpassung
- Systemeinführung und -nutzung

Anhand dieses Planungsschemas können die Informationsrechte des Betriebsrat in Hinsicht auf ihre zeitlichen und inhaltlichen Anforderungen näher bestimmt werden.
Die Beteiligung der betrieblichen Interessenvertretungen sollte in einem paritätischen Ausschuß erfolgen. Hier werden die anstehenden technisch-organisatorischen Maßnahmen, die Folgen für die Arbeitnehmer und ggf. Alternativvorschläge diskutiert. Weiterhin sollte festgehalten sein, daß der Betriebsrat Zugang zu den EDV-Geräten hat und sich dort auch Programme, Masken oder Ausdrucke ansehen kann und daß er Sachverständige hinzuziehen kann. Außerdem sollte gewährleistet sein, daß ihm die von der Geschäftsleitung benannten Personen zur Auskunft und Beantwortung von Fragen verpflichtet sind.

5.3.1.6 6. Beteiligung/Rechte der Beschäftigten

Der Arbeitgeber sollte die Beschäftigten bei der Veränderung ihrer Arbeitsbedingungen intensiver beteiligen, zum Beispiel durch die Einrichtung von Projektgruppen. Die Aufgaben der Beschäftigten, die in solch einer Projektgruppe mitmachen, besteht in einer interessenbezogenen konstruktiven Auseinandersetzung mit der neuen Technologie. Für diese Arbeit sollten sie pro Woche einen bestimmten Zeitraum während ihrer Arbeitszeit zur Verfügung stehen haben. Die Rechte des Arbeiternehmers sollten insofern erweitert werden, daß er einen Anspruch hat, jedes halbe Jahr einen Ausdruck aller über ihn gespeichten Daten in verständlicher Form zu erhalten. Die gespeicherten Daten sind auf Verlangen und im Falle ihrer Unrichtigkeit oder Unvollständigkeit zu berichtigen beziehungsweise zu vervollständigen.

5.3.1.7 7. Grundsätze der Technikgestaltung

Im Planungstadium des weiteren Einsatzes von EDV-Systemen sollten zwischen dem Betriebsrat und der Geschäftsführung beraten werden, wie ein dezentraler EDV-Einsatz betriebsorganisatorisch und technisch realisiert werden kann, inwieweit ein möglichst niedriger Vernetzungsgrad der EDV-Systeme erreicht werden kann und wie der Leistungsumfang der einzusetzenden Programme so festgelegt werden kann, daß einerseits die betrieblich notwendigen Funktionen und andererseits qualifizierte Tätigkeiten gewährleistet werden können. Darüberhinaus sollte geklärt werden, wie das Recht auf informationelle Selbstbestimmung der Beschäftigten, aber auch von Kunden, Lieferanten usw. durch technische und organisatorische Abschottungsmaßnahmen umgesetzt werden kann.

5.3.1.8 8. Datenschutz und Zugriffsregelung

Geschäftsführung und Betriebsrat sollten darin übereinstimmen, daß mit Hilfe der Verarbeitung oder Auswertung von Arbeitnehmerdaten keine Leistungs- oder Verhaltenskontrolle durchgeführt wird. Der Betriebsrat hat bei der Erhebung, Speicherung und Verarbeitung von Arbeitnehmerdaten mitzubestimmen. Die Auswertung mit Hilfe von Abfragesprachen, Berichtsgenerator oder Ähnlichem ist unzulässig. Die Weitergabe von Arbeitnehmerdaten an Dritte außerhalb des Unternehmens ist nur zur Erfüllung gesetzlicher Bestimmungen oder Tarifverträgen zulässig. Es sollte sichergestellt werden, daß der Betriebsrat für alle Dateien Zugriffsrechte erhält. Weiterhin sollte gewährleistet sein, daß die EDV-Systeme über eine permanente Protokollierungsmöglichkeit verfügen, so daß nachvollziehbar ist, ob die Abmachungen der Betriebsvereinbarungen eingehalten wurden.

5.3.1.9 9. Regelung bei Streitigkeiten

Eine Betriebsvereinbarung ohne wirksame Sanktion bei Verstößen des Arbeitgebers ist bestenfalls die Hälfte wert. Bei Verstoß des Arbeitgebers gegen die Betriebsvereinbarung sollte der Betriebsrat des Recht haben, diese fristlos zu kündigen, was zur Folge haben muß, daß das gesamte System bis auf die Lohn- und Gehaltsabrechnung nicht bedient werden darf. Weitergehend sollte man eine Vertragsstrafe festlegen [52].

5.3.2 Rechtlicher Rahmen solcher Betriebsvereinbarungen

Weder das Betriebsverfassungsgesetz noch die Personalvertretungsgesetze enthalten einen unmittelbaren Anspruch auf den Abschluß von Rahmenbetriebsvereinbarungen. Solche Vereinbarungen sind vielmehr aus der praktischen Einsicht entstanden, daß bei der Vielzahl betrieblicher EDV-Systeme nicht immer alles neu verhandelt werden kann und soll, sondern einige generelle Verfahren und inhaltliche Zielsetzungen einmalig vereinbart werden sollten. Eine Rahmenbetriebsvereinbarung zielt somit auf eine Art Grundkonsens mit der Geschäftsleitung ab. Rechtlich gibt es im Geltungsbereich des BetrVG zwei Hauptansatzpunkte für den Abschluß solcher Rahmenvereinbarungen.

Zum einen §111 des BetrVG, da die Einführung einzelner Bausteine der neuen Informations- und Kommunikationstechniken auch als eine Betriebsveränderung aufgefaßt werden kann. Dies gilt auch dann, wenn bereits Großrechner, Bildschirmgeräte oder Mikrocomputer installiert sind. Die Vernetzung vorhandener Teilsysteme oder die Anwendung integrierter Softwarepakete auf einem bereits installierten Großrechner erfüllt in aller Regel diesen Tatbestand ebenso wie die Ersteinführung eines LANs oder einer ISDN-fähigen Nebenstellenanlage. Nach der Rechtsprechung reicht es, wenn solche Maßnahmen wesentliche Nachteile, beispielsweise Qualifikationsverluste, Verzögerungen bei Wechselschicht oder zunehmende Belastungen, zur Folge haben können. Das Vorliegen einer Betriebsveränderung gibt dem Betriebsrat das Recht, über einen Interessenausgleich zu verhandeln. Eine juristisch abgesicherte Möglichkeit, das Konzept des Arbeitgebers zu blockieren oder auch nur wesentlich zu modifizieren, besteht nicht. Erzwingbar ist allein ein Sozialplan, der wirtschaftliche Nachteile der betroffenen Arbeitnehmer ausgleicht oder mildern soll [103, 39].

5.3.2.1 §111

1. Falls grundlegende Änderungen der Betriebsanlagen vorgenommen werden sollen, bedarf das der Zustimmung des Betriebsrates.

2. Falls eine Einführung grundlegend neuer Arbeitsmethoden und Fertigungsverfahren erfolgen soll, bedarf das der Zustimmung des Betriebsrates.

Ein echtes Mitbestimmungsrecht eröffnet hingegen §87 des BetrVG. Denn nahezu immer handelt es sich um die Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Nach der Rechtsprechung kommt es nur auf die technische Eignung zur Überwachung und nicht auf die Ziele des Arbeitgebers an. In der Praxis erweist sich jedes Computersystem, auf dem Arbeitnehmerdaten gespeichert oder verarbeitet werden, als mitbestimmungspflichtig [22]. Dies ist z.B. dann der Fall, wenn eine Benutzeridentifikation eingegeben oder die Nebenstellennummer einer Telefonanlage für den Verbindungsaufbau gespeichert wird. Wenn die Mitbestimmungsrechte umfassend und gründlich in jedem Einzelfall ausgeschöpft werden, steigt mit hoher Wahrscheinlichkeit die Bereitschaft des Arbeitgebers zum Abschluß einer Rahmenbetriebsvereinbarung [28, 39].

5.3.2.2 §87

1. Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung des Arbeitnehmers zu überwachen, bedürfen der Zustimmung der Betriebsrates

Ein weiterer rechtlicher Anknüpfungspunkt ist §94 des BetrVG, wonach Personalbögen der Zustimmung des Betriebsrates bedürfen. Bei der Schaffung des Gesetzes hat man sich voll auf den Erhebungsprozeß der Daten konzentriert. Allerdings ist bei dem nun vorliegenden Stand der Automatisierung die weitere Verarbeitung genauso wichtig, weshalb sich die Mitbestimmung des Betriebsrates nach §94 auch darauf beziehen muß [26].

5.3.2.3 §94 (Personalfragebogen, Beurteilungsgrundsätze)

1. Personalfragebogen bedürfen der Zustimmung des Betriebsrates.

2. Persönliche Angaben in schriftlichen Arbeitsverträgen, die allgemein für den Betrieb sowie für die Aufstellung allgemeiner Beurteilungsgrundsätze verwendet werden sollen, bedürfen der Zustimmung des Betriebsrates.

Im Geltungsbereich des Landespersonalvertretungsgesetzes von Nordrhein-Westfalen gibt es seit der Novellierung 1984 ein ausdrückliches Mitbestimmungsrecht bei Einführung, wesentlichen Änderungen oder wesentlicher Ausweitung betrieblicher Informations- und Kommunikationsnetze. Schon die unbestimmten Rechtsbegriffe „wesentliche Änderungen oder wesentliche Erweiterungen" machen eine konkretisierende Dienstvereinbarung erzwingbar. Der Personalrat kann das Arbeitgeberkonzept nur annehmen oder ablehnen, aber keine Modifikation erzwingen und das Letztentscheidungsrecht liegt häufig beim Arbeitgeber [36].

5.3.2.4 Kein Mitbestimmungsrecht wegen früherer Betriebsvereinbarungen?

Nur selten wird das Problem auftauchen, daß eine früher abgeschlossene Betriebsvereinbarung dem Arbeitgeber freie Hand für eine weitgehende Änderung wie die Vernetzung läßt. Im Regelfall werden die von einer Betriebsvereinbarung bzw. einem Einigungsstellenspruch erfaßten Systeme exakt umschrieben, allenfalls einzelne kleinere Änderungen werden dem Arbeitgeber überlassen. Sollte dies trotzdem der Fall sein, würde das von der Rechtssprechung in anderen Zusammenhängen entwickelte Verbot eingreifen, auf Mitbestimmung zu verzichten. Vernetzung ist daher auch in solch einem Fall nur mit dem Betriebsrat oder mit einem Votum der Einigungsstelle möglich.

5.4 Gewerkschaftsforderungen

5.4.1 Vorhandene Schwachstellen

Ein Hauptproblem der Umsetzung des vorhandenen theoretischen Konzepts zum Abschluß einer Betriebsvereinbarung stellt der Umstand dar, daß sich bei der Planung und Einführung von neuen Technologien zumeist nur wenige Betriebsräte um das Problem kümmern, was in der Regel zu ihrer Überforderung führt. Außerdem sehen die Betriebsräte nur kurzfristige Wirkungen in ihrem Bereich, wodurch es dann zu einer Unterschätzung weitgehender Wirkungen kommt. Wenn längere Zeit nach Einführung und Anwendung plötzlich Schlag auf Schlag die Auswirkungen sichtbar werden, tritt meist so etwas wie Panikreaktion oder aber auch Resignation ein. Daraufhin werden dann die Gewerkschaften aufgefordert, Muster-Betriebsvereinbarung zu schicken, welche dann als Rezept benutzt werden, ohne sich eigentlich ausreichend mit den Inhalten auseinandergesetzt zu haben.

Eine weitere Problemsituation ist die, daß es in manchen großen Unternehmen zwischen dem Gesamtbetriebsrat und dem Betriebsrat unterschiedliche Einschätzungen über die Regelungsprobleme gibt, was zu einer gegenseitigen Blockierung führen kann.

Für dieses fehlende oder unzureichende Handeln im Betrieb können folgende Ursachen verantwortlich sein:

- Die Verknüpfbarkeit verschiedenster Daten wird nicht gesehen und somit die isolierte Erfassung als unproblematisch eingestuft.
- Der bisherige Ansatz der reaktiven Schutzstrategie, nämlich die Folgen abzumildern und im nachhinein zu regeln [52].

5.4.2 Aktionsprogramme

Ausgehend von den Ursachen für unzureichendes Handeln wird die Notwendigkeit deutlich, ein systematisches und koordiniertes Vorgehen zu entwickeln, das zwei Elemente umfaßt: einen strategischen Arbeitsplan und ein inhaltliches Schutz- und Gestaltungskonzept.

5.4.2.1 Mögliche Vorgehensweise der Interessenvertretungen

Einflußnahme auf den Planungsprozeß

Es muß das Ziel der Interessenvertretungen sein, die Informationen bis in die erste Planungsphase hinein zu erzwingen.

Informationsbeschaffung

Information des Betriebsrates und der Belegschaft müssen frühzeitig und umfassend erfolgen, spätestens dann, wenn Alternativen vorliegen und diskutiert werden. Der Betriebsrat darf sich nicht mit der passiven Hinnahme betriebswirtschaftlicher oder technischer Informationen begnügen, sondern er muß eine aktive Informationsbeschaffung anhand von Fragelisten und Checklisten zur Bestandsaufnahme betreiben.

Beratungsphase

In der Beratung müssen die Gefährdungsbereiche geklärt werden, die personellen Folgen ausgelotet werden und die betrieblichen Auswirkungen herausgearbeitet werden.

Mobilisierung der Beschäftigten

Betriebsrat und Gewerkschaft müssen für jedermann verständlich die Gefahren aufzeigen, die PISe mit sich bringen können, z.B. über Erfahrensberichte von Betriebsratsmitgliedern, die von ähnlichen unternehmerischen Maßnahmen betroffen sind.

Schutzkonzepte entwickeln

Unter Einbeziehung von Vertrauenspersonen und Experten und unter Heranziehen von gewerkschaftlichen Hilfen müssen Kriterien entwickelt werden, die als Richtschnur für die Verhandlungen dienen.

Verhandlung und Abschluß einer Betriebsvereinbarung

Es ist sinnvoll, Vorgespräche mit der Geschäftsleitung zu führen, um ihre grundsätzliche Bereitschaft zum Abschluß einer Rahmenbetriebsvereinbarung zu erkunden. Der Vereinbarungsentwurf sollte auf keinen Fall irgendeine Muster-Betriebsvereinbarung sein, sondern selbständig in Anlehnung an einen Grundsatzkatalog für eine Betriebsvereinbarung erarbeitet worden sein. Er sollte mit Experten der Gewerkschaft diskutiert werden, bevor er als Verhandlungsgrundlage der Geschäftsführung zugestellt wird.

Laufende Kontrolle ausüben

Vor allem gehört die Aktivierung der Belegschaft zu den wirksamsten Handlungsmöglichkeiten, denn wenn ein großer Teil begriffen hat, wie mit ihren Daten Mißbrauch ausgeübt werden kann, läßt sich ein Datenmißbrauch im Unternehmen wirksam aufdecken. Das Thema gehört deshalb regelmäßig auf die Betriebsversammlung. Um sein Kontrollrecht besser ausüben zu können, sollte der Betriebsrat die Möglichkeit haben über ein eigenes Benutzerprogramm zu verfügen, das es ihm ermöglicht, auf die vereinbarten Datenkataloge und Schlüsselverzeichnisse jederzeit zuzugreifen [52].

5.5 Fazit

Die Regelung des Bundesdatenschutzgesetzes und des Betriebsverfassungsgesetzes haben sich, wie in diesem Kapitel herausgekommen ist, besonders im Bereich des Arbeitslebens, aber auch darüber hinaus, als vollkommen unzulänglich erwiesen. Daher sollte der Bundesdatenschutzbeauftragte aber auch der DGB-Bundesvorstand aufgefordert werden, sich sowohl für die Schaffung eines bereichsspezifischen Datenschutzes im Arbeitsleben als auch allgemein für den Ausbau des Datenschutzes einzusetzen.

Teil III

Computerkriminalität

Kapitel 6

Viren, Würmer und anderes Getier

Uwe Utsch

6.1 Einleitung

Im Dezember 1987 blockierte eine Weihnachtsnachricht das Netzwerk von IBM. Die Nachricht schickte Kopien von sich selbst an jeden angeschlossenen Rechner, die Anzahl der Kopien wuchs exponentiell. Zu guter Letzt mußte das Netzwerk heruntergefahren werden, da fast die ganze Rechenzeit und ein Großteil des Speichers von der Nachricht belegt wurden.

Ebenfalls 1987 wurde an der Lehigh Universität festgestellt, daß eine wachsende Zahl von Disketten unbrauchbar wurde und immer mehr Festplatten zerstört wurden [29, S. 236].

Im November 1988 wurden ca. 6000 Rechner, die am Arpanet, einem von Universitäten, Entwicklungszentren und Militär genutzten Netz, erheblich langsamer und durch Überschreitung des Speicherplatzes fielen viele Rechner ganz aus. Was ist der Grund für ein solch mysteriöses Verhalten?

Daß Rechner abstürzen oder Daten verloren gehen, ist keine Seltenheit, aber in solch einem Umfang ist dies doch befremdend. Die Beispiele beschreiben die Folgen verschiedener Ursachen, die heute viele Computerbesitzer und Systemverwalter in Angst und Schrecken versetzen.

Im ersten Fall handelt es sich um ‚Bakterien', im zweiten um ‚Viren' und im dritten um ‚Würmer'. Aus einem Artikel von P. J. Denning geht hervor, daß Bakterien sich ähnlich wie Computer-Würmer verhalten. Genau wie die Computer-Würmer verschicken auch die Bakterien Kopien von sich an angeschlossene Rechner, aber im Gegensatz zu den Würmern sind die Bakterien nicht in der Lage sich selbst zu starten. Sie benötigen einen Benutzer, der sie startet [29].

Im Fall der Weihnachtsnachricht wurde ein Tannenbaum auf den Bildschirm gemalt, im Hintergrund sendete das Programm derweil Kopien an alle angeschlossenen Computer. Da die Anzahl der Kopien exponentiell wuchs war das Netz innerhalb kürzester Zeit durch das Bakterium verstopft. Erst nachdem das Netz heruntergefahren und alle Kopien der Nachricht aus dem System entfernt waren, war ein normaler Betrieb wieder möglich.

Ebenfalls aus diesem Artikel stammt auch die Information über einen Programmtyp, der ‚Trojanisches Pferd' genannt wird. Hierbei handelt es sich um Programme, die versteckten Code beinhalten, der vom Programmierer aktiviert werden kann. Aktiviert wird dieser Code z.B. durch eine bestimmte Abfrage; werden daraufhin Files (Dateien) gelöscht, spricht man auch von logischen Bomben. Eine andere Anwendungsmöglichkeit der Trojanischen Pferde liegt darin, daß sie in Compiler eingepflanzt in jedes, mit diesem Compiler übersetzte Programm gelangen. Wird so ein Login-Programm übersetzt, besteht die Möglichkeit, ohne Passwort in das System zu gelangen; auf eine Eingabe, die nur dem Programmierer bekannt ist, werden alle folgenden Abfragen, wie z.B. die Passwortabfrage einfach übersprungen und der Eindringling gelangt so in das System. Die Vermutung man könne solchen versteckten Code innerhalb eines Programms entdecken, erwies sich als falsch, wie Ken Thompson zeigte [29, S. 237].

Auf Computer-Viren, Programme, die sich in Wirtsprogramme einnisten, und Computer-Würmer, wird im folgenden näher eingegangen.

6.2 Computer-Würmer (der Arpanet-Wurm)

Wie bereits erwähnt handelt es sich bei Computer-Würmern um Programme die ihren eigenen Code verschicken und diesen auch starten. So geschehen im November 1988. Im Arpanet verbreitete sich ein Programm selbständig und legte dadurch viele Rechner lahm. Das Ereignis wurde in der Presse groß herausgebracht, da an diesem Netz auch das Militär angeschlossen ist und auch hier der Wurm sich ausbreitete.

Wie sich später herausstellte, wurde das Programm von Robert Tappan Morris geschrieben, der eigentlich nur die Möglichkeit eines solchen Programmes zeigen wollte, aber die Ausbreitungsgeschwindigkeit des Programms bei weitem unterschätzte. Es dauerte einige Zeit, bis der Wurm aus dem Netz entfernt werden konnte, obwohl kurz nach dem Auftreten des Wurms auch schon eine Schutzmaßnahme gegen den Wurm veröffentlicht wurde. Eine öffentliche Diskussion über die Sicherheit von Netzen und der daran angeschlossenen Militär-Computer folgte. Professor Brunnstein aus Hamburg vertritt die Auffassung, daß in solchen Netzen, die unter Unix oder unixähnlichen Betriebssystemen laufen, eine Gewährleistung der Sicherheit nicht möglich ist [79, S. 86].

Doch nun zu der Funktionsweise dieses Wurms. Der Wurm besteht aus zwei Teilen, einem Vektor und einem Programmkörper. Von einem Rechner aus versucht der Wurm nun, durch Verschicken des Vektors in einen neuen Rechner zu gelangen. Unix, unter dem die meisten Rechner, die an das Arpanetz angeschlossen sind, laufen, besitzt die Möglichkeit, Prozesse, die keinem bestimmten Benutzer gehören, laufen zu lassen. Diese unabhängigen Prozesse werden Dämonen genannt. Ein solcher Dämon ist ‚fingerd', er ermöglicht Benutzern Information über andere Benutzer zu erhalten. Dies ist in einer Umgebung, in der Programme und Daten zwecks Forschung und Entwicklung gemeinsam benutzt werden, nötig. Der Wurm schickt nun eine Nachricht an einen angeschlossenen Rechner. Für eine Anfrage an ‚fingerd' übergibt der Wurm nun mehr als die benötigten Daten. So gelangen die überzähligen Daten durch einen Programmierfehler in einen Speicherbereich, der von ‚fingerd' normalerweise zur Bestimmung des nächsten Schrittes verwendet wird.

Nachdem die Daten in diesen Bereich gelangt sind, wird ein Kommandointerpreter aufgerufen und ein kleiner Teil des Betriebssystems beansprucht. Steht der Kommandointerpreter nun zur Verfügung, werden ca. 99 Zeilen Sourcecode, die den Vektor darstellen, übermittelt. Dieser Vektor wird compiliert und gestartet, die Infektion ist erfolgt. Durch Ändern des Namens und Löschen der bei der Infektion entstandenen Files, versteckt sich der Wurm. Ist dies geschehen, wird eine Verbindung vom neuen Rechner zum alten aufgebaut und die Files werden kopiert, die den Programmkörper des Wurms bilden. Jetzt besteht die Hauptaufgabe darin, an neue Namen und Adressen zu gelangen, um eine Weiterverbreitung zu ermöglichen. Dazu bricht der Wurm in Bereiche ein, die für rechtmäßige Benutzer reserviert sind. Hierbei kommt ihm die Unvorsichtigkeit und Phantasielosigkeit der Benutzer zu hilfe, die sehr sorglos bei der Wahl ihrer Passwörter umgehen. Ist das Passwort gefunden, gibt der Wurm vor, er sei der rechtmäßige Benutzer und sucht im Speicher nach Namen anderer Rechner, die er infizieren kann [31].

Der Wurm richtete keinen weiteren Schaden an, wie zum Beispiel Zerstörung von Daten, was aber ohne weiteres möglich wäre. Auch konnte durch einen einfachen Trick, der einen Fehler in der Programmierung des Wurms ausnutzte, verhindert werden, daß der Wurm in den Rechner eindrang.

Andere Programme der Gattung der Computer-Würmer sind ‚creeper', ‚town carier', ‚diagnostics' und ‚vampire'. ‚Creeper' hinterlies auf dem Bildschirm nur eine Meldung mit der Aufforderung ihn doch zu fangen, wenn man dazu in der Lage wäre. Bei ‚town crier' handelte es sich um einen Computer-Wurm, der als Bote eingesetzt wurde. ‚Diagnostics' patrollierte im Netzwerk und hielt nach Fehlfunktionen Ausschau. Der Wurm ‚vampire' bewegte sich nur Nachts durch das Netz, wenn die Rechner zum größten Teil unbenutzt waren.

Alle genannten Würmer waren von ihrer Art her ungefährlich, zeigen aber wie anfällig gerade offene Systeme sind. Die große Gefahr der Würmer besteht in der Möglichkeit, Viren und Bakterien in das System zu importieren.

6.3 Computer-Viren

6.3.1 Was ist ein Computer-Virus?

Nach Fred Cohen, einer der Ersten, die sich mit Computer-Viren und deren Ausbreitung in Rechnern befaßten, ist ein Virus ein Programm, das andere Programme infiziert, indem es eine Kopie von sich selbst in den Programmcode des Wirtsprogramms einfügt, um das Wirtsprogramm dahingehend zu ändern, daß weiter Kopien des Virusprogramms bei jedem Start des Wirtsprogramms erzeugt werden. Bei diesem Typ spricht man von Link-Viren, da sie sich in das Wirtsprogramm einbinden.

Das folgende Programm zeigt einen Computer-Virus in einer Pseudoprogrammiersprache. In dieser Programmiersprache wird das ‚:=' Symbol für die Definition verwendet, das ‚:' Symbol dient zur Kennzeichnung einer Marke, das ‚;' Symbol trennt Anweisungen, das ‚=' Symbol wird für Zuweisungen und Vergleiche benutzt und mit den Symbolen ‚{' und ‚}' werden Anweisungen zusammengefaßt.

```
program virus :=
{1234567;
subroutine infect-executable :=
  {loop: file = random-executable;
   if first-line-of-file = 1234567
         then goto loop;
   prepend virus to file;
  }

subroutine do-damage :=
  {liegt im Ermessen des Programmierers, z.B. Verdunkeln des Bildschirms}


subroutine trigger-pulled :=
  {liefert bei einer bestimmten Bedingung true, z.B. das Systemdatum}

main-program :=
  {infect-executable;
   if trigger-pulled then do-damage;
   goto next;
  }
next:
}
```

Der Virus sucht zu Beginn ein ausführbares File (Dateien), bei MS-Dos sind dies z.B. exe oder com Files. Hat der Virus nun ein solches File gefunden, überprüft er, ob am Anfang der Datei die Kennung ‚1234567' steht. Ist dies der Fall, ist dieses File bereits infiziert und der Virus sucht das nächste ausführbare File. Man stelle sich die Prozedur infect-exec so vor, daß die Prozedur abbricht, wenn keine ausführbaren Files mehr gefunden werden, die noch nicht infiziert sind, und ein Sprung nach next durchgeführt wird.

Wenn der Virus ein ‚gesundes' Programm gefunden hat, heftet er sich an den Anfang des Programms, schreibt seine Kennung in die erste Zeile und hat sich somit vermehrt. Aktiv wird der Virus dann, wenn das Wirtsprogramm aufgerufen wird. Da am Anfang der Code des Virus steht, wird dieser auch als erstes abgearbeitet. Erst wenn der Versuch einer Vermehrung beendet ist, wird das eigentlich vom Benutzer gewünschte Programm gestartet.

Die Abfrage if-trigger-pulled ist genau dann wahr, wenn ein bestimmtes Ereignis eingetreten ist; dies kann ein Datum, das Alter des Virus oder aber ein Codewort sein, das von außen in das System eingegeben wird. Falls nun trigger-pulled true ist, wird die Prozedur do-damage aufgerufen. In dieser Prozedur liegt der eigentliche Schaden oder auch in einigen seltenen Fällen der Nutzen des Virus.

Einige gutartige Viren sollen hier nun vorgestellt werden. ‚compress' wurde von Cohen selbst vorgestellt [24]. Dieser Virus sucht alle ausführbaren Files, setzt sich an den Anfang und komprimiert die Daten des Wirtsprogramms. Soll das Wirtsprogramm nun abgearbeitet werden, dekomprimiert der Virus zuerst das Programm, welches dann gestartet wird.

Versuche mit diesem Virus haben gezeigt, daß über die Hälfte des Speicherbedarfs von ausführbaren Files eingespart werden kann. Dies geht natürlich auf Kosten der Rechnerzeit, da vor jedem Lauf die Programme erst einmal dekomprimiert werden müssen. Um eine ungewollte Verbreitung des Virus zu verhindern, sieht Cohen eine Abfrage vor, die vor jeder Komprimierung eines Files den Benutzer um Erlaubnis fragt.

```
program compression-virus :=
  {01234567;

subroutine infect-executable :=
  {loop: file = random-executable;
   if first-line-of-file = 01234567
         then goto loop;
   compress-file;
   prepend compression-virus to file;
  }

main-program :=
  {if ask-permission
         then infect-executable;
   uncompress the-rest-of-this-file into tmpfile;
   run tmpfile;
  }
}
```

Der zweite ist vom CCC-Hamburg entwickelt worden und stellt das lästige Lautsprecherrauschen auf Original-IBMs ab [82]. Ebenfalls positive Eigenschaften besitzen die Antikörper, die Viren in Programmen erkennen und vernichten. Auf sie wird noch im Kapitel Schutzmaßnahen eingegangen.

Da die meisten Viren Schaden anrichten, fallen die wenigen nützlichen Viren nicht ins Gewicht. Relativ harmlose Vertreter ihrer Art verdunkeln nur den Bildschirm oder gehen in eine Endlosschleife. Von einigen Erstellern dieser Plagegeister werden aber ganz andere Überraschungen dem verdutzten Benutzer präsentiert. Vom Löschen der Daten bis zur Zerstörung der Harddisk reicht das Repertoire.

Modifizierte Arten des Urvirus von Cohen schreiben den Virusrumpf ans Ende oder in Bereiche die vom Programm nicht genutzt werden. Diese Viren heften dann an den Anfang des Wirtsprogramms ihre Identifikation und einen Sprungbefehl zum eigentlichen Virusprogramm. Im letzten Fall ändert sich die Größe des Wirtsprogrammes durch die Infektion nicht, wird der Virus aber nur eingebunden, verlängert sich das Wirtsprogramm um die Größe des Virus. Einige Viren verbergen sich nun dadurch, daß sie im Directory wieder die ursprüngliche Länge des Files herstellen. Man bemerkt das Vorhandensein eines Virus dann meist nur, wenn er seine zerstörerische Arbeit vollbracht hat. Da dies in den seltensten Fällen sofort stattfindet, kann man davon ausgehen, daß bereits ein Gros der Daten infiziert ist. Eine weitere, aber einfacher festzustellende Art der Infektion, benutzen überschreibende Viren. Dieser Typ schreibt den Viruskörper einfach auf das ausführbare File. Hierbei wird in den meisten Fällen jedoch das Programm zerstört, so daß das Programm bei einem Startversuch nicht mehr läuft.

6.3.2 Die Tests von Cohen

Am 10. November 1983 wurde das Experiment mit dem oben vorgestellten Virus auf einer VAX 11/750 unter UNIX gestartet. Ein Programm, das die UNIX Struktur graphisch darstellt, wurde infiziert. Es wurden 5 Versuche gestartet und es dauerte weniger als eine Stunde, bis der Virus auf allen Hierarchieebenen angelangt war. Der kürzeste Zeitraum war 5 Minuten, die durchschnittliche Infektionszeit betrug weniger als 30 Minuten. Die Ausbreitung des Virus wurde protokolliert, um am Ende jedes Versuchs alle infizierten Programme wieder vom Virus zu befreien. Keinem Benutzer war es aufgefallen, daß sein aufgerufenes Programm länger als sonst brauchte. Dies lag daran, daß der Virus weniger als 0,5 Sekunden benötigte, um sich zu verbreiten. Als die Ergebnisse bekannt wurden, durften keine weiteren Versuche mehr stattfinden. Obwohl zugesichert wurde, daß alle infizierten Programme wieder in ihren ursprünglichen Zustand zurück versetzt werden sollten. Der Virus, der von Cohen in das System eingeschleust wurde, nutzte keine Schwachstellen oder Fehler des Systems aus, auch wurden keine Optimierungen durchgeführt, um die Geschwindigkeit des Virus zu erhöhen. Dennoch war die Ausbreitungsgeschwindigkeit, wie die Zeiten belegen, sehr hoch.

Im Juli 1984 wurde ein weiterer Versuch auf einer UNIVAC 1108 mit einem Betriebssystem, das auf dem Bell-LaPadula Modell basiert, gestartet. Bei diesem Modell, kann ein Benutzer, der sich auf einem bestimmten

Niveau befindet, keine Daten von einem niedrigeren Niveau lesen und auf kein höheres schreiben. Cohen wollte zeigen, daß sich sogar in diesem sicher scheinenden Betriebssystem Viren ausbreiten können.

Der Virus der unter Zeitdruck entstand, bestand aus 5 Zeilen Assemblercode, ungefähr 200 Zeilen Fortran und ca. 50 Zeilen Command-files. Es konnte nachgewiesen werden, daß der Virus Benutzergrenzen überwand und in höhere Ebenen gelangte. Auch bei diesem Virus wurden keine Tricks angewendet. Die Versuche zeigten wie schutzlos heutige Betriebssysteme Viren ausgeliefert sind.

6.3.3 Beispiele bekannter Computer-Viren

Nachdem nun die Funktionsweise von Viren erläutert wurde, sollen zwei Viren, die häufig in der Presse auftauchen, kurz vorgestellt werden.

6.3.3.1 Der Israeli oder Palästina-Virus

Ein in der Presse immer wieder erwähnter Virus ist der Israeli-Virus, der 1987 von einem Studenten der Hebrew Universität entdeckt wurde. Dieser Virus verlangsamte an bestimmten Freitagen die Rechner um etwa 80 Prozent und sollte am Freitag, dem 13. Mai 1988, alle Files löschen. Dies wurde von der Presse in Zusammenhang mit dem 40. Jahrestag der Besetzung Palästinas durch die Israelis gebracht, weshalb der Virus auch den Namen Palästina-Virus bekam. In vielen Zeitungen wurde gemutmaßt, es handele sich um einen Sabotageakt der Palästinenser. Gegen diese Vermutung spricht jedoch eine Änderung des israelischen Kalenders, demzufolge der 40. Jahrestag Anfang Mai fiel, wo er auch gefeiert wurde. Der Virus konnte entdeckt werden, da er mehrmals dasselbe Programm infizieren konnte und nicht die alte Länge des Files in das Directory (Dateienverzeichnis) eintrug. Hierdurch wurden die Programme immer länger. Eine genaue Beschreibung des Virus war nicht zu finden. In [73] wird jedoch berichtet, daß der Virus seine Aktivierung ‚verschlief' und der erwartete Schaden ausblieb. Die einzigen bekannt gewordenen Störungen in diesem Zusammenhang, betrafen das Bell-Lab. Hier befürchteten einige Systemadministratoren, es könne doch etwas passieren. Das Datum wurde sicherheitshalber am Vortag einen Monat vorgestellt. Dies wurde aber von der Black-Prozedur festgestellt und die Bildschirme blieben schwarz. Wäre das Datum nicht korrigiert worden, wäre ein ordentlicher Betrieb erst einen Monat später wieder möglich gewesen [14].

6.3.3.2 Der Lehigh Virus

In der Lehigh Universität werden Computerdisketten an Studenten verliehen, um ihnen bei ihren Aufgaben, die entweder im Mikrocomputerlabor oder am eigenen PC ausgeführt werden, zu helfen. An der Diskettenausgabe wurden immer häufiger Disketten zurückgebracht, die nicht gestartet werden konnten; auch das Directory konnte nicht mehr eingelesen werden. Im Mikrocomputerlabor, das von allen Studenten der Universität benutzt werden kann, registrierte man eine wachsende Zahl von Harddisk-crashes. Beim Durchsuchen der Directories fand man unter dem Eintrag command.com ein jüngeres Datum, als auf den Sicherheitskopien. Durch diesen ‚Fehler' konnte man den Virus entdecken.

Da der Virus sich in einen Bereich des Programms kopierte, der zur Laufzeit als Stack benutzt wird, änderte sich durch die Infektion die Größe des Files auf Diskette nicht. An den Anfang des Programms wurde ein Sprungbefehl auf den Virusrumpf geheftet. Wurde eine Diskette gebootet, d.h. das System wird gestartet, wobei alle Programme geladen werden, die der Rechner braucht (z.B. Betriebssystem), blieb command.com und damit auch der Virus im Speicher und wurde aktiv. Der Virus wartete nun auf das Ausführen eines Programms, oder aber auf einen Type- oder Dir-Befehl, die unter Dos über den Interrupt 21H laufen. Trat dieser Interrupt auf, überprüfte der Virus, ob es sich um eine Bootdiskette handelte. War dies der Fall, kopierte er sich auf die Diskette und erhöhte sein Alter. Falls der Rechner mit zwei Laufwerken bestückt war, blieb der Zähler im Speicher. Bei Systemen mit Festplatte wurde das Alter auf der Platte gespeichert. Bei einem Reset wurde zwar in einem System mit zwei Laufwerken das Alter des Virus auf Null gesetzt, nicht aber wenn eine Festplatte angeschlossen war. War der Zähler nun größer als drei, begann der Virus mit seiner zerstörerischen Arbeit. Er benutzte den Interrupt 26H (absolute disk write) und schrieb eine Folge von Nullen auf die ersten 32 Sektoren der Bootdiskette bzw. der Festplatte. Durch diese Aktion wurden die Boottracks und Directory-Tabellen zerstört, womit die Diskette unbrauchbar wurde.

Der Virus war nur 346 Bytes lang und man vermutete, daß ein Student ihn über ein bulletin board in die Universität schleppte. Genau wie beim Israeli-Virus waren auch hier Fehler in der Implementierung des Virus der Grund, weshalb man ihn relativ leicht finden konnte. Zum Kopieren des Viruscodes verwendete der Programmierer die Standard-Dos-Funktionen, wodurch sich das Abspeicherdatum des command.com Files änderte. Der zweite Fehler bestand darin, daß nicht überprüft wurde, ob die Diskette im Laufwerk schreibgeschützt war oder nicht. Beim versuchten Schreiben auf eine schreibgeschützte Diskette meldete Dos einen Fehler, woran man erkennen konnte, daß sich ein Virus im System befand. Der letzte Fehler war aber nicht so gravierend, da einige Studenten einfach den Schreibschutz entfernten, um weiter arbeiten zu können [46].

6.3.4 Herkunft und Verbreitung von Viren

Sowohl der Israeli-, als auch der Lehigh-Virus verbreiten sich auf IBM PCs, das heißt aber nicht, daß nur IBM anfällig ist. Auf dem Apple Macintosh zum Beispiel machen INIT29 und MacMag dem Anwender das Leben schwer. Auf dem Amiga heißen sie ByteBandit und SCA und auch der Atari wird von Viren nicht verschont. Hier sind es vor allem Bootsektor-Viren, die haufenweise Daten vernichten.

Der Bootsektor-Virus entspricht nicht mehr der Definition von Cohen, da er nicht mehr jedes File einzeln infiziert (Link-Viren), sondern dieser Virustyp pflanzt sich in die Bootsektoren der Disketten oder Platten und infiziert so die gesamten Daten, und nicht mehr nur die ausführbaren Files. Außerdem gelangt der Virus gleich mit dem Starten in das System und übernimmt die Kontrolle. Dieser Virustyp ist leichter einzuschleusen und schwerer zu entdecken. Besondere Schutzprobleme bestehen beim Macintosh, da der ‚Finder‘, das Mac-Ladeprogramm, eine Diskette ohne Schreibschutz erwartet [14].

Wo kommen sie her und wie verbreiten sich Viren?

Sicherlich handelt es sich bei den Programmierern solch zerstörerischer Programme häufig um Jugendliche, die hiermit ihre Fähigkeiten demonstrieren wollen. Aber auch Software-Häuser sollen Viren in Umlauf gebracht haben, um dem Raubkopieren Einhalt zu gebieten. Eine sehr fragliche Methode, da in den meisten Fällen die Falschen getroffen werden. Diese Viren zerstören alle Files, wenn sie die Raubkopie eines bestimmten Programmes erkennen.

Auch die Rache eines entlassenen Programmierers kann der Ausgangspunkt eines Virus sein. Wie sonst läßt sich erklären, daß ein Virus gezielt nur GFA-Basic-Programme sucht und diese zerstört [82, S. 50]. Denkbar ist es auch, Viren in Umlauf zu bringen, um nach einiger Zeit einen Antikörper zu verkaufen und damit das große Geld zu machen.

Auf Forschungsdrang ist der SCA-Virus genannte Amiga-Bootblock-Virus zurückzuführen. Mitglieder des SCA-Computer-Clubs aus der Schweiz wollten die Machbarkeit eines solchen Virus zeigen. Irgenwie gelangte der Virus aber aus dem ‚Labor‘ sprich Computer und verbreitete sich explosionsartig in Europa. Auch in den USA wurden einige Exemplare entdeckt. Der Virus war harmlos und konnte leicht entfernt werden. Auch wurde sofort ein Antikörper als Public-Domain-Software auf den Markt gebracht. Doch irgendwie mußten einige Leute Spaß daran gehabt haben, diesen Virus zu ändern, so daß der Antikörper diese ‚Mutanten‘ nicht mehr erkennen konnte.

Die Möglichkeit einer spontanen Entwicklung von Viren durch Zufall ist sehr unwahrscheinlich. Die Entwicklung von Viren aus selbstmodifizierenden Programmen hält R. Dierstein (Zentrale Datenverarbeitung der Deutschen Forschungs- und Versuchanstalt für Luft- und Raumfahrt) jedoch für möglich. Insbesondere ‚im Hinblick auf Arbeiten im Zusammenhang mit künstlicher Intelligenz‘ sieht er eine, wenn auch verschwindend kleine Gefahr der zufälligen Entstehung von Computer-Viren [83].

Gerade auf dem Gebiet der PCs sind Viren weitverbreitet. Das liegt daran , daß Schüler und Studenten in der Lage sind, solche Rechner zu erstehen, aber dem Verlangen nach neuer Software ein kleiner Geldbeutel gegenüber steht. So werden also neue Programme einfach kopiert und nicht gekauft. Über Bekannte, die wiederum jemanden kennen, der einen kennt, der die neue Software hat, kommt der Virus ins Haus, und ist er einmal da, verbreitet er sich auch wie ein Lauffeuer auf den restlichen Disketten oder der Festplatte. In Firmen gelangen die Viren dann evtl. über Angestellte, die Disketten von Zuhause mitbringen oder sie werden gezielt von unzufriedenen Mitarbeitern ins System eingeschleust.

Eine sehr große Infektionsgefahr geht auch von Public-Domain-Programmen und Programmen von öffentlichen bulletin-boards aus.

Ein Beispiel, wie sich zufällig Viren verbreiten, ist die Infizierung von FreeHand. Hierbei handelte es sich um ein Graphikpaket für den Apple Macintosh. Der Lieferant diese Pakets war kurz vor Auslieferung bei einem kleinen Computermagazin gewesen und wollte die Kopie eines Spiels haben. Zu Hause bootete er dann das System mit dem kopierten Programm. Dabei muß im andern Laufwerk oder aber auf Platte das FreeHand-System gewesen sein, das nun seinerseits infiziert wurde. Aldus, Lieferant von Ashton-Tate, Lotus und Microsoft, vervielfältigte das Paket. So verbreitete sich der, wenn auch harmlose, Virus über die Softwarehäuser.

Ein weiterer bekannt gewordener Fall, bei dem Software-Firmen Viren durch ihre Programme verbreiteten, betraf die Firma Omikron, die eine neue Basic Version für den Atari ST auf den Markt brachte, die durch einen Virus infiziert war. Als man den Befall feststellte, waren 10.000 Kopien verseucht, 1.500 waren bereits verkauft, und so mußten die Käufer benachrichtigt und ein Antivirus entwickelt werden, um die befallenen Disketten zu säubern. Befürchtet wird, daß auch auf einigen Disketten von ‚GFA Draft ST' Viren vorhanden sind [78, S. 71].

6.3.5 Schutz gegen Computer-Viren

Für die meisten Rechner und Betriebssysteme ist es unmöglich, einen Virus vom eigentlichen Programm zu unterscheiden, da es sich beim Virus ja auch um Programmcode handelt, und dieser somit vom Rechner abgearbeitet wird. Da eine Programmverifikation von großen Systemen derzeit nicht möglich ist, kann auch nicht bewiesen werden, daß ein Programm nur seine spezifizierte Aufgabe erfüllt und weiter nichts anderes tut. Es müssen also andere Schutzmechanismen entwickelt werden, um die Systeme vor Programmänderungen zu sichern. Hier muß sowohl bei der Hard- als auch bei der Software etwas getan werden. Zum Beispiel müßte das Betriebssystem einen unberechtigten Zugriff auf Files erkennen und durch die Hardware muß sichergestellt werden, daß man dies nicht durch Programmier-Tricks umgehen kann.

Ein Mechanismus der heute verwendet wird, verschlüsselt das Programm und entschlüsselt es erst zur Laufzeit. Durch dieses Verfahren wird es Link-Viren unmöglich gemacht, ein so geschütztes File zu infizieren. Bei der Infektion wird uncodierter Programmcode an das vorhandene File angehängt. Bei der Entschlüsselung entsteht somit ein nicht lauffähiges Programm, da ja eine Entschlüsselung auch auf den unverschlüsselten Viruscode angewendet wird und so Programmcode entsteht, der nicht abgearbeitet werden kann. Der Vorteil dieses Verfahrens liegt darin, daß eine weitere Verbreitung von Viren verhindert wird, falls alle Files verschlüsselt abgespeichert werden. Nachteile bestehen darin, daß erstens ein bereits infiziertes Programm geschützt werden kann und dadurch immer noch ein Virus im System ist, und zweitens, daß durch das ständige Ver- und Entschlüsseln bei der Programmentwicklung zum Beispiel viel Zeit verbraucht wird [75]. Ebenfalls müßte ein nicht infiziertes Ver- und Entschlüsselungsprogramm gewährleistet werden, da ansonsten eine Infektion über dieses Programm stattfinden könnte.

Eine andere Methode, die eine gewisse Ähnlichkeit mit der eben vorgestellten hat, bildet eine Prüfsumme über den Programmcode und ermittelt so, ob seit der letzten Prüfsummenbildung sich ein Virus eingeschlichen hat. Stimmt die berechnete Prüfsumme nicht mit der gespeicherten überein, wird das Programm nicht gestartet, da der Verdacht einer Infektion gegeben ist. Nachteil ist auch hier wieder, daß ein bereits infiziertes Programm vorliegen könnte, dies könnte dann ungehindert weitere Programme ‚anstecken'. Ein Programm, das auf diesem Verfahren beruht, findet man in [78].

Bei den eben vorgestellten Verfahren wird bei einer Änderung der Daten auf eine Infektion geschlossen. Anders arbeiten Schutzmechanismen, die Zugriffe über Standard-Systemfunktionen protokollieren bzw. verbieten und somit die Verbreitungsmechanismen der Viren benutzen, um sie aufzufinden. In [73] werden zum Beispiel die Interruptvektoren, die beim IBM PC unter Dos zum Schreiben auf Platte oder Diskette verwendet werden, überwacht und das Schutzprogramm protokolliert und unterbindet jeden Schreibversuch. Der Benutzer erkennt an Hand des Protokolls von welchem Programm auf welche Files zugegriffen wurde, bzw. ob versucht wurde auf die Boot-Sektoren zu schreiben, und kann daraus auf das Vorhandensein eines Virus schließen. Es ist z.B. verdächtig, wenn ein Textverarbeitungsprogramm auf ausführbare Programme schreiben will. In diesem Fall ist anzunehmen, daß das Textprogramm infiziert ist. Im normalen Betrieb ist es zwar nicht möglich bzw. umständlich für jeden Schreibzugriff gesondert eine Erlaubnis zu erteilen, aber zum Testen ob ein Programm infiziert ist, sollte man diesen Aufwand in Kauf nehmen.

Viruskiller erkennen Viren an spezifischen Merkmalen. Dies führt jedoch nur dazu, ganz bestimmte Viren aufzufinden. Für den Beispielvirus von Cohen könnte eine Methode zum Auffinden des Virus darin bestehen, jedes ausführbare Programm nach der Kennung ‚1234567' hin zu untersuchen. Falls diese Kennung gefunden wird, ist das Programm infiziert und der Viruskiller entfernt nach Bestätigung des Benutzers den Virus. Dies ist möglich, da der Viruskiller diesen bestimmten Virus kennt und damit auch seine Lage und Größe kennt. Man sieht aber gleich, durch Änderung der Kennung, etwa in ‚7654321', findet der Viruskiller den Virus nicht mehr und meldet fälschlicherweise ein virusfreies Programm.

Es ist also vermessen, ja sogar gefährlich, wenn Softwarehäuser Programmpakete auf den Markt bringen und verkünden, dieses Paket schütze vor allen bekannten Viren. Die Wette eines israelischen Softwarehauses im April 1988, ihr Programm könne alle bekannten Viren erkennen, konnte nicht gewonnen werden.

6.4 Schlußwort

Wenn bis jetzt nur private Anwender durch Viren geschädigt wurden, kann man sich doch mit etwas Phantasie ausmalen, welche schwerwiegenden Folgen solch ein Programm in der Wirtschaft, in Behörden und beim Militär haben kann. Dabei soll nicht nur der finanzielle Verlust, der Banken entstehen kann, falls die Datenbestände zerstört würden, im Vordergrund gesehen werden, sondern man stelle sich vor, ein Virus legt einen Rechner lahm, der zur Überwachung einer Intensivstation eingesetzt ist. Von diesem Rechner hängt vielleicht das Leben eines Patienten ab. Es bleibt zu hoffen, daß so etwas nie vorkommt, aber auszuschließen ist es nicht. Es ist nicht zu vermuten, daß die geistigen Väter solcher Programme so weit denken. Auch die vielen Appelle an das Lager dieser Programmierer fallen sicher nicht auf fruchtbaren Boden.

Da man nicht in der Lage ist, Viren vollständig aus den Rechnern zu bannen, muß man mit ihnen leben. Der Gesetzgeber ist gefragt, Gesetze zu verabschieden, die eine Handhabe gegen solche gewissenlose Programmierer zur Verfügung stellt, falls man ihrer denn einmal habhaft werden sollte. Die Informatik hat die Aufgabe, zukünftige Systeme sicherer zu machen. Dies muß sowohl auf der Hardware- als auch auf der Softwareseite, sprich, etwa Betriebssysteme, geschehen.

Kapitel 7

Wirtschaftskriminalität: Systemeinbruch und Datenmißbrauch

Harald Blees

7.1 Einleitung

Die Verwendung von Computern in Wirtschaftsunternehmen hat in den letzten dreißig Jahren einen enormen Aufschwung erlebt. Allein in der Bundesrepublik arbeiten mehr als 700.000 EDV-Anlagen und diese Zahl wird beinahe täglich größer [23, S.156]. Verantwortlich dafür sind nicht nur die gefallenen Preise, sondern auch die gestiegene Leistungsfähigkeit der Geräte und die Entwicklung immer besserer Software. Die Entwicklung von Systemen für CAD, CAM, PPS und CAQ ermöglichen den Einsatz von Rechnern in fast allen Bereichen eines Wirtschaftsbetriebes. Textverarbeitungs- und Buchhaltungsprogramme sind aus den meisten Betrieben kaum noch wegzudenken.

Besonders in großen Unternehmen ist der Computer für das Management zur unentbehrlichen Hilfe geworden. In unserer „Informationsgesellschaft" sind die für Entscheidungen relevanten Daten kaum noch manuell zu sammeln. Der Konkurrenzkampf erfordert immer genauere Kalkulationen in Bezug auf Preis, Qualität und Termine. Daher ist es nicht verwunderlich, daß Computer in vielen Unternehmen eine Schlüsselrolle besitzen. Oft liegt ein ganzer Betrieb lahm, weil der Computer mal nicht funktioniert. Diese Abhängigkeit von einem speziellen Gerät macht die Wirtschaftsunternehmen aber auch verwundbar. Diese Verwundbarkeit wird besonders gestärkt durch die Tatsache, daß das Sicherheitsdenken über lange Zeit nicht mit der Entwicklung der Technik und ihren Möglichkeiten gewachsen ist.

Man schätzt, daß der jährliche Schaden durch Computer-Kriminelle, allein in der Bundesrepublik Deutschland mehr als 15 Milliarden DM beträgt [23, S.155], aber die Dunkelziffer für Computerkriminalität ist selbst von Fachleuten nur schwer abzuschätzen, da Computerkriminalität von den meisten Firmen geheimgehalten wird. Welches Kreditinstitut gäbe es schon gern zu, daß es möglich ist, per Computer die Konten der Kunden zu plündern. Da zahlt man lieber noch eine Ablösesumme, damit der Täter möglichst ohne Aufsehen seinen Arbeitsplatz räumt. Man bewertet hier also den möglichen Prestigeverlust höher als die Bestrafung des Täters. Dies ist insbesondere verständlich, wenn man sieht, mit welcher Freude die Medien jede Unsicherheit von Computersystemen an die große Glocke hängen. Aber auch andere Unternehmen (z.B. die Post) sind daran interessiert, daß eventuell vorhandene Sicherheitslücken nicht in das Licht der Öffentlichkeit gerückt werden [15, S.219].

Die beinahe schon als hysterisch zu bezeichnenden Reaktionen der Medien auf gelegentliche Systemeinbrüche, das heißt unbefugte Zugriffe auf Computersysteme durch Umgehung der vorhandenen Sicherungen, kann eigentlich nur mit der Unsicherheit gegenüber dem Unbekannten erklärt werden. Aber vermutlich fühlen auch die Redakteure ein gewisses Unbehagen gegenüber einer Technik, die sie nicht verstehen, und von der immer mehr abhängig gemacht wird. Anderseits wird diese Unsicherheit genährt durch die immer wieder aufgestellte

Behauptung verschiedener Anbieter, ihre Systeme seien sicher gegen unbefugte Benutzung, und der Tatsache, daß trotzdem immer wieder unbefugte Benutzungen fremder Computersysteme bekannt werden.

Ein weiterer Faktor, der von der Presse regelmäßig überschätzt wird, sind die sogenannten Hacker. Nach Schätzung der Allgemeinen Kreditversicherung AG Mainz sind es zu 80 Prozent die eigenen Mitarbeiter, die dank ihrer EDV-Kenntnisse mit digitalen Coups Kasse machen [23, S.156]. Zu einer ähnlichen Einschätzung gelangt auch C. K. Bschorr in seinem Buch „Computerkriminalität".

Welche Möglichkeiten für Wirtschaftskriminalität sich durch den Einsatz moderner Technik ergeben und welche Sicherungsmaßnahmen dagegen ergriffen werden können, ist Thema dieses Beitrags. Insbesondere werden dabei die drei klassischen Bereiche der Wirtschaftskriminalität: Sabotage, Spionage und Diebstahl im Umfeld der modernen Computertechnologie untersucht.

Vorab soll an dieser Stelle noch betont werden, daß es sich bei den meisten vorgestellten Fallbeispielen fast nur um mißlungene oder gescheiterte Versuche handelt, soweit es sich nicht um beabsichtigte Demonstrationen handelt.

7.2 Sabotage

Nach dem Großen Brockhaus ist Sabotage „die Vereitelung eines Ziels durch böswillige geheime Gegenwirkung, sowie die vorsätzliche Beschädigung oder Zerstörung von Maschinen, Arbeitsmitteln, Waren" usw.

Die im Vorwort beschriebene Stellung der Computer in Wirtschaftsunternehmen macht diese Anlagen zu einem besonderen Ziel für Sabotage. Besonders bei Großrechnern sind die Auswirkungen auf ein Unternehmen, die durch Zerstörung der Anlage oder durch Löschen oder Verfälschen der oft lebenswichtigen Datenbestände erzielt werden, kaum abzuschätzen.

Eine Methode einen Computer außer Funktion zu setzen, ist natürlich, ihn mit Hilfe einer Bombe zu beschädigen. Derartige terroristische Methoden wurden lange Zeit durch die Einstellung der Verantwortlichen: „Das Rechenzentrum ist das Schaufenster unseres Betriebes, und da gehört es auch hin" [15, S.8] sehr erleichtert. So wurde am 17.11.1986 ein terroristischer Anschlag gegen das Rechenzentrum des Wissenschaftlichen Zentrums der IBM in Heidelberg durch die „Kämpfende Einheit Hind Alameh" ausgeführt. Mit drei Bomben in Form von Feuerlöschern wurden wertvolle Installationen erheblich beschädigt [15, S.218].

Aber auch der Mitarbeiter, der mit einem starken Permanentmagneten in der Tasche an den Bandrollen mit den Datenbeständen entlanggeht, kann durchaus auf Erfolg hoffen. In diesem Fall wird der Datenverlust nicht einmal sofort bemerkt, sondern möglicherweise erst Monate nach der Tat. Ein Identifizierung des Täters ist dann in den meisten Fällen nicht mehr möglich.

Aus Schaden wird man klug! Heutzutage werden Zentralrechener in speziell abgesicherten Kellerräumen installiert, zu denen nur ein möglichst kleiner Kreis von Berechtigten Zutritt hat. Der Zugang zu derartig sicherheitsempfindlichen Bereichen wird durch maschinenlesbare Ausweise kontrolliert. Somit erreicht man eine gewisse Sicherheit vor Bombenlegern und schränkt zusätzlich den Kreis der möglichen Saboteure stark ein.

Gegen einen direkten Zugriff scheinen Zentralrechner somit verhältnismäßig einfach absicherbar zu sein. Aber es gibt noch andere als die „Holzhammermethode". Einleitend muß hierzu gesagt werden, daß man Computer nicht völlig von ihrer Außenwelt abschneiden kann, denn dies würde ja ihrer eigentlichen Funktion, nämlich der schnellen Verfügbarkeit von Informationen und Rechenleistung für die Berechtigten widersprechen. So gibt es also eine Anzahl verschiedener Zugänge zu einem Rechner, die nicht die physische Anwesenheit des Benutzers beim eigentlichen Rechner erfordern. Je nach Größe und Aufgabe der Rechner existieren neben den Terminalverbindungen noch Anschlüsse an Datennetze und Telefonleitungen.

Zusätzlich gibt es immer bestimmte Benutzer, sogenannte Systemoperateure, denen alle Funktionen eines Rechners offenstehen. Systemoperateure sind für das reibungslose Funktionieren der Rechner verantwortlich. Weiterhin gehört es zu ihren Aufgaben, gelegentliche Anpassungen der Rechnerdienstleistungen an veränderte oder erhöhte Ansprüche der anderen Benutzer durchzuführen. Dieser Aufgabenstellung kann ein Systemoperateur nicht gerecht werden, wenn ihm nicht alle Bereiche eines Rechners offenstehen.

Die besondere Vertrauensstellung der Systemoperateure macht die Betriebe aber auch in besonderem Maß abhängig von der Loyalität dieser Mitarbeiter. So wurden zum Jahreswechsel 1984/85 in einem zur Bundeswehr gehörenden Rechenzentrum sämtliche Programme gelöscht. Verantwortlich für diese „logische Bombe“ war ein Programmierer, der mit seinem Arbeitgeber in Streit lag. Der Programmierer machte für bestimmte Teile des Betriebsprogramms (GURUGS) urheberrechtliche Ansprüche geltend, denn er wollte die Entwicklung auch anderweitig verwerten. Als Beweis seiner geistigen Urheberschaft programmierte er die Löschung des Betriebssystems zum Jahreswechsel und informierte seinen Arbeitgeber. Der hätte eigentlich noch genug Zeit gehabt, die Bombe zu entschärfen. Weil aber den beauftragten Programmierern die entsprechende Systemkenntnisse fehlten, gelang das nicht. Pünktlich zum Jahreswechsel, unter den Augen der genervten Experten, löschte sich das Programm [23, S.72].

Natürlich haben Systemoperateure auch andere Möglichkeiten, einem Betrieb Schaden zuzufügen. Insbesondere in Bezug auf die im vorhergehenden Beitrag behandelten Viren, sind gerade Systemoperateure mit ihren, von ihrer Aufgabenstellung her benötigten Kenntnissen und Fähigkeiten, besonders einfach in der Lage, derartige Sabotageakte zu begehen. Es könnte sich also unter Umständen als sehr gefährlich erweisen, einem Systemprogrammierer zu kündigen. Aber auch streikende Mitarbeiter können sich der Computersabotage bedienen. In den Vereinigten Staaten wurde ein derartiger Fall bekannt. Er ereignete sich 1971 bei der Metropolitan Life Insurance Company (MLIC) in New York. Die MLIC wickelte alle ihre Geschäfte über einen Honeywell 1800 Computer ab, der in ihrer New Yorker Zentrale stand. Alle Agenturen in zahlreichen Städten im ganzen Bundesgebiet waren über Datenfernleitungen mit der New Yorker Zentrale verbunden. Jede Nacht rief der Zentralcomputer die örtlichen Agenturen nacheinander an und ließ die dort bereitliegenden Magnetbänder mit allen Verkaufsdaten überspielen. Die so anfallenden Daten wurden dann verarbeitet, und die Ergebnisse wurden über Fernleitungen wieder an die Agenturen geschickt.

1971 streikte beim Computerhersteller Honeywell ein Techniker-Team, das über das Datenverarbeitungssystem der MLIC informiert war. Die Ingenieure riefen nun jede Nacht von ihrem Gewerkschaftsbüro aus die örtlichen Agenturen von MLIC an und gaben von einem Computer aus den dortigen Terminals den Befehl zum Einlesen der Magnetbänder. Da sie jedoch nicht den Befehl eingaben, die Bänder wieder zurückzuspulen, fand der kurz darauf anrufende MLIC-Computer nur leere Bänder vor. In der Zentrale gingen keine Daten mehr ein, und in den Agenturen lagen morgens keine Arbeitsergebnisse vor. Die MLIC stand vor einem Rätsel. Alle Datensätze waren unbeschädigt vorhanden, nur die nächtliche Überspielung klappte nicht. Fast einen Monat lang wurde nach dem Fehler gesucht, bis man auf die Idee kam, die Terminals in den Agenturen nachts überwachen zu lassen. Es wurde entdeckt, daß die Bänder ordnungsgemäß liefen, wenn auch nicht auf Befehl des Zentralcomputers. Eine Fangschaltung der Telefongesellschaft führte dann auch direkt zum Streiklokal der Honeywell-Ingenieure. Obwohl keiner der Beteiligten eine Strafverfolgung wünschte, kam es zur Anklage gegen drei der Ingenieure. Es wurde ein schwieriger Prozeß, denn da die Angeklagten sich weder bereichert noch etwas zerstört hatten, konnten sie nicht wegen Sachbeschädigung oder „wire fraud“ (Betrug mittels Fernsprecheinrichtungen) belangt werden. Sie wurden schließlich zu Geldstrafen verurteilt – nach einem Paragraphen gegen obszöne Anrufe [43, S.169f].

Wie sieht es aber nun mit den in der Presse so häufig erwähnten Hackern aus? Nach der von der bekanntesten Hackervereinigung in Deutschland, dem Chaos Computer Club, veröffentlichten Literatur, sind Hacker nicht an vorsätzlicher Sabotage interessiert. Allerdings verweisen sie auf die Existenz sogenannter „Crasher“, deren erklärtes Ziel es ist, fremde Rechnersysteme zu stören und zu zerstören. Trotzdem können Hacker auch völlig unbeabsichtigt eine Rechenanlage sabotieren. Zum einen kann es beim Herumprobieren (Hacken) in einem fremden System zu Störungen kommen, die durch Unkenntnis ausgelöst werden. Zum anderen kommt es auch zu regelrechten Treffen der Hacker im Datennetz. So kann es durchaus sein, daß die Hacker, allein durch ihre „Anwesenheit“, Systeme derart belasten, daß diese kaum noch Rechenzeit für ihre eigentlichen Aufgaben erübrigen können. Aber dieser Tat fehlt der in der Definition von Sabotage erwähnte Vorsatz beziehungsweise die Böswilligkeit. Im allgemeinen sind Hacker sogar sehr darauf bedacht keinen Schaden anzurichten, da eine derartige Aktion meistens die Systembetreiber zu einer Verbesserung ihrer Sicherheitsvorkehrungen bewegt. Bis auf schon erwähnte Ausnahmen bewegt man sich möglichst unauffällig, das heißt des Nachts und an Wochenenden, in fremden Systemen.

Wenden wir uns nun den sogenannten Crashern zu. Diese begnügen sich nicht damit, in ein fremdes Rechensystem einzudringen, sondern sie machen sich meist auch massiv bemerkbar, indem sie einen fremden Rechner zum Absturz bringen (crashen) oder aber die Zugriffsberechtigung aller Benutzer löschen, sodaß nicht einmal die Systemoperateure dieses Rechners mehr Zugriff auf ihren eigenen Rechner haben. Auch das Ändern und Löschen von Dateien gehört zu den möglichen Sabotageformen dieser Leute. Bedauerlicherweise werden durch diese schwarzen Schafe auch die anderen Hacker immer mehr als Kriminelle abgestempelt.

Bisher haben wir uns nur auf die Behandlung von Sabotageakten auf Großrechner beschränkt. Aber beim Thema Sabotage spielen Kleinrechner, sogenannte PCs, kaum eine Rolle. Da diese Rechner meistens nicht von außen über eine ständige Verbindung erreichbar sind und auch die Anzahl der Benutzer an einem solchen Gerät sehr klein ist, kommen die meisten Formen der Sabotage, wie sie bisher beschrieben wurden, nicht zum Zuge. Einen PC zu sprengen, hieße mit Kanonen auf Spatzen schießen. Auch Sabotage mit Hilfe von Viren und logischen Bomben hätte normalerweise nur einen lokalen Effekt, da diese relativ isolierten Rechner nicht für eine Verbreitung geeignet sind. Es gibt derartige Killerprogramme seit einiger Zeit zwar auch für PCs, aber sie sind nicht gegen einen bestimmten Betrieb gerichtet und betreffen oft nur Rechner die ihre Software nicht vom Hersteller beziehen. Unter dem Thema Diebstahl werden wir dieses Thema noch einmal aufgreifen. Weiterhin beziehen diese Rechner ihre Software im allgemeinen von Softwarehäusern. Durch dieses, auch unter Sicherheitsaspekten zu empfehlende Verfahren, werden die Probleme der Eigenprogrammierung und Eigenwartung umgangen. Diese Probleme sind praktisch identisch mit den schon beschriebenen Problemen mit Systemprogrammierern bei Großcomputern.

7.3 Spionage

Nach dem Großen Brockhaus ist Spionage „das Auskundschaften von Geheimnissen mit dem Zweck der Weitergabe“.

Spionage ist sicherlich eines der ältesten Gewerbe auf dieser Welt. Mit dem Einsetzen der Industrialisierung hat sich für Spione ein weiteres Betätigungsfeld eröffnet. Gemeint ist die sogenannte Wirtschafts- oder Industriespionage. Allerdings sind die Grenzen zur militärischen Spionage heutzutage oft fließend. Viele Informationen, die ausgekundschaftet werden, dienen sowohl zivilen als auch militärischen Zwecken. Besonders Computer können sowohl die Flugbahn einer Rakete steuern als auch ein Unternehmen verwalten. Hier ist es also fast unmöglich eine deutliche Trennlinie zu ziehen. Deshalb behandelt der nun folgende Beitrag die Spionage im Umfeld von Computern, ohne eine spezielle Unterteilung in zivilen und militärischen Bereich zu versuchen.

Wie schon bei der Sabotage an Computern, muß man auch bei der Spionage unterscheiden, ob der Computer das Ziel der Spionage ist oder die in ihm gespeicherten Daten. Besonders seit der Verschärfung der Embargobestimmungen durch J. Carter Anfang 1980 [99, S.182], sind die Ostblockländer zur Beschaffung westlicher Technologien auf verschiedene Formen der Spionage angewiesen. Bis zum Jahr 1978 hatten die Sowjets und ihre Blockstaaten völlig legal über 1300 Computersysteme im Wert von gut 639 Millionen Dollar aus dem Westen erhalten [99, S.178]. Die Begründung für das Embargo ist vordringlich in der Tatsache zu suchen, daß die in den vorhergegangenen Jahren gekaufte Technologie immer wieder in militärischen Projekten des Ostblocks Verwendung fand. Da sich der Ostblock jahrelang auf den Kauf und die Verwendung westlicher Technologie beschränkte und die Entwicklung eigener Computer vernachlässigte, liegt man dort heute auf diesem Gebiet weit zurück. Aus diesem Grund ist man auf westliche Technologie angewiesen, die man sich seit 1980 nicht mehr auf legalem Weg beschaffen kann.

Eine Form der heutigen Spionage besteht sicherlich darin, Computer mit Hilfe sogenannter Embargoschieber zu kaufen, um diese dann zu analysieren und nachzubauen. Es würde den Rahmen dieses Beitrags sprengen, wenn man die Methoden und Wege der Embargoschieber detailliert beschreiben wollte. Verschiedene Fallbeschreibungen sind in dem Buch „Die Computerspione“ von Jay Tuck [99] zusammengetragen, auf die ich hiermit verweise. Es soll an dieser Stelle nur erwähnt werden, daß Embargoware teilweise mit Hilfe von einem halben Dutzend verschiedener Speditionen durch mindestens ebensoviele Länder und Staaten transportiert wird, wobei sich die Bezeichnung der Fracht manchmal sogar mehrfach ändert, bis sie ihren Bestimmungsort erreicht. Die Bundesrepublik Deutschland spielt in diesem Zusammenhang eine herausragende Rolle, da es verhältnismäßig einfach ist, amerikanische Hochtechnologie nach Deutschland zu importieren, und diese von hier aus mit gefälschten Papieren in andere europäische Länder wie die Schweiz, Österreich oder Schweden zu verschieben, in denen die Embargobestimmungen der USA nicht so streng überwacht werden.

Eine weitere Möglichkeit der Spionage, die uns an dieser Stelle wesentlich mehr interessiert, ist die Beschaffung von gespeicherten Daten aus Computern.

Am 3. Juni 1983 stellte ein Computerexperte der Sloan-Kettering-Krebsklinik in New York fest, daß sich in der Nacht jemand Zugang zum inneren Computerprogramm verschafft hatte. Dieser Jemand hatte fünf neue

Dateien eröffnet und einen Teil des bisherigen Speicherinhalts gelöscht. Der betroffene Rechner, eine VAX-11/780, steuerte fünf Röntgenapparate der Klinik und beantwortete außerdem Anfragen von rund 80 weiteren Krankenhäusern. Aufgrund dieses Vorfalls wurden sämtliche Geheimcodes geändert. Damit hielt man den Fall für abgeschlossen. Doch am nächsten Morgen mußte man feststellen, daß die ungebetenen Gäste sich schon wieder an dem Computer zu schaffen gemacht hatten, diesmal mit einem „Spione-Programm", das Mitarbeiter abfragte und ihre Geheimcodes speicherte, mit deren Hilfe sie jederzeit wieder in das Programm einsteigen konnten.

Als Täter wurde von der nun hinzugezogenen Polizei und dem FBI der einundzwanzigjährige G. R. Wondra in einem 2000 Kilometer entfernt liegendem Dorf West Allis/Wisconsin ermittelt. Dieser hatte mit Hilfe seines Homecomputers vom Typ Apple-II den Klinikcomputer angezapft und manipuliert. Die Hackergruppe, der Wondra angehörte, hatte sich nicht nur die New Yorker Klinik sondern auch ein Beratungsunternehmen in Dallas, eine Bank in Kalifornien und eine Betonfirma in Kanada vorgenommen. Es war ihnen sogar gelungen in nicht geheime Teile des Programms des Los Alamos National Laboratory einzudringen, wo Atombomben gebaut werden [99, S.253]. Die Aufmerksamkeit der Regierung und der Massenmedien für dieses Problem war nun geweckt. Allein das Pentagon besitzt mehr als 8000 Großrechner, und man fragte sich, was Profis erreichen können, wenn so etwas schon unbeholfenen Kindern aus Jux gelingt [99, S.254].

Um die Schwachstellen ihres Systems auszuloten, wurden von US-Sicherheitsstellen sogenannte „Tiger-Teams" gebildet. Es handelte sich hierbei um Spezialisten, die im Auftrag der Regierung die eigenen Computer knacken sollten. Ihre Erfahrung – so die Überlegung – würde helfen, die Sicherheit zu erhöhen. Zum blanken Entsetzen ihrer Auftraggeber waren sie jedes Mal erfolgreich. Scheinbar mühelos bewegten sich die Teams an der vielschichtigen Softwaresicherheit vorbei ins Herz der Rechenanlagen. Immer wieder wurden neue Sicherheitsmaßnahmen eingebaut, immer wieder konnten die Diebe vom Dienst sie knacken. Darüber hinaus bewiesen sie, daß das alles möglich war, ohne Spuren zu hinterlassen. Nicht einmal Toptechniker waren später in der Lage festzustellen, ob und wann ein EDV-Einbruch stattgefunden hatte. Über 100 Millionen Dollar wurden in den Computerschutz investiert. Doch niemand konnte garantieren, daß die Rechner vor Mißbrauch und Manipulation sicher waren [99, S.255].

Diesen Weg benutzten auch deutsche Hacker als sie in verschiedene Computersysteme der westlichen Welt eindrangen, um die so gewonnenen Daten an östliche Geheimdienste zu verkaufen. Die Reaktion der Medien auf diese Tat war beispiellos. In einer Sondersendung der ARD sprach man von „einer neuen Dimension der Spionage". Daß diese Form der Spionage sicherlich nicht neu ist, sollte dem Leser dieses Beitrags inzwischen klar sein. Aber auch die in dieser Sondersendung angesprochenen Spionageziele können in der Fachwelt eigentlich nur ein müdes Lächeln des Mitleids erzeugt haben. Begriffe wie C-Compiler und Datenbankprogramme können nur bei Laien das Gefühl einer eingetretenen Katastrophe auslösen. Die Aussage des Vorsitzenden des Chaos Computer Clubs, daß sich die Spione nur in „öffentlichen Rechnersystemen" bewegt hätten, wurde dann auch nur am Rande in der Tagespresse erwähnt. Auch wenn die Definition von „öffentlich" beim Chaos Computer Club etwas anders aussehen mag als im allgemeinen Sprachgebrauch, muß man zu der Schlußfolgerung gelangen, daß in den Medien mal wieder die Angst der Laien vor der neuen Technik zur Sensationsmache ausgenutzt wurde.

Wie schon bei der Sabotage werden auch in der Spionage Einbenutzercomputersysteme von der Literatur kaum beachtet. Aber gerade hier ist der Sicherheitsstandard oft unglaublich gering. Kaum ein Softwarehersteller für PCs implementiert eine Passwortabfrage oder eine Benutzerkennung, die in Großrechnern schon vom Betriebssystem grundsätzlich vorhanden ist. Es existieren zwar mannigfaltige Methoden, um einen PC gegen unbefugtes Benutzen zu sichern, aber oft scheuen die Verantwortlichen die damit verbundenen Kosten. Aber auch abgeschlossene Festplatten und in Stahlschränken aufbewahrte Disketten haben letztlich nur einen Sinn, wenn der verantwortliche Mitarbeiter die Sicherheitsmaßnahmen auch einhält.

Eine weitere, von der Konzeption her sehr interessante Möglichkeit zur Spionage, ist das Anpeilen und Auswerten der Bildschirmausstrahlung von Monitoren. Bildschirme sind genauso wie Fernseher nach dem Prinzip der Kathodenstrahlröhre aufgebaut. Es ist prinzipiell möglich in serieller Folge abgesandte Zeichen in der gleichen, logisch richtigen Reihenfolge wieder aufzufangen. Da Computerbildschirme bitseriell arbeiten, das heißt, daß jeder Bildschirmpunkt einzeln und in fester Reihenfolge von einem Elektronenstrahl angesprochen wird, besteht durchaus die Gefahr, daß mit geeigneten Geräten deren Austrahlung über Kilometer hinweg aufgefangen und die Bildschirmanzeige rekonstruiert wird. Einige Experten behaupten, daß es schon gelungen sei, aus einer Ansammlung von zwanzig Bildschirmen in einem Raum, einen Bildschirm auszusondern und mitzuschneiden [15, S.131].

Da besonders im Rahmen von CIM mehr und mehr wichtiges Know-How der Industrie auf den Bildschirmen erscheint, muß die Abstrahlungsgefahr der Bildschirme durchaus Ernst genommen werden [15, S.132]. Als Schutz vor derartigen „Lauschangriffen" kann das Prinzip des Faradayschen Käfigs verwendet werden, das heißt der zu schützende Raum wird mit elektrisch leitfähigen Folien tapeziert [15, S.138].

Viel weniger sensationell als Systemeinbrüche von außen ist die Spionage durch Mitarbeiter eines Unternehmens. Es gilt, daß die größte Gefahr für ein zu schützendes Objekt von den Personen ausgeht, die am häufigsten und am einfachsten Zugang haben [15, S.97]. Da es aber kaum einen Unterschied macht, ob die sicherheitsempfindlichen Informationen fotografiert, kopiert oder auf Datenträger übertragen wird, soll auf diesen Bereich der Spionage an dieser Stelle nicht näher eingegangen werden.

7.4 Diebstahl

Die vielfältigen Möglichkeiten des Diebstahls im Umfeld der Computer macht es an dieser Stelle unmöglich, eine aussagekräftige Definition zu formulieren.

Es gibt in der Computerwelt einen Basislehrsatz, der für alle Größen und Arten von Computern gilt: Was ein Computer lesen kann, kann er auch schreiben und damit läßt es sich auch kopieren [15, S.21]. Besonders bei den Herstellern von Betriebssystemen für PCs konnte man die Auswirkungen dieses einfachen Lehrsatzes leicht ablesen. Die scheinbar logische Annahme, daß jeder, der einen PC kauft, auch das Betriebssystem gleich mit erwirbt, war falsch. Obwohl jeder PC ein Betriebssystem benötigt, war im Verhältnis zu den verkauften PCs die Anzahl der abgesetzten Betriebssysteme gering [15, S.21]. Aber auch für andere Bereiche der Softwareerstellung bedeuten Raubkopien einen unkalkulierbaren Verlust. Dabei wird weniger auf jene angespielt, die aufgrund ihrer Vermögensverhältnisse sowieso keine Möglichkeit hätten, ihre oft umfangreiche Programmbibliothek zu finanzieren. In diesem Fall tritt aber im allgemeinen kein bezifferbarer Schaden für die betroffenen Softwarehersteller ein. Aber auch ein Unternehmen, daß ein einziges Programm für alle installierten Rechner kauft und dieses dann aus Gründen der Bequemlichkeit vervielfältigt, verwendet damit eigentlich Raubkopien. So mancher EDV-Leiter bekam einen Rüffel, weil er eine Programmversion dreimal bestellt hatte. Der Hinweis vom Chef: Ein Original reicht doch völlig [23, S.103].

Die Möglichkeit der Raubkopie als günstige Beschaffung von Software hat sicherlich auch bei den hohen Absatzzahlen der PCs mitgewirkt. Die PC Hersteller und Benutzer profitieren also gleichermaßen von dieser kostengünstigen Form der Softwarebeschaffung. Nur die Hersteller von Programmen haben das Nachsehen.

Aus diesem Grund versuchen viele Softwareunternehmen ihre Produkte vor der unbefugten Vervielfältigung zu schützen. Es wurden Zähler auf der Diskette eingefügt, die bei jedem Kopiervorgang hochgesetzt wurden, und ab einer gewissen Höhe für die Zerstörung der Kopie sorgten. Dieses Verfahren erwies sich als wirkungslos, da die Zähler wie das Programm einfach mitkopiert wurden. Auch der Versuch, mit Laserlöchern auf der Programmdiskette das illegale Kopieren zu verhindern, scheiterte an Kopierprogrammen, die diese Löcher auf der Kopie simulierten [15, S.23].

Ein weiterer, rechtlich strittiger Versuch, sich vor Raubkopien zu schützen, wird von einigen Programmierern unternommen, indem sie ihre Programme mit einem Viren-Kopierschutz versehen. Die Idee ist also, Raubkopierer mit Viren zu bestrafen. So lassen sich zum Beispiel mit einem Atari-Kopierprogramm Raubkopien herstellen, wer allerdings die Kopierhilfe selbst kopiert, startet eine Virusverbreitung. Alle Kopien, die mit dem kopierten Kopierprogramm hergestellt werden, setzen Viren frei [23, S.84].

Andere Formen des Diebstahls sind aber sicherlich spektakulärer als Raubkopien. Einer der bekanntesten Fälle ist sicher die Tat eines Bankangestellten, der mit Hilfe einer Programmänderung zehntel und hundertstel Pfennigbeträge, die bei Banken durch Abrundung bei verschiedenen Berechnungen entstehen, auf ein eigens eingerichtetes Konto transferierte. Sein Fehler bestand darin, daß er den Namen des Kontoinhabers mit „Zwaine" angab, der im Rechenprogramm am Ende der alphabetischen Auflistung stand. Als die Marketing-Abteilung seines Institutes zu Werbezwecken den ersten und letzten Kunden im Alphabet präsentieren wollte, stellte man fest, daß Mr. Zwaine zwar sehr reich war, aber gar nicht existierte. Dieser Bericht basiert auf Hörensagen, weil die betroffene Bank keinen Strafantrag gestellt hatte. Sie hatte kein Interesse an der öffentlichen Erörterung des Normalfalls. Denn gewöhnlich kassiert die Bank, was sich auf dem Konto von Mr. Zwaine ansammelte [43, S.181f]. Einen anderen, ungleich komplizierteren Weg schlug ein Angestellter einer Bank in Los Angeles ein.

Er war dahintergekommen, wie er mit Hilfe seines Computerterminals Geld unterschlagen konnte. Er hatte ein Konto bei einer Zweigstelle der Bank eröffnet und darauf Geld überwiesen. Dann hatte er dieses Geld auf ein weiteres, neues Konto bei einer anderen Zweigstelle transferiert. Da er wußte, wie das automatische Prüfsystem der Bank funktionierte, mußte er binnen fünf Tagen dieses Luftgeschäft durch Gegenbuchungen ausgleichen. Dafür eröffnete er wieder ein Konto, und die fehlenden Summen, die das erste Luftgeschäft ausgleichen sollten, machten ein weiteres Luftgeschäft notwendig, das innerhalb von fünf Tagen eine neue Transaktion nach sich zog. Hinzu kam, daß die langsam größer werdenden Summen den Betrag von 1 Million Dollar nicht überschreiten durften, da sonst automatisch eine Überprüfung ausgelöst worden wäre. Deshalb mußte der Angestellte nach einem immer komplizierter werdenden Zeitplan auf immer mehr Konten seine Unterschlagungen fortsetzen, um nicht aufzufallen. Er konnte nicht einmal mehr Urlaub machen, weil dann der ganze Schwindel aufgeflogen wäre. Ein einfacher Schreibfehler, ein ungenau bezeichnetes Konto, führte zu Nachforschungen und wurde ihm zum Verhängnis. Zwei Jahre lang hatte er seine Unterschlagungen durchgeführt und dabei 21 Millionen Dollar beiseite geschafft [43, S.153f].

Natürlich muß ein Dieb nicht, wie in den vorhergehenden Beispielen, direkt Bargeld klauen. So mußte im Frühjahr 1984 eine US-Universität einen neuen Computer anschaffen, weil die Speicherkapazität des alten Rechners nie für die anfallende Arbeit ausreichte. Erst nachdem der neue Computer angeschafft war und ein Aufsichtsgremium die hohen Kosten für den zweiten Rechner bemängelt hatte, wurde zufällig entdeckt, daß der alte Rechner einem ehemaligen Universitätsassistenten den Lebensunterhalt verdiente. Der Assistent hatte jahrelang diesen Rechner für sein privates Time-sharing-Unternehmen benutzt und damit die vollen Speicher verursacht [43, S.110].

Alle bisherigen Beispiele zum Thema Diebstahl bezogen sich auf Taten, die von Mitarbeitern der bestohlenen Unternehmen begangen wurden. Die, schon in den anderen Bereichen angesprochene Gefahr durch die eigenen Mitarbeiter für ein Unternehmen, zeigt sich hier besonders durch die Fülle von Fallbeschreibungen bekannt gewordener Diebstähle in der einschlägigen Literatur. Die Bedeutung des Diebstahls von außen scheint, wenn man von einigen Grenzbereichen absieht, vergleichsweise gering. Wie sehen diese Grenzbereiche aus? Als erstes wäre der Diebstahl von Software und Daten durch einen Systemeinbruch zu nennen. Diese Form der Wirtschaftskriminalität wurde aber schon im Zusammenhang mit Spionage behandelt und wird an dieser Stelle nicht noch einmal trachtet.

Ähnlich sieht es mit den Diebstählen im Zusammenhang mit Geldautomaten aus. Da hier nicht die Bankautomaten manipuliert werden, sondern die Karteninhaber, haben wir es hier mehr mit Trickbetrug als mit Computerkriminalität zu tun.

Was bleibt, ist das Verfahren vieler Hacker, die Telefone von Konzernen zu benutzen, um ihre weltweite Kommunikation zu betreiben. Der dadurch angerichtete Schaden ist aber wohl so gering, daß selbst die betroffenen Konzerne davon kein Aufheben machen.

Das Fehlen von Informationen über mit Computern ausgeführten Diebstählen von Außen lassen drei mögliche Schlußfolgerungen zu:

1. Ein derartiger Diebstahl hat noch nicht stattgefunden.
2. Der Diebstahl fand/findet statt und wurde noch nicht entdeckt.
3. Die Betroffenen haben die Entdeckung eines derartigen Diebstahls geheimgehalten.

7.5 Die Rechtsprechung

Ein Hauptproblem in der Computerkriminalität ist, einem Täter seine kriminelle Handlung nachzuweisen beziehungsweise den Täter überhaupt zu entdecken, denn es bleiben oft keine Spuren zurück, die auf den Täter hindeuten.

Ein anderes Problem, dem sich besonders Behörden und Gerichte gegenübersahen, war die Schwierigkeit, verschiedene Delikte im Zusammenhang mit Computern mit den gültigen Gesetzen zu erfassen. Als erstes soll nun erläutert werden, mit welchen Problemen sich Richter vor dem 1.8.1986 bei der Beurteilung von Vergehen im Umfeld moderner Technologie, zu befassen hatten. Im Anschluß daran werden die, nach dem 1.8.1986 gültig gewordenen, neuen Paragraphen des Strafgesetzbuches zur Bekämpfung der Wirtschaftskriminalität vorgestellt und ihre Auswirkungen kurz erläutert.

Angenommen, jemand fand eine jener Kreditkarten, mit denen sich Geldautomaten bedienen lassen. Nehmen wir weiter an, daß der Finder nicht ehrlich war, und diese Karte nicht sofort an ein Fundbüro abgab oder sie sonstwie dem Eigentümer zukommen ließ. Nehmen wir drittens an, er konnte sich die zugehörige Geheimzahl beschaffen, indem er den Besitzer der Karte anrief und sich als Bankangestellter ausgab, der aus irgendeinem Grund die Nummer der Karte braucht. (Dieser Trick hat nachweislich schon funktioniert). Nun hatte der Finder alles, was er braucht, um von einem beliebigen Geldautomaten den zulässigen Tageshöchstbetrag abzuheben. Nach der alten Rechtslage konnte er dies tun, und hätte trotzdem eine gute Chance gehabt, ohne Strafe davonzukommen, selbst wenn man ihn auf frischer Tat ertappt hätte.

Das Strafgesetzbuch aus dem Jahre 1871 beschreibt in vielen Paragraphen alle denkbaren Umstände, unter denen jemand rechtswidrig an seinem Vermögen geschädigt werden kann, und bedroht solche Taten mit Strafe. Aber all diesen Tatbeständen ist gemeinsam, daß die Handelnden, die Täuscher und die Getäuschten, die Diebe und die Bestohlenen, Menschen sind und daß diese Menschen beim Stehlen und Betrügen handfeste Hilfsmittel benutzen wie Einbruchswerkzeug und nachgemachte Unterschriften. Von elektronisch codierten Magnetbändern war dort nicht die Rede.

Daher konnte man schließen, daß der Mißbrauch der Scheckkarte kein Betrug nach §263 StGB sei, denn zum Wesen dieses Tatbestands gehört, daß ein Mensch getäuscht wird. Nach dem Wortlaut des Gesetzes wird der zum Betrüger, der „das Vermögen eines anderen dadurch beschädigt, daß er durch Vorspielung falscher oder durch Entstellung oder Unterdrückung wahrer Tatsachen einen Irrtum erregt“. In dem oben angeführten Fall gab der Kontoinhaber zwar seine Geheimnummer irrtümlich bekannt, weil er am Telefon über die Person des Anrufers getäuscht wurde. Aber diese Täuschung wäre in einem Prozeß nur schwer zu beweisen, es sei denn, das Gespräch wurde mitgeschnitten. Auf keinen Fall wurde der Geldautomat bei der eigentlichen Tat, dem Abheben des Geldes, getäuscht. Im Gegenteil, er verrichtete seine Arbeit völlig korrekt, da er nur zu prüfen hatte, ob der Benutzer den Automaten ordnungsgemäß bediente.

Aus diesem Grund kann auch §265 StGB gegen Automatenmißbrauch nicht angewendet werden, denn dieser verlangt, daß der Mechanismus des Automaten in ordnungswidriger Weise bedient wird. Auch ein Diebstahl wurde nicht begangen, da die Karte in unserem konstruierten Beispiel gefunden wurde. Das Gleiche gilt für Urkundenfälschung. Selbst wenn die verwendete Karte nicht echt, also selbst hergestellt worden wäre, könnte nicht der Vorwurf der Urkundenfälschung erhoben werden. Denn eine Urkunde muß, nach herrschender Juristenmeinung, die sogenannte Perpetuierungsfunktion erfüllen, sie muß dauerhaft gültig sein. Dazu gehört, daß sie jederzeit optisch wahrnehmbar sein muß. Die unsichtbaren Magnetfelder der elektronischen Datenträger gelten deshalb nicht als Urkunden [43, S.60ff].

Diese und ähnliche Probleme traten bei den meisten Fällen der Computerkriminalität auf. Der Gesamtverband der deutschen Versicherungswirtschaft e.V., dessen Mitgliedsfirmen schon manche Mark per Computer entwendet wurde, erklärte deshalb in einem Schreiben an den Rechtsausschuß des Deutschen Bundestages fast alle einschlägigen Paragraphen für untauglich:

- §242 (Diebstahl) verlangt die Wegnahme einer fremden beweglichen Sache und trifft daher für Computerkriminalität regelmäßig nicht zu.
- §246 (Unterschlagung) verlangt die Zueignung einer fremden beweglichen Sache, die zuvor im Gewahrsam des Täters gestanden hat. §246 ist deshalb regelmäßig hier nicht einschlägig.
- §263 (Betrug) verlangt die Täuschung einer Person, deren Irrtum und eine Vermögensverfügung. Gerade diese Tatbestandsmerkmale liegen bei der Computerkriminalität regelmäßig nicht vor.
- §265a (Erschleichen von Leistungen, Automatenmißbrauch) verlangt die Absicht, das Entgelt nicht zu entrichten und trifft damit ebenfalls für die Computerkriminalität regelmäßig nicht zu.
- §266 (Untreue) verlangt die Pflicht, fremde Vermögensinteressen wahrzunehmen. Diese wird bei dem überwiegenden Teil der Computerkriminalität nicht vorliegen.
- §267ff (Urkundenfälschung, Fälschung technischer Aufzeichnungen) treffen nicht zu, weil Daten und Datenträger regelmäßig nicht als Urkunden angesehen werden können [43, S.65f].

Seit dem 1.8.86 gilt nun die Fassung des Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität. So ist nun das Ausspähen von Daten (§202a StGB), der Tatbestand des Computerbetrugs (§263a StGB), der Mißbrauch von Scheckkarten (§266b StGB), die Fälschung beweiserheblicher Daten (§269 StGB) in Anlehnung an den Tatbestand der Urkundenfälschung, die Täuschung im Rechtsverkehr bei Datenverarbeitung (§270 StGB), die Datenveränderung (§303a StGB) sowie die Computersabotage (§303b StGB) unter Strafe gestellt [23, S.155f].

Da es bisher noch keine einschlägigen Urteile gibt, sind die Folgen dieser neuen Gesetze noch nicht absehbar. Auch wenn mit dieser Gesetzgebung eine schon lange bestehende Gesetzeslücke geschlossen wurde, wird von verschiedenen Seiten die fehlende Differenziertheit bemängelt. Ganz hart gesagt, kann besonders nach §202a, jeder, der ein Passwort knackt, schon verurteilt werden [23, S.165]. Da auch viele Jugendliche diesem Hobby fröhnen, kann das dazu führen, daß wir in naher Zukunft eine ganze Anzahl vorbestrafter jugendlicher Krimineller mehr haben. Warten wir also ab, was uns die Zukunft so bringt.

Teil IV

Sicherheit von und mit Computersystemen

Kapitel 8

Sicherheit von Daten

MATTHIAS STOFFEL

8.1 Einleitung

Die bisherigen Vorträge haben sich im wesentlichen mit der Frage des Datenschutzes und den Folgen des Datenmißbrauchs beschäftigt.

Der Datenschutz berücksichtigt im engeren Sinne rechtliche und damit eng verbunden soziale Probleme. Im Vordergrund stehen die Auswirkungen der konzentrierten Speicherung und Nutzung von Daten auf den Menschen. Diese Speicherung war durch die immer billiger werdenden Massenspeicher etwa ab 1965 möglich. In dieser Zeit kam auch die Forderung nach Datensicherheit auf. Die Datensicherheit beschäftigt sich mit den technischen und organisatorischen Möglichkeiten einen Schutz zu realisieren.

Man kann also sagen, der Datenschutz legt fest, was verboten ist – die Datensicherheit baut Mechanismen, um den Datenschutz zu unterstützen.

Bei der Datensicherheit hat man zunächst zwei grundlegende Methoden:

- man verhindert, daß ein Unbefugter an die zu schützenden Daten herankommen kann (Zugriffsschutz)
- man verschlüsselt die Daten, so daß ein Unbefugter bei einem Diebstahl nichts mit den Daten anfangen kann (Kryptologie)

Mit diesen beiden Methoden hat man nun verschiedene Möglichkeiten Daten zu schützen.

8.2 Sicherheit durch Zugriffsschutz

Um die Methode des Zugriffsschutzes darzustellen, führt man oft das folgende Modell ein [5]:

Es gibt zunächst die passiven zu schützenden Elemente, die man als Objekte bezeichnet, und die aktiven Elemente, die einen Zugriff auf die Objekte machen wollen, die Subjekte. Subjekte sind meist Prozesse. Objekte können z.B. Speicher, Dateien aber auch Prozesse selbst sein.

Nun ist es sinnvoll, gewisse Klassen von Zugriffsrechten einzuführen, z.B.:

- für den Speicher: lesen, schreiben, ausführen
- für Prozesse: stoppen, terminieren, blockieren
- für Dateien: lesen, schreiben, ausführen, anfügen

Anschaulich läßt sich so ein Modell als Zugriffsmatrix [77] darstellen:

		Objekte					
		Speicher			Prozesse		Dateien
		S1	S2	S3	P1	P2	D
Subjekte	P1	lesen schreiben ausführen			stoppen		ausführen
	P2		lesen	blockieren ausführen	stoppen	terminieren	
	P3	lesen ausführen		lesen schreiben		blockieren	anfügen

Durch eine geschickte Repräsentation wird das Modell gespeichert und bei jedem Zugriff überprüft, ob der Zugriff zugelassen werden kann.

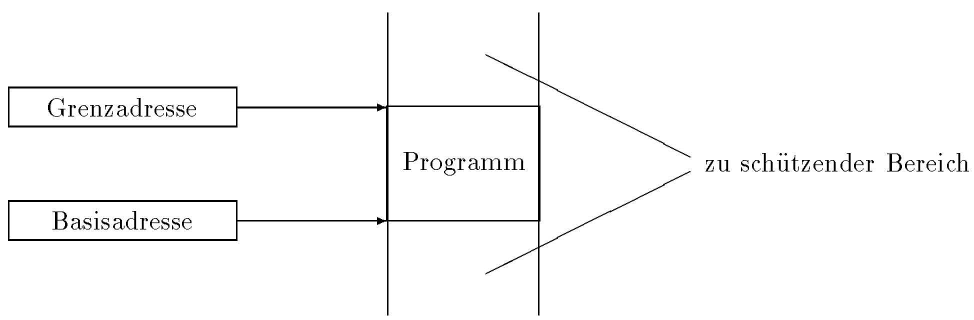
Ausgehend von dieser Darstellung werden nun einige wichtige Methoden zur Sicherung dargestellt.

8.2.1 Zugriffsschutz für den Speicher

Da sich bei Mehrbenutzerrechnern mehrere Programme den Speicher teilen, ist es notwendig, den Zugriff auf fremden Speicher zu schützen.

8.2.1.1 Grenzregister

Für jeden rechnenden Prozeß wird ein Basisregister und ein Grenzregister mit Werten geladen. Nur innerhalb dieser Grenzen ist eine Adressierung möglich [101].



Dazu wird hardwaremässig bei jeder Adreßberechnung ein Vergleich gemacht, ob:

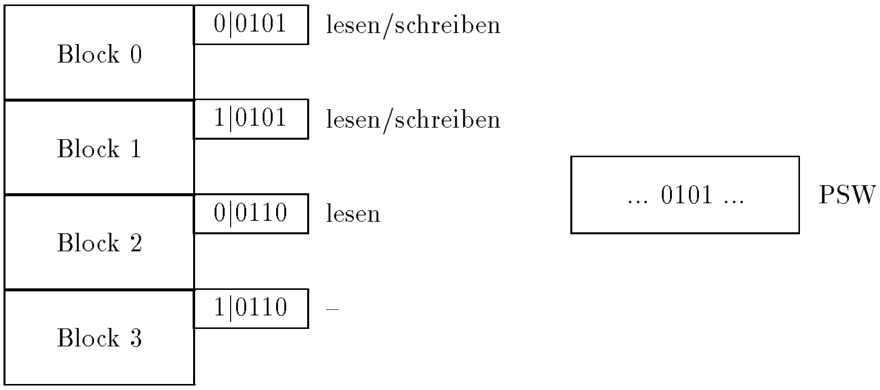
$$Basisadresse + Programmadresse > Grenzadresse$$

ist, also ob ein Zugriff aus dem erlaubten Bereich heraus geht. Ist dies der Fall, so wird ein Interrupt ausgelöst.

Dieses Verfahren findet bei der IBM 360 Verwendung.

8.2.1.2 Schutzschlüssel

Der Speicher wird in feste Blöcke aufgeteilt. Jeder Block erhält einen Schlüssel, der festlegt, ob der Bereich von Anderen gelesen werden darf und wer Schreiberlaubnis hat [67].



Die Leseerlaubnis wird durch ein Bit geregelt. Die Schreiberlaubnis haben nur solche Prozesse, deren eigene Identifikation mit dem Schlüssel eines Blockes übereinstimmt. Diese Identifikation ist Bestandteil des Prozessorstatuswortes (PSW). Hat ein Programm die Identifikation 0, so ist es priviligiert und kann auf den gesamten Speicher zugreifen. Anwendung findet dieses Verfahren bei der IBM 370. Hier wird ein 4 Bit langer Schlüssel verwendet. Ein deutlicher Nachteil dieser Methode besteht allerdings darin, daß nie mehr als 15 Programme gleichzeitig laufen können.

8.2.1.3 Virtuelle Adressierung

Hierbei wird der Speicher, den ein Prozeß benötigt, auf den physikalischen Speicher abgebildet. Das heißt, jeder Prozeß verfügt über seinen eigenen Adreßraum und es ist somit nicht möglich auf fremden Speicher zuzugreifen, ohne spezielle Kommunikationsroutinen des Betriebssystems zu benutzen. Die Zugriffe werden über Seitentabellen geregelt, die vor Änderungen durch den Benutzer geschützt werden, indem auf sie nur in einem priviligierten Zustand zugegriffen werden kann [100].

8.2.2 Zugriffsschutz für den Prozessor

Um Sicherheit im Betriebssystem zu schaffen, ist es wichtig, daß der Benutzer nicht alle Möglichkeiten des Prozessors ausnutzen darf. So ist zu beachten, daß keine uneingeschränkten Speicherzugriffe oder E/A-Instruktionen ausgeführt werden können. So muß zum Beispiel das direkte Lesen eines Massenspeichers oder das Sichtbarmachen der Ein- bzw. Ausgaben eines fremden Terminals unterbunden werden.

Die Lösung dieses Problems erfolgt durch Einführung verschiedener Betriebszustände [100]. Üblicherweise sind dies zwei Modi:

- der Supervisormode, der alle Maschinenbefehle zuläßt
- der Usermode, in dem gewisse Instruktionen verboten sind

Natürlich darf einem normalen User kein unerlaubter Zugang zum Supervisormode gestattet sein.

8.2.3 Zugriffsschutz für Dateien

Ein Zugriffsschutz von Dateien erfolgt in Betriebssystemen üblicherweise schon mit dem Einloggen des Benutzers. Hierbei wird eine Identifikation und eine Autentikation gefordert. Durch die Identifikation wird festgestellt, ob der Benutzer dem System bekannt ist. Dies geschieht durch eine Benutzerkennung. Da allerdings eine oft allgemein bekannte Kennung alleine nicht ausreicht, muß durch die Autentikation die Identifizierung auf Korrektheit überprüft werden [33].

Üblicherweise geschieht dies durch ein Passwort. Erst dadurch erhält der Anwender Zugriff auf das System und seine Dateien. Natürlich muß auch ein Schutz vor Zugriff auf Dateien anderer Benutzer erfolgen. Während das früher durch Geheimhaltung der Dateinamen geschah, ist das heute nicht mehr möglich, da man sich in modernen Betriebssystemen die Dateien fremder Benutzer auflisten lassen kann.

Eine Möglichkeit des Schutzes besteht darin, den Zugriff auf eine Datei durch ein Passwort zu regeln, welches bei Bedarf weitergegeben wird. Eine andere Möglichkeit entsteht dadurch, daß alle Benutzer in Gruppen unterteilt werden: Eigentümer – Gruppe, in der sich der User befindet – Welt, also alle Anderen. Weiterhin legt man Zugriffsrechte fest: lesen, schreiben und ausführen.

Mit jeder Datei werden nun auch die Zugriffsrechte für Eigentümer, Gruppe und Welt abgespeichert. Eine Festlegung dieser Rechte erfolgt durch den Eigentümer.

	Eigentümer	Gruppe	Welt
read	×	×	
write	×		
execute	×	×	×
Bitfolge	rwe	r−e	−−e

Durch dieses Prinzip, das in UNIX [67] realisiert ist, ist es möglich, Zugriffsrechte individuell zu regeln und gegebenfalls zu ändern.

Weiterhin wird oft noch unterschieden, ob ein Fremder, der eine Datei ausführt, währenddessen die Rechte des Eigentümers erhält, um wenn nötig auf Zusatzdaten des Besitzer zugreifen zu können.

Außerdem sollte darauf geachtet werden, daß eine Leseerlaubnis auch ein Kopieren beinhaltet. Dadurch kann der neue Eigentümer die Rechte für die Kopie ändern. In vielen Systemen, nicht in UNIX, wird darum eine Änderung der Rechte für Kopien verboten.

8.2.4 Zugriffsschutz in Datenbanken

In den meisten Datenbanken werden viele vertrauliche Daten gespeichert sein. Es ist daher schwer zu regeln, wer auf welche Daten Zugriff haben soll. So sind zum Beispiel in einer Personaldatenbank ärztliche Informationen vor dem Lesen durch Andere zu schützen.

Ein Modell für den Schutz besteht in einer zentralen Instanz, dem „Arbiter“, welcher jede durchzuführende Verarbeitung von Daten auf ihre Verträglichkeit mit allen betroffenen Geheimhaltungsaspekten überprüft und gegebenenfalls die Datenausgabe verweigert.

Wie allerdings diese Geheimhaltungsaspekte geregelt sind, liegt im Ermessen des Betreibers bzw. des Programmierers. Dem Benutzer und auch den Personen, die in der Datenbank erfaßt sind, sind diese Regelungen dann oft unbekannt und sie glauben, daß ihre Daten vor unbefugtem Lesen geschützt sind.

8.2.4.1 Sicherheit in statistischen Datenbanken

Bei der Verwaltung eines größeren Personenkreises ist es oft nötig, den Zugriff auf alle Daten für statistische Analysen zuzulassen, ohne jedoch Sensitives, also Privates eines Einzelnen, zu verraten.

In einer Personaldatenbank ist zum Beispiel eine Statistik über die Verteilung der Gehälter in Abhängigkeit von Alter, Position und Familienstand üblich. Trotzdem sollte der Benutzer der Datenbank nicht in der Lage sein, das Gehalt einer bestimmten Person zu erfragen.

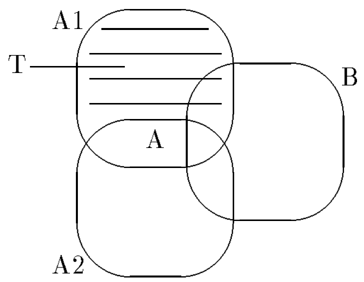
Es scheint, daß durch rein statistische Ausgaben diese Schutzforderung erfüllt sind. Doch durch mehrere geschickte Anfragen kann der Benutzer häufig zu sensitiven Daten gelangen.

Kennt ein Benutzer zum Beispiel das Alter, den Wohnort, die Kinderzahl und die Abteilung eines Mitarbeiters, dessen Gehalt er wissen möchte, so kann er durch Anfrage des durchschnittlichen Gehalts aller Personen mit den genannten Kriterien, die wahrscheinlich nur auf eine Person zutreffen, zu einem Ergebnis gelangen.

Die Gefahr besteht also darin, daß durch das Bekanntsein vieler Informationen über eine Person, der Zugriff auf sensitive Daten ermöglicht wird. So werden Statistiken, die zuviel Information über ein Datenobjekt direkt zugänglich machen, als sensitive Statistiken bezeichnet.

Dies trifft insbesondere dann zu, wenn Anfragen auf nur einen geringen Prozentsatz aller zutreffen, also eine einzige Person extrahiert wird. Aber auch durch Unterdrückung des Zugriffs auf sensitive Statistiken kann keine Sicherheit erzeugt werden. Eine vereinfachte Möglichkeit besteht darin, eine Anfrage nach der Anzahl aller Datensätze zu richten und dann die Anfrage so abzuwandeln, daß ein Datensatz ausgeklammert wird (Differenzbildung). So könnte sich eine Person zum Beispiel nach der Anzahl aller Vorbestraften erkundigen und dann nach der Anzahl der Vorbestraften ohne die, die ein gewisses Kriterium erfüllen, das nur auf die eine Person zutrifft. Durch Vergleich beider Ergebnisse wird klar, ob die Person vorbestraft ist. Also liegt die Gefahr auch darin, daß sich eine Anfrage nach einem zu großen Anteil richtet.

Aber auch dies ist noch nicht ausschlaggebend. Dies zeigt sich an dem „Tracker"-Verfahren [100]: Ein „Angreifer" kennt eine Anfrage A an eine Datenbank, die einen einzigen Datensatz eindeutig bestimmt. Er will wissen, ob auch Kriterium B auf den Datensatz zutrifft. Liefert eine Anfrage $A \wedge B$ wieder einen Datensatz, so trifft das Kriterium B zu. Allerdings wird das System erkennen, daß eine solche Anfrage nicht zugelassen werden darf. Also geht er wie folgt vor: A wird in zwei Teilbedingungen $A1$ und $A2$ aufgespaltet mit: $A = A1 \wedge A2$ und weiterhin dürfen $A1$ und $T = A1 \wedge \neg A2$ nicht sensitiv sein.



Der Angreifer stellt nun die Anfrage nach $A1 \wedge B$ und nach $T \wedge B$. Sind die Anzahl beider Ergebnisdatensätze gleich, so trifft Kriterium B auf den durch A festgelegten Datensatz nicht zu.

Bsp.:

A : wohnt in KL, 1940 geboren, keine Kinder

B : hat keine Schulden

$A1$: wohnt in KL, 1940 geboren

$A2$: keine Kinder

T : wohnt in KL, 1940 geboren, Kinder

- Anfrage nach $A1 \wedge B$: *„wohnt in KL, 1940 geboren, hat keine Schulden"* liefert 5 Datensätze
- Anfrage nach $T \wedge B$: *„wohnt in KL, 1940 geboren, Kinder, hat keine Schulden"* liefert 5 Datensätze

$\Longrightarrow$ er hat Schulden

Allerdings gibt es große Probleme beim Finden eines Trackers. Trotzdem müssen Schutzmaßnahmen getroffen werden:

- zufällige Rundung des Ergebnisses einer Anfrage (der Anwender hat keine genauen Werte)
- Auswahl einer Teilmenge der Gesamtheit, auf die die Anfrage bezogen wird
- Austausch von einzelnen Datenwerten unter verschiedenen Datensätzen
- Austausch durch erfundene statistische Werte, die die gleichen Eigenschaften haben

Bei all diesen Verfahren eine Datenbank abzusichern, ist zu beachten, daß sie keine zu große Veränderung der Daten und Statistiken bewirken, da sonst die Funktion und Effizienz der Datenbank beeinträchtigt werden kann.

8.3 Kryptologie

Sicherheit von Daten kann auch dadurch erreicht werden, daß man die Daten verschlüsselt. Die Kryptologie, die sich mit diesem Thema beschäftigt, ist schon sehr alt. Die Spartaner haben schon 500 v. Chr. durch Transpositionen ihre Nachrichten für Fremde unleserlich gemacht. Ab dem 15. Jahrhundert beschäftigte man sich ernsthaft mit der Chiffrierung aber auch der Dechiffrierung, also dem Knacken von Codes. Etwa bis Anfang des 20. Jahrhunderts waren alle wesentlichen Methoden der klassischen Kryptologie bekannt. Neue Aspekte kamen durch die Nutzung von elektromechanischen Verschlüsselungsgeräten während des 2. Weltkrieges auf, so zum Beispiel die deutsche Enigma-Maschine, die von Alan Turing geknackt wurde.

Als Wendepunkt ist das starke Aufkommen von Rechenanlagen zu sehen. Durch die zunehmende Datenverarbeitung und Kommunikation in militärischen, in wissenschaftlichen und in kommerziellen Bereichen mußten immer mehr Daten geheimgehalten werden.

So ist der Data Encryption Standard (DES) als neuste Entwicklung (1977) der klassischen Kryptologie zu nennen, ein sehr sicheres Verfahren, das starke Verbreitung findet.

In dieser Zeit kam es auch zu einer Veröffentlichung von Diffie und Hellman [32] über ein völlig neues Konzept, das Public Key Kryptosystem. Bei diesem Verfahren ist dem Angreifer das Verschlüsselungsverfahren und der zugehörige Schlüssel bekannt, trotzdem ist keine Dechiffrierung möglich.

8.3.1 Klassische Kryptologie

Man unterscheidet hier zwei grundlegende Verfahren:

- Substitutionen
- Tranpositionen

Bei den Substitutionen hat man die Möglichkeit, jedem Buchstaben oder Wort aus dem Alphabet A des Klartextes eineindeutig einen Buchstaben oder ein Wort aus dem Codealphabet B zuzuordnen. Dies nennt man monoalphabetisch. Erfolgt die Zuordnung ohne Eineindeutigkeit auf mehrere Alphabete, so nennt man dies polyalphabetisch [48].

Eine weitere Einteilung erfolgt unter dem Gesichtspunkt, ob man Einzelbuchstaben (monographisch) oder ob man Zeichenketten (polygraphisch) ersetzt.

All diese klassischen Verfahren sind für den professionellen Gebrauch nur dann geeignet, wenn sie kombiniert werden. Sonst ist es leicht möglich, durch einen Vergleich der Häufigkeitsverteilung der Buchstaben der deutschen Sprache mit der Verteilung der Codebuchstaben den Code zu knacken.

8.3.1.1 Monoalphabetische monographische Substitution

Es wird eine injektive Abbildung zwischen Klartextalphabet und Codealphabet gemacht.

Bsp.:

$A = \{A, ..., Z\}$ $\qquad$ $B = \{ij | i, j \in \{1, ..., 5\}\}$

Sei x der Buchstabe der in Zeile i und Spalte j steht. Dann ist: $f(x) = (ij)$.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

GEHEIM $\rightsquigarrow$ 22 15 23 15 24 32

8.3.1.2 Polyalphabetische monographische Substitution

Es können verschiedene Symbole für den gleichen Buchstaben stehen. *Vigenere-Chiffre:*

Vigenere Tableau:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Ein zu verschlüsselndes Zeichen bestimmt in dem Tableau eine Zeile i und jedes Schlüsselzeichen eine Spalte j. Der Schnittpunkt ist das Schlüsseltextzeichen.

Um zu entschlüsseln sucht man das Schlüsseltextzeichen in der durch das Schlüsselzeichen bestimmten Spalte. Das Klartextzeichen ist dann der Wert der entsprechenden Zeile.

Bsp.:

Klartext:	I	N	F	O	R	M	A	T	I	K
Schlüssel:	U	N	I	U	N	I	U	N	I	U
Schlüsseltext:	C	A	N	I	E	U	U	G	Q	E

8.3.1.3 Monoalphabetische polygraphische Substitution

Es werden Worte eineindeutig verschlüsselt. *Dellastello-Chiffre* [48]:

Man ordnet das Alphabet jeweils in vier 5×5 Matrizen an:

$$M_1 \begin{array}{|ccccc|} \hline A & X & Y & G & I \\ W & B & F & Z & H \\ U & \mathbf{V} & C & P & Q \\ T & S & R & O & D \\ K & L & M & N & E \\ \hline \end{array} \qquad M_3 \begin{array}{|ccccc|} \hline L & G & C & Y & U \\ F & B & X & T & P \\ A & W & S & \mathbf{O} & K \\ V & R & N & I & E \\ Q & M & H & D & Z \\ \hline \end{array}$$

M_4

A	**H**	B	P	C
Q	D	R	E	S
F	T	G	U	O
C	I	W	K	X
L	Y	M	Z	N

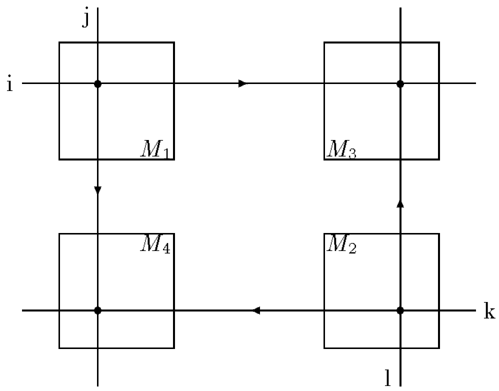
M_2

X	U	V	**W**	K
Y	T	S	I	L
Z	G	H	R	M
F	B	E	Q	N
A	C	D	P	Q

Sei m_{xab} der Buchstabe der in M_x in Zeile a und Spalte b steht.

Verschlüsselt werden je 2 Buchstaben wie folgt:

- $f(m_{1ij}, m_{2kl}) = (m_{3il}, m_{4kj})$



Im Bild ist $f(V, W) = (O, H)$.

8.3.1.4 Polyalphabetische polygraphische Substitution

Es können verschiedene Worte für gleiche Klarworte stehen.

Bsp.: Man verschlüsselt die Worte seines Textes unregelmäßig abwechselnd nach einem Vigenere-Chiffre oder einem Verfahren wie es unter ‚monoalphabetischen polygraphischen Sustitution‘ vorgestellt ist.

8.3.1.5 Transpositionen

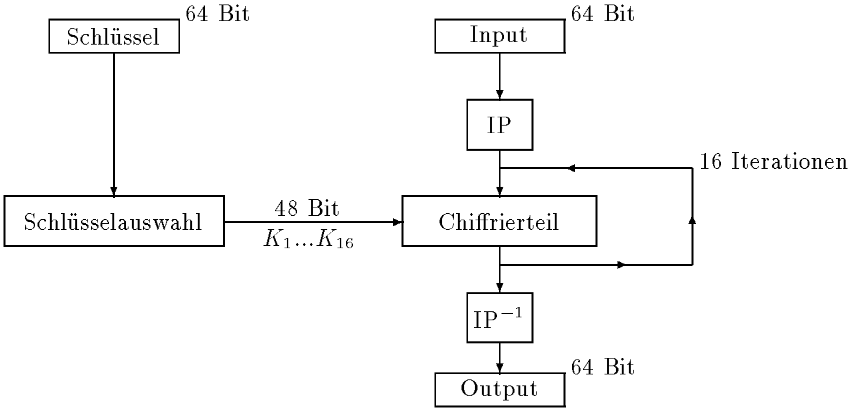
Die Reihenfolge der Buchstaben des Klartextes werden vertauscht. Dazu werden häufig Permutationsmatrizen eingeführt.

Bsp.: $p = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 0 & 1 \end{pmatrix} \quad \Longrightarrow \quad f_p(STIL) = LIST$

8.3.2 Date Encryption Standard

Der Data Encryption Standard (DES), eine Kombination klassischer Verfahren, wurde 1977 als Verschlüsselungsstandard vom National Bureau of Standards (NBS) genormt. Bei diesem von IBM entwickelten Verfahren wird der Klartext in 64 Bit Blöcke unterteilt. Das Schlüsselwort besteht ebenfalls aus 64 Bit, davon 8 Paritätsbit. Dadurch ergeben sich $2^{56} \approx 7 \cdot 10^{16}$ unterschiedliche Schlüssel.

Das Verfahren arbeitet nun folgendermaßen: Zunächst wird der Klartextblock mit einer Permutation kodiert. Anschließend durchläuft der Block 16 mal eine Chiffrierung mit jeweils verschiedenen Schlüsseln $K_1 \ldots K_{16}$, die sich aus dem ursprünglichen Schlüssel ableiten. Das Ergebnis schließlich wird der inversen Anfangspermutation unterworfen.



Was passiert im Chiffrierteil?

Der 64 Bit lange Block wird in 2 gleichlange Blöcke L und R zerlegt. Darauf werden folgende Operationen ausgeführt:

$$
\begin{aligned}
&L(0) := L \\
&R(0) := R \\
&FOR\ i := 1\ TO\ 16\ DO \\
&BEGIN\ L(i) := R(i-1) \\
&\qquad\qquad R(i) := L(i-1) \oplus f(R(i-1), K_i) \\
&END
\end{aligned}
$$

Den wichtigsten Teil bildet die Funktion f: Hier wird durch Erweiterung von R(i) auf 48 Bit und anschließender Verknüpfung mit dem Schlüssel K_i kodiert. Aus dem Ergebnis werden durch Substitutionstabellen (polyalphabetisch - monographisch) gewisse Bits ausgewählt und einer Permutation unterworfen.

Das Verfahren ist so konstruiert, daß man es auch zum Entschlüsseln nehmen kann. Dazu werden lediglich die Schlüssel in umgekehrter Reihenfolge benutzt [48].

Da der DES inzwischen sehr stark verbreitet ist, sind Sicherheitsaspekte besonders wichtig. Insbesondere deshalb, weil zum Beispiel die EC-Karte für den Geldautomaten damit gesichert ist. Rein theoretisch läßt sich für 40 Millionen DM ein Rechner bauen, der jeden DES-Code durch Probieren aller Schlüssel an einem Tag knackt. Benutzt werden dazu spezielle Schaltkreise, die den DES hardwaremäßig implementieren. Diese Chips kodieren heute schon 2 MegaByte/sec. Darum ist das Verfahren für militärische Zwecke, wo Geld keine Rolle spielt, ungeeignet.

Es gibt aber auch andere Kritikpunkte. Da nie genaue Gründe für die Wahl der vielen Substitutionstabellen bekannt gegeben wurden, kann es sein, daß die Entwickler des DES eine Möglichkeit haben, das Verfahren zu verkürzen und direkt den Klartext zu bestimmen. Weiterhin wurden Ergebnisse eines Sicherheitstests nie veröffentlicht. Auch die Forderung nach einem 128 Bit langen Schlüssel wurden verworfen. Schließlich gehen seit Anfang 1989 Gerüchte um, der DES sei durch sowjetische Mathematiker schon lange dechiffriert worden. Allerdings liegen dazu nur Gerüchte und noch keine richtigen Veröffentlichungen vor, so daß der DES auch weiterhin das dominierende System bleiben wird.

8.3.3 Public Key Kryptosysteme

Diese seit 1977 veröffentlichten Verfahren stellen bis heute die weitaus sicherste Kodierung dar. Hierbei wird das Prinzip der Einwegfunktionen (one way function) ausgenutzt. Das sind Funktionen, deren Funktionswerte leicht zu berechnen sind, deren Umkehrfunktionen aber nur sehr schwer zu bestimmen oder sogar unlösbar sind. Bei einer Falltürfunktion (trap door function), der Spezialfall einer Einwegfunktion, wird durch Kenntnis eines Parameters die Umkehrfunktion sehr einfach zu berechnen.

Dies ist auch die Idee der Public Key Verfahren.

Will Benutzer A an Benutzer B eine Nachricht schicken, so fordert er von B das Verfahren zur Kodierung und das Schlüsselwort, das er verwenden soll an. Dies braucht nicht geheim zu sein. A verschlüsselt nun damit den Text und schickt ihn B. Ein Fremder hat keine Möglichkeit den Code zu brechen, obwohl er das genaue Verfahren kennt, denn es handelt sich um eine Einwegfunktion. B hingegen hat einen Parameter der geheim ist und mit ihm nutzt er den Falltüreffekt aus und entschlüsselt die Nachricht. Neben dem RSA-Verfahren spielt das Merkle Hellman Verfahren [48] eine große Rolle.

8.3.3.1 Merkle Hellman Verfahren (1978)

0-1 Knapsack:

Man hat eine Menge von Werten und soll daraus solche heraussuchen, deren Summe eine gewisse Grenze trifft.

Gegeben: $a = (a_1, \ldots, a_n) \in N^n$; $s \in N$

Gesucht: $x = (x_1, \ldots, x_n) \in \{0,1\}^n$ mit $\sum_{i=1}^{n} a_i \cdot x_i = s$

Das 0-1 Knapsack-Problem ist NP-vollständig, hat also praktisch exponentiellen Zeitaufwand.

Extra simpler Knapsack:

Ist $a = (a_1, \ldots, a_n) \in N^n$ und $a_j > \sum_{i=1}^{j-1} a_i$, dann ist a extra simpel.

Bsp.: (1,2,4,8) oder (10,20,80,150) sind extra simpel

Ein extra simpler Knapsack kann in O(n) Schritten gelöst werden.

Das Verfahren:

Voraussetzungen:

1. $\bar{a} = (\bar{a}_1, \ldots, \bar{a}_n) \in N^n$ extra simpel
2. $k \in N$ mit $k > \sum_{i=1}^{n} \bar{a}_i$
3. $w \in \{0, \ldots, k-1\}$ mit w und k sind teilerfremd
   w^{-1} ist das multiplikativ Inverse zu $w \bmod k$
4. $a = w \cdot \bar{a} \bmod k$
5. eine Nachricht $m = (m_1, \ldots, m_n)$

Schlüssel:

1. zum Verschlüsseln: a öffentlich
2. zum Entschlüsseln: $\bar{a}, w^{-1}, k$ alle geheim

Chiffrierung:

1. Verschlüsselung: $E(m) = \sum_{i=1}^{n} \bar{a}_i \cdot m_i$
2. Entschlüsselung: $D(m) = F_{\bar{a}}^{-1}(w^{-1} \cdot m \bmod k)$
   $F_{\bar{a}}^{-1}$ sei eine Funktion, die einen extra simplen Knapsack a berechnet.

Dabei ist $n \approx 100$ und die $a_i \approx 10^{50}$.

Bsp.:

- A will an B die Nachricht (1,1,0) schicken

Dazu bestimmt B:

1. $\bar{a} = (1, 3, 6), \quad \sum_{i=1}^{n} \bar{a}_i = 10$
2. $k = 13$
3. $w = 7 \;\Rightarrow\; w^{-1} = 2,$ denn $7 \cdot 2 \bmod 13 = 1$
4. $a = w \cdot \bar{a} \bmod k \;\Rightarrow\; a = (7 \cdot 1 \bmod 13,\; 7 \cdot 3 \bmod 13,\; 7 \cdot 6 \bmod 13) = (7, 8, 3)$

B teilt nun A das Tripel $a = (7, 8, 3)$ mit.

Darauf berechnet A: $E(1, 1, 0) = 7 \cdot 1 + 8 \cdot 1 + 3 \cdot 0 = 15$

Diese Zahl „15" wird zu B übermittelt.

Ein Angreifer müßte, um die Nachricht zu entschlüsseln, einen nicht simplen 0-1 Knapsack mit den Werten (7,8,3) und 15 lösen. All diese Werte kennt er. Doch bei großen Zahlen ist dies nur mit exponentiellem Aufwand lösbar.

Erhält jetzt B die Nachricht, so berechnet er:

- $D(15) = F_{\bar{a}}^{-1}(2 \cdot 15 \bmod 13) = F_{(1,3,6)}^{-1}(4) = (1, 1, 0)$

Somit hat B die von A gesendete Nachricht.

8.4 Zusammenfassung

Es wird sich zeigen, daß die Geheimhaltung von Daten in der Zukunft noch wichtiger wird, denn die Verbreitung von Computern und Rechnernetzen wird zunehmen. Die Forderung nach Sicherheit wird sich darum zunächst an die Systeme selbst richten. Der Programmierer darf trotz der Größe des Systemprogrammes keine Lücken offen lassen. Da Systemfehler jedoch nie ganz ausgeschlossen werden können und auch der Einfallsreichtum von Hackern oder Spionen immer neue Schwächen auffinden wird, sollte man die Möglichkeit der Verschlüsselung von Daten zu Hilfe nehmen. Zusammen mit Methoden des Zugriffsschutzes und vielleicht mit der Einsicht des Benutzers, fremde Daten nicht zu lesen, sollte man eine Verbesserung der Sicherheit erreichen können.

Kapitel 9

Zuverlässige Software?

Georg Meyer

Immer wieder hört man in den Medien von Katastrophen, Unglücken und Beinaheunfällen, die den Einsatz von hochriskanter Technologie zur Ursache und die Bedrohung oder Auslöschung von zum Teil vielen Menschenleben zur Folge haben. Nicht immer ist dies auf fehlerhafte Maschinen und Technik zurückzuführen. Häufig ist die Steuerung dieser Maschinen – die Software – daran Schuld. Gerade als Informatiker muß man sich im klaren sein, daß die Herstellung sicherer und zuverlässiger Software ein großes Problem darstellt.

Im folgenden sollen Möglichkeiten und Ziele, aber vor allem auch Grenzen und Kritikpunkte von zuverlässiger Software aufgezeigt werden.

9.1 Einführung

9.1.0.2 Was heißt eigentlich zuverlässige Software?

Hier muß man eigentlich drei Aspekte betrachten, die man unter dem Begriff Zuverlässigkeit zusammenfassen kann:

Die *Richtigkeit* bezieht sich auf die Übereinstimmung zwischen funktioneller Spezifikation und dem Programm. Tatsächlich braucht das Programm in einer bestimmten Umgebung nicht zu laufen.

Bei der *eigentlichen Zuverlässigkeit* „handelt es sich um die Wahrscheinlichkeit, mit der ein Softwaresystem die beabsichtigte Aufgabe für eine vorgegebene Anzahl von Eingabefällen unter festliegenden Eingabebedingungen erfüllt, vorausgesetzt Hardware und Eingabe sind fehlerfrei“.

Schließlich stellt die *Robustheit* einen Zusammenhang zwischen Softwarezuverlässigkeit und Systemzuverlässigkeit her. Hier kommt die Komponente der Systemabhängigkeit hinzu [59].

Weiterhin ist als Softwarezuverlässigkeit der erweiterte Begriff aus den eben erklärten Komponenten gemeint. Dabei ist die Softwarezuverlässigkeit nur eine, wenn auch die vielleicht bedeutenste Merkmalsausprägung der Softwarequalität. Daneben gibt es zum Beispiel noch: Flexibilität, Benutzbarkeit, Effizienz, Portabilität und Verknüpfbarkeit. Sicherlich sind die einzelnen Qualitätsziele nicht alle gleichgerichtet, sondern eher gegensätzlich: Ein flexibles System, das nicht nur auf die speziellen Wünsche eines Benutzers zugeschnitten ist, wird wahrscheinlich – auf Grund der Größe – weniger effizient und auch fehleranfälliger sein.

Im Gegensatz zu handelsüblichen Waren, etwa einem Staubsauger oder einer Hifianlage, ist es sehr schwierig, die Qualität von Software zu messen. Zum Messen benötigt man Maßstäbe und Normen, die bei Software nicht einfach zu bestimmen sind. Einerseits ist dies aufgrund der vielfältigen gegensätzlichen Merkmale problematisch. So kann man nicht generell behaupten, ein zeiteffizientes aber unkomfortables Programm sei besser oder schlechter als das Gegenteil. Andererseits haben viele Programme gerade in größeren Systemen Unikatcharakter, so daß man sie schlecht mit anderen vergleichen kann. Von verschiedenen Gesellschaften (IEEE et al.) gibt es Ansätze zu Qualitätsnormen [102]. Um all diese Qualitätsziele zu erreichen, bedient man sich der Methoden des Software Engineerings.

9.1.0.3 Wo ist zuverlässige Software überhaupt gefordert?

Grundsätzlich überall! Wer möchte schon, daß ein Programm während des Ablaufs einfach aussteigt. Sicherlich betrifft dies meist nur eine oder wenige Personen und ist daher nicht von weitreichender Bedeutung. Wichtig wird die Zuverlässigkeit vor allem bei:

- Datenbanken

  Hier kann ein Fehler der Software zu großem Daten- und damit auch finanziellem Verlust führen oder Auswirkungen auf die darin abgespeicherten Personen haben, wie der folgende Fall berichtet:

  In Düsseldorf hat eine 54jährige Frau ihre 15jährige Tochter erwürgt und versucht, auch ihren 13jährigen Sohn und sich selbst umzubringen. Sie wurde wegen Mordes angeklagt. Man sprach sie schließlich frei, als das Gericht erfuhr, daß ihre Versicherungsgesellschaft sie über Testergebnisse benachrichtigt habe, nach denen sie an einer unheilbaren Syphilis leide. Sie habe ebenfalls ihre beiden Kinder infiziert. Die Frau war so schockiert, daß sie die Wahnsinnstat beging. Kurze Zeit später widerrief die Gesellschaft die Information über ihre Krankheit, mit der Begründung, es habe sich um einen Computerfehler gehandelt [71].

- Fertigung

  Zum einen können fehlerhafte, computergesteuerte Teile einer Produktreihe diese unbrauchbar machen, zum anderen kann es durch z.B. falsches Setzen einer Schweißnaht durch einen computergesteuerten Roboter zum Ausfall einer Baureihe kommen. Im geringsten Fall wird der Fehler rechtzeitig erkannt und ausgebessert. Hier kommt es *nur* zu einem finanziellen Verlust. Wesentlich schlimmer wird es, wenn Mensch und Umwelt bedroht sind. Auch hierzu ein Beispiel:

  14.000 neue Autos der Marke Lincoln Mark VII mußten zurückbeordert werden, weil einige Wagen scheinbar grundlos in Flammen aufgingen, nachdem sie abgeschaltet waren. Der Grund lag in der computergesteuerten Klimaanlage. Beim Abschalten des Systems verursachte ein Modul einen elektrischen Impuls, anstatt sich selbst abzuschalten. Dadurch blieben Relais geschlossen, die wiederum die Überhitzung elektrischer Drähte verursachten. Schließlich kam es in Einzelfällen zum Feuerausbruch [71].

- Realzeitprobleme

  Sowohl in der friedlichen (Verkehrsmittel, Kernkraftwerk, Raumfahrt etc.), als auch in der militärischen Nutzung bedarf es geringen Vorstellungsvermögens, welche Katastrophen für Menschheit und Umwelt durch Unzuverlässigkeit möglich sind.

An dieser Stelle sei auf Abschnitt 9.4: ‚Kritik an Hand von Fallbeispielen' verwiesen.

9.1.0.4 Wie kommt es zu unzuverlässiger Software?

Die Quelle der Fehler ist in den Unzulänglichkeiten des Menschen zu suchen: ‚Schon bei der Formulierung des Gedankens entstehen zwischen dem menschlichen Gedächtnis bzw. seiner Intelligenz und der natürlichen Sprache die ersten Übertragungsschwierigkeiten' [95].

Das Gleichnis vom Mathematiker, der a meint, b sagt, c rechnet und d aufschreibt, ist hier sicherlich angebracht. Je komplexer ein Sachverhalt ist, desto weiter liegen a, b, c, d zwangsläufig auseinander. Die Aussage bleibt natürlich nicht nur auf Mathematiker beschränkt. Daher kann man schon vorab resümieren, daß zuverlässige Software, solange sie vom Menschen erstellt wird, eine Utopie bleibt.

Im nächsten Abschnitt soll gezeigt werden, wie man sich diesem Ziel weitgehend annähert.

9.2 Theoretische Grundlagen

Um zuverlässige Software zu erreichen, muß man bestrebt sein, Fehler auszuschließen oder auszuschalten. Dabei gilt es zu beachten, daß der ‚Fehler' ein relativer Begriff ist, da man einen gegebenen Sachverhalt an einer existierenden Norm messen muß. So mag bei einem Schüler, dessen Gewissenhaftigkeit und Fleiß von seinen Mitschülern als Fehler (Strebertum) gedeutet werden, während dies der Lehrer als durchaus positive Tugenden anerkennt. Beim Softwaresystem wird die Bezugsnorm durch den Benutzer gegeben. Es gibt grundsätzlich drei Möglichkeiten, Fehler zu vermeiden:

- Fehler schleichen sich gar nicht erst ein
- Fehler werden beseitigt
- Fehler werden ‚bedeutungslos'

9.2.1 Softwarekonstruktion

Die Softwarekonstruktion stellt die Basis und den Rahmen zur Erreichung der Zuverlässigkeit dar, denn sie versucht, durch sequentielle, strukturierte Entwicklung der Software, Fehler gar nicht erst aufkommen zu lassen. Durch eine solche Entwurfsmethodik kann vielleicht eines Tages weitgehend auf Testverfahren und Fehlerbehebung verzichtet werden. Momentan ist diese Technik jedoch noch nicht so weit, um allein durch die Entwicklung Zuverlässigkeit zu erreichen.

Das ‚A' und ‚O' der Softwareentwicklung bildet die richtige Organisation. Sie scheitert häufig an dem Irrglauben, daß es sich hierbei um einen linearen Prozeß von der Problemanalyse bis zur Systemabnahme handelt. Es handelt sich vielmehr um einen iterativen Vorgang (Abbildung 9.1), da ein Softwaresystem sehr komplex ist. Je größer die geforderte Softwarequalität, um so häufiger muß der Konstruktionszyklus durchlaufen werden. Oft wird nach dem ersten Durchgang schon das Produkt an den Benutzer übergeben, und man wendet sich einem neuen Projekt zu. Genauso erfolgt die Budgetplanung, in der die Weiterentwicklung nicht mehr mit einbezogen wird. Tatsächlich ergibt sich aus den Untersuchungen von Böhm, daß nur 30% der Gesamtkosten vom ersten Entwicklungsgang verbraucht werden. Er sollte lediglich Modellcharakter besitzen, auf dem sich solide aufbauen läßt.

Nun zu den einzelnen, bereits angesprochenen Entwicklungsstufen bzw. -phasen: Der Unterschied zwischen Stufen und Phasen besteht darin, daß Stufen sequentieller Natur sind, während letztere auch parallel ablaufen können. H. Müller-Merbach ist Vertreter der Phasentheorie, da er in der Parallelität eine größere Effizienz sieht [66]. H. M. Sneed, Anhänger der Stufentheorie, hält dagegen, daß Ergebnisse einer Stufe vorliegen müssen, auf denen die nächste erst aufbauen kann [94]. In der Praxis ist es wohl so, daß die Grenzen fließend sind.

Zunächst erfolgt die *Systemspezifikation*: Sie beschreibt auf der einen Seite die Leistung, auf der anderen die Einschränkungen, die sowohl durch die Hardware, als auch durch finanzielle, organisatorische und rechtliche Aspekte gegeben sind. Im einzelnen sind dies:

- was ein System tun soll (Funktionen)
- worauf ein System wirken soll (Daten)
- unter welchen Bedingungen das System arbeiten soll (physische Umgebung)
- welchen Einschränkungen das System unterliegen soll (Grenzen)

Das Hauptproblem liegt in der Unterschiedlichkeit der Systeme, die es schwierig macht, eine allgemeingültige Beschreibungsform zu finden. Diese kann formal (Mathematiker), graphisch (Ingenieur) oder tabellarisch (Kaufmann) erfolgen. Wichtig ist, daß sie fachlich richtig, vollständig und konsitent ist, und auf ihr aufbauend, eine DV-technische Lösung gefunden werden kann. Durch die Systemspezifikation wird also das ‚Was' realisiert und zwar meistens in den Fachabteilungen.

Das ‚Wie' stellt die nächste Stufe dar und wird als *Softwareentwurf* bezeichnet. An ihm arbeiten vor allem die DV-Spezialisten. Hier werden die spezifizierten, aber abstrakten Objekte und logischen Funktionen zunächst

Abbildung 9.1: Softwarekonstruktionszyklus

verfeinert, um sie dann in maschinell speicherbare Objekte und programmierbare Funktionen zu transformieren. Die Aufgabe besteht darin, ‚die Kluft zwischen den Wünschen des Benutzers und den Fähigkeiten der Maschine zu überbrücken'. Der Softwareentwurf umfaßt mindestens zwei Stufen: den *Systementwurf* und den *Programmentwurf*.

Beim Systementwurf muß man je nach Systemtyp einen anderen Aufbau wählen. Man unterscheidet nämlich nach:

- Stapelsystem
- Onlinesystem
- Realzeitsystem

Hierauf näher einzugehen, würde zu weit führen. Es soll lediglich gesagt werden, daß der Aufbau von Realzeitsystemen sich von den anderen beiden stark unterscheidet, weil dessen Ablauf nicht vorherbestimmbar ist, sondern von Prioritäten gesteuert wird. Systemabhängige und -unabhängige Elemente des Systementwurfs sind in [94] zu finden.

Beim Programmentwurf liegt der Abstraktionsgrad eine Etage tiefer. Gleichzeitig ist auch das Blickfeld eingeschränkt. Während vorher das Gesamtkonzept beachtet werden mußte, braucht der Programmentwerfer nur noch eine Komponente, deren Schnittstellen und Funktionen zu beachten. Eine Komponente kann zwar mehrere Moduln umfassen, muß aber dennoch eine Laufeinheit bilden. Zum Programmentwurf setzt man z.B. Struktogramme ein, in der Systementwurfsphase (aufgrund der häufigen Überlappung mit der Systemspezifikation) werden noch die graphische (z.B. Petrinetz), tabellarische (z.B. Zuordnungstabellen) und formale Darstellung (z.B. Struktursprachen) verwendet.

Auf die darauf anschließende Programmierung – unterteilt in Modulentwurf, Codierung und Modultest – soll nicht näher eingangen werden, da dies jedem Informatiker hinreichend bekannt sein sollte. Vielfach wird damit der Softwareentwicklungsprozeß als abgeschlossen gesehen. In Wahrheit fallen nun aber noch 40% der Kosten eines Entwicklungsganges an. Diese werden für die *Qualitätssicherung* [42] und die *Integration* gebraucht. Die Schwierigkeiten der Qualitätssicherung wurden bereits in 9.1.0.2 behandelt. Auch die Integration stellt einen sehr wichtigen Teil dar, denn ein bereits als korrekt getesteter Programmteil braucht im übergeordneten System noch lange nicht die gleiche Zuverässigkeit zu zeigen. Daher ist ein Gesamttest notwendig.

Parallel zur Programmentwicklung muß auch die Dokumentation erstellt werden, die einen festen Bestandteil der Gesamtsoftware darstellt und die Qualität entscheidend beeinflußt.

Aber gerade durch die Aufspaltung in Entwicklungsstufen oder -phasen birgt dieser Vorgang Fehlerquellen. So kann es in jedem Entwicklungsschritt und an jeder Schnittstelle zu Fehlern kommen. Im Einzelnen kann dies der Abbildung 9.2 entnommen werden. Es ist daher äußerst wichtig, in allen Stufen mit der gleichen Sorgfalt heranzugehen und keine überzubewerten. Denn bei einem Fehler in der Entwicklungskette kommt es, auch bei der internen Korrektheit aller Folgeglieder, zwangsläufig zu einem fehlerhaften Ganzen und erfordert einen erneuten Zyklusdurchlauf [94].

9.2.2 Fehlerbeseitigung und Testverfahren

Bereits gemachte Fehler sollen nun aus dem System entfernt werden. Das Testen ist jedoch die unbeliebteste Aufgabe im ganzen Entwicklungsprozeß und darf sich gleichzeitig nicht beliebig ausdehnen. Dieses Dilemma beschreibt das Pferdegleichnis ganz treffend:

Ein Knecht soll ein hungriges Pferd mit Heu füttern. In dem Heu sind aber eine Vielzahl von Stecknadeln. Der Knecht steht nun vor einem Problem. Gibt er dem Pferd einfach zu Fressen, und das Pferd stirbt, so ist der Bauer wütend auf ihn. Andererseits kann er nicht jeden Halm untersuchen, sonst ist das Pferd fortgelaufen oder verhungert. Ein vernünftiger Kompromiß scheint der zu sein, den Haufen möglichst genau in einer vertretbaren Zeit zu durchsuchen. Allerdings kann das Pferd gerade an der einen Stecknadel eingehen, die der Knecht übersehen hat.

Dieses Beispiel gibt die Problematik des Testens genau wieder. Auf der einen Seite muß die Software sicher sein, andererseits darf die Entwicklung aus Gründen der Wirtschaftlichkeit nicht zu viel Zeit in Anspruch nehmen. Um möglichst viele Fehler zu beseitigen, stehen unterschiedliche Testansätze zur Verfügung:

statische Programmanalyse: Hierbei wird der Softwaretext – in einer Entwurfs- oder Programmiersprache oder der formalen Spezifikation gegeben – mittels syntaktischer Analyse in Elemente zerlegt. Danach werden Struktur und Verwendung untersucht. Im einzelnen kann der Zieltext

- auf Vollständikeit und Konsistenz geprüft werden (Variableninitialisierung, Schleifentermination, Typkompatibilität etc.),
- gegen eine Reihe von vorgegebenen Regeln getestet werden. Hierzu gibt es auch Automatisierungsansätze, die z.B. Verschachtelungstiefe oder unerwünschte Nutzung globaler Daten erkennen,
- gegen einen inhaltlich gleichen Text anderer Ebene getestet werden (z.B. Spezifikation).

Mit der statischen Programmanalyse werden nur 20-30% der Fehler erkannt.

Beim *Ablaufbezogenen Testen* wird das Programm gegen sich selbst getestet. Man versucht die Überdeckung der möglichen bzw. relevanten Pfade eines Programms in einer Testreihe festzustellen. Diese kann man durch statische Analyse ableiten. Mit dieser Methode werden 50% aller Fehler entdeckt, nämlich grobe Abbruchfehler,

Abbildung 9.2: Fehlerquellen in den einzelnen Entwicklungsschritten

unerreichbare Zweige, Irrpfade, endlose Schleifen und unvollständige bzw. inkonsistente Bedingungen. Aber vergessene Funktionen, unberücksichtigte Daten, inkonsistente Schnittstellen, Tippfehler oder gar Abweichungen von der Spezifikation werden nicht erkannt.

Das *Datenbezogene Testen* hat seinen Ursprung im Random-Datentest, wobei das Programm mit willkürlich gestreuten Eingabedaten gefüttert wird. Die Qualität hängt von der Streuung der Eingabedaten ab. Der Nachteil besteht hierbei, daß in größeren Programmen nie alle Daten durchgetestet werden können, so daß Fehler nicht auszuschließen sind. Man versucht, diskrete Daten mit gleicher Auswirkung auf das Programm zu Äquivalenzklassen zusammenzufassen und damit mehrere Daten gleichzeitig durchzutesten.

Das *Funktionsbezogene Testen* ist relativ unerforscht. Es überprüft nicht nur Ablaufpfade, sondern das funktionelle Verhalten einzelner Programmteile einschließlich der Ein- und Ausgabewerte und der Schnittstellen. Diesem Verfahren wird sicherlich die Zukunft gehören.

Zum *Back-To-Back-Testen* benötigt man mehrere Programmversionen einer Spezifikation und führt sie nebeneinander aus. Man weiß nun, wieviele Fehler nur in einem und wieviele in mehreren Programmversionen vorkommen. Aus der Anzahl der gemeinsamen Fehler kann die Restfehlerrate hochgerechnet werden. Dieses Testverfahren gilt als zuverlässiger als alle anderen konventionellen. Es ist aufgrund der Mehrproduktion der gleichen Software aber wesentlich teurer. Daher wird es nur dort eingesetzt, wo die Zuverlässigkeit sehr wichtig ist.

Die heutigen Testmethoden sind sicher noch nicht zufriedenstellend. Aber die Entwicklung neuer Technologien geht langsam voran. Die Literatur hinkt den Kongressen ein bis zwei Jahre hinterher, die Praxis sogar fünf Jahre. Es zeigt sich, daß Europa gegenüber den USA einen gewissen Nachholbedarf hat. Dies ist auch an der unterschiedlichen Schwerpunktsetzung zu sehen: Während die Amerikaner daten- und funktionsbezogenes Testen favorisieren, wird in Europa hauptsächlich auf dem Gebiet des ablaufbezogenen Testens geforscht [95].

9.2.3 Verwendung von Redundanzen

Diese Methode unterscheidet sich von den vorangegangenen entscheidend. Denn hierbei akzeptiert man, daß der menschliche Gedankengang fehlerbehaftet ist. Dies versucht man durch die Ausnutzung von Redundanzen abzuschwächen und die Folgen zu kontrollieren. Man erhöht die Zuverlässigkeit (Wahrscheinlichkeit) einfach durch eine Parallelschaltung gleichartiger, aber unabhängiger Systeme, bei dem schon jedes einzelne für den korrekten Ablauf des Ganzen garantieren kann. Ist bei einem System die Ausfallwahrscheinlichkeit $1/n$ und setzt man k Systeme ein, so sinkt die Wahrscheinlichkeit für den Gesamtausfall auf $1/n^k$ [59].

Die drei Konzepte sind nicht voneinander losgelöst zu sehen und wurden nur zur einfacheren Erklärung getrennt behandelt. Sie bilden nur im sinnvollen Zusammenspiel eine Chance, eine hohe Softwarezuverlässigkeit zu erlangen. So muß gerade das Testen in den Software-Entwicklungsprozeß integriert werden.

Bis jetzt konnte der Eindruck entstehen, daß der Grad an Zuverlässigkeit relativ hoch ist oder zumindest erreicht werden kann. Faktoren und Beispiele, die dagegensprechen, werden in den folgenden Abschnitten behandelt.

9.3 Einflußfaktoren

9.3.1 Allgemein

Hierbei spielt einerseits die Aufgabenstellung eine Rolle, andererseits die EDV-abhängigen Einflüsse. Der Mensch als Faktor wird im nächsten Abschnitt gesondert behandelt.

Bei der Aufgabenstellung ist zunächst die Problembeschreibung von großer Bedeutung. Nur wenn die Anforderungen an ein Programm genau spezifiziert sind, wird dies eine hohe Qualität erzielen können. Wenn Anwenderschnittstellen sich ständig ändern und Programmkorrekturen und -verbesserungen zur Folge haben, wirkt sich dies negativ aus.

Unter den EDV-abhängigen Einflüssen versteht man zunächst Software- und Hardwareumfeld, in das ein Programm integriert werden muß. Dann spielt natürlich die Programmiersprache mit dem jeweiligen Komfort und ihren Möglichkeiten eine Rolle. Schließlich kommen die Programmierumgebung, also Arbeitsumgebung und die zur Verfügung gestellten Hilfsmittel zum Tragen [61].

9.3.2 Der Einflußfaktor Mensch

Hier sei zunächst die fachliche Qualifikation betrachtet. Prinzipiell kann das fachliche Wissen eines Informatikers in zwei Kategorien unterteilt werden:

- *das auswendiggelernte Wissen*

  Es läßt sich **nur** durch Auswendiglernen aneignen. Dabei handelt es sich um die spezifischen Kenntnisse über eine Programmiersprache.

- *das strukturelle Wissen*

  Dieses Wissen umfaßt wichtige allgemeine Konzepte zur Lösung von Aufgaben sowie die Umsetzung in Programme. Dabei ist es weitgehend unabhängig von einer speziellen Programmiersprache. Es wird durch das Lösen neuartiger Aufgaben sowie das Erlernen zusätzlicher Programmiersprachen erweitert.

Diese Unterteilung wird an folgender Erfahrung klar, die sicherlich jeder Informatiker schon gemacht hat: Lernt man zum erstenmal eine Programmiersprache (etwa Pascal), so hat man viel mehr Schwierigkeiten als bei der Erlernung einer weiteren Sprache mit gleichem Konzept (z.B. Modula II oder C). Das liegt daran, daß die gleiche Struktur der prozeduralen Programmiersprachen zugrundeliegt, und nur die Syntax sowie spezifische Eigenschaften neu gelernt werden müssen. Ist zu diesem auswendiggelernten Wissen auch das strukturelle Wissen unbekannt (z.B. beim funktionalen LISP), so treten ähnliche Schwierigkeiten wie bei der ersten Programmiersprache auf.

Genauso entscheidend wie die fachliche Qualifikation ist das Persönlichkeitsbild für den Softwareentwicklungsprozeß: Ein besonders *ängstlicher Mensch* wird seine Aufgabe zögernd und vielleicht nur unter Anleitung ausführen. Er ist besonders anfällig in Stressituationen und zeigt auch allgemein keine Innovationsfähigkeit. Zuviel *Risikobereitschaft* ist ebenfalls fehl am Platz, denn dadurch werden überschnell Annahmen gemacht, woraus falsche Entscheidungen resultieren. Schließlich ist auch die Neigung zum *Perfektionismus* verhängnisvoll, da diese die Projektdauer unnötig verlängert. Denn unter Perfektionismus ist nicht unbedingt Zuverlässigkeit zu verstehen, sondern eher die Liebe zum Detail.

Natürlich machen sich auch andere Faktoren beim Menschen bemerkbar: Zunächst wirkt sein privates Umfeld auf die Qualität seiner Arbeit ein. Fühlt sich jemand innerhalb seiner Abteilung oder eines Projekts in die Defensive gedrängt, so wird er versuchen, seine Arbeit zu verteidigen und eventuelle Schwachpunkte oder Fehler zu vertuschen. Auch Kompetenzstreitigkeiten bei abteilungsübergreifenden Softwareentwicklungen führen einerseits zu Verzögerung, andererseits zu Unzuverlässigkeit.

Die vielleicht zwei wichtigsten psychologischen Aspekte, die auf den Menschen einwirken, sind der *Leistungsdruck* und das *Nachtwächtersyndrom*. Der Leistungsdruck wird durch das Konkurrenzdenken der Unternehmen hervorgerufen. Um geschäftsfähig zu bleiben, gilt es, ein Produkt als erster auf den Markt zu bringen, und damit den Standard zu setzen oder sonstige Terminvorgaben einzuhalten. Daß darunter die Zuverlässigkeit leidet, ist offensichtlich. Man nimmt sogar das Nachtwächtersyndrom in Kauf. Dieses besagt, daß in einem Betrieb, in dem es noch nie gebrannt hat, der Nachtwächter bei einem Feuerausbruch entweder schläft oder betrunken ist. Man hofft also, daß keine Komplikationen eintreten, die nicht noch behoben werden können. Leistungsdruck und Nachtwächtersyndrom gelten als Hauptursache für die Challengerkatastrophe.

Diese Punkte wirken alle auf den Produktionsfaktor Mensch ein und machen ihn damit zum bedeutungsvollsten. So vertritt J. Witt die Auffassung, daß Unzuverlässigkeit gerade in großen Softwareprojekten weitmehr durch den psychologischen Aspekt als durch den technischen hervorgerufen wird [61, 102].

9.4 Kritik an Hand von Fallbeispielen

Die folgenden Beispiele sind den ACM Software Engineering Notes entnommen und dort unter dem Titel ‚Risks to the Public' abgedruckt.

Zunächst ein Beispiel aus der zivilen Luftfahrt: Bei einer Boeing 747 der China Airlines fiel am 19. Februar 1985 ein Triebwerk aus. Der Autopilot versuchte, die Maschine auf 41.000 ft zu halten; das war jedoch mit nur drei Triebwerken in dieser Höhe nicht möglich, zumal sich die Maschine stark nach vorne neigte. Die anderen drei Triebwerke fielen (vielleicht durch Aussetzer bedingt) ebenfalls aus. Daraufhin verlor das Flugzeug 32.000 ft an Höhe, und nur Sekunden bevor die Maschine auf dem Pazifik aufgeschlagen wäre, konnte der Kapitän dem Autopilot die Kontrolle entreißen und die Triebwerke erneut starten. Der Heckstabilisator war zwar beschädigt, doch das Flugzeug, ursprünglich auf dem Weg nach Los Angeles, landete sicher in San Franzisco. In diesem Beispiel wurde der Notfall nicht simuliert. Der Autopilot hätte das Unmögliche nicht versuchen dürfen. Zumindest hätte eine Anzeige dem Piloten sagen müssen, was er versucht zu tun, um schneller eingreifen zu können. Die Moral, die sich für Programmierer daraus ergibt, ist die, daß ein Programm nicht nur in sich richtig sein muß, sondern daß es auch noch in einer fehlerhaften Umgebung sinnvoll funktionieren muß [70].

Das nächste Beispiel befaßt sich mit der militärischen Luftfahrt: Die F-16 Steuersoftware hat unter anderem dafür zu sorgen, daß das Flugzeug wieder in die horizontale Ausgangsposition kommt, wenn es schräg fliegt oder auf dem Kopf steht. Dabei wählt sie die kürzere Drehrichtung. Was passiert aber, wenn das Flugzeug exakt verkehrt herum fliegt? Dies ist ein typischer Fall für eine Stresssituation eines Computers. Tatsächlich kam es hier zu einem Deadlock. Der Fehler wurde in der Simulation behoben. Schließlich war nur eine weitere Abfrage notwendig [69].

Auch im Falklandkrieg wurden Softwarefehler aufgedeckt: So erkannte das Radarsystem der britischen ‚Sheffield' die angreifenden Exocet-Raketen der Argentinier nicht, die von einem Schiff russischer Bauart abgeschossen wurden. Die Software war nicht programmiert, diesen Raketentyp zu erkennen, weil man ihn auf einem russischen Schiff nicht vermutete. An dieser Stelle ging man also von falschen Prämissen aus. Es gilt, das *Unmögliche* vorauszusehen und zu erwarten. Aber auch auf argentinischer Seite passierten Fehler. Folgender basiert einfach auf schlechter Software: Viele Raketen flogen über die Briten hinweg und attakierten die eigenen Leute; ihre Sensoren erkannten nicht genug Metall unter sich [68].

Viele Fehler entstehen auch durch falsche Eingaben. Die Software muß so sicher gemacht werden, daß solche menschlichen Fehler weitgehend abgefangen werden können. Vor allem, wenn es – wie im nächsten Beispiel – um hohe finanzielle Verluste geht:

In einer Firma hatte eine Abteilung nur mit ganzzahligen Vielfachen von $1.000 zu tun. Daher ließ die Abteilung bei der Datenerfassung die letzten drei Nullen weg. Dies war dem ganzen Haus bekannt. Eines Tages sollte eine Transaktion von $500.000 getätigt werden. Die Person, die diese Summe überweisen sollte, hängte wieder drei Nullen an, in der Annahme, der Auftrag käme von jener oben beschriebenen Abteilung, was aber nicht der Fall war. Also wurde daraus eine Transaktion von $500.000.000. Ein Disaster konnte nur dadurch verhindert werden, daß die Firma, zu der der Betrag transferiert werden sollte, noch nie so hohe Abschlüsse getätigt hatte und vor Vollendung des Handels rückfragte [71].

Gefährlich werden können auch nicht beachtete Seiteneffekte: So ist zum Beispiel bekannt, daß sich ein Mann einer Mikrowellen-Arthritis-Therapie unterzog, wodurch sein Herzschrittmacher neu programmiert wurde, und er schließlich starb. Am Flughafen gibt es bereits schrittmacherschützende Untersuchungsgeräte; aber es ist auch der Fall bekannt, daß ein Herzschrittmacher durch die Diebstahlsicherung am Eingang von Kaufhäusern umprogrammiert wurde [70].

Dann gibt es auch die Möglichkeit, daß ein Problem auftritt, das man sich nicht erklären kann und die Lösung in der unzuverlässigen Software sucht, so wie beim Geisterzug von San Franzisco: Dort erkannte das Signalsystem der Metro einen Zug, der ein Gleis versperrte. In Wirklichkeit war aber nichts vorzufinden. Da man auch keinen Fehler im Kontrollsystem erkennen konnte, mußten alle Funktionen manuell ausgeführt werden. Dies führte zu erheblichen Verzögerungen, zumal der Vorfall während der morgendlichen Hauptverkehrszeit passierte. Nach zwei Stunden verschwand der Geisterzug genauso lautlos, wie er vorher erschienen war [68].

Auch Industrieroboter können für den Menschen gefährlich oder sogar tödlich sein. In Japan wollte ein Mechaniker eine Fehlfunktion eines Roboters reparieren. Er betrat dazu eine Sperrzone. Seltsamerweise kam der Arbeiter durch einen danebenstehenden Roboter zu Tode, der wohl eine noch nicht bemerkte Fehlfunktion hatte. Er heftete den Mann mit seiner ‚Kralle' an einer Maschine zur Fahrwerkherstellung fest [71].

Als abschließendes Beispiel sei das Leap-Year-Problem genannt, ein Problem, das alle vier Jahre auftritt – eben in jedem Schaltjahr: Zwei britische Banken, wir nennen sie einmal A und B, benutzten kompatible Geldautomaten. Anfang 1984 hatte Bank A die Software auf 366 Tage umgestellt, Bank B nicht. So kam es, daß Kunden von Bank A, die an Automaten von Bank B Geld abheben wollten, die Ausgabe verweigert bekamen. Auch umgekehrt konnte kein Bank-B-Kunde an Bank-A-Automaten Geld erhalten. Man gab dem Computer die Schuld, fand aber erst nach Tagen den eigentlichen Fehler. Der Metallstreifen in der Karte hatte keine kompatiblen Informationen mit den Automaten. Die Kunden von Bank B waren aber noch schlimmer dran. Ihre Karten wurden verschluckt, und damit verloren sie gleichzeitig die Möglichkeit, Schecks auszustellen, denn die Karten hatten Doppelfunktion.

Dieses Beispiel zeigt, daß eventuell spätere Abweichungen schon zur Entwicklungszeit mit einkalkuliert werden müssen. So bleibt zu hoffen, daß im Jahre 2000 nicht zuviele Abfragen sich nur auf die letzten beiden Ziffern beziehen; sonst kommt bei der Abfrage $00 > 99$ nicht das gewünschte Ergebnis heraus [70].

Natürlich könnte man auch den ‚Krieg aus Zufall' als Beispiel anführen. Dieses Thema wird jedoch gesondert in Kapitel 11 behandelt.

9.5 Normal Accidents

Charles Perrow, ein amerikanischer Soziologe, beschreibt in seinem Buch „Normal Accidents: Living with High Risk Technologies“ die Bedrohung durch riskante Technologien:

Darin sagt er, daß diese nicht gefährlicher seien als früher, die Kontrollsysteme hingegen wesentlich komplexer und fehleranfälliger. Verfechter dieser Technologien stellten Unfälle als sehr unwahrscheinlich dar. Ein besseres Management und ausgebildete Operateure bieten, im Gegensatz zu deren Meinung, nach Perrow keine Abhilfe.

Er geht sogar soweit, Katastrophen in Zukunft als alltäglich anzusehen. Aber die Technologien seien vom Menschen geschaffen, also seien sie auch von ihm modifizierbar oder könnten von ihm ganz abgeschafft werden. Die öffentliche Meinung über die Risiken sollte nicht durch wenige diktiert und durch angeblich *objektive Analysen* untermauert werden, sondern sich in einem demokratischen Prozeß herausbilden.

Perrow bietet ein Konzept an, das einerseits Möglichkeiten für die Einschränkung von Unfällen enthält und andererseits die Kosten für die Abschaffung von riskanten Technologien minimiert. Dabei unterscheidet er drei Kategorien:

1. Bei geringer Katastrophenmöglichkeit oder hohen Kosten für Alternativen ist lediglich eine Verbesserung angebracht.

2. Bei mäßiger Katastrophenmöglichkeit und mäßigen Kosten für Alternativen sollte eine strenge Regulierung vorgenommen werden.

3. Bei großer Katastrophenmöglichkeit und relativ niedrigen Kosten für Alternativen fordert er die Abschaffung und Ersetzung.

Zu dieser dritten Kategorie zählt Perrow die friedliche und militärische Nutzung der Kernenergie [70].

Softwarezuverlässigkeit ist, da es sich um eine Wahrscheinlichkeit handelt, immer gegeben. 100% werden hingegen niemals erreicht werden, da es immer nicht einkalkulierbare Zwischenfälle gibt. Dennoch muß man gerade als Informatiker bestrebt sein, durch Verwendung von Software-Engineering-Mitteln dieser Marke möglichst nahe zu kommen. Gleichzeitig sollten die Methoden zur Verbesserung der Qualität weiterentwickelt werden. In hochbrisanten Technologien muß man nach geeigneten Alternativen suchen, denn **normale** Unfälle dürfen nicht an der Tagesordnung sein.

Kapitel 10

Sicherheit durch Simulation

Hermann Müller

10.1 Einführung

Zum Begriff der Simulation existiert in der einschlägigen Literatur keine eindeutige Definition. Aus den vielen Versuchen, eine möglichst exakte Aussage zu finden, läßt sich etwa folgende Zusammenfassung herausziehen:

10.1.1 Definition

Simulation ist ein Verfahren zur Durchführung von Experimenten unter Benutzung mathematischer Modelle mit dem Ziel, durch eine wirklichkeitsäquivalente Nachahmung der Realität, Aussagen über das Verhalten des nachgebildeten Systems zu gewinnen.

Bei dieser Formulierung ist besonderes Augenmerk auf die Worte **MODELL** und **NACHAHMUNG** zu legen. Von der Güte der Nachbildung des zu simulierenden Systems im Modell hängt unmittelbar die Qualität der gewinnbaren Informationen ab. Gleichfalls bedeutend ist, daß eine Nachahmung, sei sie auch noch so perfekt, immer eine Nachahmung bleibt und als solche auch verstanden werden muß.

10.1.2 Grundsätzliche Bemerkungen

Wichtigste Aussage, die aus den obigen Ausführungen bereits klar geworden sein dürfte, ist, daß es eine Simulation ohne ein Modell nicht geben kann. Man erkennt weiter, daß es sich bei der Simulation nicht um eine feststehende Methode, wie z.B. bei der Simplex-Methode der linearen Optimierung handelt, sondern um eine Methodik der Vorgehensweise, die je nach der Problemstellung sehr unterschiedlich ausfallen kann [74]. Neben dieser Tatsache muß ebenfalls herausgestellt werden, daß Simulation als Ergebnisse in den seltensten Fällen ein Optimum liefert. In der Regel wird es sich dabei um einen geplanten Zufall handeln. Simulation ist also auch kein Lösungs- oder Optimierungsverfahren im Sinne von analytischen Methoden, sondern ist im Anwendungsfall lediglich neben einem bestimmten (meist heuristischen) Verfahren Bestandteil eines Lösungsweges [60].

Der Zwang, ein Modell zu entwickeln, das ein System möglichst genau wiedergibt, setzt eine eingehende Analyse des zu modellierenden Systems voraus. Simulation liefert, wenn das Modell ausreichend genau ist, Daten, die ein genaues Studium des Systemverhaltens ermöglichen, aber, wie schon angedeutet, nicht notwendig zu einer Systemoptimierung führen. Dadurch, daß das Modell auf realen Gegebenheiten beruht, ist auch klar, daß sich nur Bekanntes simulieren läßt. Das Ergebnis angewandter Simulation liefert daher grundsätzlich keine neuen Erkenntnisse. Simulation kann aber helfen, Hindernisse zu überwinden, die es erschweren oder unmöglich machen, daß man in der Realität zu neuen Einsichten gelangt [60].

10.1.3 Welche Informationen können geliefert werden?

Es ist schon angeklungen, daß Simulation zum Studium des Verhaltens des modellierten Systems eingesetzt werden kann. Dabei lassen sich besonders über das zukünftige Verhalten wichtige Daten erheben. Dadurch, daß die Modellbildung ein eingehendes Studium des Systems erfordert, lassen sich indirekt Strukturinformationen gewinnen.

Die wichtigste Simulationsform ist wohl die **Faktoranalyse**, bei der pro Simulationslauf einzelne Parameter verändert werden, um dadurch die Einflußmöglichkeiten dieser Änderungen auf das Verhalten des abgebildeten Systems studieren zu können. Durch die Beobachtung läßt sich dann auf dem Weg der „optimalen Steuerung“ auch eine heuristische Optimierung dieses Verhaltens in bezug auf vorgegebene Zielkriterien erreichen.

10.1.4 Anwendungsbereiche

Simulation wird heute in den unterschiedlichsten Bereichen mehr oder weniger sinnvoll eingesetzt. In der folgenden Aufzählung ist eine kurze, bei weitem nicht vollständige Übersicht gegeben, um eine bessere Einordnung des noch Folgenden durchführen zu können.

- Beurteilung von Planungsvarianten (Anlagenbau, Lagerhaltung)
- Systemanalyse (Astronomie, Meteorologie)
- Schulungsmittel (Management-Spiele)
- Energieanlagenbau, Kerntechnik, Fusionstechnik [76]
- Physik (Atomphysik, Plasmaphysik, Gaskinetik, Optik) [54]
- Biologie (Zellforschung, Genetik)
- Chemie (Reaktionstechnik)
- Mathematik (komplexe Differential- und Integralgleichungen)
- Operationsforschung (Reihenfolgeproblem, Problem der Ablaufplanung, Bedienungsmodelle)
- Luftfahrt-, Raumfahrt-, Automobilindustrie [86]
- Medizin
- Gesellschaftsforschung
- Strategische Planspiele [80, 49]
- Raumplanung, Städtebau

10.2 Verfahren und Werkzeuge

10.2.1 Klassifizierung der Simulationsverfahren

Eine klare Klassifizierung der verschiedenen Simulationsverfahren fällt nicht leicht, da sie nach den unterschiedlichsten Gesichtspunkten erfolgen kann. Es lassen sich aber doch drei wesentliche Klassifizierungsmerkmale herausheben [74]:

1. **Art des Experimentierens**

   Hier kann man die gezielte oder geplante Simulation der Monte-Carlo- oder zufallsbedingten Simulation gegenüberstellen. Im erstgenannten Fall folgen die den Experimenten zugrunde liegenden Bedingungen einem exakt vorbestimmten Plan, während sie im zweiten Fall ganz oder zumindest teilweise zufällig ausgewählt werden.

2. **Art der angestrebten Lösung**

   Das Verhalten von Systemen kann durch statische oder dynamische Lösungen charakterisiert werden. Unter einer statischen Lösung ist ein mathematischer Zusammenhang zu verstehen, der objektiv gültig ist und über Experimente aufgedeckt wird. Bei einer dynamischen Lösung will man das Verhalten des Systems in Abhängigkeit von der Zeit kennenlernen.

3. **Art der Zeitkopplung**

   Diese Einteilung bezieht sich im wesentlichen auf Simulation mit dynamischer Lösung. So kann man solche mit statischer Lösung und einen Teil der Simulationen mit dynamischer Lösung in die Kategorie zeitunabhängige Simulation einordnen und sie damit der Simulation in diskreten Zeitpunkten gegenüberstellen. Dieses ist z.B. bei Prozeßsteuerungen der Fall.

10.2.2 Klassifizierung der Modellbildung

Bei der Frage der Modellformulierung ist es von entscheidendem Interesse zu wissen, welcher Natur das zu modellierende System ist. Man kann dabei zwischen **kontinuierlichen** [88] und **diskreten** [87] Systemen unterscheiden. Die Grenze *kontinuierlich-diskret* ist dabei durchaus fließend und vom Beobachterstandpunkt abhängig [62]. So ist der Verkehr für einen Betrachter, der neben einer Straßenkreuzung steht, eine ständige Folge einzelner Fahrzeuge. Will man die Verkehrsabläufe auf der Kreuzung nachbilden, so wird hierzu ein diskretes Modell geeignet sein. Dagegen beobachtet ein Verkehrspolizist aus einem Hubschrauber auf der Autobahn unter sich einen Verkehrsstrom, auf den sich Engpässe wie Flaschenhälse auswirken. Hier ist die Nachbildung des Verkehrsflusses als kontinuierlicher Strom durchaus adäquat.

Daneben existieren auch Systeme, die sich nicht als eindeutig kontinuierlich, aber auch nicht als diskret einstufen lassen, sogenannte **hybride** Systeme. Jedoch ist eine solche Klassifizierung von rein theoretischem Interesse und führt in der Praxis nicht zur Bildung von Hybrid-Modellen [6].

Sowohl bei einem kontinuierlichen als auch bei einem diskreten System unterscheidet man weiter *deterministische* und *stochastische* Systeme (s.o.). Im wesentlichen lassen sich somit 4 Modellklassen unterscheiden:

- determiniert-diskret
- determiniert-kontinuierlich
- stochastisch-diskret
- stochastisch-kontinuierlich

10.2.3 Simulationswerkzeuge

Zur Beschreibung kontinuierlicher Simulationsprobleme haben sich zahlreiche, spezielle, problemorientierte Programmiersprachen entwickelt (ACSL oder CSSL-IV). Im Zuge dieser Entwicklung wurden vom Prinzip her parallel arbeitende *Analogrechner* [88] durch immer leistungsfähigere, aber seriell arbeitende *Digitalrechner* soweit zurückgedrängt, daß deren heutige Rolle fast ausschließlich Echtzeit-Simulationen umfaßt.

Auf dem Gebiet der diskreten Simulation erfolgte die Bereitstellung geeigneter Werkzeuge ähnlich zur kontinuierlichen Simulation, doch zeitlich später. Ohne auf Wechselwirkungen einzugehen, ist auf jeden Fall festzustellen, daß die Verfügbarkeit digitaler Rechner stetig steigender Leistung das Gebiet der numerischen Mathematik voll zur Entfaltung gebracht und nachhaltig zur Entwicklung der digitalen Simulationstechnik beigetragen hat.

Die heute im Einsatz befindlichen Superrechner, die besonders im Zusammenhang mit Simulationen komplexer Modelle an Bedeutung gewonnen haben, erreichen relative Geschwindigkeiten im Vergleich zum Modell IBM 700 (1954) mit einem Faktor bis etwa 130.000. Zu nennen sind hier unter anderem die Rechner der CRAY-Serie, aber auch Rechner von Hitachi, NEC und CYBER [1].

10.3 Ablauf einer Simulation

Grundsätzlich läßt sich die Durchführung einer Simulation von Anbeginn in der unterschiedlichsten Weise strukturell erfassen. Für die folgenden Darstellungen seien 5 Phasen unterschieden:

10.3.1 Phase I

In dieser Phase beginnt alles damit, daß das *Problem*, das simuliert werden soll, *formuliert* und die zu erreichenden *Ziele spezifiziert* werden. Von diesem Arbeitsschritt läßt sich die *Frage, ob Simulation eingesetzt werden soll*, nicht trennen. Eventuell wird nämlich bereits hier erkannt, daß das Modell zu aufwendig oder gar unmöglich in der Erstellung ist. Hier entscheidet sich also, ob es überhaupt sinnvoll ist, Simulation einzusetzen oder ob man nicht vielleicht die angegebenen Ziele auf anderem Wege leichter bzw. billiger erreichen kann [62].

Gründe, die für eine Simulation sprechen können, wären dann gegeben, wenn das Objektexperiment zu teuer, zu gefährlich, zu langwierig oder aus anderen Gründen unpraktikabel ist. Möglicherweise ist aber auch der Ausgang des realen Experiments zu ungewiß, mögliche Folgeerscheinungen des Experiments sind in der Realität nicht mehr behebbar, oder aber das reale Experiment ist schlicht unmöglich.

10.3.2 Phase II

Anschließend an die eben besprochenen Arbeiten werden nun wesentliche *Voraussetzungen* zu *schaffen* sein, nachdem die Entscheidung für eine Simulation gefallen ist. Zu diesen Voraussetzungen gehören unter anderem die Überprüfung, ob ein geeigneter Computer zur Verfügung steht und ob sich die erforderlichen Daten, deren Natur sich während der ersten Phase herauskristallisiert hat, beschaffen lassen.

Wesentlich ist, daß das eingesetzte Projektteam die erforderlichen Kenntnisse und Fertigkeiten besitzt. Dazu gehören intensive Kenntnisse und Erfahrungen in dem Fachgebiet, aus dem das Simulationsproblem stammt, aber auch Kenntnisse und Erfahrungen auf dem Gebiet des Operations Research zur Modellformulierung. Bei stochastischen Simulationen sind zusätzliche Kenntnisse der Wahrscheinlichkeitstheorie und der mathematischen Statistik unerläßlich. Das Vorhandensein von guten Programmierkenntnissen (evtl. Beherrschung einiger Programmier- und Simulationssprachen) ist von Vorteil, aber nicht unerläßlich.

10.3.3 Phase III

Nach Schaffung der Grundvoraussetzungen für einen Simulationslauf kommt es jetzt darauf an, notwendige *Daten* in ausreichendem Umfang zu *sammeln* und bereitzustellen. Parallel zu diesem Arbeitsprozeß sollte die *Modellformulierung* durchgeführt werden. Wahrscheinlich ist, daß sich Wechselwirkungen zwischen Modellbildung und Datenfindung ergeben und die Nachbildung des realen Systems positiv beeinflussen. Bei der Modellierung des nachzuahmenden Systems ist insbesondere von Interesse, ob eine diskrete oder kontinuierliche Modellbildung durchzuführen ist (s.o.). Zur Modellbildung gehört ebenfalls die Erstellung von leistungsfähigen Computerprogrammen und deren Überprüfung.

10.3.4 Phase IV

In dieser wichtigsten aller 5 Phasen wird es darum gehen, das in der vorhergehenden Phase III geschaffene Modell zu *validieren*. Es stellt sich demnach eine Genauigkeitsfrage bezüglich der Qualität, mit der die Nachbildung des realen Systems erfolgte. Daraus wird schon ersichtlich, daß es sich bei der Validierung um einen zentralen Punkt der Simulation handelt, der mit äußerster Sorgfalt durchzuführen ist. Von dieser Phase hängt es ab, ob das Modell verworfen oder modifiziert werden muß. In den seltensten Fällen wird eine Validierungsphase ohne Schwierigkeiten durchgeführt werden können, da entweder die geschaffenen Systemabbildungen für eine Komplettvalidierung zu komplex sind oder aber die zur Validierung herangezogenen Vergangenheitsdaten mit zu großen Unsicherheitsfaktoren behaftet sind.

Es sei noch einmal ausdrücklich betont, daß die Validierung nicht den Test der in Phase III erstellten Computerprogramme beinhaltet.

Grundsätzlich bestehen 2 Möglichkeiten der Validierung:

a) Vergleich von Ergebnissen mit Vergangenheits- und aktuellen Daten aus dem nachgebildeten System.

b) Vergleich von Simulationsergebnissen mit analytischen Lösungen beim vereinfachten Modell.

Bei a) ergeben sich besonders bei einer stochastischen Simulation Schwierigkeiten, da ermittelt werden muß, ob die realen und simulierten Daten der gleichen statistischen Grundgesamtheit mit genügend großer Sicherheit entstammen können. Hier setzt z.B. die Varianzanalyse an [2].

Bei b) geht man davon aus, daß das Modell eine Anzahl von Spezialfällen enthält, in denen die Struktur des Problems stark vereinfacht ist. Für solche Spezialfälle existiert häufig eine analytisch gefundene Lösung, deren Übereinstimmung mit dem nachgebildeten System als genügend sicher gelten kann. Häufig ist dann nach Validierung der Spezialfälle der Schluß berechtigt, daß das Modell allgemein das reale System zutreffend abbildet. Die Betonung muß hierbei aber auf dem Wort „**häufig**" liegen.

Bei großen Modellen komplexer Systeme ist eine Komplettvalidierung nahezu unmöglich. Hier wird man das Modell zergliedern und schrittweise vorgehen [62]:

1. Kontrolle der im Modell verwendeten Relationen durch fundierte wissenschaftliche Untersuchungen.
2. Validierung von Modellsegmenten nach einem der angegebenen Verfahren.
3. Validierung des Gesamtmodells.

10.3.5 Phase V

Neben der *Planung der Simulationsläufe* wird in dieser Phase ebenfalls eine *Auswertung der Ergebnisse* und eine *Dokumentation des Modells* und der gewählten Vorgehensweise durchgeführt. Planung meint in diesem Zusammenhang nicht eine Neuformulierung des Problems, sondern ein sorgfältiges Abwägen, welche Experimente erforderlich sind, um gezielt die in Phase I formulierten Fragen zu beantworten. Der Hintergedanke dabei ist die Kostenreduktion, die durch verringerte Rechenzeit entsteht. Weiter wird man zur Klärung von Abhängigkeiten im Modell bei Strukturanalysen und Steuerungsproblemen eine Unterteilung in „Faktoren", die vorgegeben werden, und „Reaktionen", die durch das Experiment ermittelt werden, vornehmen [62].

Bei stochastischen Simulationen wird man sich zudem überlegen müssen, welche Genauigkeit noch erforderlich ist bzw. welche Fehler noch durch nachbehandelnde statistische Verfahren kompensiert werden können (*Gesetz der Großen Zahl*).

Bei der Auswertung ist vor allen Dingen eine problem- oder sachbezogene Aufbereitung der Ergebnisse und eventuelle Fehlerkorrekturen durchzuführen. Wichtig ist hierbei ebenfalls, um den Nutzen der Simulation auch anderen Personen zugänglich zu machen, daß die erhaltenen Informationen des Modellexperimentes verständlich und interpretierbar gemacht werden, damit auch solche Personenkreise, die sich in dem Problemgebiet nicht auskennen, daraus Nutzen ziehen können.

Für die zukünftige Verwendung und Weiterentwicklung des erstellten Modells ist, um effizient weiterarbeiten zu können, unbedingt eine Dokumentation der Modellstruktur, aber auch der Simulationsläufe notwendig. Diese Forderung nach Dokumentation ist sicherlich eine der trivialsten im gesamten Projektablauf, mindestens ebenso sicher jedoch auch die in der Praxis am meisten mißachtete.

10.4 Modelle

Wie weiter oben schon diskutiert wurde, wird Simulation immer zur Umgehung eines in der Realität zu schwierigen oder zu aufwendigen oder zu unsicheren Experimentes eingesetzt. Bei einem solchen Realexperiment würde der Experimentator durch eine geeignete Versuchsanordnung auf das Objekt seiner Wahl einzuwirken versuchen. Über die Reaktionen des Objektes, die der Experimentator beobachtet und analysiert, versucht er anschließend mit Rückschlüssen sein Wissen über das System zu erweitern.

Im Modellexperiment hingegen findet als allererste Maßnahme eine Abbildung des zu analysierenden Systems in ein Modell statt. Das Einwirken des Experimentators richtet sich in der Folge nicht auf das Objekt selbst, sondern auf das dieses ersetzende Modell. Somit werden auch nicht die Reaktionen des Realobjektes, sondern des Modelles aufgenommen und analysiert. Diese Reaktionen werden allerdings jetzt dazu benutzt, um ebenfalls wieder Rückschlüsse auf das reale System zu ziehen. Aus diesen Überlegungen sieht man schon, daß eine Modellreaktion der Reaktion des Objektes möglichst genau entsprechen muß, um nicht die Gültigkeit der gezogenen Rückschlüsse in Frage zu stellen.

10.4.1 Modellbildung

Man unterscheidet die verschiedensten Modelle. Das wichtigste Kriterium ist die Unterscheidung in **materiell** und **abstrakt**. Unter materiellen Modellen versteht man grundsätzlich solche, die **künstlich** (Miniaturmodell eines Flugzeuges) geschaffen werden oder die **natürlich** vorhanden sind (Maus im Irrgarten). Für diese Art der Modelle wird man als mögliche Untersuchungsmethode die Analogsimulation bevorzugen.

Bei abstrakten Modellen unterscheidet man die weniger bedeutsamen **bildlich-verbalen** Modelle von den bedeutungsvolleren **mathematischen** Modellen. Die bildlich-verbalen Modelle, die durch eine verbale Diskussion untersucht werden können, finden besonders in der Volkswirtschaftslehre ihre Anwendung. Die interessantesten und die Modelle, auf die digitale Simulation angewendet wird, sind die abstrakten mathematischen Modelle, bei denen man *analytische* Verfahren oder die *digitale Simulation* zur Lösungsfindung einsetzt.

10.4.2 Zeitbindung

10.4.2.1 Zeitschrittbildung

- konstant

  Im Laufe der Simulation werden immer alle Elemente nach einem fixen Zeitintervall betrachtet und jene, die für eine Tätigkeit bereit sind, bearbeitet. Diese Methode wird – allerdings mit gewissen Abweichungen bei Grenzfällen (sogenannte Anpassung der Schrittweite) – vor allem bei Simulationen kontinuierlicher Systeme (Differentialgleichungssysteme) benutzt. Sie ist für die Simulation wirklich diskreter Ereignisse selten in Gebrauch, da sie viele funktionslose Schritte bringt.

- variabel

  Im Laufe der Simulation führt jedes Element den Begriff „nächste aktive Zeit“ (= Weckzeit) mit. Das Simulationssystem wird damit in die Lage versetzt, Zeitabschnitte mit wenig Aktivität in großen Sprüngen zu überspringen, während beliebige Feinheit dort möglich ist, wo dies vom praktischen Modell her notwendig ist. Der dadurch erkaufte Nachteil, daß Zeitreihen nicht überall gleich genau bearbeitet sind, kann dabei als durchaus tragbarer Verlust angesehen werden [6].

10.4.2.2 Zeitorganisation

Bei den variablen Zeitschritten ist für jedes Element die nächste aktive Zeit zu betrachten. Das ist eine Eigenschaft (Wert einer Variablen!) des Elements. Um diese Eigenschaft effizient verwalten zu können, liegt der Aufbau einer Reihenfolge-Liste gemäß der Element-Weckzeiten nahe. Damit ergeben sich zwangsläufig auch neue Aufgaben, die in der Wartung und Verwaltung dieser Liste liegen.

Die Zugehörigkeit zur Liste ist eine zentrale und zugleich einmalige Eigenschaft jedes Elementes. Daher ist es eine typische (sogar *die* typische) Eigenschaft von Simulationssprachen für diskrete Ereignisse, daß sie die Elementmenge „Reihenfolge-Liste“ automatisch aufbauen, nachführen und oft durch besondere Anweisungen sehr einfach manipulierbar machen.

10.4.3 Fehlerkritiken

Jede Modellbildung im hier besprochenen Sinn wird auf Grund ihrer Leistung beurteilt, d.h. auf Grund ihrer Präzision, mit der eine Wirklichkeit dargestellt wird. Abweichungen vom Urbild sind Fehler, die auf ganz verschiedenen Ebenen auftreten können.

- **Systemfehler**

  Das zu modellierende System wurde falsch erfaßt, falsch in Elemente gegliedert, die Beziehungen der Elemente untereinander und zur Umwelt falsch gesehen.

- **Modellfehler**

  Die Übertragung auf das Modell entspricht in wichtigen Teilen nicht dem Original; die Elemente des Modells haben falsche, eventuell ungenügende Eigenschaften; die Darstellung der Zufallsabhängigkeit ist nicht angemessen.

- **Datenfehler**

  Die verwendeten Daten sind falsch, ungenau oder dem Modell nicht angepaßt (d.h. außerhalb des für das Modell zulässigen Bereiches).

- **Rechenfehler**

  Das Modell ist für die numerische Rechnung schlecht geeignet, hat Unstabilitäten oder eine schlechte Konvergenz (insbesondere bei stochastischen Modellen); das Modell berücksichtigt innere Beziehungen der Daten nicht (Autokorrelation, etc.)

- **Interpretationsfehler**

  Die Ergebnisse des Modells werden falsch interpretiert, für falsche Zwecke angewandt oder mit einer nicht vorhandenen Genauigkeit verstanden.

Generell muß wohl festgestellt werden, daß sich Fehler nicht absolut sicher vermeiden lassen. Augenmerk muß darauf gelegt werden, daß durch eine möglichst sorgfältige Planung und Realisierung das Fehlerpotential so weit wie möglich reduziert wird. Es läßt sich außerdem folgendes feststellen:

Die Fehler aller Stufen, die durchaus vorhanden sein dürfen, müssen aufeinander abgestimmt sein und erkannt werden. Mehraufwand zur Fehlerreduktion ist nur dann gerechtfertigt, wenn der Gesamtfehler einer Simulation dadurch entsprechend gesenkt werden kann [6].

10.4.4 Standardmodelle

Da die Simulation praktisch in allen Bereichen eingesetzt wird, die die Formulierung quantitativer Modelle erlauben, ist das Anwendungsgebiet sehr weit und vielfältig. So kann hier nur eine Auswahl von Anwendungen dargestellt werden. Natürlich muß eine solche Auswahl bei der schon angesprochenen Fülle willkürlich sein.

Für viele der aufgelisteten Anwendungsbereiche existieren hierbei sogenannte Standardmodelle, die, einmal entwickelt, sich leicht in anderen Situationen, evtl. modifiziert und erweitert, einsetzen lassen [62].

1. Modelle zur Lösung von Management-Aufgaben

   - Warteschlangenmodelle
   - Investitions- und Finanzierungsmodelle
   - Modelle zur Ablaufplanung
   - Marketingmodelle
   - Instandhaltung und Wartung
   - Forschnungs- und Entwicklungsmodelle

- Lagerhaltungsmodelle

2. Ökonomische Modelle
3. Verhaltensmodelle
4. Modelle von Computer-Systemen
5. Verkehrsmodelle
6. Modelle von Städten und Regionen
7. Planspiele
8. Sonstige Modelle
    - Informationsfluß in einem Stahlwerk [86]
    - Zuckerraffinerie
    - Kommunikationssystem der Polizei
    - Chemische Fabrik
    - Krankenhaus
    - Lebensversicherung
    - kommunales Gesundheitswesen

10.5 Zufall und Simulation

10.5.1 Zufallszahlen

Standardzufallszahlen sollen das bei allen Simulationen verwendete Rohmaterial bilden, aus dem alle weiteren stochastischen Größen gewonnen werden. Aus diesem Grund sollten (in Rechenzentren) generelle Verfahren (*Basisgeneratoren*) zur Produktion solchen Zufallszahlen bereitgestellt werden.

Man wählt dazu als Standardzufallszahlen *stochastisch unabhängige*, über dem Intervall [0,1] *gleichverteilte* Zufallsgrößen.

Bei Simulationen werden in der Regel sehr viele Zufallszahlen benötigt, in einfachen Fällen schon einige zehntausend. Deshalb ist es wichtig, einfache und rasch arbeitende Zufallszahlengeneratoren zur Verfügung zu haben.

Da die stochastische bzw. Monte-Carlo-Simulation meist mit Hilfe von Digitalrechnern durchgeführt wird, ist zu beachten, daß wegen der endlichen Länge der Register der Rechenanlagen immer nur eine diskrete Approximation der Gleichverteilung über [0,1] erreicht werden kann [20].

10.5.1.1 Zufallszahlengeneratoren

- **extern**

  Wenn man Zufallszahlen benötigt, liegt der Gedanke nahe, sie dort zu gewinnen, wo sie in der Natur oder in technischen Geräten zwangsläufig anfallen (z.B. beim Zerfall radioaktiver Substanzen, bei Rauschvorgängen in Röhren, etc.), d.h. mit einem speziellen Zusatz zur Rechenanlage die Resultate eines *physikalischen Zufallsprozesses* in Zahlen zu transformieren und nach jedem Rechenschritt eine neue Zahl in ein Register zu speichern. Tatsächlich sind Ende der 30er Jahre nach diesem Prinzip umfangreiche Tafeln von Zufallszahlen hergestellt worden, und in neuester Zeit werden solche Zusatzgeräte kommerziell produziert.

  Der Vorteil dieser Methode ist, daß man „echte“ (nicht vorhersagbare) Zufallszahlen erhält. Etliche Nachteile der physikalischen Zufallsgeneratoren ergeben sich daraus, daß zum einen die Anschaffung und

Wartung eines solchen Zusatzgerätes Kosten verursachen, zum anderen regelmäßige Stabilitätsuntersuchungen durchzuführen und manchmal zweifelhafte Verteilungsannahmen und -approximationen zu machen sind. Bei Parameterveränderungen innerhalb einer Simulationsstudie erweist es sich ferner als Nachteil, daß es ohne besondere Vorkehrungen nicht möglich ist, eine Rechnung ein zweites Mal mit denselben Daten (einschließlich der Zufallszahlen!) durchzuführen. Überdies sind physikalische Zufallszahlengeneratoren für die Anwendungen oft noch zu langsam, da sie nur bis zu mehreren tausend Zahlen pro Sekunde liefern können.

- **intern**

  Wegen der Nachteile der externen physikalischen Generatoren hat man sich schon früh Gedanken gemacht, ob man nicht arithmetische Algorithmen dazu benutzen kann, vom Rechner selbst „Zufallszahlen“ erzeugen zu lassen. Natürlich verliert man bei einem solchen Vorgehen die wichtige Eigenschaft der „Zufälligkeit“ der erhaltenen Zahlen, da diese streng deterministisch bestimmt werden. Man bezeichnet solche Zufallszahlen demnach auch als **Pseudozufallszahlen**.

  Von einem guten Generator für Pseudozufallszahlen wird man verlangen, daß sich die erzeugten Zahlen in einem präzisierten Sinn „wie echte“ Zufallszahlen verhalten; dann wird man den Verlust der Zufälligkeit in Kauf nehmen, da auf diese Art erreicht wird, daß man kein Zusatzgerät und keine Zusatzuntersuchungen benötigt und bei Wiederholungen der Rechnungen die verwendeten Pseudozufallszahlen reproduzieren kann.

  Die wichtigsten Pseudozufallszahlengeneratoren für Digitalrechner sind die **Rekurrenzgeneratoren**, bei denen die Pseudozufallszahlen mit Hilfe einer Rekurrenzrelation vom Typ

  $$z_{i+1} = f(z_{i-j}, ..., z_i)$$

  erzeugt werden. Unter diesen Generatoren sind wegen ihrer leichten und schnellen Realisierbarkeit besonders die **linearen Kongruenzgeneratoren** von Interesse, bei denen

  $$z_{i+1} = y_{i+1}/m$$
  $$y_{i+1} = a_0 y_i + ... + a_j y_{i-j} + r \bmod m$$

  erzeugt wird. Generatoren dieser Art gehen zurück auf D. H. Lehmer (1951)

Jeder auf einer Rechenanlage benutzte Rekurrenzgenerator ist periodisch. Bei jedem solchen Generator folgt also auf eine aperiodische Anfangsfolge eine sich ständig wiederholende Periode. Als brauchbare Pseudozufallszahlen kommen daher nur die Zahlen der Anfangsfolge und der ersten Periode in Frage. Beispielhaft seien hier zwei Generatoren angeführt [35]:

- RANDU – Periodenlänge $2^{29} \approx 5,37 \cdot 10^8$
- GGUBS – Periodenlänge $2^{31} - 1 \approx 2,15 \cdot 10^9$

10.5.2 Monte-Carlo-Simulation

Unter der Bezeichnung „Monte-Carlo-Methode“ versteht man eine Klasse von recht allgemein verwendbaren Verfahren zur Lösung unterschiedlichster Probleme. Nicht immer handelt es sich dabei um Simulation im eigentlichen Sinn, sondern es werden lediglich der stochastischen Simulation verwandte Techniken als Ersatz für analytische Lösungsverfahren eingesetzt, ohne daß die behandelten Objekte notwendigerweise Modelle dynamischer Systeme sind. Es ist für den Einsatz der Monte-Carlo-Methode nicht einmal erforderlich, daß das vorliegende Objekt stochastischer Natur ist. Vielmehr können die Methoden durchaus zur Lösung determinierter Probleme, etwa der Lösung von Gleichungen oder bestimmter Integrale, dienen. Trotzdem findet man heute oft auch die Bezeichnung Monte-Carlo-Simulation.

Die Durchführung der Monte-Carlo-Simulation beinhaltet die Generierung von Stichproben, aus deren Eigenschaften (Wahrscheinlichkeitsverteilung, Mittelwert, Varianz, etc.) auf die Grundgesamtheit geschlossen wird. Bei der Simulation handelt es sich definitionsgemäß um Abläufe in dynamischen Systemen, bei der Monte-Carlo-Methode um den Einsatz der stochastischen Methoden auf beliebige Bereiche.

Ein Anwendungsgebiet der Monte-Carlo-Methode, das gerade für die Simulation von Bedeutung ist, liegt darin, Funktionen von zufälligen Variablen zu bestimmen (sogenannte Zufallsfunktionen). Eine Zufallsfunktion unterscheidet sich von einer gewöhnlichen Funktion einer oder mehrerer Variablen dadurch, daß die Argumente Zufallsvariable sind und dadurch auch die abhängige Variable der Funktion. Nur in einfachen Fällen läßt sich die Verteilung der abhängigen Variablen y exakt angeben, wenn die der unabhängigen Variablen x vorgegeben ist. Schon, wenn x eine empirische Verteilung besitzt, müssen zur Bestimmung der Verteilung von y andere Methoden herangezogen werden. Die Lösung dieses Problems führt bei der Monte-Carlo-Methode über Stichproben der Variablen x und y. Nach dem Hauptsatz der Statistik wird die gesuchte Verteilung von y beliebig genau angenähert, wenn die Stichprobe nur genügend groß ist.

Beispiele für eine Anwendung einer solchen **Sampling-Technik** lassen sich viele finden. Genannt seien hier nur die Vereinigung von Straßenzügen, die Kundenverteilung auf Supermarktkassen und die Kfz-Verteilung an Tankstellen.

Während bei der Sampling-Technik dem Verfahren noch eine stochastische Fragestellung zugrundeliegt, ist anhand der Berechnung eines Flächeninhaltes leicht zu demonstrieren, wie die Monte-Carlo-Methode auch im Fall nicht stochastischer Probleme eingesetzt werden kann.

Zu berechnen sei der Flächeninhalt eines Kreises mit dem Radius $r = 0,5$. Dazu legt man um den Kreis eine Fläche mit bekanntem Inhalt, z.B. ein Quadrat mit der Kantenlänge 1. Nun wählt man zufällige Punkte aus, die gleichmäßig im Einheitsquadrat gestreut sind. Dazu erzeugt man Punktepaare, deren Koordinaten Zufallszahlen im Intervall [0,1] sind. Die von der Gesamtpunktzahl n (als Stichprobe) im Kreis liegenden Punkte n_k geben die Größe des Kreisinhaltes F_k im Verhältnis zum Quadratinhalt Q_k an:

$$n_k/n = F_k/F_q \Longleftrightarrow F_k = n_k \cdot F_q/n$$

Natürlich gilt auch diese Beziehung nur für genügend große Stichproben. Die Genauigkeit der Lösung kann bei allen Monte-Carlo-Techniken nur in dem Maße zunehmen, wie Verteilungen und Parameter (Mittelwert, Varianz) der Stichproben gegen die exakten Werte der Grundgesamtheit gehen. Es gelten also stets Fehlerabschätzungen mit ihren zu diskutierenden Konsequenzen für die Konvergenz der Lösungen [62].

Da auch auf schnellen Rechenanlagen dem Umfang der Stichproben Grenzen gesetzt sind, wurden bei den Monte-Carlo-Methoden schon früh andere Wege zur Genauigkeitssteigerung ohne unerträgliche Erhöhung des Stichprobenumfanges gesucht. Die dazu gefundenen Techniken sind allgemein auch unter dem Schlagwort *Variance- and Sample-Size-Reducing-Techniques* (Techniken zur Reduzierung der Standardabweichung und des Stichprobenumfangs) bekannt. Dazu zählt man unter anderem [60]:

- Importance Sampling
- Russian Roulette
- Splitting
- Use of Expected Values
- Correlation
- Regression
- Systematic Sampling
- Stratified Sampling (Quota Sampling)
- Correlated Sampling

Für eine nähere Diskussion der angeführten Verfahren sei auf die Literatur verwiesen [56, 55, 40].

10.6 Simulationssprachen

10.6.1 Charakteristika

- Geeignete Erzeugung von Ereignissen und deren Beschreibung
- Flexible und einfache aufdatierbare Zeitablaufsteuerung, welche für eine exakte Bestimmung der Ereigniszeitpunkte und für eine zeitgerechte Ausführung der Ereignisse sorgt
- Behandlung von gleichzeitig eintretenden Ereignissen nach den im Modell geltenden Regeln
- Entsprechend der Problemstellung ereignisorientierte, tätigkeitsorientierte oder prozeßorientierte Realisierung des Modells auf dem Computer
- Flexible Beschreibung von Elementen und deren Zusammenfassung (Prozesse) sowie deren Verknüpfung und Einordnung in Mengen (Sets)
- Dynamische Erzeugung und Zerstörung von Elementen und Prozessen
- Verfahren für eine gute Speicherausnutzung
- Erzeugung von Pseudozufallszahlen
- Hilfsmittel zur Aufbereitung von Zeitreihen und zur Erstellung von Statistiken [6]

Zu einer Simulationssprache gehören allgemein:

1. die eigentliche Sprache
2. der Compiler
3. Steuer- und Hilfsprogramme

Dabei bedeutet Compiler nicht unbedingt, daß eine direkte Übersetzung in die Maschinensprache durchgeführt wird. Vielmehr ist es häufig so, daß bei Simulationssprachen, die in eine Basissprache eingebettet sind, zuerst eine Übersetzung in diese Sprache erfolgt (SIMSCRIPT, CSL, SIMULA, SOL, SIMON, SIM, etc.).

Generell haben Simulationssprachen den Vorteil, daß sie nur geringe Kenntnisse vom Computer und seiner Programmierung benötigen und der Zeitaufwand für die Erstellung und Änderung der Programme durch die Verwendung höherer Sprachstrukturen reduziert ist. Es ergeben sich generell sehr kurze und dadurch übersichtliche Programme. Außerdem sind die Fehlermöglichkeiten stark eingeschränkt, da die Programmierung vom Problembearbeiter mitübernommen werden kann.

10.6.2 Nachteile von Simulationssprachen

Die begrenzte Einsatzbreite von Simulationssprachen erfordert problemorientiert die Auswahl einer geeigneten Sprache. Das setzt aber wieder gute Kenntnisse mehrerer Sprachen voraus, wodurch ein Mehraufwand entsteht. Weiter sind eingehende Kenntnisse über die Modellphilosophie, die Modellsteuerung, sowie die Ergebnisanalyse der einzelnen Sprachen unbedingt erforderlich, um die volle Kraft der jeweiligen Sprache effektiv nutzen zu können. Außerdem seien noch die Mehrkosten, die durch die Anschaffung zusätzlicher Soft- und Hardware entstehen, angeführt.

Machen Einschränkungen den Einsatz einer Simulationssprache unmöglich, bietet sich als Alternative eine direkte Programmierung in einer höheren Programmiersprache an.

10.6.3 Überblick

So vielfältig und unterschiedlich Simulationsmodelle gestaltet sind, so groß ist die Zahl der bisher entwickelten Simulationssprachen. Schon bei oberflächlicher Durchsicht der Literatur findet man schnell über 20 verschiedene Namen. Diese Vielzahl macht eine Klassifizierung der Sprachen erforderlich, die unter 3 Gesichtspunkten möglich ist:

1. **nach funktionalen Merkmalen**

   Grundsätzlich ist zwischen Simulationssprachen für kontinuierliche und diskrete Systeme zu unterscheiden. Die *Sprachen für kontinuierliche Systeme* lassen sich weiter nach der Form der Modellformulierung aufgliedern. In einer *blockorientierten* Sprache (DAS, MIDAS, DYSAC, PACTOLUS) wird durch jeweils eine Anweisung ein Element des Ananlogrechners (wie Integrator oder Relais) oder eine andere spezifische Funktion beschrieben. Eine solche Anweisung wird als Block bezeichnet. Ursprünglich war es das Ziel, mit Hilfe von blockorientierten Sprachen den Analogrechner auf dem Digitalrechner nachzubilden und dabei einige seiner Nachteile auszuschalten. Offensichtlich ist dieser Weg jedoch wenig flexibel und wird nicht den Möglichkeiten moderner Computer gerecht.

   Bei den *gleichungsorientierten* Sprachen (DYNAMO, DYSYS 71) weicht man diesen Nachteilen aus, indem der Benutzer für sein Modell selbst Gleichungen aufstellt, die er in einer der mathematischen Schreibweise ähnlichen Notierung formuliert. Häufig geschieht das auch in einer höheren Programmiersprache wie FORTRAN, ALGOL oder PL/1. Das Simulationssystem übernimmt dann lediglich noch die Sortierung der Gleichungen und die Steuerung des zeitlichen Ablaufes.

   Unter den *Simulationssprachen für diskrete Systeme* werden zwei Gruppen gebildet. Die *Sprachen der 1. Stufe* (SIMSCRIPT, SIMULA, CSL, OPS) liefern dem Benutzer ein allgemeines Modellkonzept zur Nachbildung realer Systeme sowie eine Ablaufsteuerung und Ablaufkontrolle. Daneben stehen in den meisten Fällen Standard-Output-Möglichkeiten zur Verfügung. Nicht vorhanden sind in diesen Sprachen bereits vorgefertigte, auf eine bestimmte Funktion festgelegte Modellelemente. Die *Sprachen der 2. Stufe* (GPSS, GPS, SIAS, SOL) bieten neben den eben aufgeführten Eigenschaften auch Modell-Elemente, deren Funktion bereits festgelegt ist (z.B. für den Aufbau einer Warteschlange).

2. **nach Implementierungsformen**

   Von besonderer Bedeutung für den Benutzer sind hier solche Simulationssprachen, die in eine höhere Programmiersprache (als Basis) eingebettet sind. Daher ist es naheliegend, den Benutzer nicht auf die Verwendung der Elemente der Simulationssprache zu beschränken, sondern ihm auch die Möglichkeit zu geben, in der Basissprache selbst beliebige weitere Modell-Elemente zu formulieren. Diese Programmierung ist recht komfortabel, da sie auf dem Niveau von Sprachen wie FORTRAN, ALGOL oder PL/1 erfolgen kann. Dadurch ist eine solche Simulationssprache natürlich sehr viel flexibler in der Handhabung. Man bezeichnet solche Sprachen auch als „*open ended*" bezüglich der Basissprache (SIMSCRIPT, CSL, SIMULA, SOL). Ähnliche Vorzüge weisen auch die als „*offene*" Sprachen (GASP, SIMON, SIM) bezeichneten Simulationssystem auf, bei denen es nicht möglich ist, eigene Modell-Elemente, sondern nur eigene Steuer- und Grundroutinen zu formulieren.

3. **nach der Verbreitung der Sprache**

   Was diesen Punkt betrifft, sei auf [62] verwiesen.

Teil V

Rüstung

Kapitel 11

Krieg aus Versehen

THOMAS STRAUCH

11.1 Einleitung

Das Gesicht eines Krieges hängt in großem Maß von den technischen Möglichkeiten ab, die den kriegführenden Parteien zur Verfügung stehen. In dem zu Beginn des 20. Jahrhunderts geführten Weltkrieg wurde der Sieger in sogenannten Materialschlachten bestimmt. Technik und Wirtschaftskraft waren hierbei die kriegsentscheidenden Faktoren. Um die Mitte des 20. Jahrhunderts hat die technische Entwicklung Waffen hervorgebracht, deren Zerstörungskraft die Erde nicht mehr gewachsen ist. Sie wird auf Millionen von Jahren nicht in der Lage sein, sich von dem ihr durch diese Waffen zugefügten Schaden zu erholen. Die Menschheit droht bei einem Masseneinsatz solcher Waffen für immer von diesem Planeten zu verschwinden. Mit der zunehmenden Technisierung zeichnet sich die Möglichkeit ab, daß ein die Menschheit auslöschender Krieg aufgrund eines Fehlers ausgelöst wird. Ein solcher Krieg aus Versehen würde keinen Chronisten hinterlassen, der die Daten des Krieges in ein Geschichtsbuch eintragen könnte. Wie es zu einem solchen Krieg kommen könnte, versucht dieser Artikel zu beschreiben.

11.2 Militärische Kommandostrukturen und Strategien

Die klassische Kommandostruktur basiert auf einer streng hierarchisch gegliederten Pyramidenstruktur [3, S.106]. In ihr läuft der Befehlsfluß von der Spitze, dem Stab bzw. der politischen Führung, zum Fundament, den einzelnen aufgabenunterteilten Kampfeinheiten. Der Informationsfluß läuft in die entgegengesetzte Richtung von unten nach oben. Eine militärische Entscheidung wird im Einpendeln zwischen der über und den unter einer Kommandoebene liegenden Ebenen herbeigeführt. Eine solche Entscheidung benötigte auch noch in den letzten Tagen des 2. Weltkrieges mindestens Stunden, meistens jedoch Tage. Die Grundstrategie besteht darin, dem Gegner auf den höchsten Ebenen einen größtmöglichen Schaden zuzufügen. Dazu mußte man aber eine bestimmte Anzahl weiter unten gelegene Ebenen außer Funktion setzen.

Der Abwurf der ersten A-Bombe auf Japan veränderte diese Struktur grundlegend. Jetzt war man in der Lage, mit einem Schlag die Spitze der Befehlspyramide zu treffen und damit den gesamten Apparat lahmzulegen. Diese Tatsache hatte einen revolutionären Einfluß auf das strategische Denken. Man legte fest, daß jeder Angriff ein Angriff auf die gesamten Streitkräfte darstelle und dieser Angriff mit maximalem Einsatz d.h. Atomwaffen beantwortet werde (Big Bang). Big Bang läßt sich auf eine simple Formulierung zurückführen. *Wer zuerst schießt, der stirbt als zweiter.* Für die neuen Waffen behielten sich die Politiker (Präsident bzw. Spezialabteilung des KGB [13]) die direkte Befehlsgewalt vor. Mit dem Aufkommen der Raketentechnik und der Reduktion der Vorwarnzeit in den Minutenbereich wurden die A-Waffen-Einheiten aus Gründen der Reaktionszeit in die militärische Hierarchie eingegliedert. Der Präsident behielt sich nur noch die Genehmigung des Einsatzes von Atomwaffen vor.

Unter dem Eindruck der Kuba-Krise, in der dem US-Präsidenten zeitweise die Kontrolle über das Militär zu entgleiten schien [3, S.106], und auf das spezielle Engagement des Präsidenten J. F. Kennedy wird die Zweigleisigkeit der Kommandostruktur wieder eingeführt. Es werden auf höherer Ebene Kommandozentren errichtet, die direkt dem Präsidenten unterstehen und die Aufgaben der A-Kampfeinheiten koordinieren sollen. Diese Kommandostruktur hat sich bis heute erhalten, wenn sich auch ihre technischen Parameter geändert haben.

Zielgenauigkeiten, elektromagnetischer Impuls (EMP), Raketenflugzeiten und mehrfacher Overkill verändern zu Beginn der 70er Jahre die Qualität eines Zweitschlages. Galten vorher gesicherte Detonationsmeldungen als Kriterium zum Auslösen eines Zweitschlages aus gesicherten Betonsilos (**Launch on Impact**), so machten die Militärs jetzt geltend, daß die Raketen bereits vor der Detonation der angreifenden Raketen in der Luft sein müssen. Der Start aufgrund von gesicherten Sensormeldungen soll die ICBM (Intercontinental Ballistic Missile) vor einer Zerstörung in ihren Silos bewahren (**Launch on Warning**). Um diesen Veränderungen auch strategisch Rechnung zu tragen, führten die USA das Konzept der **Flexible Response** ein, das eine abgestufte Reaktion im Konfliktfall vorsieht [3, S.190 ff].

Strategisch brachten dann die 80er Jahre fundamentale Veränderungen. 1982 wird das **Air-Land-Battle-2000**-Konzept vorgelegt, um deren Akzeptanz die USA momentan bei ihren Verbündeten wirbt. Air-Land-Battle sieht eine Verstärkung der konventionellen Komponente der Nato-Streitkräfte vor. In gewissem Rahmen sollen diese in die Lage versetzt werden, Präventivoperationen durchzuführen. Ein weiterer Pfeiler des Konzeptes ist die „Abriegelung in die Tiefe“ [9, S.103], wobei der gegnerische Nachschub bereits tief in seinem eigenen Land vernichtet werden soll. Diese Maßnahmen erfordern eine schlagkräftige Rakete kurzer Reichweite, um die sich 1989 eine angespannte Diskusion unter den Mitgliedern der Allianz entwickelt hat.

1983 stellt Präsident Reagan die Strategische Verteidigungsinitiative SDI der Öffentlichkeit vor. Ihre Konzepte und Strategien werden in einem späteren Kapitel vorgestellt.

11.3 C^{3}I (Command Control Communication and Intelligence)

11.3.1 C^{3}I in der Bundesrepublik Deutschland

Die Abkürzung C^{3}I wird in der deutschen Literatur mit verschiedenen Begriffen übersetzt. So existieren Begriffe wie Frühwarn- und Entscheidungssystem oder Aufkärungs- und Führungssystem [9, S.99]. Die Bundeswehr verfügt über ein System namens **ADLER** (Artillerie-Daten Lage und Einsatzrechnerverbund), dessen Hauptaufgabe in der Feuerleitung und der Koordination der Gefechtsfeldartillerie besteht [9, S.117]. Desweiteren ist die Bundesrepublik als potentielles Schlachtfeld in Europa in die meisten C^{3}I Komponenten eingebunden.

11.3.2 C^{3}I und Politik

Die militärischen Grundkonzepte werden in den Vereinigten Staaten durch die sogenannten **President Directives** festgelegt [9, S.101 ff].

In der President Directive 53 vom 15.11.1979, der National Security Telecommunication Policy, legt der Präsident die Grundlagen für die Schnittstellen zwischen den einzelnen Kommandostellen der US-Amerikanischen C^{3}I Systeme fest.

Die President Directive 58 vom 30.6.1980 fixiert die Konzepte, mit denen die Regierungs- und Reaktionsfähigkeit des Präsidenten im Verteidigungsfall erhalten werden sollen.

Im Zusammenhang mit der Strategie der Flexible Response steht die President Directive 59 vom 25.7.1980. Nach einer Diskusion über die Dauer eines Atomkrieges stellte man fest, daß das momentane C^{3}I Konzept der USA auf einen Krieg längerer Dauer nicht eingerichtet sei. Die Dauer der verschiedenen Planspiele liegt zwischen 60 und 175 Tagen.

Präsident Reagan gibt schließlich am 2.10.1982 der Reorganisation und dem Ausbau der C^{3}I Komponenten der USA oberste Priorität.

11.3.3 Beispiele für C^3I

11.3.3.1 WWMCCS (World Wide Military Command and Control System)

1962 gründet Präsident Kennedy das WWMCCS. Es koordiniert weltumspannend die Arbeit aller Befehls- und Kommunikationseinrichtungen der US-Streitkräfte. Nach seiner Reorganisation 1971 umfaßt es 60 große Sensordaten-Erfassungsstellen, 27 Kommandozentren mit 35 Honeywell-6000 Rechnern, auf denen Software mit ca. 20 Millionen Cobol Anweisungen implementiert ist. Mit einem Etat von 560 Millionen $ ordnet 1983 Präsident Reagan eine erneute Reorganisation an und benennt es in WIS (WWMCCS Information System) um. Ziel dieser Reorganisation ist die Einbeziehung neuer Systeme und das Umstellen der Software auf die Programmiersprache ADA [9, S.100].

11.3.3.2 NAVSTAR

Das NAVSTAR-Programm wird 1973 gestartet und mit seiner zweiten Phase 1988 in Dienst gestellt. Es dient der Satellitenkommunikation und der atomaren Detonationsbestimmungen. Damit ist NAVSTAR ein Element zur Führung eines längeren Atomkrieges und in das Konzept der Flexible Response eingebunden. Daneben enthält NAVSTAR noch die Komponente GPS (Global Positioning System), die der Orts- und Zeitbestimmung für die Einheiten der US-Streikräfte dient. Diese Komponente ist besonders für die Atom-U-Boote der USA von Bedeutung, da die genaue eigene Positionsbestimmung entscheidenden Einfluß auf die Zielgenauigkeit von SLBM (Submarine Launched Ballistic Missiles) hat. GPS erhöht die Zielgenauigkeit von SLBM auf 7 bis 17m [9, S.100 f].

11.3.3.3 MILSTAR (Military Strategic Tactical and Relay)

MILSTAR steht bis zum Jahr 1987 ein Etat von 1 Milliarde $ zur Verfügung. Es hat sich zum Ziel gesetzt, gehärtete Satelliten und mobile Bodenkommunikationseinheiten zu stationieren [9, S.102].

11.3.3.4 MEECN (Minimum Essential Emergency Communication Network)

MEECN verfügt bis 1987 über einen Etat von 430 Millionen $ und zielt auf die Errichtung eines Notkommunikationssystems. Daneben sollen von MEECN die Raketen automatisch gestartet werden, wenn alle militärischen Möglichkeiten ausgeschöpft sind oder die Kommunikation zwischen den Komponenten des C^3I nicht mehr möglich ist [9, S.102].

11.3.4 Prinzipieller Aufbau anhand eines Beispiels (USA)

11.3.4.1 Sensordaten Erfassungs- und Verarbeitungssystem

Mobile Erfassungssysteme Diese Systeme führen die Erstdetektion durch. Es gehören dazu Satelliten, die mit Infrarotsensoren die charakteristische Handschrift der Raketen in der Boost-Phase erkennen, das luftgestützte RADAR-System AWACS oder das Bordradar konventioneller Flugkörper.

Stationäre Erfassungssysteme Dazu zählen die **PAVE PAWS** (gepflasterte Tatzen), die der Erfassung und ersten groben Trackberechnung von SLBM (Submarine Launched Ballistic Missiles) dienen. Diese Raketen sind vor allem auf U-Booten der sowjetischen Yanckee-Klasse, deren Positionsbestimmung und Verfolgung von FOSIC (Fleet Ocean Surveillance Information Center) übernommen wird, stationiert [3, S.173].

Wegen der Erdkrümmung werden die erkannten Flugobjekte erst ab einer gewissen Höhe von Boden-Radarstationen **BMEWS** (Ballistic Missiles Early Warning Systems) übernommen und eine erste genauere Trackberechnung (Flugbahn einer Rakete) wird durchgeführt.

Die Feinauswertung und Zielverfolgung führt das **PARCS** (Perimeter Acquisition Radar Attack Characterisation System) durch.

Probleme der Sensordatenerfassung liegen in der Störanfälligkeit und Täuschbarkeit der Sensoren, der Mehrdeutigkeit von Sensordaten, in der Übermittlungssicherheit und für erdgestützte Systeme in der Krümmung der Erdoberfläche.

11.3.4.2 Datenverarbeitungssysteme

In diesem Zusammenhang versteht man darunter Rechenzentren zur Bündelung und Auswertung von Daten der Erfassungssysteme und zur Erstellung einer ersten strategischen Lagebeurteilung. Ein solches System soll an einem Beispiel vorgestellt werden.

Im Cheyenne-Mountain in Colorado befindet sich das bedeutendste Kommandozentrum der USA. Sein Name ist **NORAD** (North American Aerospace Defense Command). Insgesamt setzt es sich aus einem 427M Computersystem zusammen, das aus 84 Computern mit über 10 Millionen Zeilen Software besteht. Es unterteilt sich in 3 Hauptsegmente [3, S.173 f].

Das **CSS** (Communication System Segment) gilt als das wichtigste Segment, denn hier wird im Stand-By Betrieb zweier Rechner die Vermittlung zwischen den verschiedenen Komponenten des Frühwarnsystems durchgeführt.

Das **NCS** (NORAD Computer System) übernimmt das Display der Sensordaten und erstellt eine erste strategische Lagebeurteilung. Daneben werden Reaktionsvorschläge erteilt und eine Versicherung der Erfassungsdaten versucht.

Das **SCC** (Space Computational Center) ist die Zentrale Erfassungsstelle aller zivilen und militärischen Flugobjekte im All und ist in Zukunft als militärische Koordinationsstelle der Raumstation geplant. Weiter übernimmt SCC eine Analyse und Voraussage des zu erwartenden Schadens aufgrund von Trackberechnungen und Detonationsmeldungen.

11.3.4.3 Entscheidungssystem

Ein Entscheidungssystem liegt an der Schnittstelle zwischen Politik und Militär. Hier soll eine Beurteilung der strategischen Situation und die Einleitung von Gegenmaßnahmen durchgeführt werden. Dafür existieren in den USA im wesentlichen 4 Kommandozentren:

- NORAD (North American Aerospace Defense Command in Colorado)
- SAC (Strategic Air Command)
- NMCC (National Military Command Center im Pentagon)
- ANMCC (Alternate National Military Command Center in Fort Richie Maryland)

Daneben gibt es noch 3 lokale Kommandozentren. Es sind dies PAC (Pacific Command), LANT (Atlantic Command) und EUR (European Command) [3, S.175].

In NORAD wird eine Bedrohung in 3 Grade gestaffelt [3, S.183 ff].

- *Missile Display Conference*, die im Jahr 1980 2159 mal routinemäßig einberufen wurde. Dabei ergab sich 78 mal die Vorlage eines möglichen Angriffes.
- *Threat Assessment Conference*, die in den Jahren 1979/80 5 mal einberufen wurde.
- *Missile Attack Conference*, die bis 1980 noch nicht einberufen worden sein soll.

11.3.5 C^{3}I und Krieg aus Versehen

11.3.5.1 Potentionelle Fehler

Darunter fallen beabsichtigtes und unbeabsichtigtes Fehlverhalten des Systems. Ein unbeabsichtigtes Fehlverhalten kann durch die Fehlinterpretation von Sensordaten, Kommunikationsfehler, Fehler in Soft- oder Hardware oder menschliches Versagen an einem hochtechnisierten Arbeitsplatz herbeigeführt werden. Ein beabsichtigtes Fehlverhalten kann durch Spionage und Sabotage, durch kriminelle Machenschaften oder einfach durch Abenteurer hervorgerufen werden.

11.3.5.2 Zeitrestriktionen

Bei der Entscheidung, welche Qualität ein Angriff hat und wie die Reaktion auszusehen hat, stellen sich im wesentlichen folgende Fragen:

- Liegt überhaupt ein Angriff vor?
- Wann sollen Gegenmaßnahmen eingeleitet werden?
- Welche Dimension hat der Angriff?
- Wo befindet sich wer und welche Entscheidungsorgane sind noch intakt?

Zur Beantwortung dieser Fragen stehen in Europa 6-8 Minuten (Mittelstrecken-Raketen) und in den USA 30 Minuten (ICBM) bzw. 10 Minuten (SLBM) zu Verfügung. Bei sofortigem Detektieren entsprechen diese Zeiten im groben den Flugzeiten der jeweiligen Raketen [98, S.63].

11.3.5.3 Automatisches Auslösen bei Kontaktverlust

Aufgrund ihrer Aufgabenstellung müssen die Komponenten eines Frühwarnsystems in ständigem Kontakt miteinander stehen. Im Falle eines Kontaktverlustes muß mit der Zerstörung der Komponente gerechnet und die entsprechenden Gegenmaßnahmen veranlaßt werden [3, S.182].

11.3.5.4 Psychische Belastung des Menschen in diesem Entscheidungsprozeß

Dem Präsidenten bleibt nach Abzug der zur Datenerfassung und Auswertung benötigten Zeit noch eine Entscheidungsfrist von 3-5 Minuten, um die Zweitschlagsfähigkeit zu erhalten. Die ständige Konfrontation mit diesem Zeitdruck und die Verantwortung für die Menschheit üben einen enormen Druck auf alle Beteiligten aus. So wurden im Zeitraum zwischen 1975 und 1977 ca. 5.000 Personen aus dem Bedienpersonal der Frühwarnkomponenten aufgrund von Suchtproblemen entlassen. Daneben birgt auch der in einem so komplexen System vorprogrammierte Kompetenzstreit zwischen Personen oder Kommandoeinrichtungen eine nicht zu vernachlässigende Gefahr [3, S.181].

11.3.5.5 Expertensysteme als Lösung

Wegen der immensen Menge der Eingangsdaten und der Kürze der Zeit plant man derzeit, die Aufgabe der Entscheidungsfindung Expertenystemen zu übertragen. Dabei vernachlässigt man sträflich die Tatsache, daß der Krieg zwar immer seine Regeln hatte, aber daß die Geschichte zeigt, daß gerade die „großen“ Feldherrn Kriege gewannen, indem sie sich nicht an diese Regeln hielten. Der zivile Einsatz von XPS macht deutlich, daß diese nicht in der Lage sind, Randbedingungen, die bei militärischen Entscheidungen oftmals größtes Gewicht haben, mit in den Entscheidungsprozeß einzubeziehen. Technisch läßt sich ferner noch bezweifeln, ob XPS solcher Komplexität überhaupt realisierbar sind. Zur Bewältigung der gestellten Aufgaben werden verteilte Expertensysteme mit etwa 20.000 Regeln in einer Verarbeitungsgeschwindigkeit von 10^{10} Instruktionen pro Sekunde benötigt [11, S.23].

11.3.5.6 Organisation

Die Organisation eines militärischen Entscheidungssystem erfordert eine schnelle Reaktionsfähigkeit und einen maximalen Selbstschutz. Die erste Forderung bevorzugt eine zentrale, die zweite eine dezentrale Organisation. Die Bevorzugung einer Organisationsform kann sich fatal auf die jeweils andere Forderung auswirken und damit zu Unsicherheiten über die Zuverlässigkeit des Systems führen.

Schnittstellenprobleme treten bei solch komplexen Systemen immer wieder auf und können zu unübersehbaren Folgen führen. Solche Probleme treten besonders dort auf, wo alle Informationen zusammenlaufen.

11.3.5.7 Politische Situation

Eine militärische Situation wird in einer politisch gespannten Situation anders beurteilt, als bei politischem Tauwetter. Und doch ist die Fehlerwahrscheinlichkeit in militärischen Systemen nur gering von der politischen Wetterlage abhängig. Beispiele zeigen sich während der Kuba-Krise, als der Verteidigungsminister bei der Blockade der Karibikinsel in die Detailarbeit der Marine eingriff, worauf es in den höheren Stäben zu gespannten Auseinandersetzungen kam.

Ein weiteres Beispiel liefert der frühe November des Jahres 1956. Fast zur gleichen Zeit, als die Briten und Franzosen im Suez eingriffen, besetzt die UdSSR Ungarn. Um Briten und Franzosen unter Druck zu setzen, drohen die Sowjets in aller Öffentlichkeit mit dem Einsatz von Atomwaffen am Suez. Zusätzlich überreicht Moskau am 5. November Washington eine Note mit der Forderung nach einem gemeinsamen Vorgehen am Suez. Diese Note trifft in Washington mit vier weiteren Nachrichten zusammen:

- Nicht identifizierte Düsenjäger über der Türkei gesichtet, worauf die türkische Luftwaffe in Alarmbereitschaft versetzt wird.
- 100 MIG-15 Düsenjäger über Syrien gesichtet.
- Britischer Canberra-Bomber über Syrien abgeschossen (wozu zu dieser Zeit nur die hochfliegenden MIGs in der Lage waren).
- Die sowjetische Flotte verläßt durch die Dardanellen das Schwarze Meer, in das sie im Kriegsfalle eingeschlossen wäre.

Später stellt sich heraus, daß

- die Düsenjäger eine Schwanenschar waren,
- die 100 MIGs eine wesentlich kleinere Anzahl von Flugzeugen waren, die den syrischen Präsidenten begleiteten,
- der britische Canberra-Bomber wegen eines technischen Fehlers abgestürzt war und
- die sowjetische Schwarzmeer Flotte sich auf einer lange geplanten Manöverfahrt befand.

Die Reaktion des Weißen Hauses auf die Ereignisse ist nicht vollständig bekannt, doch wird berichtet [37, S.418-421], daß General Goodpaster befürchtete, die Ereignisse könnten die NATO-Einsatzpläne auslösen, die zu jener Zeit einen totalen nuklearen Vergeltungsschlag gegen die Sowjetunion vorsahen [3, S.187 f].

11.3.5.8 Kurzschlußreaktion

Die Existenz eines funktionierenden totalen BMD (Ballistic Missile Defense) löst beim potentiellen Gegner eine unsichere Lagebeurteilung aus. Er kann nicht mehr gewährleisten, daß seine militärische Macht noch von Bedeutung ist und wird versuchen seine letzten militärischen Trümpfe auszuspielen, bevor sie nutzlos sind.

11.3.5.9 Launch on Warning

Hat man sich auf eine Reaktion auf der Basis des Launch on Warning festgelegt, dann wird der potentielle Gegner aus Reaktionsgründen ebenfalls dieses System einführen müssen. Dadurch wird erstens die Reaktionszeit noch einmal reduziert und zweitens liefert man sich den Sensordatenerfassungssystemen auf Gedeih und Verderb aus. Eine Sensorwarnmeldung erzwingt damit eine sofortige Mobilmachung der Zweitschlagskomponenten, was im Falle eines Fehlalarms den jeweiligen Gegner zu der Annahme verleitet, daß man selbst einen Erstschlag plant. Ein Mißverstehen der Lage ist in der Kürze der zur Verfügung stehenden Zeit vorprogrammiert.

11.3.5.10 Ein Unbefugter löst einen Krieg aus

Hier sind grundsätzlich zwei Möglichkeiten denkbar. Zum ersten gewinnt jemand versehentlich über die Kommunikationsnetze des C^3I die Kontrolle über das System und löst im Glauben es handele sich um ein Spiel einen Weltkrieg aus. Die zweite Möglichkeit besteht darin, daß Kriminelle absichtlich das System unter ihre Kontrolle bringen, um durch Erpressung mit der so gewonnenen Macht ihre Ziele durchzusetzen. Das Einspeisen von Viren oder ähnlichen Programmen kann die Funktionalität des Systems stören und es können unbeherrschbare Situationen entstehen. Daß diese Möglichkeiten auch für militärische Rechenanlagen nicht ausgeschlossen sind, liegt unter anderem daran, daß diese Rechner aus Finanzgründen und Gründen der militärischen Infrastruktur an zivile Netze angeschlossen sind. [13]

11.3.5.11 Der Gegner setzt das System außer Kraft

Eine genaue Analyse der Schwachstellen des C^3I Systems durch den Gegner kann diesem die Möglichkeit in die Hand geben, das System auszuschalten und dadurch einen für ihn risikolosen Angriff zu führen.

11.3.6 Dokumentierte Fehlalarme

Am **3.10.1979** melden Pave Paws einen SLBM Angriff auf die USA. Die Situation wird so eingestuft, daß eine Threat Assessment Conference einberufen wird. Die Ursache des Fehlers liegt bei der Software der Sensordatenerfassung.

Am **3.11.1979** wird in NORAD ein Massenangriff von Raketen angezeigt und sofort eine Threat Assessment Conference einberufen. Die Ursache dieses Fehlers liegt wiederum bei der Software, denn ein Simulationsprogramm war im Rechner verblieben und aus Zufall gestartet worden. Seither werden Simulationen auf speziellen Rechnen durchgeführt.

Am **15.3.1980** trifft in NORAD die Meldung ein, daß 4 SLBM in Kamschatka gestartet wurden. Eine dieser Raketen entwickelt eine Flugbahn mit einem Ziel in den USA. Eine Threat Assessment Conference wird einberufen. Es stellt sich heraus, daß die Flugbahn falsch berechnet wurde.

Am **3.6.1980** und am **6.6.1980** verursachte derselbe Fehler Alarm. Es werden jeweils Massenangriffe von SLBM angezeigt. Eine Threat Assessment Conference wird einberufen, die B-52 Bomber laufen warm und das Luftleitkommando startet in Hawaii. Wie von Geisterhand verschwinden die gemeldeten Raketen wieder vom Anzeigeschirm. Zur Aufrechterhaltung der Kommunikation sendet der Communication Multiplexer bei Abwesenheit von Raketen immer den Wert Null. Ein Wert ungleich Null bedeutet Angriff. Ein Hardware-Fehler war hier die Ursache, daß an Stelle der Null andere Werte gesendet wurden und somit ein Angriff vorgetäuscht wurde [3, S.182 f].

Wegen der Häufigkeit der Fehler setzt der US-Senat einen Untersuchungsausschuß unter den Senatoren Hart und Goldwater ein und es ist wohl diesen zu verdanken, daß die Vorfälle überhaupt veröffentlicht wurden. Der Bericht schließt mit dem Resümee, daß die speziellen Fehlerursachen beseitigt wurden. Aber auch nach Abstellen der Fehler kann nicht sichergestellt werden, daß dieselben oder ähnliche Fehler noch einmal vorkommen können. Manche Systeme wurden sogar ersetzt, doch es stellt sich die Frage, ob die neuen Systeme nicht mit ähnlichen Fehlern behaftet sind. Es gibt trotz aller Anstrengungen auch in der militärischen Technik keine fehlerlosen Systeme. [41]

11.4 SDI (Strategic Defense Initiative)

11.4.1 SCI (Strategic Computing Initative)

Im Jahre 1958 starten die USA im Zusammenhang mit dem Start der sowjetischen Sputnik Rakete das **DARPA-Programm** (Defense Advanced Research Projects Agency). Es stellt sich die Aufgabe, die Nutzung und Erforschung grundsätzlich neuer Technologien für militärische Anwendungen zu erforschen und zu koordinieren [9, S.75]. DARPA soll diese Koordination zwischen Militär und Forschung durchführen. Dafür verfügt DARPA über einen Jahresetat von 900 Millionen $ [11, S.21]. Daneben soll DARPA die Koordination zwischen Forschung und Militär durchführen. Schon bald erlangt hierbei die Informatik eine Schlüsselrolle [72, S.29 ff].

Aus diesem Grund wird 1983 SCI als auf 10 Jahre ausgelegtes Programm ins Leben gerufen. Die Bedeutung, die dem Projekt beigemessen wird, läßt sich am besten an der Höhe des Etat ablesen. Dieser beläuft sich für die ersten 5 Jahre auf 600 Millionen $ und bis zum Jahr 1990 auf ca. 1 Milliarde $. Seine Hauptziele sind [38, S.165] die Entwicklung

- von Expertensystemen für militärische Aufgaben,
- eines rechnergestützten Pilotenassistenten,
- von gehärteten VHSIC (Very High Speed Integrated Circuits) auf GaAs Basis,
- von Fire and Forget Waffen, AGV (Automatic Guided Vehicles) und Kampfrobotern und
- eines Battle Managers zur Führung von Seeschlachten.

Nach dieser Aufgabenstellung konzentrieren sich die Forschungen auf Chipentwicklung, Lasertechnologie, Datenbanken und die KI. Auf dem Gebiet der KI sind fast alle Gebiete für SCI von Interesse. Die Palette reicht von Wissensrepräsentation über Bildverarbeitung bis zu Expertensystemen. Daneben sind die Entwicklung der „Rechner der 5. Generation“ und die Härtung von Technik gegen Radioaktivität von Interesse.

11.4.2 Die Vision vom Krieg der Sterne

Am 23. März 1983 unterbreitet Präsident Ronald Reagan in einer Fernsehansprache den USA die Vision einer neuen Verteidigung. Die Idee selbst ist nicht neu, denn in den 70er Jahren war ein ähnliches Konzept, das der **ABM** (Anti Ballistic Missile) an der technischen Realisierung gescheitert. Reagan zeigt das Bild einer **BMD** (Ballistic Missile Defense), deren Komponenten in der Lage sind, alle angreifenden Raketen zu zerstören, bevor sie ihre totbringenden Sprengköpfe ins Ziel tragen können. Er fordert die Vereinigten Staaten auf:

„Alle Wissenschaftler sollen ihre Fähigkeiten einsetzen, damit uns die Mittel an die Hand gegeben werden, um Atomwaffen unwirksam und obsolet zu machen. Dazu sollen Systeme entwickelt werden, die angreifende Interkontinentalraketen unschädlich machen, bevor sie die USA oder ein anderes befreundetes Land erreichen und dort Schaden anrichten können.“ [9, S.143]. Damit war das Zeitalter des Krieg der Sterne eingeläutet. Die neue Strategie bekommt den Namen SDI (Strategic Defense Initiative).

11.4.3 Anforderungen an eine BMD (Ballistic Missile Defense)

11.4.3.1 Anforderungen an die Hardware

SDI erfordert eine neue Generation von Rechnern, die fähig sind Realzeitaufgaben zu lösen und die an die Konzepte der Künstlichen Intelligenz angelehnt sind (Parallelrechner, Neuralrechner). Ihre Größe, ihr Energieverbrauch und ihr Gewicht müssen minimal sein, was den Einsatz von VLSI (Very Large Scale Integration) nahelegt. Heutige „Superrechner“ (z.B. Gray, CDC) verfügen nicht über diese Technik. Sie müssen Strahlendosen von bis zu 1 Million Rad auch auf längere Zeit schadlos verkraften. Weiterhin werden höchste Anforderungen an die Fehlertoleranz gestellt, denn die Komponenten sind für eine Einsatzdauer von ca. 10 Jahren konzipiert [9, S.152].

11.4.3.2 Anforderungen an die Software

Die Programmpakete müssen von hoher Komplexität und realzeitfähig sein. Wegen ihrer Aufgabenstellung sind die Programme in der Realität nicht testbar, sondern nur simulierbar. Dazu muß zuerst eine neue Generation von Simulatoren entwickelt werden. Die Software wird in der Programmiersprache ADA entwickelt, über deren Tauglichkeit die Meinungen der Experten auseinandergehen. Wie man aus den Erfahrungen der zivilen Softwareentwicklung weiß, wird es aufgrund der Komplexität des Systems zwischen den einzelnen Komponenten der BMD zu Schnittstellenproblemen kommen [9, S.153].

11.4.3.3 KI

Die KI wird wegen der Realzeitanforderungen nur in Randbereichen eingesetzt werden können. Die Frage, ob die KI innerhalb der kurzen Zeit in der Lage sein wird, die Anforderungen, die an sie gestellt werden, zu lösen, kann nicht gewissenhaft mit ja oder nein beantwortet werden. Zu diesen Anforderungen zählen die Situationsanalyse, die Bildverarbeitung und Erkennung, Heuristiken (Auswahl der Waffen, Reaktionsprinzipien) und die Erarbeitung von Strategien. Aber auch das Problem von Selbstreparaturen und deren Strategien stellt für die KI eine Herausforderung dar [9, S.153].

11.4.4 Krieg im Weltraum

11.4.4.1 Charakteristische Flugbahn einer ICBM

Die UdSSR besitzt in ihrem Raketenarsenal heute ungefähr 1.400 ICBM Raketen. Deren Flugverhalten ist im Prinzip für alle Modelle gleich [9, S.144].

Die erste Phase nach dem Start nennt man **Boost Phase** oder Startphase. Sie dauert heute ca. 100-300 Sekunden, ist aber nach Meinung von Experten bis auf 60 Sekunden reduzierbar. Die Boost-Phase ist die Phase, in der die Raketen am besten detektierbar sind, weil die Antriebsstufen der Raketen einen heißen Schweif hinter sich ziehen, der mit Infrarotsensoren erkennbar ist.

Die zweite Phase nennt man **Bus Phase**. Hier bewegen sich die Raketen in einem antriebslosen ballistischen Flug. Jede Rakete d.h. Sprengkopf-Bussystem enthält ca. 10 Sprengköpfe und läd zum Verwirren der feindlichen Abwehr elektronische Gegenmittel aus. Dies sind zum Beispiel Aluminiumstreifen, Radar reflektierendes Material, Infrarot reflektierende Gase oder beschichtete Ballons.

Die dritte Phase heißt die **Midcourse Phase**. Die Tracks der Raketen werden korrigiert und das Abtrennen der Sprengköpfe vorbereitet.

In der letzten Phase, der **Terminal Phase**, treten die Sprengköpfe, die sich inzwischen vom Bus getrennt haben, wieder in die Atmosphäre ein, erreichen ihre Ziele und detonieren.

11.4.4.2 Planspiel *High Frontier* von General Graham

Das Planspiel von General Graham unterteilt die Raketenabwehr in 4 Teile. Ziel ist es die Raketen in Boost oder Bus Phase zu vernichten, da hier durch Zerstören einer Trägerrakete mehrere Sprengköpfe (bis zu 10) ausgeschaltet werden können [9, S.147].

Im ersten Teil übernehmen 432 Kampfsatelliten mit je 40 konventionellen ABM (Anti Ballistic Missiles) die Aufgaben die detektierten ICBM in der Boost und der Bus Phase zur vernichten.

Im zweiten Teil übernimmt eine Laser Kampfstation die Raketen, die den ersten Teil überwunden haben. Ein bodengestützter Laser liefert die Energie für 70 Spiegel mit ca. 100m Durchmesser, die auf einer geostationären Umlaufbahn (36.000 km) die Erde umkreisen. Wegen der Fraunhoferbeugung beträgt der Durchmesser des Strahls im Ziel noch 50cm. Diese 70 Spiegel speisen 70 Kampfspiegel in einer Höhe von ca. 3.000km über der Erdatmosphäre. Da ihre Geschwindigkeit größer ist als die Rotationsgeschwindigkeit der Erde müssen, ca. 400 Kampfspiegel stationiert werden, damit 70 jederzeit bestrahlt werden können. Das Zielverfolgungs- und Ortungssystem trägt den Namen „Talon Gold“([53, S.95] und hat eine fast unlösbare Aufgabe. Die gigantischen Spiegel müssen in einer Zeit von 0,5 Sekunden auf 0,00003 Grad genau ausrichten werden [9, S.147 ff].

Den dritte Teil nennt Graham die Pop-Up Phase, in der Boden-Luft Raketen mindestens 900m (wegen der Erdkrümmung) hoch geschossen werden. Wegen der Kürze der Boost Phase steht hierfür nur eine Zeit von 240 Sekunden zur Verfügung. Eine Reduktion der Boost-Phasenzeit auf 60 Sekunden würde eine völlige Bedeutungslosigkeit der Pop-Up Phase bedeuten. Die Reaktionszeit wäre schlicht und einfach zu gering. Die Zündung einer Atombombe versorgt einen Röntgen-Laser mit Energie. Dieser Laser hat die Aufgabe in direktem Bestrahlen angreifende Bussysteme oder Sprengköpfe zu vernichten.

Der letzte Teil besteht aus Zivilschutzmaßnahmen, die zivile und militärische Personen und Einrichtungen vor den Sprengköpfen schützen sollen, die die vorhergehenden Abwehrphasen überwunden haben.

11.4.5 SDI und Krieg aus Versehen

Wie wir bereits im Abschnitt 11.2 gesehen haben, existiert bereits heute die Gefahr eines Krieges aus Versehen. Diese Gefahr wird aber durch die erhöhte Akzeptanz der Technik und die Vervielfältigungen der Kapazitäten erhöht. Dabei ist nicht einsichtig, mit welchem Faktor diese Erhöhung wächst. Die Gefahren, die bei der Stationierung von SDI zusätzlich hinzukommen, lassen sich im Groben in zwei Gruppen klassifizieren. Gefahren, die SDI selbst erzeugt und Gefahren, die das Funktionieren von SDI in Frage stellen.

11.4.5.1 Beispiele für die erste Gruppe

- Durch SCI wird die gesamte Forschung und Technologie auf das Militär konzentriert und durch den gigantischen Haushalt des Pentagon gesteuert. Die Ausweitung des militärisch-industriellen Komplexes und seines Einflusses auf die Politik hat eine Militarisierung der gesamten Gesellschaft zur Folge.
- Das kompliziert ausgependelte Gleichgewicht der Mächte wird gestört und die Rüstungsspirale dreht sich erneut um eine Runde.
- Die USA müssen von der minimalen Leistungsfähigkeit des System ausgehen und deswegen trotzdem noch die klassischen Verteidigungsmittel in Reserve halten. Die UdSSR dagegen müssen von der maximalen Leistungsfähigkeit des System ausgehen und deshalb die Qualität ihrer Waffen und Strategien verbessern.
- SDI raubt dem potentiellen Gegner nicht nur seine Erstschlagsfähigkeit, sondern als gefährliches Nebenprodukt seine Zweitschlagsfähigkeit. Danach wären die USA in der Lage, die dann schutzlosen Staaten zu erpressen. Diese Tatsache könnte die anderen Staaten zu Kurzschlußreaktionen verleiten.

11.4.5.2 Beispiele für die zweite Gruppe

- Die technischen Beurteilungen über die Qualität des Angriffes gehen vom heutigen Stand aus. Die Lösungen in SDI werden für das nächste Jahrzehnt gemacht.
- Technische Vorgaben, von denen nachfolgende Komponenten abhängen, sind technisch noch nicht realisiert und getestet. In diesem Zusammenhang steht, daß bis heute noch kein Laser entwickelt wurde, der die benötigte Energie liefert. Weiter steht auch noch das Verhalten eines 100m Spiegels im Weltraum in den Sternen. Ferner gibt es noch das Transportproblem. Wie sollen diese Mengen von Material in den Wetraum transportiert werden? Das äußerst zeitkritische Zielverfolgungs- und Ortungssystem ist mit Zeitannahmen von heute erstellt und wird wahrscheinlich mit zukünftigen Angriffen gar nicht fertig. Die Software und hier speziell die Expertensysteme haben noch nicht die geforderte Komplexität. Hier lassen sich noch eine Fülle von Beispielen anbringen.
- Von Seiten der UdSSR wird man nicht tatenlos zusehen, wie sich die USA aus dem Gleichgewicht des Schreckens auskoppeln. Ihre Gegenmaßnahmen sind viel effektiver und billiger als SDI. So genügt wegen der hohen Geschwindigkeiten der einfache Transport von Stahlkügelchen in den Weltraum, die dort stationierten Komponenten zu zerstören. Daneben verschlimmert die technisch simple Reduktion der Boost-Phase auf 60 Sekunden oder die Verdoppelung der Raketen und Drohnen die Probleme von SDI um ein Vielfaches [9, S.150].
- Ein System wie SDI kann nie real getestet werden, so daß Aussagen über seine Zuverlässigkeit allein aufgrund von Simuationsdaten gemacht werden können.
- Die Kosten dieses Systems stehen in keiner Relation zu seinem Nutzen, denn es destabilisiert politisch und kann nur eine Hälfte des NATO-Bündnisses schützten und dieses deshalb spalten. Die europäischen Verbündeten müssen weiterhin mit der nuklearen Bedrohung leben.
- Mit der Verlagerung eines Großteils der Komponenten in den Weltraum erhöht sich das Wartungsproblem. Die Reparaturzeiten sind in der Regel sehr lange und die Reparaturen selbst sehr kompliziert. Daneben wird allein der Transport der Komponenten an ihren Einsatzort Unsummen verschlingen und die Kapazität heutiger Transportmittel übersteigen [9, S.148].

- Wegen der hohen Transport- und Wartungskosten sind lange Stationierungszeiten nötig, um das System möglichst wirtschaftlich zu halten. Dafür sind fehlertolerante und selbstreparierende Systeme erforderlich, die noch nicht verfügbar sind. Mit der verlängerten Stationierungsdauer steigt aber die Wahrscheinlichkeit eines Fehlers.
- Die zu erwartende Menge von Eingangsdaten wird nur von speziellen Programmen oder Expertensystemen zu verarbeiten sein. Ein Übertragen von für die Menschheit vitalen Entscheidungen auf Expertensysteme ist wegen der Irreversibilität der Entscheidungen und des „Fachidiotentums“ von Expertensystemen nicht verantwortlich.
- Die Energiefrage für SDI ist noch nicht geklärt. Wissenschaftler errechneten, daß die geplanten Laser-Stationen den Energiebedarf von 300 Kraftwerken einer Leistung von 1.000 MWatt benötigen werden. Dies ist ca. 60% des Energieverbrauchs der USA [9, S.148].

11.5 Präzisionsgelenkte Munition und Kampfroboter

11.5.1 Präzisionsgelenkte Munition

11.5.1.1 Definition

Darunter versteht man Geschosse mit mikroelektronisch gesteuerter Endphasensteuerung (in der englischen Literatur Fire and Forget). Die Geschosse werden in die Richtung des Gegners abgefeuert und suchen sich autonom mit Hilfe einer Sensorik ihre Ziele selbst. Bei Überschreitung eines Schwellwertes (Hot Spot) identifizieren, verfolgen und zerstören sie ihr Ziel. Hierbei ist im Gegensatz zu klassischen Systemen keine ballistische Bahnberechnung, Vermessung und Feuerleitung nötig.

11.5.1.2 Beispiele

MLRS (Multiple Launch Rocket System) Die Kosten dieses Projektes sind mit 4,2 Milliarden DM veranschlagt und das System soll zu Beginn der 90er Jahre bei der Bundeswehr eingeführt werden. Auf einem Werferfahrzeug stationiert, hat dieses System eine Reichweite von 40km. Jede Rakete besteht aus 6 Submunitionsträgern, von denen jeder 4 endphasengelenkte Gefechtsköpfe enthält. Der Werfer hat eine Schußfolge von 50 Sekunden und es können 288 Projektile ins Ziel gebracht werden. Der Werfer schießt in Feindrichtung eine Rakete ab, die die Submunitionsträger auslegt. Diese Submunitionsträger gleiten an einem Fallschirm zu Boden und werden in einer Höhe von ca. 30m in Rotation versetzt, wobei Infrarotsensoren kreisflächenförmig die Oberfläche abtasten und die Projektile nach außen geschleudert werden. Wird ein Ziel (z.B. heißer Motor eines Fahrzeuges) erkannt, durchschlägt das Projektil die Panzerung und explodiert. Im anderen Fall detoniert der Sprengkörper als Splitterbombe [9, S.115 f].

MW-1 Die Projektkosten diese Systems belaufen sich auf 3,5 Milliarden DM. Bei MW-1 handelt es sich um ein luftgestütztes System, das gegen Ziele im Hinterland (z.B. Panzer, Fahrzeugansammlungen oder Flugplätze) entwickelt wurde. Es ist ca. 4.600 kg schwer und zum Einbau unter das Mehrzweckkampfflugzeug Tornado geplant, von wo die 112 Submunitionsträger im Einsatzfall seitlich weggeschleudert werden. Die Submunitionsträger können mit verschieden Submunitionsarten geladen werden. Hierbei sind besonders die Tandem-Projektile zum Zerstören gegnerischer Flugplätze von Bedeutung. Ihre erste Ladung durchschlägt die Piste und die zweite detoniert unter ihr und reißt sie auf [9, S.116].

11.5.2 Kampfroboter mit Künstlicher Intelligenz

11.5.2.1 Prinzipielle Anforderungen

Grundsätzlich läßt sich sagen, daß die Anforderungen, die an einen Kampfroboter gestellt werden, den Anforderungen an einen zivilen autonomen Roboter ähneln So werden in ihm Konzepte verwirklicht sein müssen wie zum Beispiel

- Spracheingabe, Bilderkennung- und Verarbeitung und andere Kommunikationsschnittstellen,
- Motorik zur Bewegung in Outdoor Umgebungen,
- motorischer Apparat zur Durchführung der anwendungsspezifischen Aufgaben,
- Mechanismen zur Einbindung in die militärische Befehlshierarchie,
- Expertenwissen über militärische Situationen und über das Anwendungsgebiet und
- Mechanismen, sich der Befehlsgewalt des Gegners zu entziehen.

11.5.2.2 Vorteile des Einsatzes von Robotern

Die Vorteile von Robotern gegenüber Menschen bei einen militärischen Einsatz können im wesentlichen in den folgenden Kriterien zusammengefaßt werden [9, S128]:

- Einsatz in verseuchten, gefährlichen und schwer zugänglichen Gegenden möglich
- Wirtschaftlichkeit im Friedensfall
- eventuell (je nach Einsatzgebiet) bieten Roboter erhöhte Präzision, Geschwindigkeit und Beweglichkeit
- verbesserte „Modernisierbarkeit“ des zukünftigen „Soldaten“
- weniger Probleme im System von Befehl und Gehorsam
- bessere Wiederverwertbarkeit des „eingesetzten Materials“, als bei Einsatz von „Menschenmaterial“

11.5.2.3 Einsatzmöglichkeiten

Die Einsatzmöglichkeiten für Kampfroboter könnten wie folgt aussehen [9, S.134 ff]:

- **Einsatz in der Gefechtsführung**
  - Verwendung von Robotern in der Logistik und der Personaldatenverarbeitung
  - Einsatz in Täuschungsgefechtständen
  - Als Träger eines mobilen Expertensystem zur Unterstützung der Gefechtsführung
  - Aufgaben der elektronischen Kampfführung, der Kommunikationsherstellung (wichtig für multinationale Kampfeinheiten) und der Verschlüsselung
- **Einsatz im direkten Gefecht**

  Roboter-Wachposten, Luftraumbeobachter, Feuerleitroboter, ABC - Melde-und Abwehrtrupps, Dekontamination und Bergung von Toten und Verwundeten sind Beispiele für einen Einsatz im direkten Kampfgebiet.
- **Einsatz als Minenleger**

  Roboter können die gefährliche Aufgabe des Legens und Beseitigens von Minen übernehmen.
- **Einsatz im Lazarett**

  Im Feldlazarett können sie als „eiserne Krankenschwestern“ die Zahl der direkt in den Konflikt verwickelten Menschen vermindern.

11.5.3 Bedeutung

Diese Waffen haben für das Air-Land-Battle-2000-Konzept die wohl größte Bedeutung, da sie als konventionelle Waffen Vernichtungspotentiale wie Atomwaffen erreichen [9, S.118]. Daneben begrenzt die Zielgerichtetheit solcher Systeme den Schaden, der an der Umgebung angerichtet wird und erhöht die Nutzbarkeit des eroberten Landes.

11.5.4 Risiken

Der Roboter wird wegen seiner programmierten Intelligenz dazu beitragen, den Krieg weiter zu entmenschlichen. Durch die programmierbare Befehlsstruktur kann der Roboter zum Handlanger von Kriminellen werden. Das Fehlen von Erfahrungen über den Kriegseinsatz von Robotern erhöht das Kriegsrisiko, da man sich über ihre tatsächliche Einsatzmöglichkeiten täuscht. Für künftige Verhandlungen stellt sich die Frage, ob diese Waffen noch die Bezeichnung konventionell tragen sollten.

11.6 Perspektiven zur Verhinderung eines Krieges aus Versehen

11.6.1 Technische Perspektiven

Hier gilt es, in erster Linie das Verhältnis und die Akzeptanz von Technik neu zu überdenken. Die technischen Einrichtungen haben auf dem militärischen Sektor einen Grad erreicht, in dem der kleinste Fehler den Untergang der Menschheit zur Folge haben kann. Damit sind höchste Anforderungen an die Sicherheit in diesen Systemen gestellt. Hier sind Fehlertoleranz, Robustheit, Zuverlässigkeit, und Geschwindigkeit nur Auszüge aus dem großen Katalog der Anforderungen. Grundsätzlich aber läßt sich bereits heute schon absehen, daß die technischen Präventivmaßnahmen keinen hochprozentigen Schutz vor einem Krieg aus Versehen bieten. Aus diesem Grund legten 1983 fünf nahmhafte Professoren gegen die Mitwirkung der Bundesregierung am *Aufbau und Betrieb eines Frühwarn- und Entscheidungssystems für atomare und militärische Auseinandersetzungen in Europa* Verfassungsbeschwerde ein [91].

11.6.2 Politische Perspektiven

11.6.2.1 Beispiele für politische Lösungsansätze

ABM-Vertrag Der ABM (Anti Ballistic Missile) Vertrag regelt die Stationierung von Antisatelliten und Antiraketen Systemen. Er gilt als bedeutender Vertrag insofern, als hier in relativ kurzer Zeit eine tragfähige Lösung zustande kam, in der beide Supermächte der anderen Seite das Zweitschlagsrecht zugestand.

Die SALT-Verträge Die SALT (Strategic Arms Limitation Talks) Verträge zielen auf das Abstoppen des Wettrüstens. So war der SALT I Vertrag der erste Vertrag zwischen den USA und der UdSSR, der Obergrenzen für Massenvernichtungswaffen festlegt. Der SALT II Vertrag wurde zwar unterzeichnet, aber wegen der sowjetischen Invasion in Afganistan vom US-Senat nicht ratifiziert.

Die START-Verhandlungen Die START (Strategic Arms Reduction Talks) Verhandlungen sollen auf den SALT-Verhandlungen aufbauen. Sie werden zwar mit nur mäßigen Ergebnissen weitergeführt, tragen aber dazu bei, Abrüstungsrichtlinien und Normen sowie die Probleme der Überprüfbarkeit der Vereinbarungen zu diskutieren.

Das Mittelstrecken-Raketen Abkommen Dieses Abkommen steht in der Folge der START-Verhandlungen. Zum ersten Mal in der Kriegsgeschichte haben sich potentielle Gegner darauf geeinigt, neue Systeme zu begrenzen und bereits stationierte zu verschrotten.

Die MBFR-Verhandlungen Die MBFR (Mutual Ballance Forces Reduction Talks) in Wien wurden nach 15 Verhandlungsjahren in diesem Jahr offiziell ergebnislos abgebrochen, um neuen Verhandlungen Raum zu geben. In diesen Gesprächen haben die Nato und der Warschauer Pakt Probleme konventioneller Abrüstung erörtet. Dabei waren vor allem die Vergeichbarkeit, die Erstellung militärischer Normen und die Überprüfbarkeit der konventionellen Armeen, sowie die Herstellung eines stabilen militärischen Gleichgewichts von Bedeutung.

11.6.2.2 Beurteilung der politischen Ansätze

Zu den Versuchen den Krieg aus Versehen durch **vertrauensbildende Maßnahmen** zu verhindern gibt es wohl keine Alternativen. Allein die strategische Stabilisierung gibt beiden Seiten die Sicherheit, zu deren Erhaltung heute der risikoträchtige Zweitschlags-Militärapparat benötigt wird. Besitzen aber beide Kontrahenten keine Angriffsfähigkeit, weder auf konventionellem noch auf atomarem Gebiet, so besteht die Hoffnung, daß ein Krieg aus Versehen verhindert werden kann.

Literatur

[1] **W. Ameling** *Simulationstechnik – 5. Symposium Simulationstechnik Aachen, September 1988* (1988) Springer-Verlag, Berlin Heidelberg

[2] **K. Backhaus, B. Erichson, W. Plinke, Chr. Schuchard-Ficher, R. Weiber** *Multivariate Analysemethoden – Eine anwendungsorientierte Einführung* (1986) Springer-Verlag, Berlin Heidelberg

[3] **H. Bähren** *Wissenschaft und Rüstung* (1985) Steinweg-Verlag

[4] **Wolfgang Baier, Rainer Salm** *Betriebsvereinbarung zur Personaldatenverarbeitung* (1986) in Die Mitbestimmung Nr.11, S.621-623, Hans-Böckler-Stiftung, Düsseldorf

[5] **W. Ballin, H. Lüke** *Sicherheit in Betriebssystemen* (1981) Vorlesungsskript, Universität Karlsruhe

[6] **K. Bauknecht, J. Kohllas, C. A. Zehnder** *Simulationstechnik – Entwurf und Simulation von Systemen auf digitalen Rechenautomaten* (1976) Springer-Verlag, Berlin Heidelberg

[7] **Dr. Baumann** *9. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz* (1987) Bundestagsdrucksache 10/6816

[8] **Dr. Baumann** *10. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz* (1988) Bundestagsdrucksache 11/1693

[9] **J. Birkenbach** *Wissenschaft und Frieden* (1985) J. A. Koch

[10] **Jochen Boelsche** *Der Weg in den Überwachungsstaat* (1988) Rowohlt, Hamburg

[11] **K.-H. Böker** *Verantwortung des Informatikers* (1987) Universität Paderborn

[12] **Frank Braatz** *Neue Technologien und die gewerkschaftliche Diskussion um ihre sozialverträgliche Gestaltung am Beispiel der Auseinandersetzung um Personalinformationssysteme* (1988) Werkstattbericht 39, Ministerium für Arbeit, Gesundheit und Soziales, NRW, Düsseldorf

[13] **P. Bracken** *The Command and Control of Nuclear Forces* (1983) Yale University Press

[14] **Prof. Dr. Klaus Brunnstein** *PC-Viren: Dichtung und Wahrheit* (1988) Computer Magazin 9'88, S.47-49

[15] **Christian K. Bschorr** *Computerkriminalität* (1987) ECON-Verlag

[16] **Hans-Peter Bull** *Ziele und Mittel des Datenschutzes* (1981) Athenäum, Königstein/Ts.

[17] **Hans-Peter Bull** *Datenschutz oder die Angst vor dem Computer* (1984) Piper, München

[18] **Hans-Jörg Bullinger** *Testanwendung in der Arbeitswelt* (1979) Giradet Taschenbücher

[19] **Bundesregierung** *Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes des Bundes und der Länder* (1986) Bundesregierung, Bonn

[20] **N. P. Buslenko** *Simulation von Produktionsprozessen* (1971) B. G. Teubner Verlagsgesellschaft, Leipzig

[21] **CILIP** *CILIP 31* (1988) Kirschkern, Berlin

[22] **Jens Clausen** *Personalinformationssysteme durch Betriebsvereinbarungen entschärfen* (1986) in Die Mitbestimmung Nr.11, S.619-620, Hans-Böckler-Stiftung, Düsseldorf

[23] **Chaos Computer Club** *Das Chaos Computer Buch* (1988) Rowohlt Verlag

[24] **Fred Cohen** *Comuter Viruses* (1987) Computers & Security, Vol.6, S.22-35

[25] **DGB** *Personal-Datenverarbeitung (Freitag, der 13. – Ein ganz normaler Arbeitstag)* (1988) DGB-Bundesvorstand, Düsseldorf

[26] **DGB-Bundesvorstand** *Datenschutzfibel* (1980) DGB-Bundesvorstand, Abt. Werbung, Düsseldorf

[27] **Datenschutzkommission Rheinland-Pfalz** *Unterrichtung durch die Datenschutzkommission Rheinland-Pfalz 1985-1987* (1988) Rheinland-Pfälzische Landesregierung, Mainz

[28] **Wolfgang Däubler** *Mitbestimmung des Betriebsrats bei innerbetrieblicher Vernetzung* (1987) in Die Mitbestimmung Nr.5, S.264-266, Hans-Böckler-Stiftung, Düsseldorf

[29] **Peter J. Denning** *Computer Viruses* (1988) Americam Scientist, Vol.76, S.236-238

[30] **Deutsches Institut für Betriebswirtschaft e.V.** *Datenschutz im Betrieb* (1978) Erich Schmidt Verlag, Berlin

[31] **A. K. Dewdney** *Computer Recreations* (1989) Scientific American, March 89, S.90-93

[32] **W. Diffie, M. E. Hellman** *New Directions In Cryptography* (1976) IEEE Information Theory

[33] **K. R. Dittrich** *Datenschutz* (1979) Skript, Universität Karlsruhe

[34] **Dr. Einwag** *11. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz* (1989) Bundestagsdrucksache 11/3932

[35] **H. Exner, N. Schmitz** *Zufallszahlen für Simulationen* (1983) Institut für Mathematische Statistik der Westfälischen Wilhelms-Universität Münster, Münster

[36] **Jürgen Fickert, Herbert Kubicek, Rolf Reihsner** *Vernetzung und Integration von EDV-Systemen, Auswirkungen auf Beschäftigte – Handlungsmöglichkeiten für Betriebs- und Personalräte* (1988) Heft 10 der Technologieberatungsstelle beim DGB-Landesbezirk NRW, Oberhausen

[37] **H. Finer** *Dullez over Suez* (1964) Chicago Quadroupel

[38] **Reinhold Franck** *Unterschiedliche Ansätze zur Weiterentwicklung der Informatik* (1987) in Umdenken in der Informatik, Elefanten Press, Berlin

[39] **P. Gola, K. Hümmerich, U. Kerstan** *Datenschutzrecht, Teil 2: Einzelvorschriften des Bundes zum Datenschutz* (1978) J. Schweitzer Verlag, Berlin

[40] **J. M. Hammersley** *Monte-Carlo-Methods* (1964) Methuen & Co. Ltd., London

[41] **G. Hart, B. Goldwater** *Recent False Alerts from the Nation's Missile Attack Warning System* (1980) Commitee on Armed

[42] **H. L. Hausen, M. Müllerburg und M. Schmidt** *Über das Prüfen, Messen und Bewerten von Software* (1987) in Informatik Spektrum Nr.10, S.123-144, Springer, Berlin

[43] **Werner Heine** *Die Hacker* (1985) Rowohlt Taschenbuch Verlag

[44] **L. Heinrich, M. Pils** *Betriebsinformatik im Personalbereich* (1979) Physica-Verlag, Würzburg-Wien

[45] **Landesregierung Hessen** *Informationsgesellschaft oder Überwachungsstaat?, Gutachten* (1984) Symposium der hessischen Landesregierung, Wiesbaden

[46] **Dr. Harold Joseph Highland** *Random Bits & Bytes* (1988) Computers & Security, Vol.7, S.3-11

[47] **Harald Hohmann** *Freiheitssicherung durch Datenschutz* (1987) Suhrkamp, Frankfurt

[48] **Patrick Horster** *Kryptologie* (1985) BI, Wien

[49] **R. K. Huber, J. G. Taylor** *A Tactical Air War Analysis Game* (1980) Hochschule der Bundeswehr, München

[50] **Humanistische Union** *Sicherheitsgesetze – Notstandsgesetze für den alltäglichen Gebrauch?* (1988) Humanistische Union, München

[51] **IGM** *Gläserner Mensch – Gläserne Arbeit* (1984) IGM Bundesvorstand, Abteilung Automation/Technologie, Frankfurt

[52] **IGM** *Seminar-Modell Personalinformationssysteme* (1985) IGM Bundesvorstand, Abteilung Bildungswesen/Bildungspolitik, Frankfurt

[53] **B. Jasani** *Waffen im Weltraum* (1985) rororo Taschenbuch

[54] **KFA Jülich** *Computersimulation in der Physik* (1989) KFA Jülich

[55] **H. Kahn** *Methods of Reducing Sample Size in Monte-Carlo-Computations* (1953) in Operations Research, Vol.1

[56] **H. Kahn** *Use of Different Monte-Carlo-Sampling-Techniques* (1958) in Symposium on Monte-Carlo-Methods, J. Wiley & Sons Inc., New York

[57] **Wolfgang Kilian** *Personalinformationssysteme in deutschen Großunternehmen* (1981) Springer-Verlag, Berlin Heidelberg New York

[58] **Lutz Klingelhöfer** *Personaleinsatzplanung durch ein computergestütztes Informationssystem* (1975) Verlag Harry Deutsch, Frankfurt, Zürich

[59] **Hermann Kopetz** *Software-Zuverlässigkeit* (1976) Carl Hanser, München Wien

[60] **R. Koxholt** *Die Simulation – ein Hilfsmittel der Unternehmensforschung* (1967) R. Oldenbourg, München

[61] **Manfred Kraft** *Verhaltensweise von Programmierern und deren Einflüsse auf die Produktion von Software* (1983) in H. Schelle, P. Molzberger: Psychologische Aspekte der Software-Entwicklung, R. Oldenbourg, München Wien

[62] **S. Krüger** *Simulation – Grundlagen, Techniken, Anwendungen* (1974) W. de Gruyter, Berlin

[63] **Michael Loewe, Rudolf Wilhelm (Hrsg.)** *Risiken polizeilicher DV* (1988) in Schöne neue Computerwelt, VAS, Berlin

[64] **Karlheinz Merten** *Datenschutz und DV-Probleme bei den Sicherheitsbehörden* (1985) Kriminalistik-Verlag, Heidelberg

[65] **Model, Creifelds** *Staatsbürgerliches Taschenbuch* (1982) Ch. Beck Verlag, München

[66] **Heiner Müller-Merbach** *Systemanalyse als gelenkter kreativer Prozeß* (1983) in H. Schelle, P. Molzberger: Psychologische Aspekte der Software-Entwicklung, R. Oldenbourg, München Wien

[67] **Jürgen Nehmer** *Betriebssysteme* (1988) Skript, Universität Kaiserslautern

[68] **Peter G. Neumann** *Letter From The Editor* (1983) ACM SIGSOFT: Software Engineering Notes Vol.8, No.3

[69] **Peter G. Neumann** *Letter From The Editor* (1984) ACM SIGSOFT: Software Engineering Notes Vol.9, No.5

[70] **Peter G. Neumann** *Letter From The Editor* (1985) ACM SIGSOFT: Software Engineering Notes Vol.10, No.2

[71] **Peter G. Neumann** *Risks To The Public In Computer Systems* (1983) ACM SIGSOFT: Software Engineering Notes Vol.10 No 3

[72] **J. Perry** *Winning Through Sophistication* (1982) Technology Review

[73] **Jörg Peter** *Protect* (1989) Toolbox, Vol.1, S.58-63

[74] **J. Piehler, H.-U. Zschiesche** *Simulationsmethoden* (1975) B. G. Teubner Verlagsgesellschaft, Leipzig

[75] **Maria M. Pozzo, Terence E. Gray** *An Approach to Containing Computer Viruses* (1987) Computers & Security, Vol.6, S.321-331

[76] **D. Reppmann, E. Waibel** *Schulungssimulatoren für Kernkraftwerke in: Jahrestagung Kerntechnik 1985* (1985) Deutsches Atomforum e.V., Heussallee 10, 5300 Bonn 1

[77] **L. Richter** *Betriebssysteme* (1977) Teubner, Stuttgart

[78] **Hans-Jürgen Risch** *Angst vor Computer-Viren* (1988) c't, Heft 7, S.70-71

[79] **Hans-Jürgen Risch** *Latente Bedrohung* (1988) c't, Heft 7, S.84-88

[80] **D. Ruloff** *Konfliktlösung durch Vermittlung: Computersimulation zwischenstaatlicher Krisen* (1975) Birkhäuser Verlag, Basel Stuttgart

[81] **Horst Sackstetter** *Überwachung in Untertürkheim: Daimler-Benz* (1984) in Chips & Kabel Nr.13 Dezember-Heft, S.11-16, Kommedia Medienbuchladen GmbH, Berlin

[82] **Martin Schlöter** *Zauberlehrlinge und Geister* (1989) Toolbox, Vol.1, S.48-50

[83] **Egon Schmidt** *Computerviren – wie sie schaden, was sie nutzen* (1987) Computerwoche 3. April, S.42-47

[84] **Karl Schmitz** *PAISY durchleuchtet* (1984) in Chips & Kabel Nr.13 Dezember-Heft, S.6-10, Kommedia Medienbuchladen GmbH, Berlin

[85] **Dr. Gerhard Schneider** *Der Bürger und seine Daten* (1985) Der Landesbeauftragte für Datenschutz, Saarland, Saarbrücken

[86] **A. Schöne** *Simulation technischer Systeme, Band 2* (1976) Carl Hanser Verlag, München Wien

[87] **A. Schöne** *Simulation technischer Systeme, Band 3* (1974) Carl Hanser Verlag, München Wien

[88] **A. Schöne** *Simulation technischer Systeme, Band 1* (1974) Carl Hanser Verlag, München Wien

[89] **Eggert Schwan** *Auf dem Weg zum Überwachungsstaat?* (1987) in Hohmann: Freiheitssicherung durch Datenschutz, Suhrkamp, Frankfurt

[90] **Jürgen Seifert** *Der Lauschangriff als Erhebung personenbezogener Daten* (1987) in Hohmann: Freiheitssicherung durch Datenschutz, Suhrkamp, Frankfurt

[91] **Jörg H. Siekmann** *Verfassungsbeschwerde* (1983) Karlsruhe

[92] **Spiros Simitis** *16. Tätigkeitsbericht des hessischen Datenschutzbeauftragten* (1987) hessische Landesregierung, Wiesbaden

[93] **Spiros Simitis** *17. Tätigkeitsbericht des hessischen Datenschutzbeauftragten* (1988) hessische Landesregierung, Wiesbaden

[94] **Harry M. Sneed** *Software-Entwicklungsmethodik* (1980) Rudolf Müller GmbH, Köln-Braunsfeld

[95] **Harry M. Sneed** *Software-Testen* (1988) in Informatik Spektrum Nr.11, S.303-311, Springer, Berlin

[96] **Wilhelm Steinmüller** *Zehn Punkte gegen Personalbespitzelung* (1984) in Chips & Kabel Nr.13 Dezember-Heft, S.17-21, Kommedia Medienbuchladen GmbH, Berlin

[97] **Tinnefeld, Tubies** *Datenschutzrecht* (1988) Oldenbourg, München

[98] **J. Tirman** *SDI – Der Krieg im Weltraum* (1986) Scherz-Verlag

[99] **Jay Tuck** *Die Computer-Spione* (1984) Wilhelm Heyne Verlag, München

[100] **Gerhard Weck** *Datensicherheit* (1984) Teubner, Stuttgart

[101] **Horst Wettstein** *Aufbau und Struktur von Betriebssystemen* (1978) Hanser, Wien

[102] **Jan Witt** *Zur Quantifizierung von Software* (1987) in Informatik Spektrum Nr.10, S.121-122, Springer, Berlin

[103] **Hans Wohlgemuth** *Datenschutz bei konzernweiter Personaldatenverarbeitung* (1987) in Die Mitbestimmung Nr.5, S.271-272, Hans-Böckler-Stiftung, Düsseldorf

Index