dem AGB-Gesetz zu achten ist. Nicht vergessen werden darf die Regelung der Mitwirkungspflichten des Auftraggebers.

Mit diesen Mitwirkungspflichten des Anwenders bei Wartung und Pflege von EDV-Systemen befaßte sich RA Dr. *F. A. Koch,* München. Er stellte zwei Thesen auf:

1. Es gibt keinen einheitlich formulierbaren Katalog der Mitwirkungspflichten des Anwenders. Art und Umfang der jeweiligen Pflichten können nur anwendungsspezifisch formuliert werden.

2. Vielfach ist die Tendenz feststellbar, die Anwenderpflichten der Mitwirkung auszuweiten, um hierdurch den Risikobereich des Anbieters einzuschränken. Dies kann im Ergebnis zu erhöhter Unsicherheit für beide Seiten führen. Maintenance komplexerer Systeme erfordert ein stetes Anpassen der Erfüllungskriterien für Leistungs- und Mitwirkungspflichten an neue Gegebenheiten und erweiternder Anwendungsbedingungen. Diese Probleme machen deutlich, wie wichtig eine gute Zusammenarbeit zwischen Anwender und Software-Lieferant ist; vielleicht kann sogar von einer Kooperationspflicht des Software-Anwenders gesprochen werden. Dementsprechend sorgfältig und genau müssen die EDV-Verträge — auf welche Teilaspekte sie sich auch immer beziehen — ausgestaltet sein.

Zur Bewertung der Software in der Bilanz nahm *H.-J. Weiss,* Wirtschaftsprüfer und Steuerberater, Andersen & Co. GmbH, Stuttgart, Stellung. Die Entwicklung von Software durch das Software-Haus läßt sich nicht als Vorräte aktivieren, da kein Auftragsverhältnis (Kaufvertrag) vorliegt. Unklar ist, ob es sich um Anlagevermögen handelt. Selbst wenn dies bejaht wird, besteht für immaterielle Wirtschaftsgüter ein Aktivierungsverbot. Eine gängige, wenn auch strittige Lösung ist die Gestaltung über eine Entwicklungs- und eine Vertriebsgesellschaft. Am Anteilskauf bzw. -verkauf eines Software-Hauses soll der Teilwert einer Software beim Hersteller auf der Basis eines Ertragswertes ermittelt werden, wobei aus Planungsrechnungen der Ertrag der einzelnen Software-Produkte errechnet und kapitalisiert werden kann.

Juristisch noch vollkommen ungeklärt ist die Frage des Schicksals einer Software-Lizenz im Konkurs des Software-Herstellers. Geht man davon aus, daß die im Konkurs befangene Software urheberrechtlich geschützt ist, so ist zu bedenken, daß eine Exekution in Urheberrechte nicht möglich ist, sondern nur in die Verwertungsrechte, hier vor allem in das Bearbeitungsrecht. Handelt es sich um nicht urheberrechtlich geschützte Software, so ist als Vorfrage zu klären, ob es sich um ein Pacht-, Lizenz- oder Kaufverhältnis handelt. Ferner ist zwischen Individual- und Standardsoftware zu unterscheiden. Eine Lösungsmöglichkeit wäre die Schaffung eines Treuhandverhältnisses, im Rahmen dessen der Source-Code versiegelt bei einem Treuhänder hinterlegt wird, wobei vertraglich festgelegt wird, daß der Treuhänder den Source-Code bei Vorliegen bestimmter Umstände (z. B. Konkurs) an den Anwender herausgeben muß. Hierbei ist zu überlegen, ob der Treuhandvertrag in den Lizenzvertrag eingebunden sein soll, ob Treugeber nur der Software-Hersteller oder auch der Software-Erwerber sein soll, ob eine solche Konstruktion zweier Treugeber im Rahmen einer BGB-Gesellschaft erfolgen kann, wie kontrolliert werden kann, daß der Software-Hersteller immer die aktuelle Version des Source-Codes dem Treuhänder übergibt, wer Treuhänder sein soll bzw. dazu in der Lage ist.

Dieser Kongreß hat viele Fragen aufgeworfen und gezeigt, daß den Juristen noch einige Arbeit bevorsteht. Doch sollte bei künstigen Veranstaltungen darauf geachtet werden, daß juristische Aspekte des Computerrechts verstärkt aus dogmatischer Sicht behandelt werden. Denn nur auf einer wissenschaftlich fundierten Basis können den Beteiligten juristisch einwandfreie Lösungen angeboten werden. Managementmaßnahmen können immer nur juristische Maßnahmen ergänzen, für die Praxis erstellte juristische Lösungsmöglichkeiten müssen aber stets auf dogmatisch gesicherten Erkenntnissen aufbauen.

RAA Dr. Moritz Röttinger (Wien)

Tagung „Strategien zum Software-Know-how-Schutz für Anwender und Hersteller"

Die Gesellschaft für Informatik führte zu diesem Thema am 20. und 21. Mai 1987 in Bad Godesberg eine Tagung durch, um das Informationsbedürfnis von DV-Praktikern unter den Aspekten Recht, Technik und Versicherbarkeit zu befriedigen.

Sieber (Freiburg) führte in seinem Beitrag „Der Rechtsschutz der Computersoftware" aus, daß das Strafrecht gegen Softwarediebstahl wenig helfe, auch nicht nach der Reform von 1986, das spezielle Strafvorschriften im Hinblick auf Computer einführte. Da der Patentschutz nur ausnahmsweise eingreife, könne Schutz vor allem durch das Urheberrechtsgesetz erreicht werden. Da dieses nicht nur Unterlassungs- und Schadensersatzansprüche, sondern auch Strafvorschriften vorsehe, ermögliche es, die Strafverfolgungsbehörden einzuschalten und damit wesentlich günstiger an Beweismittel zu kommen.

Das Wettbewerbsrecht (UWG) verbiete in Ergänzung des Urheberrechts bestimmte Handlungen. Nach allgemeinem Arbeitsrecht dürfe der Angestellte zwar alles normal erlangte Wissen nach Beendigung des Arbeitsverhältnisses nutzen, er dürfe aber keine Unterla-

gen für sich kopieren. Dementsprechend sei auch das, was nach Urheberrecht schon eine freie Benutzung sei, hier oft noch verbotene Ausnutzung.

Die Absicherung liege erst einmal in der sorgfältigen Abfassung von Verträgen mit Mitarbeitern und mit Auftragnehmern. Sodann sind vorbeugende Maßnahmen zu treffen, die eine einfache Identifikation der Programme erlauben würden. Die Kontrolle der Mitarbeiter sei auf Grund der bisherigen Erfahrungen wichtig, insb. bei deren Ausscheiden.

Seit dem 1. 4. 1987 sei in der Strafprozeßordnung verankert, daß der Verletzte bei berechtigtem Interesse Einblick in die Strafermittlungsakten verlangen könne. Inwieweit auf dem Zivilrechtsweg Auskunft verlangt werden könne, sei in der Praxis noch nicht geklärt.

RA Axel Bauer (Hamburg) zeichnete in seinem Referat „Wie weist man eine Urheberrechtsverletzung technisch und rechtlich nach" die Grundsatzentscheidung des BGH „Inkassoprogramm" nach, die eine hohe gestalterische Leistung in der Darstellung verlange. Daraus ergebe sich als erste Stufe, die schöpferische Darstellung des eigenen Programms vorzutragen, in der zweiten Stufe dann, die Verletzung im urheberrechtlich relevanten Bereich vorzutragen und natürlich auch nachzuweisen.

Bauer will den Bereich des Urheberrechtsschutzes dadurch erweitern, daß er das Schwergewicht auf die Codierung legt. Es würden häufig nicht so phasenmäßig Dokumente erstellt werden, wie das der BGH auf der Basis der Softwaretechnologie der 70iger Jahre gesehen habe. Es gäbe heute auch viele Hilfsmittel, die der Kreativität Raum geben würden.

Bauer gab Hinweise, wie bei Fehlen des Quellcodes die Verletzung nachgewiesen werden könne, auch wenn es sich nicht um eine identische Kopie handele:

- Vergleich der Gestaltung von Bildschirmmasken und Listen und von Abläufen,
- Vergleich von identischen Elementen, z. B. von untypischen Abkürzungen,
- Rückkompilierung — falls möglich,
- Vergleich der beiden Programme in hexadezimalem Ausdruck hinsichtlich identischer Zeichenfolgen,
- Ablaufanalyse mit Hilfe eines Debugger-Programms, was die innere Struktur des Ablaufs zu vergleichen erlaubt,
- Identische Programmfehler.

RA Dr. Koch (München) führte die Zuhörer in die in der juristischen Literatur verschiedentlich aufgeführte „Abhängigkeit des Arbeitgebers vom angestellten Programmurheber" ein. Den Bereich des Arbeitgebers, der die Programme nicht als Anwender, sondern als Anbieter nutze, klammerte er als wenig problematisch aus. Es gäbe eine Reihe zwar weniger wichtige, aber ungeklärter Fragen. Es empfehle sich, die Fragen im Vertrag schriftlich zu klären.

Sieber führte zur „Computerkriminalität" aus, daß jede neue Technik neuen Mißbrauch mit sich bringe. Der Computer ermögliche Mißbrauch in wesentlich größerem Umfange und begünstige den Täter zugleich durch schlechtere Kontroll- und Nachweismöglichkeiten. Beweismittel könnten oft DV-technisch vernichtet werden. Kontrollmaßnahmen auf normalem Niveau könnten relativ leicht umgangen werden. Die Tendenz ginge von der Schädigung durch eigene Mitarbeiter zur Schädigung durch Dritte, seien es Auftragnehmer oder Dritte (z. B. Hacker).

Die Lücken im deutschen Strafrecht seien durch die Reform 1986 geschlossen; die neuen Vorschriften müßten in der Praxis noch umgesetzt werden. Auf OECD- und EG-Ebene seien Reformbestrebungen in Gange. Zum Datenschutzstrafrecht beklagte Sieber die vage Formulierung der Strafbestimmungen.

Es bedürfe eines mehrstufigen Sicherungskonzepts, wobei keine absolute Sicherheit erwartet werden dürfe:

— Verhindern (personell, technisch, organisatorisch, präventiv)
— Protokollieren
— Schadensminderung; damit verbunden auch Verhinderung bzw. Verringerung der Auswirkungen bei fahrlässigen Bedienungsfehlern, Naturkatastrophen oder Streiks
— absichernde Maßnahmen: Hebung des Risikobewußtseins der Mitarbeiter
— Maßnahmen gegen Umgehung von Sicherungsmaßnahmen.

RA Dr. Zahrnt (Neckargemünd) schloß den Bereich der Rechtsfragen mit der Fragestellung ab „Wer erhält bei Werkverträgen und bei Überlassungsverträgen welche Rechte an den Programmen?". Bei Werkverträgen über die Erstellung von Individualprogrammen hänge die Antwort von den Interessen des Auftraggebers nicht nur von der eigenen Nutzung der Ergebnisse ab, sondern auch davon, inwieweit der Auftragnehmer von der Nutzung seinerseits im übrigen ausgeschlossen werden solle, sei es, daß der Auftragnehmer die Investition, sei es, daß er das gewonnene know-how nicht nutzen dürfe.

Bei der Überlassung von Standardprogrammen gehe es um eine Reihe von praktischen Fragen (z. B. auf wieviel DV-Anlagen der Anwender das Programm einsetzen darf), auf die es bisher kaum verbindliche Antworten gäbe. Die Antworten würden von der Einordnung dieses neuen Vertragstyps abhängen. Ansatz dafür sei eine neue Variante der Überlassung von know-how. Das Problem liege darin, daß diese Variante eine Reihe von Untervarianten habe, deren Anwendungsbereich ungeklärt sei.

Kiefer (IBM) brachte in seinem Beitrag „Ansatz eines Systems zur Informationssicherung" mehr als einen Ansatz zu diesem Problem. Den Ausgangspunkt bildete seine Erfahrung, daß im Rechenzentrum ziemlich viel getan worden sei, in der Hauptverwaltung einiges, in den Fachbereichen noch zu wenig. Es gäbe bereits partiell zuständige Funktionsträger in Sachen Informationsträger wie Datenschutzbeauftragte, Kontaktpersonen oder die Interne Revision, es komme aber darauf an, hier eine übergeordnete Aufgabe zu sehen, für die dementsprechend ein Funktionsträger auf höchster Managementebene anzusiedeln sei. Es könne Berater geben, die Funktion selber sei aber als Linienfunktion zu behandeln. Innerhalb der Linie sei insb. eine klare Berichtspflicht durchzusetzen.

Damit sei auch klar, daß die Verantwortung in erster Linie beim Fachbereich liegen müsse und nicht beim Rechenzentrum: Es ginge um Daten/Informationen des Fachbereichs und nicht des Rechenzentrums. Gerade hier mangele es oft am richtigen Bewußtsein bei allen Beteiligten.

Schmid (Gesellschaft zur Prüfung von Software GmbH) stellte unter dem Thema „Vertragliche Qualitätssicherung durch Gütezeichen für Software" das Verfahren zur Güteprüfung gemäß DIN V 66285/RAL GZ 901 in Form einer vertraglichen Vereinbarung zwischen Kunden und Lieferanten vor. Wer geprüfte Standardsoftware kaufe, brauche das also nicht mehr zu vereinbaren, weil diese Prüfung bereichts durchgeführt worden sei. Bei der Erstellung von Individualsoftware könne dieser Formulierungsvorschlag zu Grunde gelegt werden.

Bis heute sei das Gütezeichen — erst — 26mal erteilt worden. Als entscheidende Ursache für diese niedrige Zahl sei auf der Mitgliederversammlung der Gütegemeinschaft Software e.V. im Mai 1987 festgemacht worden, daß die Kundschaft nicht nach dem Gütezeichen gefragt habe. Alle anderen Gesichtspunkte seien nachrangig, auch die Frage der Kosten.

Schmid betonte die Vorteile einer Prüfanweisung, die eine bestimmte Menge an Prüfschritten im Hinblick auf die genau definierten Funktione habe, gegenüber dem Testen („Testen, testen, testen ... gegen nnbekannt").

Weck (Infodas) schilderte zum Thema „Technische Maßnahmen zur Absicherung gegen Viren" erst einmal die Gefahren: Die Verbreitung von Viren sei bei normalen Systemen fast nicht zu vermeiden und nur beschränkt zu erschweren. Mit einigen technischen Aufwand sei einiges zu machen, mit viel Aufwand — mit neuen Konzepten — sei viel zu machen. Dennoch endete Weck mit einer düsteren Progrnose, daß wir hier auf einer Zeitbombe sitzen würden.

RA Engel (Karlsruhe) begann den dritten Teil Versicherbarkeit rdit einem Überblick über „Die Produzentenhaftung für Software". Es sei anzunehmen, daß die Rechtsprechung Standardprogramme als Produkte ansehen werde, so daß der Weg für die Produzentenhaftung frei sei. Bisher seien Fälle der Produzentenhaftung für Software noch nicht vor Gericht gekommen.

Die Bereiche für fehlerhafte Programme seien zahlreich:

— Anwendung der Meß- und Regeltechnik
— Sicherungstechnik/Überwachungstechnik: Schaden könne auch durch Unterlassen entstehen
— Informationsdatenbanken (wenn die Informationen unmittelbar auf Personen/Sachen bezogen werden sollen)
— Programme, die auf andere Programme einwirken.

Borgmann (Haftpflichtverband der deutschen Industrie) stellte ein Konzept für die „Versicherbarkeit von Folgeschäden durch Fehler in der Informationsverarbeitung beim Anwender" jenseits bisher bekannter Versicherungsnormen (z.B. der Betriebsunterbrechungsversicherung dar). Das Potential rür Vermögensschäden sei groß.

Grundlage sei eine Überprüfung der EDV des Versicherungsinteressenten auf Risiken hinsichtlich Organisation, Ressourcen, Software und Operating. Der ermittelte Istzustand werde mit Sollvorstellungen verglichen; daraus würden Verbesserungsmaßnahmen abgeleitet werden. Da sich dann über alle versicherungsmäßig relevanten Faktoren Aussagen machen lassen würden, seien alle klassischen Bedingungen für Versicherbarkeit gegeben.

Noch werde kein solcher Versicherungsschutz angeboten; er werde aber kommen. Derzeit würde in seinem Hause versucht, die Risikofaktoren zu quantifizieren. Dabei sei man noch ziemlich am Anfang, ebenso wie bei der Formulierung der Police und der Prämienberechnung.

Heidinger (Hermes Kreditversicherung) stellte zum Thema „Versicherung gegen Computer-Mißbrauch" klar, daß es hier um vorsätzliche Schädigungen durch Vertrauenspersonen geht. Insgesamt würden Gefahren drohen

— von außen (ca. 40 Anschläge auf Rechenzentren pro Jahr)
— von der Fachabteilung — da würde der Schwerpunkt liegen —
— von der DV-Abteilung.

Es werde insgesamt eine Vielzahl von Versicherungen angeboten. Damit das nicht zur Doppeldeckung führe, müßten Ausschlüsse gemacht werden. Das erschwere die Vergleichbarkeit der Angebote.

Die Computer-Mißbrauchsversicherung bringe eine Reihe von Problemen mit sich, die zu einer Überarbeitung der Versicherungsbedingungen führen würden:

Der Schädiger müsse bisher festgestellt werden; da sei oft schwierig oder werde nicht gewünscht. Die Höhe des Schadens sei oft nicht feststellbar, insb. bei Computerspionage. Es würde auch gewünscht werden, z.B. Fremdprogrammierer, oder sogar Dritte außerhalb, die auf die EDV einwirken könnten, z.B. Hacker.

RA Dr. Christoph Zahrnt