Sicherheit in der Information

Autor(en): **Steiner, Albert P.**

Objekttyp: **Article**

Zeitschrift: **Schweizer Ingenieur und Architekt**

Band (Jahr): **110 (1992)**

Heft 10

PDF erstellt am: **28.04.2024**

Persistenter Link: https://doi.org/10.5169/seals-77871

Sicherheit in der Information

Das Ziel ist, die gesamte Problematik betreffend der Sicherheit in, um und mit der EDV und der EDV-Revision aufzudecken, transparent zu machen und Möglichkeiten zur Lösung aufzuzeigen, unabhängig von der betroffenen Einheit in Wirtschaft oder Verwaltung. Der Beitrag wendet sich an die Interessenten, die sich über dieses Thema informieren oder einen Überblick verschaffen wollen oder müssen, will die Verantwortlichkeiten für die Fragen der Sicherheit und EDV-Revision ansprechen, wendet sich an die Praktiker, an diejenigen, die mit der Ausführung, Ausgestaltung und Kontrolle beauftragt werden.

VON ALBERT P. STEINER, KÜSNACHT

Die elektronische Datenverarbeitung hält mit Riesenschritten in allen Bereichen des öffentlichen und privaten Lebens, der Verwaltung und der Wirtschaft Einzug. Alle sind in vielfältiger Form zu «Betroffenen» dieser neuen Art von Informationsverarbeitung geworden. Die Sicherheit in, um und mit der Datenverarbeitung ist zu einem Politikum geworden. Sie ist zu einer gewichtigen Managementaufgabe und -funktion herangewachsen.

Einleitung

Was bedeutet Sicherheit? Sicherheit bedeutet in erster Linie Wissen. Wissen um die Gefahren, mit denen zu rechnen ist, und Wissen um die Möglichkeiten, mit denen den Gefahren begegnet werden kann. Das heisst, Sicherheit bedeutet Systematik, aber auch Koordination, Technik, Information, Diskussion, Vergleich und Kontrolle.

Dieses Ziel soll durch die stufenweise Aufgliederung und Vertiefung der Deskriptoren Wirtschaftskriminalität, Computerkriminalität, Datensicherungssystem und EDV-Revision erreicht werden.

Das Zielsystem

Die Bedeutung und der Wert der Datenverarbeitung hat mit dem Einzug der Elektronik, der fortschreitenden Automation, der rasanten technischen Entwicklung und der zunehmenden Integration der EDV in alle Bereiche der Verwaltung und des Wirtschafts-Unternehmens neue Dimensionen erreicht. Der Machteinfluss einerseits, der sich durch die Konzentration, die Fülle und die beliebige Kombinierbarkeit immer relevanterer Daten an einem Ort ergibt, aber auch die Abhängigkeit und die Folgen bei bewusstem Missbrauch, Zerstörung oder Verfälschung und aus Mängel in der Organisation entstandene Schäden andererseits werden immer grösser. Der Manipulation von Daten werden Tür und Tor geöffnet, was insbesondere im personenbezogenen Datenbereich ein grosses Unbehagen auslöst, aber auch fehlerhafte oder falsche Daten können betriebswirtschaftlich katastrophale Auswirkungen haben.

Datenschutz/Datensicherheit

Aus dieser Situation resultiert der scheinbare Dualismus von Datenschutz – dem Ruf und der Forderung nach Bewahrung der persönlichen Interessensphäre des Einzelnen und von Datensicherung – dem Verlangen nach Fehlerfreiheit, Genauigkeit und umfassender Information des Datenverarbeitenden. Dieser Dualismus ist aber nur scheinbar, da beide Forderungen dasselbe Endziel verfolgen und auch praktisch dieselben Methoden zu ihrer Erfüllung aufweisen. Hierbei gilt es, die Datenverarbeitung funktionell, wirtschaftlich, ordnungsgemäss und sicher abzuwickeln, um das Vertrauen in die Integrität und Zuverlässigkeit der EDV wiederherzustellen, kurz: die Sicherheit in der Daterverarbeitung zu gewährleisten.

Planmässiges Vorgehen

Sicherheit kann aber nicht den Ansätzen und Lösungen einzelner überlassen werden. Sicherheit verlangt planmässiges, systematisches Vorgehen. Sie verlangt den Einsatz von der Wirtschaft, der Behörde, der Gesetzgebung, von uns allen. Sicherheit bedeutet aber auch permanente Kontrolle, d.h. Hinweise auf vorhandene Schwachstellen geben und Möglichkeiten zu strafbaren Handlungen aufzeigen. Hierbei werden interne und externe Revisionen direkt mit EDV-spezifischen Problemen konfrontiert. Ohne fundierte Ausbildung und dem Einsatz technischer Hilfsmittel ist eine sachgerechte EDV-Prüfung nicht durchführbar. Zu ihrer Auftragserfüllung bedarf die Revision der fachspezifischen Unterstützung. Eine Aufgabe, die es in der Folge der EDV-Revision zu übertragen gilt.

Inhalt und Abgrenzung

Der wachsende Einsatz der elektronischen Datenverarbeitung (EDV) in allen Bereichen der Unternehmung und Verwaltung unter Verwendung von Datenbanken hat zur Folge, dass an einem einzigen Ort immer mehr und gewichtigere Informationen gespeichert, verarbeitet und ausgewertet werden. Diese Informations-Konzentration und die damit verbundene Informations-Vormachtstellung setzt den Inhaber solcher Datenzentren der zunehmenden Kritik und den verschiedensten Gefahren aus. Präventivmassnahmen gesetzlicher und organisatorischer Art zur Gewährleistung der Sicherheit in, um und mit der Datenverarbeitung sind heute aktueller denn je. Sicherheit verlangt Systemdenken, fordert ein Systemkonzept

Gefahrenbereiche

Es gilt, die Gefahrenbereiche zu erfassen und zu bewerten und die Schwachstellen zu analysieren, um auf diese Weise zu einer sicheren Risikobeurteilung zu kommen (Bild 1). Sind die Risiken einmal erkannt und eingeschätzt, lassen sich die notwendigen Sicherungsmassnahmen definieren, planen und einführen. Ein Sicherheitssystem lebt. Es muss ständig neuen Situationen angepasst werden. Eine permanente Überwachung und Kontrolle ist erforderlich. Mit Gewaltverbrechen muss zwar jederzeit gerechnet werden, doch sind ihre Methoden zu augenfällig, zu spektakulär. In der Folge haben sich neue, raffiniertere, sich am Rande der Legalität bewegende oder in der Grauzone angesiedelte Methoden entwickelt. Die Wirtschaftskriminalität ist zu einer echten Bedrohung herangewachsen. Als eine neue Art darin hat sich die Computer-Kriminalität herausgeschält, denn gerade die EDV erweist sich in vermehrtem Masse als lohnendes Ziel von oder als Werkzeug für kriminelle Handlungen. Schäden, die durch bewusste Herbeiführung in Form von Manipulationen an Datenbeständen oder Softwareprodukten, von Sabotageakten, von Spionage und/oder von Zeitdiebstählen entstehen, bilden keinesfalls die einzigen Gefahrenquellen. Auch Irrtum und Nachlässigkeit, technische Defekte oder höhere Gewalt können zu Gefahren für die EDV werden. Ein Datensicherungssystem muss individuell, flexibel und zuverlässig

sein. Nur verschiedene Alternativen, die aus der Risikobeurteilung und der Kombination von Abwehrmassnahmen entstehen, lassen eine betriebsspezifische Problemlösung zu. Dabei ist immer einzukalkulieren, dass hundertprozentige Sicherheit – wenn überhaupt realisierbar – wirtschaftlicher Unsinn wäre. Man muss versuchen, mit vertretbaren Mitteln und Kosten so nahe als möglich an die optimale Sicherheit zu kommen. Darunter wollen wir die Verhinderung jeden Missbrauches von Daten und Datenverarbeitungsmitteln durch Gesetze und Normen mit dem Ziel der ordnungsgemässen Datenverarbeitung (= Datenschutz) und die Kombination all jener Sicherungsvorkehrungen und -massnahmen organisatorischer, technischer, baulicher und personeller Art verstehen, um die Daten vor Verfälschung, Zerstörung und unzulässiger Bekanntgabe zu schützen und einen funktionellen, wirtschaftlichen und sicheren Ablauf zu gewährleisten (= Datensicherung).

Voraussetzungen

Jedes Datensicherungssystem hat zwei wesentliche Voraussetzungen: erstens das Sicherheitsbewusstsein und zweitens die Eingliederung und direkte Unterstellung unter den Unternehmensplan und unter das Unternehmensziel. Auf diese Art wird es selber zur unabdingbaren Voraussetzung und Träger des gesetzlichen Datenschutzes. Eine wesentliche Kontrollaufgabe ist es, die betrieblichen Funktionen auf die Erfüllung und Erreichung der auf sie abgestimmten Unternehmensziele im Sinne der Unternehmensleitung zu prüfen. Diese Tätigkeit kann aber nur erfüllen, wer über die notwendigen Erfahrungen, Kenntnisse und Unterstützung seitens der Geschäftsleitung verfügt. Mit Blick auf die EDV-Anwendungen und EDV-Weiterentwicklungen wird die Zukunft der internen Revision von der EDV-Revision massgeblich beeinflusst. Ziel muss es sein, die EDV-Revision – heute oft als Spezialgebiet betrachtet – in die Gesamtrevision einzubeziehen.

Es gehört auch zur allgemeinen Aufgabe der Revision, die EDV selbst und EDV-gestützte Fachfunktionen mit der personellen und EDV-maschinellen Abwicklung sowie die Ergebnisse daraus auf Wirtschaftlichkeit, Funktionalität, Ordnungsmässigkeit und Sicherheit zu prüfen. Konkret bedeutet das, dass sich die Revision mit den Abläufen in der EDV, den eingesetzten Hard- und Softwaremitteln und allen damit zusammenhängenden Detailproblemen wie Datenspeicherung, Datensicherung, Datenintegrität, Datenmanipulation usw. befassen muss. Auch sind individuelle Prüfprogramme und -verfahren zu entwickeln, welche die vorhandenen Daten nach den definierten revisionsrelevanten Kriterien auswerten.

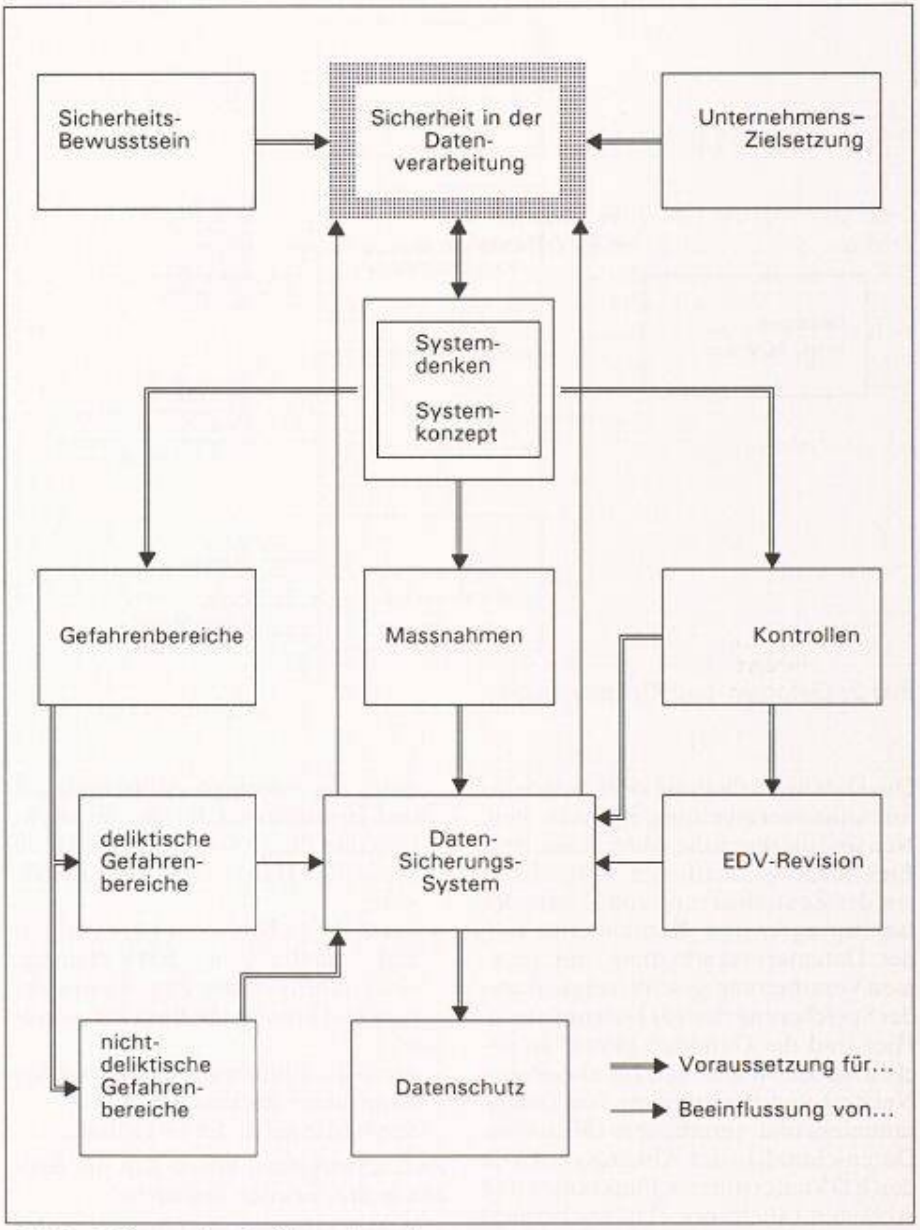

Bild 1. Erfassen der Gefahrenbereiche

Diese Aufgabe muss von EDV-spezifischen Fachleuten (der EDV-Revision) in enger Zusammenarbeit mit der konventionellen Revision übernommen werden.

Gefahren- und Risikenbereiche

Wo liegen die Gefahren, Schwachstellen und Risiken in der Datenverarbeitung? Es wird versucht, diese Fragen an einem an das St.Galler Unternehmungsmodell angelehntes «Gefahren- und Risikomodell» zu beantworten.

Datenverarbeitung heisst: Informationen aufnehmen, speichern, verarbeiten (umformen) und weitergeben, wobei unter manueller, automatischer oder elektronischer Verarbeitung, je nach verwendeten Mitteln, unterschieden wird. Die Informationen werden in erster Linie in der unmittelbaren Umgebung, den betrieblichen oder verwaltungsinternen Fachbereichen, gewonnen und ausgewertet.

Das Unternehmen wie auch die Behörde muss sich am Wirtschaftsleben und an der Öffentlichkeit orientieren, von da Informationen empfangen und wieder abgeben. Durch die Verarbeitung von Daten entstehen neue Kombinationen und Gesichtspunkte, damit werden die Tätigkeiten der Datenverarbeitung selber zu Produzenten und Lieferanten von Informationen. Die Aufgaben der Datenverarbeitung können nur durch eine fundierte Organisation (das sind die EDV-Fachleute mit ihren Funktionen, Aufgaben und Pflichten, aber auch Stellen und Stellenbeschreibungen), durch funktionelle Abläufe und durch geeignete Mittel (Hard- und Software) wahrgenommen werden.

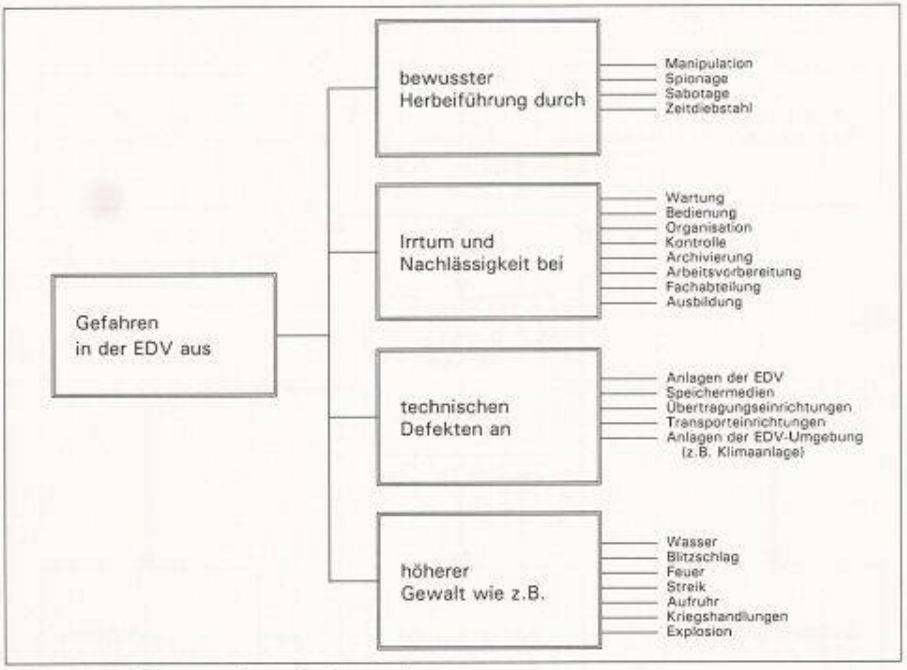

Bild 2. Gefahren- und Risikenbereiche

Die Datenverarbeitung oder besser Informationsverarbeitung ist nicht neu. Neu sind die durch die Automation bzw. Elektronik geschaffenen Möglichkeiten der Zentralisierung von Daten, der fast unbegrenzten Kombinierbarkeit, der Datenfernverarbeitung, der enormen Verarbeitungsgeschwindigkeit und der Speicherung riesiger Datenmengen. Hier sind die Gefahren primär zu suchen: in der Möglichkeit zur einseitigen Nutzung und Bevorteilung von Datensammlern und -verarbeitern (Stichwort: Datenschutz), in der Abhängigkeit von den EDVunterstützten Funktionen und Abläufen (Stichwort: Datensicherung) und in der Bedeutung bzw. dem Wert der Daten, gemessen an dem damit verbundenen Interesse an diesen Daten für Dritte (Stichwort: Computerkriminalität). Demgegenüber steht das Bedürfnis und Recht auf eine funktionierende Datenverarbeitung, auf die Aktualität und Vollständigkeit der Daten. Denn auch nicht erstandene oder entgangene Daten können zu einer Gefahr werden. Schwache Stellen in und um die EDV sind Angriffspunkte für deliktische Handlungen und besonders anfällig bei betrieblichen Pannen oder Störungen (Bild 2).

Solche Möglichkeiten entstehen oder bieten sich nur allzuoft an:

- auf dem Informationsweg: die Erfassung, die Aufbereitung, die Speicherung, die Verarbeitung, die Aus- und Weitergabe;
- durch die technische Entwicklung;
- durch die zunehmende Integration in alle betrieblichen und öffentlichen Bereichen bei gleichzeitiger Konzentration der Daten an einem Ort;
- durch die enormen Aufwendungen und Investitionen für die Entwicklung und Pflege von EDV-Verfahren sowie für Hard- und Betriebssoftware;
- durch das Fehlen einer kurz-, mittel- und langfristigen EDV-Planung, einer schrittweisen Projektentwicklung und konstanten Projektkontrolle;
- durch die Einführung komplexer Systeme unter starkem Zeitdruck;
- durch Mängel in der Organisation.

Zusammengefasst lassen sich die Risiken in drei Ebenen ansiedeln:

- in der Datenverarbeitung
- in der Zusammenarbeit mit den verschiedenen betrieblichen oder verwaltungsinternen Fachbereichen;
- im Verkehr mit den Wirtschaftsbereichen (Umwelt).

Computerkriminalität

Die Diskussion über die Existenz, Umfang und Gefährlichkeit der «Computerkriminalität» ist in der wissenschaftlichen Literatur äusserst kontrovers. Auf der einen Seite wird die Computerkriminalität als ein sehr schwerwiegendes und ernstes Problem der innerbetrieblichen Kriminalität angesehen – es wird geschätzt, dass bereits jedes 10. Rechenzentrum in Deutschland dadurch geschädigt wurde – und auf der anderen Seite wird behauptet, diese Art von Kriminalität existiere überhaupt nicht.

Fehlende Statistik

In der Tat erweist es sich als äusserst schwierig, zu genauem, empirischem Material zu gelangen, da diese Art von Delikten besonders schwierig aufzudecken sind, aufgedeckte Delikte von den betroffenen Firmen aus Furcht vor Schädigung ihres Rufes meist nicht bekanntgegeben, sondern innerbetrieblich geregelt werden und die wenigen rechtshängig gewordenen Delikte als solche in keiner amtlichen Statistik erscheinen. Fehlende Statistiken und Unwissenheit dürfen aber keinesfalls für den Beweis der Nichtexistenz eines Problems herangezogen werden. Die allgemein steigende Kriminalität und sinnlose Zerstörung lassen für den EDV-Bereich mit seinen immensen Möglichkeiten bei mangelnder positiver Einstellung oder böswilliger Absicht entsprechend viele Angriffspunkte konstruieren. Eine neutrale, wertfreie Untersuchung dieses Phänomens wird ihren Wert einerseits in einer exakten Risikobeurteilung und -bewertung in Form von einschlägigen Präventivmassnahmen und andererseits in der Kontrollphase in der Gestaltung von gezielten Checkpunkten und -fragen manifestieren.

Computer als Werkzeug

Im Mittelpunkt dieser neuen Art von Kriminalität steht der Computer als Werkzeug (Mittel) oder Ziel deliktischer Handlungen. Es sind alle kriminellen Vorgänge, die sich in, um und mit dem Computer in der Form von Manipulationen, Spionage, Sabotage und Zeitdiebstahl abwickeln, der folgenden Betrachtungsweise zu unterziehen:

- strafrechtliche Aspekte, d.h. kriminologische Bedeutung unter Berücksichtigung, dass sich durch den Computer zahlreiche neue Arten von Straftaten ergeben und andere so modifiziert werden, dass die bestehenden gesetzlichen Bestimmungen nicht mehr ausreichen, um bestimmte Tatbestände strafrechtlich zu behandeln;
- betriebswirtschaftliche Aspekte, d.h. die innerbetrieblichen Gefahrenquellen und Abwehrmassnahmen zur Erreichung der Datensicherheit im Unternehmen, gegliedert nach den Missbrauchsmöglichkeiten: Daten-Manipulationen, Informations-Diebstahl, Zeitdiebstahl, Sachbeschädigungen und Datenfernübertragung;
- wirtschaftsrechtliche Aspekte, d.h. die Normierung der Datensicherungsmassnahmen unter dem Gesichtspunkt der Prävention, wie sie zur Zeit in der Diskussion um den Datenschutz und die Datensicherung vollzogen wird.

Schwachstellen

Objekte des Missbrauchs werden immer die Schwachstellen in und um die

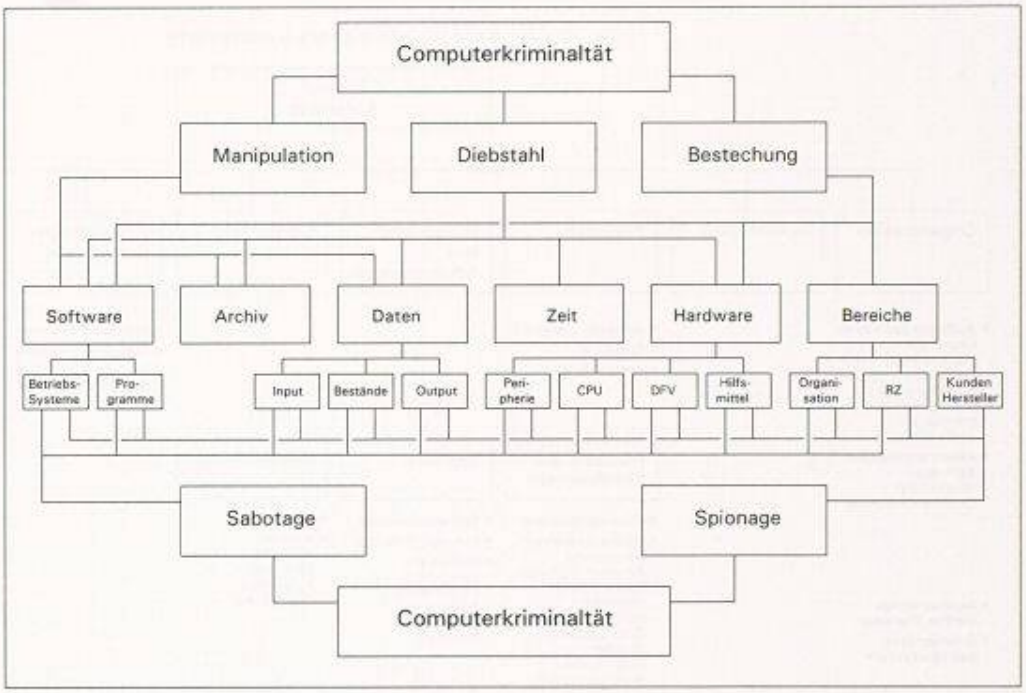

Bild 3. Computerkriminalität in bezug auf EDV-Systeme

EDV sein, die die Täter aus den verschiedensten Motiven heraus suchen, wie z.B. wirtschaftliche Situation, Konkurrenzkampf, blosse Neugier auf das Gelingen einer unverhofft gebotenen Gelegenheit usw. Solche Möglichkeiten bieten sich durch

- rasante technische Entwicklung;
- starke Vermehrung der EDV-Anlagen (Home-Computer, Computer für den Klein- und Mittelbetrieb);
- Einführung komplexer Steuer- und Informations-Systeme unter starkem Zeitdruck (dadurch keine internen und externen Kontrollen);
- keine Basis, die durch eine kurz-, mittel- und langfristige Planung vorgegeben wird;
- fehlende Positionen in den Budgets und fehlende Kapazitätenpläne für die Position «Sicherheit in/um die EDV»;
- keine schrittweise Projekt-Realisierung und Stufen-Kontrolle;
- Übergang auf Software-Standardpakete ohne Kenntnisse des genauen Inhalts und Ablaufs der Programme.

Charakteristiken der Computerkriminalität

Die allgemeinen Charakterien der Wirtschaftskriminalität, wie Erscheinungsformen, Täter und Opfer und deren Bekämpfung müssen, zuzüglich den spezifischen Gegebenheiten der EDV, den Tatbestandsmässigkeiten und Missbrauchsmöglichkeiten, in der Computer-Kriminalität eingehendst untersucht werden. Die Charakteristiken der Computerkriminalität sind:

- Permanenz der deliktischen Tat;
- Höhe der verursachten Gesamtschäden, auch wenn nur Kleinstbeträge manipuliert werden;
- Exklusivität im Fachwissen der möglichen Täter;
- Ausweitung und Bildung neuer Gefahren durch die technische Entwicklung und die damit verbundenen neuen Anwendungs- und Ablaufmethoden, die Konzentration innerbetrieblicher relevanter Daten, Übernahme weiterer betrieblicher Funktionen auf die EDV;
- Möglichkeiten der Datenfernverarbeitung.

Computerkriminalität nimmt bedrohlich zu

In Unternehmen und in der Öffentlichkeit fehlt das Bewusstsein der drohenden Gefahr.

Mit einem Computer verübte Verbrechen werden rasch zur beliebtesten und bedrohlichsten Straftat des 20. Jahrhunderts, behauptet der amerikanische Rechtsanwalt und Experte für die Computergesetzgebung, Joshua J. Kaufmann. Nach Kaufmann erleichtern Computerkriminelle die amerikanische Industrie um mehr als 100 Millionen Dollar im Jahr, und dies sei erst der Anfang. Wir stehen – so Kaufmann – vor einer Expansion des Heim-Informationssystemmarktes auf 30 Milliarden Dollar. Dies hätte dramatische Änderungen in der Art und Weise unserer Kommunikation zur Folge. Während sich im Zusammenhang damit überall in der Gesellschaft lohnende Ziele abzeichnen, könnte man leider auch eine entsprechende Zunahme krimineller Missbräuche dieser modernen Kommunikationsmittel feststellen. Es sei, wie Kaufmann betont, eines der am leichtesten durchzuführenden Verbrechen, man könne sich bequem davonstehlen, und es sei in den meisten Fällen äusserst lohnend.

Robin-Hood-Syndrom

Die Verübung von Computerstraftaten ist praktisch risikolos. Experten schätzen, dass nur einer von 500 Computerkriminellen den Weg ins Zuchthaus antritt.

In Amerika haben erst wenige Staaten die gesetzlichen Grundlagen zum Vorgehen gegen Computerstraftaten geschaffen. Es gibt auch noch keine Bundesgesetzgebung, so dass eine Strafverfolgung oft wenig wirksam oder überhaupt unmöglich ist.

Gegenwärtig ist der Computerkriminelle eine bisher noch nicht dagewesene Spezies von Rechtsbrecher. Er ist jung, hochgradig motiviert, sehr intelligent und leidet an dem, was Psychologen das Robin-Hood-Syndrom nennen. Er rechtfertigt seine Handlungsbeweise mit Abenteuertum, wo man sich zu bewähren hat, und hält es für Spiel. In diesem Stadium sei es aber erst ein Anfang. Noch hat sich das organisierte Verbrechen nicht eingeschaltet, doch es sondiert bereits an den Pforten zum Computerverbrechen. Der bargeldlose Zahlungsverkehr, vertrauliche Datenbanken, Computerservice jeder Art, Diebstahl von Eigentum, Sabotage, Vandalismus und sogar internationaler Terrorismus sind die Ziele der organisierten Computerkriminalität.

Das Datensicherungssystem

Seit einigen Jahren versuchen Wirtschaftsunternehmen und Verwaltungs-

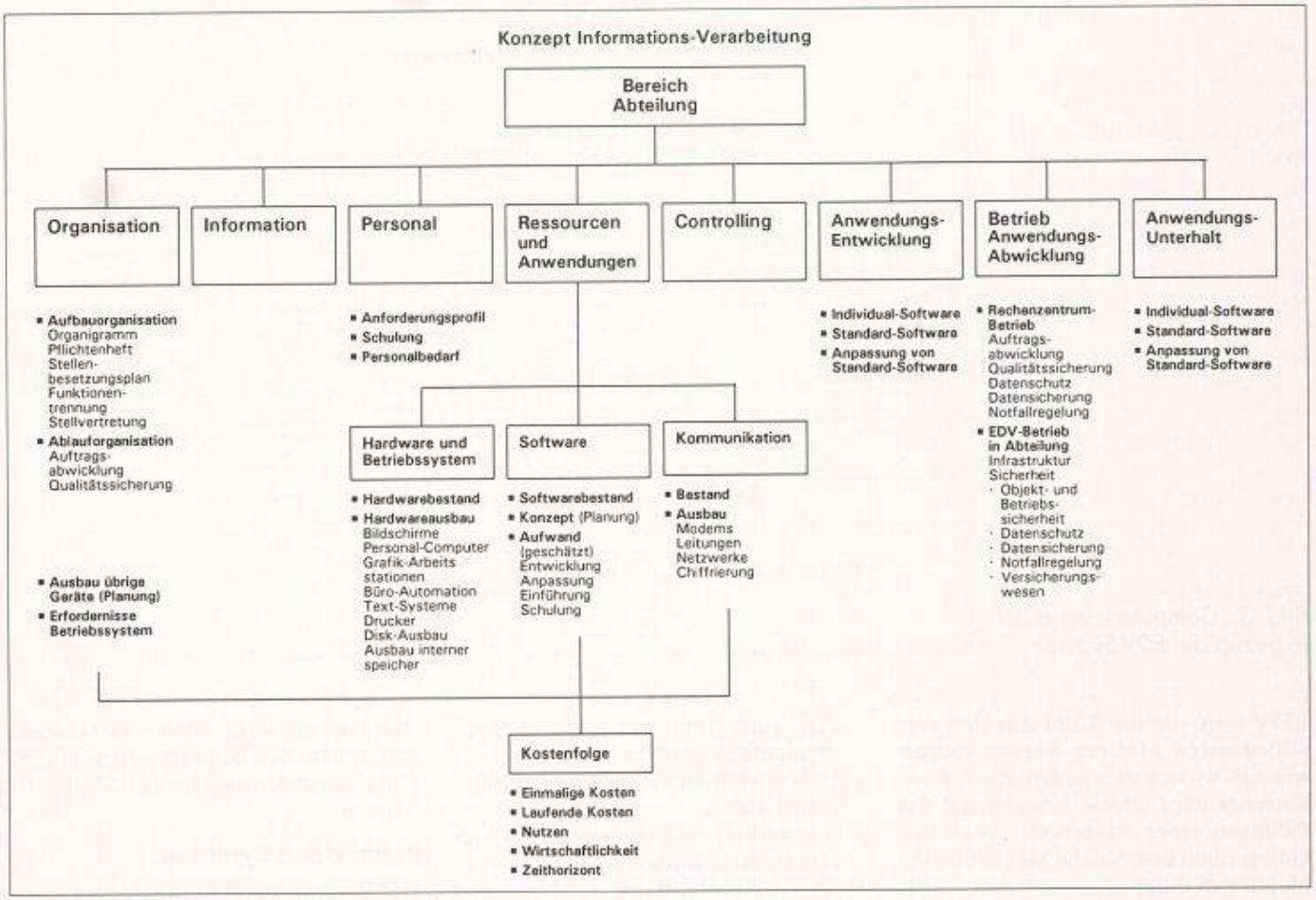

Bild 4. Konzept einer Informations-Verarbeitung

einheiten in verstärktem Umfang mit Hilfe der elektronischen Datenverarbeitung integrierte Informations- und Steuersysteme im grossen Stile aufzubauen. Wesentliche Voraussetzungen für die Realisierung solcher Systeme sind, dass die einzelnen früher autonomen Dateien zu einer gemeinsamen Datenbank zusammengefasst werden, die Verständigung zwischen Benutzern und Datenbank möglichst auf einfache Art erreicht und die räumliche Entfernung durch Datenfernverarbeitungs-Einrichtungen überbrückt wird. Mit der schnellen Verfügbarkeit des Gesamtbildes und den fast unbegrenzten, dynamischen Verknüpfungsmöglichkeiten der Daten wurde die Grundlage für eine optimale und umfassende Informationsgewinnung geschaffen. Gleichzeitig initiiert diese Entwicklung aber auch die Diskussion zum Thema Datenschutz und Datensicherung, da jetzt im hohen Umfang die Datenbestände transparent und manipulierbar werden.

Die möglichen Schäden und deren Ursachen im Bereich der Datenverarbeitung dürfen aber keinesfalls nur auf die bewusste Herbeiführung eingeschränkt werden. Auch Irrtum und Nachlässigkeit in der Wartung, Bedienung und Entwicklung, Mängel in der Organisation, Kontrolle, AVOR und Ausbildung, technische Defekte an den Anlagen der EDV und umliegenden Geräten, aber auch höhere Gewalt, wie z.B. Feuer, Wasser, Streik, Aufruhr, Explosion usw. sind zu beachten.

Massnahmen

Die Realisierung von Datensicherungsmassnahmen ist zu einer wesentlichen organisatorischen Aufgabe geworden (Bild 3). Echter Schutz lässt sich nur durch den Aufbau eines umfassenden integrierten Datensicherungssystems erreichen. Mit allem Nachdruck ist festzuhalten, dass ohne ein ausreichendes Sicherheitsbewusstsein in der Unternehmensleitung und ohne klar definierte Zuständigkeit für die Fragen der Sicherheit in der Geschäftsführung oder Verwaltungsorganisation, sich in keinem Unternehmen ein brauchbares und lückenloses Sicherheitskonzept realisieren lässt. Zu seiner Verwirklichung bedarf es der Autorität der Unternehmensleitung, die allein in der Lage ist, Widerstände in der Betriebshierarchie zu überwinden. Systemdenken ist die weitere unabdingbare Voraussetzung! Man kann die Datensicherung nicht mehr der improvisierten Absprache der im System agierenden Personen überlassen und sich vorwiegend mit einzelnen, punktuellen Massnahmen zufriedengeben. Der Problematik kommt man nur dann näher, wenn man sich überlegt was und unter welchen Umständen etwas schutzbedürftig ist (Ermittlung der kritischen Daten) und welche Folgen es haben könnte, wenn es missbraucht oder zerstört würde.

Voraussicht kritischer Situationen

Nach solchen Überlegungen lässt sich das Sicherheitsbedürfnis besser klären und auch bewerten. Es ist ganz normal, dass auch die betroffenen Sicherheitsmassnahmen in der EDV nicht automatisch funktionieren (Bild 4). Es ist deshalb, wie beim Werkschutz, notwendig, für die möglichen eintretenden Fälle Katastrophenpläne und -handbücher zu erstellen und von Zeit zu Zeit auf ihre Funktionsfähigkeit zu überprüfen.

Genauso wie in den anderen Bereichen der betrieblichen Leistungserbringung laufend Änderungen und Anpassungen an die neuen Gegebenheiten erforderlich sind, gilt dies auch für den Bereich der Sicherheit eines Unternehmens. Sicherheit ist ein dynamisches Problem. Sie wird laufend von externen und internen Bestimmungsfaktoren beeinflusst und löst einen Prozess der Risikobeurteilung, der Konzeptentwicklung und der Massnahmeneinführung aus. Sie bedarf aber auch der steten Kontrolle und Überprüfung, deren Re-

sultate wieder zu einer erneuten Beurteilung führen können.

Gerade im zuletzt genannten Punkt lassen sich heute viele Firmen wieder von ihrem einst begonnenen Weg abbringen und begnügen sich mit einem «eingefrorenen» Sicherheitssystem.

Auch wenn der Datenschutz und die Datensicherung nur ein Teil des gesamten Sicherungskonzeptes einer Unternehmung sind, so nehmen sie doch eine bedeutende Rolle darin ein. Es gilt für jeden einzelnen Bereich der EDV-Organisation, den EDV-Betrieb, die Fachabteilung und die Verbindungswege, unter Beachtung der möglichen eintretenden Katastrophen die notwendigen technischen, personellen, organisatorischen und baulichen Sicherungsmassnahmen zu planen und einzuführen.

Wirtschaftlichkeit

Der Zweck der Datensicherung besteht aus der Erfüllung der bestehenden (und zukünftigen) gesetzlichen Forderungen und aus der optimalen Gewährleistung der internen Verarbeitungssicherheit. Die Einhaltung der gesetzlichen Normen umfasst einerseits den Schutz von Personen und Institutionen vor rechtswidrigen Eingriffen in ihre Privatsphäre (das Problem des Datenschutzes) und andererseits die vollständige und schlüssige Nachweisführung der Rechnungslegung (das Problem der ordnungsgemässen Buchführung). Wie bei jedem Sicherheitssystem gilt auch hier: es gibt keine absolute Datensicherheit. Letztlich geht es um die Bestimmung adäquater Massnahmen bzw. Kombination von Massnahmen zur Sicherung von schutzbedürftigen Tatbeständen unter dem Aspekt der Wirtschaftlichkeit und Realisierbarkeit und um das Übertragen des restlichen verbleibenden finanziellen Risikos auf Versicherungen

EDV-Revision

Die elektronische Datenverarbeitung bedarf anderer Arten von Kontrollen und Sicherungsmassnahmen als manuelle Abläufe. So wird die Stichprobenprüfung, d.h. die direkte Verfolgung einzelner Buchungen vom Urbeleg zur Bilanz bzw. Erfolgsrechnung und umgekehrt, bei der Übernahme integrierter Buchhaltungssysteme auf die EDV nicht mehr möglich sein. An ihre Stelle tritt die indirekte Prüfung, d.h. die Systems- oder Verfahrensprüfung, die von der Konklusion ausgeht, dass bei elektronischer Datenverarbeitung die Richtigkeit des eingesetzten EDV-Verfahrens auf die Richtigkeit der mit ihm erarbeiteten Ergebnisse schliessen lässt.

<table>
<tr><th colspan="6">EDV-Revision</th></tr>
<tr><th colspan="4">Prüffelder</th><th>Prüfungs-Kriterien</th><th colspan="2">Prüfungsarten</th></tr>
<tr><td colspan="2" rowspan="3">Applikations-unabhängige Prüffelder</td><td colspan="2" rowspan="3">Applikations-abhängige Prüffelder</td><td>Ordnungs-mässigkeit</td><td>Abschluss-prüfung</td><td>Sonder-prüfung</td></tr>
<tr><td>Funktio-nalität</td><td rowspan="3">Bestätigung der Ordnungs-mässigkeit der Buch-führung bei EDV-Einsatz</td><td rowspan="3">Überprüfung der EDV aus unterschiedli-chen Motiven und mit ver-schiedenen Zielsetzungen</td></tr>
<tr><td>Sicherheit</td></tr>
<tr><td>For-mell</td><td>Mate-riell</td><td>For-mell</td><td>Mate-riell</td><td>Wirtschaft-lichkeit</td><td></td></tr>
<tr><td colspan="4"></td><td></td><td>Ex post</td><td>Ex ante</td><td>Ex post</td></tr>
</table>

Bild 5. Wirkungsbereiche der EDV-Revision

Bedingt durch den zunehmenden Einsatz von Datenfernverarbeitung, des Dialogverkehrs und der Speicherung miteinander beliebig verknüpfbarer Informationen (Datenbanken), genügt es nicht mehr, nur «um die EDV bzw. den Computer herum» zu prüfen, d.h. auf die formelle Abwicklung, Ordnungsmässigkeit der Eingabe- und Ausgabe-Daten sowie der Stammdaten und in vereinzelten Fällen auf die Programmänderungen zu achten.

Nachholbedarf

Die Forderung, durch den Computer hindurch zu prüfen, d.h. die EDV-Verfahren, die EDV-Organisation, aber auch die EDV-Planung und Wirtschaftlichkeit der eingesetzten EDV-Mittel in die Kontrollen einzubeziehen, wird sich nicht mehr länger aufschieben lassen. Der Umfang des EDV-Einsatzes, die Wahrung berechtigter externer und interner Interessen und die gegebenen Möglichkeiten, vermehrt betriebliche Funktionen, aber auch Unternehmensleitungen konstruktiv zu unterstützen, unterstreichen die Bedeutung und Notwendigkeit einer wirksamen EDV-Revision. Dennoch lassen sich die Aktivitäten auf dem Bereich EDV-Revision nach doch rund 30 Jahren elektronischer Datenverarbeitung eher als unterentwickelt ansehen.

Drei Revisionsarten

Obwohl die sachlichen Voraussetzungen, d.h. die Grundlagen aus der Diskussion um das Datensicherungssystem im vorhergehenden Kapitel entwickelt und das aus den Mitteln und Methoden der internen Revision abgeleitete praxisnahe Instrumentarium durchaus vorhanden wären, sind aber offensichtlich die personellen Voraussetzungen noch zu überdenken. Es fehlt ein ausgewogenes Anforderungsprofil bzw. Berufsbild und, darauf aufbauend, entsprechende gezielte Aus- und Weiterbildungsmöglichkeiten, um die komplexen Aufgaben der EDV-Revision vom Fachwissen her erfüllen zu können.

Wir unterscheiden drei Revisionsarten: die externe Revision und die interne Revision, die beide, obwohl mit unterschiedlichen Aufgabenstellungen betraut, sich mit der Datenverarbeitung befassen müssen und ferner die permanenten Kontrollen, der im Sicherheitskonzept ausgewählten Massnahmen auf ihre Aktualität, Anwendbarkeit und Erfüllung.

Die EDV-Revision hat somit zwei Gesichtspunkte zu berücksichtigen:

- aus externer Sicht die Beurteilung und Begutachtung, bzw. Erfüllung der gesetzlichen Vorschriften, d.h. die Ordnungsmässigkeit der Datenverarbeitung zu vergegenwärtigen;
- aus interner Sicht die Funktionsfähigkeit, Wirtschaftlichkeit und Sicherheit der Datenverarbeitung unter den EDV-technischen Möglichkeiten zu garantieren.

Dies kann zu Interessenskonflikten führen, insbesondere dann, wenn sogenannte integrierte Systeme verschiedene Bereiche, Erlasse und Funktionen berühren.

Revisionsgebiete

Die primäre Aufgabe der internen Revision ist es, das Unternehmen vor Verlust zu schützen. Dass diese Aufgabe auch die EDV einbeziehen muss, zeigen Personalaufwendungen, Investitionen in EDV-Mittel und Systempflege sowie der zunehmende Drang, weitere betriebliche Funktionen mit der EDV abzuwickeln, mit grosser Deutlichkeit. Das Revisionsgebiet umfasst somit kurz

gesagt alles, was dazugehört, um die betriebliche Funktion mit einer EDV-Anlage zu erfüllen und erstreckt sich auf:

- Kontrollen im vor- und nachmaschinellen Kreis
- organisatorische Kontrollen
- Kontrollen bei der Systementwicklung
- Arbeitsablaufkontrollen
- Verarbeitungskontrollen
- Kontrollen der Dokumentation
- DV-spezifische Kontrollen bei Datenverarbeitung ausser Haus und Benutzung von Fremdpackages.

Die Prüfungsfelder können in diesen Fällen EDV-Verfahren/-Systeme, Hard- und Software, EDV-Planung und -Realisierung oder EDV-Dienststellen sein. Die Prüfungstechniken werden vom Wissensstand der Anwender, von der EDV-Anlagen-Ausstattung und EDV-Durchdringung sowie von der Quantität und Qualität der EDV-Revisoren abhängen, und es wird entscheidend sein, ob die Revision

- um den Computer herum
- von Teilgebieten der EDV
- des Rechenzentrums geführt

oder ob bereits mit

- System-/Verfahrenrevision
- Programmrevision

begonnen werden kann.

Dabei kann die EDV-Revision grundsätzlich beratend mitwirken oder ex-ante-/ex-post-Prüfungen oder Nachrevisionen durchführen. Ein sinnvoller und wirksamer EDV-Revisions-Einsatz ist aber nur dann gegeben, wenn die gewonnenen Erkenntnisse den unmittelbar Betroffenen mittels Berichten aufgezeigt und ferner in neutraler Form Schwachstellen und Risiken, zusammen mit vorgeschlagenen Zielrichtungen zur Beseitigung an die Geschäftsleitung, weitergereicht werden. Für den verantwortlichen Verfahrensentwickler und Organisator sind die Mängel Verpflichtung zur Behebung und für die Unternehmensleitung sind sie Anlass genug, die EDV-Revision durch ihr Vorhandensein nicht nur präventiv wirken zu lassen (Bild 5).

Adresse des Verfassers: A. P. Steiner, Inhaber der Firma ISBAdata, Unternehmens-, Informatik- und Sicherheits-Beratung, Küsnacht/ZH.

Der leicht gekürzte Beitrag stammt aus der Dokumentation der Suter+Suter-Informationstagung zum Thema «Verwaltungsgebäude und Rechenzentren im Brennpunkt von High-Tech und High-Touch».

Tagungsberichte

Bodenrechtspolitik

VLP-Tagung vom 23. Januar 1992 in Zürich

Unter dem Titel «Bodenrecht – Aufbruch zu neuen Ufern oder Quadratur des Kreises?» veranstaltete die Schweizerische Vereinigung für Landesplanung eine Tagung über das bundesrätliche «Anschlussprogramm» zur Bodenrechtspolitik und stellte daraus zwei Bereiche zur Diskussion: die Förderung des Baulandangebotes und den Mehrwertausgleich.

Der erste Teil des Untertitels, Aufbruch zu neuen Ufern, musste sehr rasch verneint werden. Veranstaltungsteilnehmer, die neue Ideen und Wege aus dem Dilemma der Boden- und Mietpreiserhöhungen erwarteten, wurden enttäuscht. Verschiedene Referenten wiesen darauf hin, man müsse zuerst die bekannten Ufer erreichen, bevor nach neuen aufgebrochen wird.

In der Begrüssung und Einleitung stellte VLP-Präsident und Regierungsrat *Eduard Belser,* Baudirektor des Kantons Basel-Landschaft, fest, die Bodenrechtspolitik müsse eine Antwort auf die Frage geben, welche Nachfrage (nach Bodennutzungen) befriedigt werden solle und welche nicht.

Dr. *Heinrich Koller,* Direktor des Bundesamtes für Justiz, stellte die Ziele und Inhalte des bundesrätlichen «Anschlussprogrammes» (Bunderatsbeschluss vom 11. September 1991) vor. Das «Anschlussprogramm» schliesst an die bisherigen Massnahmen in der Bodenrechtspolitik an, insbesondere nach dem Scheitern der zu radikalen Stadt-Land-Initiative 1988 und den anschliessenden dringlichen Bundesbeschlüssen. Eine radikale Umorientierung des Eigentumsrechts komme aus politischen Gründen nicht in Frage. Die Vorschläge des Bundesrates zielten deshalb vorab auf die Verbesserung jener Lösungen, die sich aus dem Zusammenspiel von Marktkräften und staatlichen Einwirkungen bisher ergeben haben.

Vorarbeiten für das «Anschlussprogramm» wurden durch eine verwaltungsinterne Arbeitsgruppe «Weiterentwicklung des Bodenrechts» (Schlussbericht «Bausteine der Bodenrechtspolitik» 1990; vergriffen), eine Expertenkommission «Hypothekarmarkt» sowie die Eidgenössische Wohnbaukommission geleistet. Auch die Resultate des Nationalen Forschungsprogrammes «NFP Boden» seien in das «Anschlussprogramm» eingeflossen.

Dieses Programm enthält nun Vorentwürfe und Berichte, die im Sommer/Herbst 1992 in die Vernehmlassung gehen, wie z.B. zum Vorkaufsrecht des Mieters und des Gemeinwesens. Im Raumplanungsrecht sollen bis zum Sommer 1993 die Mehrwertabschöpfung, das Erschliessungsrecht, die Erschliessungsbeiträge, der Wohnanteilplan und Vereinfachungen des Baubewilligungsverfahrens bearbeitet werden. Aus den weiteren Aufträgen sind noch speziell zu erwähnen: der Ausbau des Grundbuches zu einem Bodeninformationssystem, Mustererlasse für das kantonale Bau- und Planungsrecht sowie die Expertenkommissionen «Marktmiete» und «Fiskalrecht».

Abschliessend meinte Koller, erst die Vernehmlassungsverfahren würden zeigen, in welche Richtung der künftige Weg der Bodenrechtspolitik führen würde.

Der Ökonom Prof. Dr. *Jörg Baumberger*, St. Gallen, wies auf zwei Probleme hin, die durch die neuen, aber trotzdem als Zwischenlösung zu wertenden Instrumente entstehen. Erstens eine Verunsicherung des Marktes: Der Investor könne die neuen Instrumente nur als Zwischenlösung für weitere (unbekannte) Veränderungen betrachten und verhalte sich entsprechend zurückhaltend. Zweitens die Gefahr der «Regulierungsspirale» (Intervention – Fehlleistung – neue, zusätzliche Interventionen...) und die Ineffizienz von Interventionen: (Bürokratie-)Kosten der Interventionen, die grösser als der Nutzen seien.

Über das bestehende Baulandangebot orientierte Prof. Dr. *Hans Flückiger,* Direktor des Bundesamtes für Raumplanung. Aus verschiedenen Studien – «NFP Boden», «Raumbeobachtung Schweiz», kantonale Analysen – könne gefolgert werden, dass das Baulandangebot genügend sei; dagegen sei das Problem der Verfügbarkeit nicht gelöst. Die Erhöhung des Baulandangebotes müsse daher durch die Mobilisierung der bestehenden Reserven erfolgen, durch eine Entwicklung nach innen.

Regierungsrat Dr. *Josef Egli,* Baudirektor des Kantons Luzern, nannte dazu insbesondere folgende kantonale Aufgaben und Möglichkeiten: Information und Mithilfe des Kantons bei den Gemeinden, Anpassung der Grundstücksgewinnsteuerung von eingezontem Land, sofortige Fälligkeit von Erschliessungsbeiträgen sowie die Landumlegung.

Zum Mehrwertausgleich gab Prof. Dr. *Peter Locher,* Bern, einen Überblick über bestehende kantonale Modelle, von der Minimallösung einer (erweiterten) Grundstücksgewinnsteuer bis zum eigentlichen Mehrwertausgleich. Die vom Bund verlangten Minimalanforderungen an die Ausgestaltung des Mehrwertausgleichs entsprächen zwar nicht vollständig dem angestrebten Ziel, seien aber besser als gar kein Mehrwertausgleich.

Stadt- und Kantonsplaner *Rolf Plattner,* Basel, stellte schliesslich das Basler Modell des Mehrwertausgleichs vor, das seit 1978 mit Erfolg angewendet wird.

Im abschliessenden Podiumsgespräch kam die Boden- und Mietpreisentwicklung als Hauptproblem nochmals zur Sprache. Über die pragmatische Symptombekämpfung hinweg konnte auch hier kein Konsens gefunden werden. Als Fazit der Tagung muss damit festgestellt werden, dass sich in der Bodenrechtspolitik wenig Neues tut und dass kein Wille für grundsätzlich neue Lösungswege besteht.

Thomas Glatthard