

Spiel mit Schlüsseln

Bürger, Unternehmen und Ämter sind mehr denn je von Ausspäher bedroht. Nur neueste Chiffrierverfahren werden Daten und Informationen wirksam sichern können.

Mit „53 = + 305)...“ beginnt einer der berühmtesten Geheimtexte. Wie die Zeichenfolge entschlüsselt und damit der Schatz des Piraten Kapitän Kidd gehoben werden konnte, erzählte Edgar Allan Poe in

seiner 1843 erschienenen Abenteuergeschichte „Der Goldkäfer“.

Der amerikanische Schriftsteller nutzte jedoch nicht nur detektivische Sprachanalyse als Spannungsmoment. Er nahm literarisch-spielerisch eine Entwicklung vorweg, bei der es bald um Leben und Tod ging.

Bereits im amerikanischen Bürgerkrieg kam das Anzapfen von Telegraphenleitungen auf. Die Nachrichtentruppen mußten deshalb dazu übergehen, gemorste Meldungen zu chiffrieren.

Es sei allerdings „sehr zu bezweifeln“, hatte Poe gemeint, „ob menschlicher Scharfsinn ein Rätsel erfinden

könne, das menschlicher Scharfsinn nicht wieder zu lösen vermöchte“. In der Tat fanden bis in die jüngste Vergangenheit fast alle Verschleierungstaktiken noch ihre Meister.

So hörte im Zweiten Weltkrieg die deutsche Abwehr Transatlantik-Gespräche Winston Churchills mit. Dem britischen Geheimdienst wiederum gelang es, Funksprüche der deutschen Wehrmacht, die mit der Chiffriermaschine „Enigma“ (griechisch = Rätsel) verschlüsselt worden waren, wieder in Klartext umzusetzen; das Spionage-Kabinettsstück half den Alliierten insbesondere bei der Abwehr der Luftoffensive gegen England, im Afrika-Feldzug und bei der Invasion in der Normandie.

Mittlerweile aber steht mit erfolgreicher Kryptologie, der Kunst des Ver- und Entschlüsselns von Daten und Nachrichten, noch mehr auf dem Spiel: Die Gefahren mangelhafter Datensicherung reichen vom Bruch der Persönlichkeitsrechte einzelner Bürger, dem Ausspähen von Betriebsgeheimnissen oder internationalen Finanz-Transaktionen und dem Vorschub für Computer-Kriminalität bis zur Bedrohung des Weltfriedens.

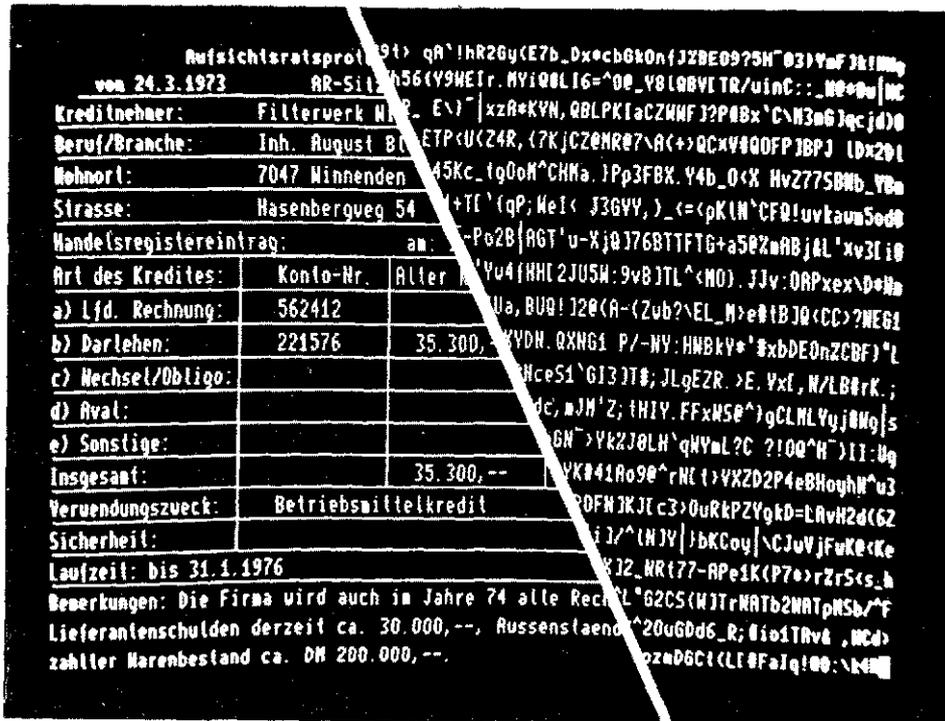
Denn seit Einführung der Elektronik schwellen die zentral in sogenannten Datenbanken gesammelten Informationen über Personen und Unternehmen, über wirtschaftliche, militärische und politische Aktionen und Pläne wie eine Springflut an. In gleichem Maße aber wuchs auch das Risiko des Mißbrauchs.

Vor allem bei der Übertragung, etwa über Telephon- und Fernschreibleitungen oder Richtfunk, sind Daten gefährdet. „Nachrichtendienste und Werkspione“, erklärte erst letzte Woche Alexej Stachowitsch, Leiter der Abteilung Datenschutztechnik bei AEG-Telefunken, „können alles abhören, was sie wollen, wenn nur der Aufwand hoch genug ist.“

In der Bundesrepublik trat zwar zu Jahresbeginn ein Datenschutzgesetz in Kraft. Dennoch werden weiterhin in staatlichen und privaten Datenbanken Hunderte von Angaben über jeden Bürger unverschlüsselt gespeichert und mit Rechenzentren ausgetauscht.

Technische Sicherungen verlangt das Gesetz erst vom kommenden Jahr an — und „nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht“.

Das Problem, wo dabei „die Grenze zwischen Sicherheit für alle und Freiheit des einzelnen“ zu ziehen sei, ist nach Ansicht von Stachowitsch „von einer Brisanz, die sich nur mit der Debatte über den Schutz der Umwelt vergleichen läßt“. Wie viele Kollegen sieht der AEG-Experte lediglich ein wirksames Hindernis gegen Eingriffe von Unbefugten, gegen Datenraub,



„Telekrypt“-Textverschlüsselung*: „Spione können abhören...“



... was sie wollen“: Datenschutz-Experte Stachowitsch, „Telekrypt“-Gerät

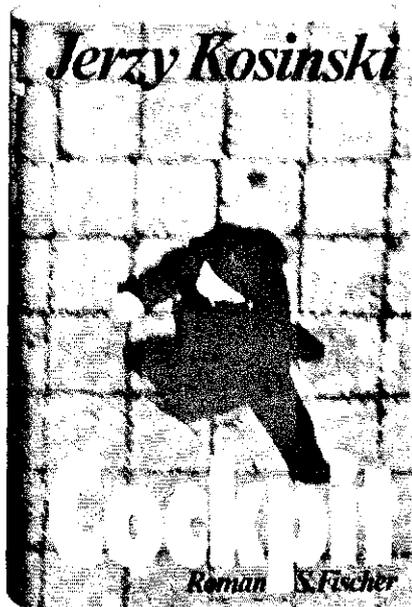
* Links: Klartext; rechts: derselbe Text in chiffrierter Form.

»Jerzy Kosinski hat eine der stärksten persönlichen Erfahrungen durchlebt, die dieses Jahrhundert anzubieten hatte.«

Time Magazine

„Kosinski braucht die Tarnung eines Spions, um andere zu enttarnen – Systeme zu durchleuchten. Er gleicht einem einsamen Habicht in der literarischen Landschaft, der über den Abgründen und Schrunden menschlich-gesellschaftlicher Beziehungen kreist – mit den Augen des Raubvogels jegliche Einzelheit wahrnimmt, registriert und gnadenlos ohne sichtbare Bewegung aufzeichnet. Nur wer so zu lesen imstande ist, dem erschließt sich vielleicht das Versöhnende in diesem Buch: die poetische Kraft einer sprachlichen Brillanz, die wie ein Brokatvorhang hinter den Worten zur Wirkung kommt und der eine fast weiche, musikalische Sensibilität zugrunde liegt.“

Gideon Schüler



Jerzy Kosinski

Cockpit

Roman. 320 S. geb. DM 32,-

S. Fischer

Lauschangriff während der Verarbeitung oder Übertragung von Daten und gegen Manipulation der Computer-Programme: Verschlüsselung.

Mit internationalem Schutz von Daten müssen sich schon seit Jahren Gremien wie die OECD, die EG-Kommission und der Europarat beschäftigen. Vereinbarungen stehen noch aus; dabei laufen Informationen, die — wie etwa Produktionsverfahren oder Bankanweisungen — nicht minder schutzbedürftig sind als Diplomatenpost oder Militärbefehle, inzwischen häufig via Satellit rund um die Erde.

Mitunter werden Daten sogar wie Rohstoffe zur Verarbeitung über die Grenzen transportiert. So schickte die kanadische Sozialversicherung Unterlagen nach Taiwan, die dort billiger als im eigenen Land auf Lochkarten übertragen werden. Die Feuerwehr des schwedischen Malmö läßt die Liste der Brand-Gefahrenherde in der Stadt von einem Rechenzentrum in Cleveland, USA, auf dem laufenden halten.

Von Geheimschlüsseln hängt schließlich sogar das Pakt der Nuklearmächte ab. Der Vertrag über die Begrenzung unterirdischer Atomwaffenversuche sieht unter anderem vor, daß amerikanische Überwachungsgeräte in der Sowjet-Union installiert werden; bislang aber streiten Washington und Moskau darüber, in welchem Kode die Meßdaten übermittelt werden sollen.

Die Amerikaner wollen diesen Kode allenfalls teilweise offenbaren, damit die Sowjets nicht die Verschlüsselungsverfahren durchschauen und dann womöglich die automatisch aufgezeichneten Meßwerte der Stationen verfälschen können. Die Sowjets hingegen fürchten, daß mit unkontrollierbaren Meßwerten auch Spionage-Erkenntnis in die USA gelangen.

Vor diesem Dilemma, daß Verschlüsselungen hinreichend sicher, aber praktikabel sein müssen, haben die Kryptologen seit je gestanden. Zwei grundsätzlich verschiedene Methoden wurden dabei immer weiter verfeinert:

- ▷ das Kodieren, das nur die Übermittlung von Nachrichten mit vorher vereinbarter Bedeutung ermöglicht (simples Beispiel: „Tante Emma ist gestorben“ für „Die geplante Aktion ist abgeblasen“), oder
- ▷ das Chiffrieren, das auch die Übermittlung von Nachrichten zuläßt, deren Inhalt völlig neu ist.

Übliche Chiffriermethoden, für die der Empfänger lediglich eine Übersetzungsanweisung — den Schlüssel — braucht, sind etwa

- ▷ das Austauschen von Klartext-Buchstaben gegen Geheimzeichen, wie es schon Edgar Allan Poe vorführte (so steht in der „Goldkäfer“-Erzählung die Zeichenfolge „5 3 = = + 3 0 5)“ für „A good glass“), oder



Schriftsteller Poe

Geheimtext zur Schatzsuche

- ▷ Anwendung eines mathematischen Schemas („Algorithmus“) — so kam der Computer in Stanley Kubricks Film „2001“ zu seinem Namen HAL, indem die Buchstaben des Firmennamens IBM im Alphabet um jeweils eine Position nach vorn versetzt wurden.

In der einfachsten Form sind derartige Tricks freilich leicht zu durchschauen. Denn Eigentümlichkeiten der Sprache, vor allem die Häufigkeit bestimmter Buchstaben, Buchstaben-Kombinationen und Silben, bleiben dabei erhalten und geben die wichtigsten Hinweise zum Dechiffrieren.

Im Deutschen beispielsweise sind die häufigsten Buchstaben e, n, i, r, s, t, a, d, die häufigsten Zweiergruppen („Bigramme“) en, er, ei, ch, die häufigsten Dreiergruppen („Trigramme“) ein, sch, der, nde.

Überaus sicher sind dagegen Chiffriermethoden, die den Klartext Buchstabe für Buchstabe mit einem sinnlosen Schlüsseltext überlagern. So gebrauchen Diplomaten für ihre Geheimbotschaften Zufallsfolgen von Ziffern, die beim Chiffrieren zuverlässig die Sprachmuster zerstören. Hinderlich an diesem Verfahren war zunächst, daß Sender und Empfänger ständig mit neuen Ziffer-Katalogen ausgestattet werden müssen.

Seit aber Computer eingesetzt werden, konnte die Spezialwissenschaft Kryptologie in vordem ungeahnte Dimensionen vorstoßen. Chiffrier-Experten entwickelten Schwierigkeitsgrade des Geheimschreibens, die mit allen gegenwärtig vorstellbaren Methoden unlösbar sind — sie können „Konfusion“ und „Diffusion“, das Durchmischen der einzelnen Ziffern und Ersetzen durch Chiffren, nahezu beliebig

steigern und leicht miteinander kombinieren.

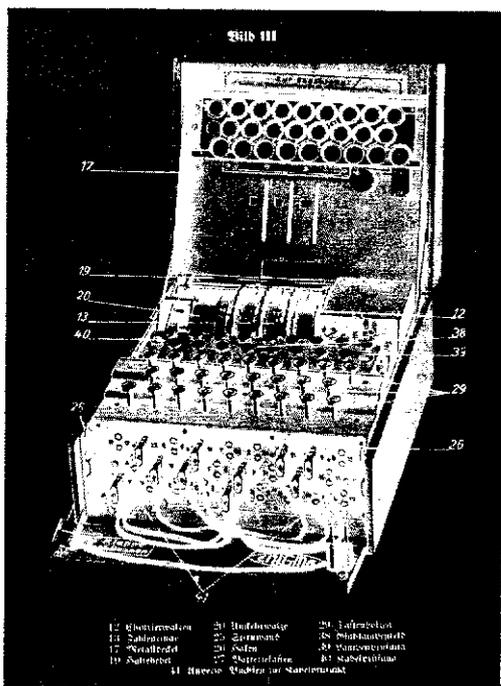
Dennoch müssen die Kryptologen Kompromisse machen, wenn es darum geht, die Unmengen vertraulicher Daten in Wirtschaft und Verwaltung zu schützen. „Wir wissen zwar, was ideal wäre“, erklärte IBM-Forscher Thomas Feistel, „aber wir können das Ideal nicht in die Praxis umsetzen.“

Über solche Kompromisse bei der Chiffrier-Schwierigkeit ist gegenwärtig in den USA eine Diskussion entbrannt, die aktuellen Anlaß hat. Dabei kam ein schlimmer Verdacht gerade gegen jene Institutionen auf, die den Datenschutz garantieren sollen — gegen staatliche Behörden.

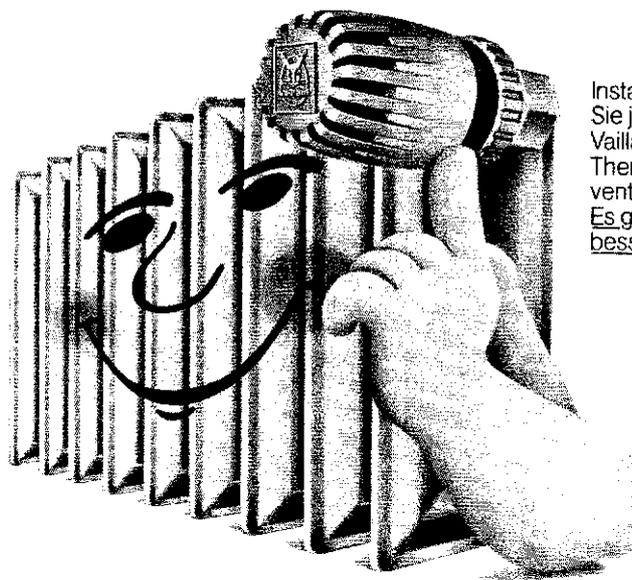
Da immer mehr Ämter und Privatunternehmen, voran die Banken, sich gegen Computer-Kriminalität schützen müssen, suchte Amerikas National Bureau of Standards nach einem universell anwendbaren Chiffrier-System von hohem Sicherheitsgrad. Ein solches System wurde von IBM entwickelt und von der Behörde zugelassen; seit letztem Jahr ist es unter dem Namen „Data Encryption Standard“ (DES) auf dem Markt.

Jeder Benutzer erzeugt mit einem Gerät, das seiner elektronischen Datenverarbeitung vorgeschaltet wird, seinen eigenen Chiffrierschlüssel. Er wird durch eine Zufallsfolge von 56 Ziffern (0 oder 1) gebildet; das Risiko, daß zwei solcher Schlüssel identisch sind, daß also jemand sich einen Nachschlüssel herstellen und unbefugt Daten abrufen oder verändern kann, beträgt nur rund 1:100 Milliarden.

Doch eine Gruppe von Forschern, konstatierte die angesehene Wissen-



Chiffriermaschine „Enigma“
Klartext beim Feind



Installieren Sie jetzt Vaillant Thermostatventile. Es gibt keine besseren.

Heizen mit Köpfchen. Mit Vaillant Thermostatventilen.

Die denken und regeln, rechnen und sparen. Bringen Wunschwärme in jeden Raum – senken die Heizkosten bis zu 20%.

Fragen Sie Ihren Heizungsfachmann.



Vaillant

Europas große Marke für Heizen, Regeln, heißes Wasser.

Das Vaillant Qualitäts-Programm: Gas-Zentralheizungen: Heiz-Geysier, Combi-Geysier, Gas-Heizkessel mit oder ohne Warmwasserbereitung, Gas-Heizautomaten, Öl-Zentralheizungen: Öl-Spezialkessel mit oder ohne Warmwasserbereitung, Umstellbrandkessel für Öl, Gas, Koks, Warmwassergeräte für Gas und Strom, Heizkörper-Thermostatventile, Regelgeräte für Heizungs-Anlagen.

schaftszeitschrift „Science“, „argwöhnt, das System sei vorsätzlich gerade so sicher gemacht worden, daß Wirtschaftsspione außerhalb der Regierung einen Benutzer-Schlüssel nicht brechen können, aber doch noch verletz-lich genug, daß der National Security Agency das Entschlüsseln gelingen könnte“.

Experten wie Professor Martin E. Hellman und sein Doktorand Whitfield Diffie von der kalifornischen Stanford University haben durchgerechnet, daß ein DES-Schlüssel sogar innerhalb eines Tages zu brechen sei — durch bloßes Probieren. Einzusetzen wäre dafür ein superschnell alle Möglichkeiten durchspielender Spezialcomputer, der, wie die Forscher kalkulieren, für 20 Millionen Dollar gebaut werden könnte.

Andere Kritiker meinen laut „Science“, der Staat brauche, wolle er seine Bürger und Unternehmen aus-schnüffeln, derartigen Aufwand gar nicht zu treiben: Die National Security Agency, geheimster der militärischen Geheimdienste, „war an der Entwick-lung von DES beteiligt“, und verächt-lich scheine, daß sie „etliche wichtige Teile des Verschlüsselungsschemas für geheim erklärt“ habe.

Manche US-Firmen, darunter die Bell Telephone Company und die Ban-ker's Trust Company, haben sich wohl deshalb gegen DES entschieden. Die New Yorker Citibank hingegen, einer der Großanwender von komplizierter Kryptographie, hält DES für einen gro-ßen Fortschritt im Chiffrierwesen; das Hauptproblem damit, erklärte einer der Manager, sei psychologischer Art — „wenige Leute in den USA trauen un-seren Geheimdiensten“.

Ähnliche Probleme kommen auf die Bundesrepublik zu: US-Firmen wollen Computergeräte, die das umstrittene Chiffrier-Standard-system DES verwen-den, exportieren. Und IBM drängt da-mit auf den westdeutschen Markt.

Ein vergleichbares System ist, ohne daß es darüber Kontroversen gegeben hätte, allerdings schon im Handel. Die Firma AEG-Telefunken, die aus Nato-Kontrakten große Erfahrung mit Ver-schlüsselungsverfahren hat, bietet seit einiger Zeit für zivilen Gebrauch die Geräte-Familie „Telekrypt“ zum Schutz von Daten bei der Übertragung an.

Das Geräte-Set, das äußerlich einem HiFi-Rack ähnelt, birgt für den Laien schier unfaßbare Möglichkeiten.

Der Schlüsseltext, mit dem die über-tragenen Daten oder auch Telephone-sprache unkenntlich gemacht werden, ist von einer wirklichen Zufallsfolge von Zeichen nicht mehr zu unterschei-den. Er würde sich auch bei Verwen-dung von 10 000 Zeichen in der Sekun-de erst nach einer Zeit wiederholen, die

dem billionenfachen Alter der Erde entspricht.

Damit Verschlüsselung beim Sender und Entschlüsselung beim Empfänger synchron ablaufen, wird ein Grund-schlüssel verwendet, den die Benutzer selbst herstellen. Die Vielfalt dabei ist so groß, daß die Lochkarten mit sämtli-chen Möglichkeiten den Erdball mit einer 60 000 Kilometer dicken Papier-schicht bedecken würden.

Zur weiteren Sicherheit, vor allem gegen Erpressung und Verrat, kann der einmal gewählte Grundschlüssel auf mehrere Personen verteilt werden; erst alle Teilschlüssel zusammen erlauben — nach dem Prinzip von Safe-Schlös-sern — das Chiffrieren. Und schließ-lich wird bei jeder neuen Daten-Über-



Mathematiker Hellman, Chiffriergerät
Will der Staat schnüffeln?

tragung ein variabler „Spruchschlüs-sel“ eingesetzt, den das Gerät automa-tisch erzeugt.

Dieses System, meinen die Herstel-ler, wäre selbst mit Hilfe von Groß-computern nicht zu knacken. Wollte ein Unbefugter ein oben verwendetes Programm durch Probieren entschlüs-seln und könnte er pro Sekunde eine Million Versuche machen, müßte er dafür gleichwohl durchschnittlich 1000 Billionen Jahre aufwenden.

Den Aufwand für Versuche, der neuen Computer-Kryptologie beizu-kommen, werden sich allenfalls noch die Großmächte USA und UdSSR lei-sten können. Für den kleinen und mitt-leren Privatspion, kommentierte das amerikanische Wirtschaftsmagazin „Business Week“, werde es hingegen „zunehmend attraktiver, Chefsekretä-rinnen zu verführen“.

MEDIZIN

Blinder Eifer

Der Aufwand für Vorsorge-Unter-suchungen von Herz- und Kreislauf-leiden ist „hinausgeworfenes Geld“. Zu diesem Ergebnis gelangt der hannoversche Sozialmediziner Pflanz in einem Gutachten für Bonn.

U nter den Glückwünschen, die der Wolfsburger Autoschlosser zum 45. Geburtstag bekam, war auch ein Brief von der Betriebskrankenkasse. Im eigenen Interesse, so las der VW-Mann, solle er doch die Untersuchungen zur Früherkennung von Herz- und Kreis-laufkrankheiten mitmachen.

Am Schwarzen Brett oder in der Werkszeitung fanden die Mitarbeiter anderer Großunternehmen ähnliche Hinweise. In Cochem an der Mosel wurden per Postwurfsendung gleich alle Bürger über 15 Jahren zum großen Check-up aufgefordert: Mit Hilfe sol-cher Untersuchungen, so hieß es aller-orten in der Bundesrepublik, lasse sich die moderne Seuche der Herz- und Kreislaufleiden eindämmen, das größte Gesundheitsproblem der industriena-tionen.

Doch solchem Optimismus setzte nun der hannoversche Sozialmediziner und Epidemiologe Professor Manfred Pflanz einen Dämpfer auf — in einem Gutachten über verschiedene Früher-kennungs-Modelle, angefertigt im Auf-trag der Bonner Ministerien für Ge-sundheit und Arbeit.

Fazit der Pflanz-Analyse: Das Geld für die aufwendigen Vorsorge-Pro-gramme gegen Herz- und Kreislauflei-den sei „aus dem Fenster geworfen“. Fast ausnahmslos werde außer dem Anhäufen von bloßen Daten und Befunden kaum etwas gewonnen. Insbe-sondere fehle die Nachbetreuung der einmal als gefährdet ermittelten Perso-nen.

Bei den Experten weicht die allge-meine Vorsorge-Euphorie der frühen siebziger Jahre bereits seit einiger Zeit zunehmender Ernüchterung. „Skepsis, ja Resignation“ sei weithin den großen Erwartungen gefolgt, gestand der Bie-lefelder Medizinsoziologe Christian von Ferber im Juli dieses Jahres auf einem Vorsorge-Symposium in Davos. „Der alte Schwung ist hin“, resümierte die „Neue Zürcher Zeitung“ zum Ab-schluß der Tagung.

Den Schweizer Internistenpapst Walter Siegenthaler ärgert besonders der „Unsinn der jährlichen Check-ups“, der medizinischen Rundum-Kon-trolle, wie sie etwa manche Großfirmen für ihre Spitzenmanager eingeführt ha-ben. Diese Art Gesundheits-Tivv hatten auch amerikanische Mediziner schon kritisiert.

Daß bei vorsorglichen Herz- und Kreislauftests die Erwartungen zu hoch